



Switch storage

Cluster and storage switches

NetApp
April 25, 2024

Sommario

Switch storage	1
Cisco Nexus 9336C-FX2	1
NVIDIA SN2100	70

Switch storage

Cisco Nexus 9336C-FX2

Panoramica

Panoramica dell'installazione e della configurazione degli switch storage Cisco Nexus 9336C-FX2

Lo switch di storage Cisco Nexus 9336C-FX2 fa parte della piattaforma Cisco Nexus 9000 e può essere installato in un cabinet di sistema NetApp. Gli switch storage consentono di instradare i dati tra server e array di storage in una SAN (Storage Area Network).

Panoramica della configurazione iniziale

Per configurare inizialmente uno switch Cisco Nexus 9336C-FX2 su sistemi che eseguono ONTAP, attenersi alla seguente procedura:

1. ["Completare il foglio di lavoro per il cablaggio"](#).
2. ["Installare lo switch"](#).
3. ["Configurare lo switch"](#).
4. ["Installare lo switch nel cabinet NetApp"](#).

A seconda della configurazione, è possibile installare lo switch Cisco Nexus 9336C-FX2 e il pannello pass-through in un cabinet NetApp con le staffe standard incluse con lo switch.

5. ["Preparazione all'installazione di NX-OS e RCF"](#).
6. ["Installare il software NX-OS"](#).
7. ["Installare il file di configurazione RCF"](#).

Installare l'RCF dopo aver configurato lo switch Nexus 9336C-FX2 per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

Ulteriori informazioni

Prima di iniziare l'installazione o la manutenzione, verificare quanto segue:

- ["Requisiti di configurazione"](#)
- ["Componenti e numeri di parte"](#)
- ["Documentazione richiesta"](#)
- ["Requisiti Smart Call Home"](#)

Requisiti di configurazione per gli switch storage Cisco Nexus 9336C-FX2

Per l'installazione e la manutenzione dello switch Cisco Nexus 9336C-FX2, verificare la configurazione e i requisiti di rete.

Supporto ONTAP

A partire da ONTAP 9.9.1, è possibile utilizzare gli switch Cisco Nexus 9336C-FX2 per combinare funzionalità di storage e cluster in una configurazione di switch condivisa.

Se si desidera creare cluster ONTAP con più di due nodi, sono necessari due switch di rete supportati.

Requisiti di configurazione

Per la configurazione, è necessario il numero e il tipo di cavi e connettori appropriati per gli switch.

A seconda del tipo di switch che si sta configurando inizialmente, è necessario connettersi alla porta console dello switch con il cavo console incluso; è inoltre necessario fornire informazioni di rete specifiche.

Requisiti di rete

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

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

Per ulteriori informazioni sulla configurazione iniziale dello switch, consultare la seguente guida: "[Guida all'installazione e all'aggiornamento di Cisco Nexus 9336C-FX2](#)".

Componenti e codici ricambio per switch storage Cisco Nexus 9336C-FX2

Per l'installazione e la manutenzione dello switch Cisco Nexus 9336C-FX2, consultare l'elenco dei componenti e dei codici dei componenti.

La seguente tabella elenca il codice ricambio e la descrizione dello switch, delle ventole e degli alimentatori 9336C-FX2:

Codice del ricambio	Descrizione
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Kit di accessori X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W PSU - flusso d'aria di scarico laterale

Codice del ricambio	Descrizione
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W PSU - flusso d'aria di aspirazione lato porta
X-NXA-FAN-65CFM-PE	N9K-9336C 65CFM, flusso d'aria di scarico lato porta
X-NXA-FAN-65CFM-PI	N9K-9336C 65CFM, flusso d'aria di aspirazione lato porta

Requisiti della documentazione per gli switch storage Cisco Nexus 9336C-FX2

Per l'installazione e la manutenzione dello switch Cisco Nexus 9336C-FX2, consultare la documentazione relativa a switch e controller specifici per la configurazione degli switch Cisco 9336-FX2 e del cluster ONTAP.

Documentazione dello switch

Per configurare gli switch Cisco Nexus 9336C-FX2, è necessaria la seguente documentazione disponibile sul ["Supporto degli switch Cisco Nexus serie 9000"](#) pagina:

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

Titolo del documento	Descrizione
<i>Note sulla versione di Cisco Nexus 9000 Series NX-OS (scegliere le note per la release NX-OS installata sugli switch)</i>	Descrive le funzioni, i bug e le limitazioni di Cisco Nexus serie 9000.
Conformità alle normative e informazioni sulla sicurezza per Cisco Nexus serie 9000	Fornisce informazioni legali, sulla conformità e sulla sicurezza degli switch Nexus serie 9000 a livello internazionale.

Documentazione sui sistemi ONTAP

Per configurare un sistema ONTAP, sono necessari i seguenti documenti per la versione del sistema operativo in uso dal ["Centro documentazione di ONTAP 9"](#).

Nome	Descrizione
<i>Istruzioni di installazione e configurazione specifiche del controller</i>	Descrive come installare l'hardware NetApp.
Documentazione ONTAP	Fornisce informazioni dettagliate su tutti gli aspetti delle release di ONTAP.
"Hardware Universe"	Fornisce informazioni sulla compatibilità e sulla configurazione dell'hardware NetApp.

Kit di guide e documentazione del cabinet

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

Nome	Descrizione
"Cabinet di sistema 42U, guida dettagliata"	Descrive le FRU associate all'armadio del sistema 42U e fornisce istruzioni per la manutenzione e la sostituzione delle FRU.
"Installare uno switch Cisco 9336-FX2 in un cabinet NetApp"	Descrive come installare uno switch Cisco Nexus 9336C-FX2 in un cabinet NetApp a quattro montanti.

Requisiti Smart Call Home

Per utilizzare la funzione Smart Call Home, consultare le seguenti linee guida.

Smart Call Home monitora i componenti hardware e software della rete. Quando si verifica una configurazione di sistema critica, viene generata una notifica basata su email e viene generato un avviso a tutti i destinatari configurati nel profilo di destinazione. Per utilizzare Smart Call Home, è necessario configurare uno switch di rete del cluster per comunicare tramite e-mail con il sistema Smart Call Home. Inoltre, è possibile configurare lo switch di rete del cluster in modo da sfruttare la funzione di supporto Smart Call Home integrata di Cisco.

Prima di utilizzare Smart Call Home, tenere presente quanto segue:

- È necessario che sia installato un server di posta elettronica.
- Lo switch deve disporre di connettività IP al server di posta elettronica.
- È necessario configurare il nome del contatto (contatto del server SNMP), il numero di telefono e l'indirizzo. Questo è necessario per determinare l'origine dei messaggi ricevuti.
- Un ID CCO deve essere associato a un contratto Cisco SMARTnet Service appropriato per la tua azienda.
- Cisco SMARTnet Service deve essere disponibile per la registrazione del dispositivo.

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

Installare l'hardware

Installare lo switch storage 9336C-FX2

Seguire questa procedura per installare lo storage switch Cisco Nexus 9336C-FX2.

Di cosa hai bisogno

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

Fasi

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

Se si sta installando...	Quindi...
Cisco Nexus 9336C-FX2 in un cabinet di sistema NetApp	Vedere "Installare lo switch nel cabinet NetApp" Per istruzioni sull'installazione dello switch in un cabinet NetApp.
Apparecchiatura in un rack Telco	Consultare le procedure fornite nelle guide all'installazione dell'hardware dello switch e le istruzioni di installazione e configurazione di NetApp.

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

Quali sono le prossime novità?

Passare a. ["Configurare lo switch storage Cisco Nexus 9336C-FX2"](#).

Configurare lo switch storage 9336C-FX2

Seguire questa procedura per configurare lo switch Cisco Nexus 9336C-FX2.

Di cosa hai bisogno

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


Fasi

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

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

Prompt	Risposta
Interrompere il provisioning automatico e continuare con la normale configurazione? (sì/no)	Rispondere con sì . Il valore predefinito è no
Applicare lo standard di password sicura? (sì/no)	Rispondere con sì . L'impostazione predefinita è sì.
Inserire la password per admin.	La password predefinita è "admin"; è necessario creare una nuova password complessa. Una password debole può essere rifiutata.
Accedere alla finestra di dialogo della configurazione di base? (sì/no)	Rispondere con yes alla configurazione iniziale dello switch.
Creare un altro account di accesso? (sì/no)	La risposta dipende dalle policy del sito relative agli amministratori alternativi. L'impostazione predefinita è NO .
Configurare la stringa di comunità SNMP di sola lettura? (sì/no)	Rispondere con no . Il valore predefinito è no
Configurare la stringa di comunità SNMP in lettura/scrittura? (sì/no)	Rispondere con no . Il valore predefinito è no

Prompt	Risposta
Inserire il nome dello switch.	Il nome dello switch può contenere al massimo 63 caratteri alfanumerici.
Continuare con la configurazione di gestione out-of-band (mgmt0)? (sì/no)	Rispondere con yes (impostazione predefinita) al prompt. Al prompt mgmt0 IPv4 address: (Indirizzo IPv4: Mgmt0), immettere l'indirizzo IP IP: ip_address (Indirizzo_ip).
Configurare il gateway predefinito? (sì/no)	Rispondere con sì . Al prompt dell'indirizzo IPv4 del gateway predefinito, immettere default_gateway.
Configurare le opzioni IP avanzate? (sì/no)	Rispondere con no . Il valore predefinito è no
Abilitare il servizio telnet? (sì/no)	Rispondere con no . Il valore predefinito è no
Servizio SSH abilitato? (sì/no)	<p>Rispondere con sì. L'impostazione predefinita è sì.</p> <div>  <p>SSH è consigliato quando si utilizza Cluster Switch Health Monitor (CSHM) per le funzioni di raccolta dei log. SSHv2 è consigliato anche per una maggiore sicurezza.</p> </div>
Inserire il tipo di chiave SSH che si desidera generare (dsa/rsa/rsa1).	L'impostazione predefinita è rsa .
Inserire il numero di bit della chiave (1024-2048).	Inserire il numero di bit della chiave compreso tra 1024 e 2048.
Configurare il server NTP? (sì/no)	Rispondere con no . Il valore predefinito è no
Configurare il livello di interfaccia predefinito (L3/L2)	Rispondi con L2 . L'impostazione predefinita è L2.
Configurare lo stato di interfaccia della porta dello switch predefinito (shut/noshut)	Rispondere con noshut . L'impostazione predefinita è noshut.
Configurare il profilo di sistema Copp (rigido/moderato/lenient/denso)	Rispondere con Strict . L'impostazione predefinita è rigorosa.

Prompt	Risposta
Modificare la configurazione? (sì/no)	A questo punto, viene visualizzata la nuova configurazione. Esaminare e apportare le modifiche necessarie alla configurazione appena inserita. Rispondere con no al prompt se si è soddisfatti della configurazione. Rispondere con yes se si desidera modificare le impostazioni di configurazione.
Utilizzare questa configurazione e salvarla? (sì/no)	<p>Rispondere con yes per salvare la configurazione. In questo modo vengono aggiornate automaticamente le immagini del sistema e del kickstart.</p> <div>  <p>Se non si salva la configurazione in questa fase, nessuna delle modifiche sarà effettiva al successivo riavvio dello switch.</p> </div>

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

Quali sono le prossime novità?

Se lo si desidera, è possibile ["Installare uno switch Cisco Nexus 9336C-FX2 in un cabinet NetApp"](#). In caso contrario, passare a. ["Preparazione all'installazione di NX-OS e RCF"](#).

Installare uno switch Cisco Nexus 9336C-FX2 in un cabinet NetApp

A seconda della configurazione, potrebbe essere necessario installare lo switch Cisco Nexus 9336C-FX2 e il pannello pass-through in un cabinet NetApp. Le staffe standard sono incluse con lo switch.

Di cosa hai bisogno

- Per ogni switch, è necessario fornire le otto viti da 10-32 o 12-24 e i dadi a clip per montare le staffe e le guide di scorrimento sui montanti anteriori e posteriori dell'armadio.
- Per installare lo switch in un cabinet NetApp, è necessario utilizzare il kit guide standard Cisco.



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

Documentazione richiesta

Esaminare i requisiti di preparazione iniziale, il contenuto del kit e le precauzioni di sicurezza nel ["Guida all'installazione dell'hardware di Cisco Nexus serie 9000"](#).

Fasi

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

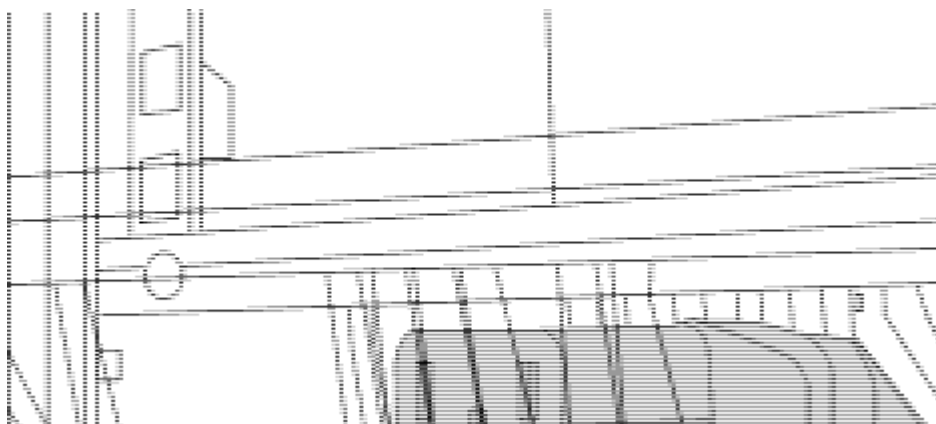
Il kit pannello pass-through è disponibile presso NetApp (codice X8784-R6).

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

- Un pannello di chiusura pass-through
- Quattro viti 10-32 x 0,75
- Quattro dadi a clip da 10-32
 - i. Determinare la posizione verticale degli interruttori e del pannello di chiusura nell'armadio.

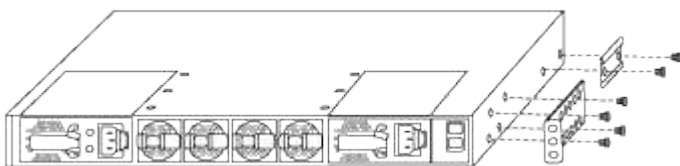
In questa procedura, il pannello di chiusura verrà installato in U40.

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

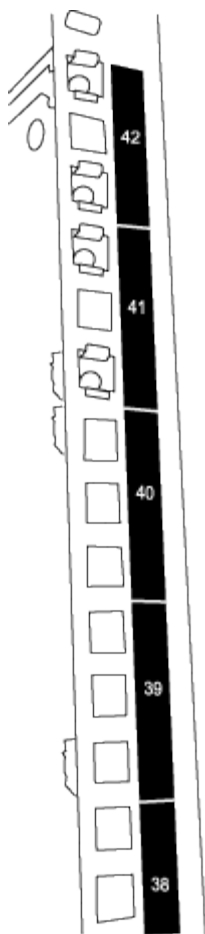


(1) *connettore femmina del cavo di collegamento.*

2. Installare le staffe per il montaggio in rack sullo chassis dello switch Nexus 9336C-FX2.
 - a. Posizionare una staffa anteriore per il montaggio su rack su un lato dello chassis dello switch in modo che l'orecchio di montaggio sia allineato con la piastra anteriore dello chassis (lato alimentatore o ventola), quindi utilizzare quattro viti M4 per fissare la staffa allo chassis.



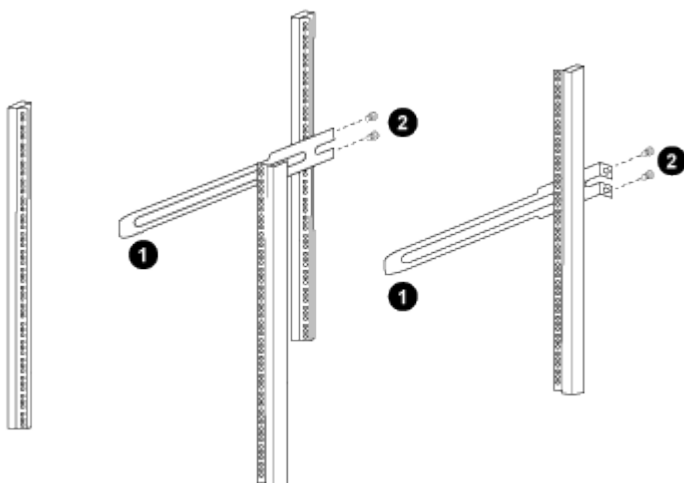
- b. Ripetere il punto [2a](#) con l'altra staffa anteriore per il montaggio in rack sull'altro lato dello switch.
 - c. Installare la staffa per il montaggio su rack posteriore sul telaio dello switch.
 - d. Ripetere il punto [2c](#) con l'altra staffa posteriore per il montaggio su rack sull'altro lato dello switch.
3. Montare i dadi a clip nelle posizioni dei fori quadrati per tutti e quattro i montanti IEA.



I due switch 9336C-FX2 saranno sempre montati nella parte superiore 2U del cabinet RU41 e 42.

4. Installare le guide di scorrimento nel cabinet.

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



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

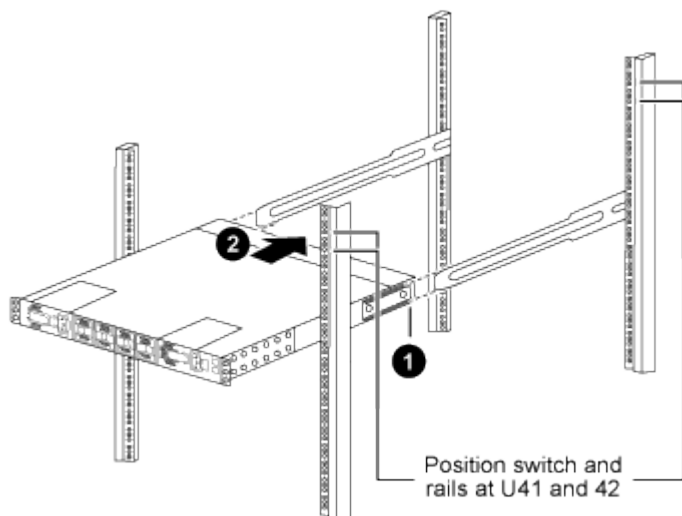
(2) serrare le viti delle guide di scorrimento ai montanti dell'armadietto.

- a. Ripetere il punto 4a per il montante posteriore destro.
 - b. Ripetere i passaggi 4a e 4b Nelle posizioni RU41 del cabinet.
5. Installare lo switch nell'armadio.



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

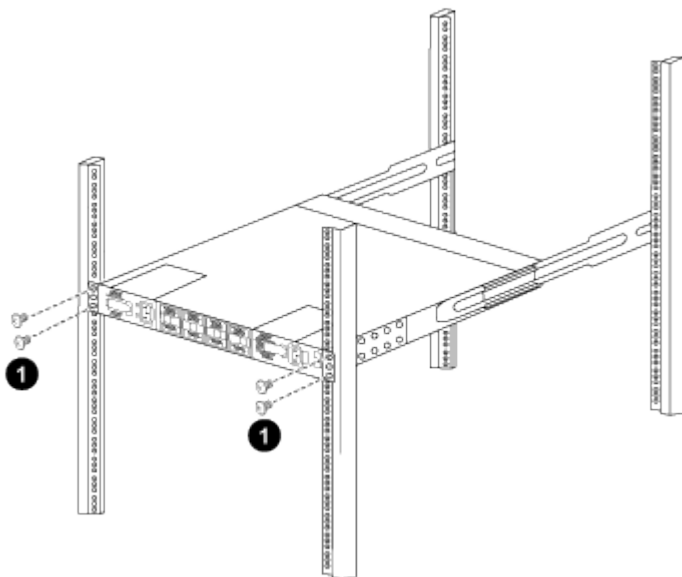
- a. Posizionare la parte posteriore dell'interruttore su RU41.



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

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

- b. Collegare lo switch al cabinet.



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

- a. Con il telaio ora supportato senza assistenza, serrare completamente le viti anteriori sui montanti.
- b. Ripetere i passaggi [5a](#) attraverso [5c](#) Per il secondo switch nella posizione RU42.



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

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



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

8. Collegare la porta di gestione di ogni switch 9336C-FX2 a uno degli switch di gestione (se ordinati) o collegarli direttamente alla rete di gestione.

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

Configurare il software

Workflow di installazione del software per switch storage Cisco Nexus 9336C-FX2

Per installare e configurare il software per uno switch Cisco Nexus 9336C-FX2, attenersi alla seguente procedura:

1. ["Preparazione all'installazione di NX-OS e RCF"](#).
2. ["Installare il software NX-OS"](#).
3. ["Installare il file di configurazione RCF"](#).

Installare l'RCF dopo aver configurato lo switch Nexus 9336C-FX2 per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

Preparare l'installazione del software NX-OS e RCF

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

A proposito degli esempi

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

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

A proposito di questa attività

La procedura richiede l'utilizzo di entrambi i comandi ONTAP e Cisco Nexus 9000 Series Switches; i comandi

ONTAP vengono utilizzati se non diversamente indicato.

Fasi

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

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



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

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

```
set -privilege advanced
```

Il prompt avanzato (*>).

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

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

Mostra esempio

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp				
	e0a	cs1	Eth1/2	N9K-
C9336C				
	e0b	cs2	Eth1/2	N9K-
C9336C				
cluster1-01/cdp				
	e0a	cs1	Eth1/1	N9K-
C9336C				
	e0b	cs2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

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

a. Visualizzare gli attributi della porta di rete:

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

Mostra esempio

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

Node: cluster1-02

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

Node: cluster1-01

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

4 entries were displayed.
```

b. Visualizzare le informazioni sui LIF:

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


Mostra esempio

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

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

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

4 entries were displayed.

5. Ping delle LIF del cluster remoto:

```
cluster ping-cluster -node node-name
```

Mostra esempio

```
cluster1::*> cluster ping-cluster -node cluster1-02
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)
```

6. Verificare che il comando di auto-revert sia attivato su tutte le LIF del cluster:

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

Mostra esempio

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

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.

7. Per ONTAP 9.8 e versioni successive, attivare la funzione di raccolta dei log dello switch Ethernet per la raccolta dei file di log relativi allo switch, utilizzando i comandi seguenti:

```
system switch ethernet log setup-password e. system switch ethernet log enable-collection
```

Mostra esempio

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

8. Per le release di patch ONTAP 9.5P16, 9.6P12 e 9.7P10 e successive, attivare la funzione di raccolta dei log di Health monitor dello switch Ethernet per la raccolta dei file di log relativi allo switch, utilizzando i comandi:

```
system cluster-switch log setup-password e.system cluster-switch log enable-  
collection
```

Mostra esempio

```
cluster1::*> system cluster-switch log setup-password  
Enter the switch name: <return>  
The switch name entered is not recognized.  
Choose from the following list:  
cs1  
cs2  
  
cluster1::*> system cluster-switch log setup-password  
  
Enter the switch name: cs1  
RSA key fingerprint is  
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc  
Do you want to continue? {y|n}::[n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster1::*> system cluster-switch log setup-password  
  
Enter the switch name: cs2  
RSA key fingerprint is  
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1  
Do you want to continue? {y|n}:: [n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster1::*> system cluster-switch log enable-collection  
  
Do you want to enable cluster log collection for all nodes in the  
cluster?  
{y|n}: [n] y  
  
Enabling cluster switch log collection.  
  
cluster1::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

Quali sono le prossime novità?

["Installare il software NX-OS".](#)

Installare il software NX-OS

Seguire questa procedura per installare il software NX-OS sullo switch del cluster Nexus 9336C-FX2.

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

Verifica dei requisiti

Di cosa hai bisogno

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- ["Pagina switch Ethernet Cisco"](#). Consultare la tabella di compatibilità degli switch per le versioni supportate di ONTAP e NX-OS.
- Le guide appropriate per il software e l'aggiornamento sono disponibili sul sito Web di Cisco per le procedure di aggiornamento e downgrade dello switch Cisco. Vedere ["Switch Cisco Nexus serie 9000"](#).

A proposito degli esempi

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

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

Installare il software

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

Fasi

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

Mostra esempio

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

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

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

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

Mostra esempio

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

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

cs2# copy sftp: bootflash: vrf management

Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

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

```
show version
```

Mostra esempio

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

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

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

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



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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

5. Installare l'immagine NX-OS.

L'installazione del file immagine ne provoca il caricamento ogni volta che lo switch viene riavviato.

Mostra esempio

```
cs2# install all nxos bootflash:nxos.9.3.5.bin
```

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

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

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

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

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

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

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

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

Images will be upgraded according to following table:

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

```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[#####] 100% -- SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

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

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

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

```
show version
```

Mostra esempio

```
cs2# show version
```

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

Software

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

Hardware

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

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

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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

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

Mostra esempio



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

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

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 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	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. Dopo il riavvio dello switch, accedere nuovamente e verificare che la nuova versione di EPLD sia stata caricata correttamente.

Mostra esempio

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

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

9. Ripetere i passaggi da 1 a 8 per installare il software NX-OS sullo switch CS1.

Quali sono le prossime novità?

["Installare il file di configurazione RCF"](#).

Installazione del file di configurazione di riferimento (RCF)

È possibile installare RCF dopo aver configurato per la prima volta lo switch Nexus 9336C-FX2. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

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

Verifica dei requisiti

Di cosa hai bisogno

- Backup corrente della configurazione dello switch.
- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Il file RCF corrente.
- Una connessione console allo switch, necessaria per l'installazione di RCF.

Documentazione consigliata

- ["Pagina switch Ethernet Cisco"](#) Consultare la tabella di compatibilità degli switch per le versioni ONTAP e RCF supportate. Si noti che esistono dipendenze di comando tra la sintassi del comando in RCF e quella presente nelle versioni di NX-OS.
- ["Switch Cisco Nexus serie 3000"](#). Consultare le guide all'aggiornamento e al software appropriate disponibili sul sito Web di Cisco per la documentazione completa sulle procedure di aggiornamento e downgrade dello switch Cisco.

Installare RCF

A proposito degli esempi

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

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

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



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

A proposito di questa attività

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

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



Prima di installare una nuova versione del software dello switch e gli RCF, è necessario cancellare le impostazioni dello switch ed eseguire la configurazione di base. È necessario essere collegati allo switch mediante la console seriale. Questa attività ripristina la configurazione della rete di gestione.

Fase 1: Preparazione per l'installazione

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

```
network device-discovery show
```

Mostra esempio

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

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

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

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

Mostra esempio

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

Node: cluster1-01

Ignore

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

Node: cluster1-02

Ignore

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

8 entries were displayed.

Node: cluster1-03

Ignore

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

Node: cluster1-04

Ignore

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 del cluster (LIF) siano sulla porta home:

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

Mostra esempio

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

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

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

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

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

Mostra esempio

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

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

3. Disattiva l'autorevert sulle LIF del cluster.

Mostra esempio

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

Fase 2: Configurare le porte

1. Sullo switch del cluster cs2, spegnere le porte collegate alle porte del cluster dei nodi.

Mostra esempio

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

2. Verificare che le LIF del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

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

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

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

3. Verificare che il cluster funzioni correttamente:

```
cluster show
```

Mostra esempio

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

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

```
show running-config
```

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



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

- a. Pulire la configurazione:

Mostra esempio

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Riavviare lo switch:

Mostra esempio

```
(cs2)# reload

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


6. Copiare l'RCF nella flash di avvio 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 in ["Cisco Nexus 9000 Series NX-OS Command Reference"](#) guide.

Mostra esempio

Questo esempio mostra l'utilizzo di TFTP per copiare un RCF nella flash di avvio sullo switch cs2:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

7. Applicare l'RCF precedentemente scaricato al bootflash.

Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in ["Cisco Nexus 9000 Series NX-OS Command Reference"](#) guide.

Mostra esempio

Questo esempio mostra il file RCF Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt in fase di installazione sullo switch cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

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

Mostra esempio

```
cs2# show banner motd

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

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

```
show running-config
```

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

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

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

10. 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 in ["Cisco Nexus 9000 Series NX-OS Command Reference"](#) guide.

Mostra esempio

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

11. Riavviare lo switch cs2. È possibile ignorare gli eventi "cluster ports down" riportati sui nodi durante il riavvio dello switch.

Mostra esempio

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

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

- a. Verificare che le porte e0d siano in buone condizioni su tutti i nodi del cluster:

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

Mostra esempio

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

Health						Speed(Mbps)	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.

- a. Verificare lo stato dello switch dal cluster (potrebbe non essere visualizzato lo switch cs2, poiché le LIF non sono presenti 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
N9K-C9336C			
	e0d	cs2	Ethernet1/7
N9K-C9336C			
cluster01-2/cdp			
	e0a	cs1	Ethernet1/8
N9K-C9336C			
	e0d	cs2	Ethernet1/8
N9K-C9336C			
cluster01-3/cdp			
	e0a	cs1	Ethernet1/1/1
N9K-C9336C			
	e0b	cs2	Ethernet1/1/1
N9K-C9336C			
cluster1-04/cdp			
	e0a	cs1	Ethernet1/1/2
N9K-C9336C			
	e0b	cs2	Ethernet1/1/2
N9K-C9336C			


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

Switch	Type	Address
Model		

cs1	cluster-network	10.233.205.90
NX9-C9336C		
Serial Number: FOCXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(5)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91

```
NX9-C9336C
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                9.3(5)
  Version Source: CDP

2 entries were displayed.
```

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

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

13. Sullo switch del cluster cs1, spegnere le porte collegate alle porte del cluster dei nodi.

Mostra esempio

Nell'esempio seguente viene utilizzato l'output dell'esempio di interfaccia:

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

14. Verificare che le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi.

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

Mostra esempio

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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::*>				

15. Verificare che il cluster funzioni correttamente:

```
cluster show
```


Mostra esempio

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

16. Ripetere i passaggi da 4 a 11 sullo switch cs1.
17. Abilitare il ripristino automatico sulle LIF del cluster.

Mostra esempio

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

18. Riavviare lo switch cs1. Questa operazione consente di attivare le LIF del cluster per ripristinare le porte home. È possibile ignorare gli eventi “cluster ports down” riportati sui nodi durante il riavvio dello switch.

Mostra esempio

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

Fase 3: Verificare la configurazione

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

```
show interface brief
```

Mostra esempio

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

2. Verificare che i nodi previsti siano ancora connessi:

```
show cdp neighbors
```

Mostra esempio

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1        133      H                FAS2980
e0a
node2              Eth1/2        133      H                FAS2980
e0a
cs2                Eth1/35       175      R S I s          N9K-C9336C
Eth1/35
cs2                Eth1/36       175      R S I s          N9K-C9336C
Eth1/36

Total entries displayed: 4
```

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

```
show vlan brief
```

```
show interface trunk
```

Mostra esempio

```
cs1# show vlan brief
```

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

```

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

```

```
cs1# show interface trunk
```

```

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

```

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

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

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



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

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

```
show port-channel summary
```

Mostra esempio

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports      Channel
-----
-----
1      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

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

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


Mostra esempio

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

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

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

6. Verificare che il cluster funzioni correttamente:

```
cluster show
```

Mostra esempio

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

7. Eseguire il ping delle interfacce del cluster remoto per verificare la connettività:

```
cluster ping-cluster -node local
```

Mostra esempio

```
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)
```

Raccolta registro monitoraggio stato switch Ethernet

È possibile utilizzare la funzione di raccolta dei log per raccogliere i file di log relativi allo switch in ONTAP.

+

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug. Questa procedura guida l'utente attraverso il processo di impostazione e avvio della raccolta di registri **supporto** dettagliati dal centralino e avvia una raccolta oraria di dati **periodici** raccolti da AutoSupport.

Prima di iniziare

- Verificare di aver configurato l'ambiente utilizzando lo switch cluster 9336C-FX2 **CLI**.
- Il monitoraggio dello stato dello switch deve essere abilitato per lo switch. Verificare questo assicurandosi che `Is Monitored:` il campo è impostato su **true** nell'output di `system switch ethernet show` comando.

Fasi

1. Creare una password per la funzione di raccolta dei log dello switch Ethernet Health monitor:

```
system switch ethernet log setup-password
```

Mostra esempio

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Per avviare la raccolta dei log, eseguire il comando seguente, sostituendo **DEVICE** con lo switch utilizzato nel comando precedente. Questo avvia entrambi i tipi di raccolta di log: I log dettagliati **Support** e una raccolta oraria di dati **Periodic**.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Mostra esempio

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Attendere 10 minuti, quindi verificare che la raccolta dei log sia completa:

```
system switch ethernet log show
```



Se uno di questi comandi restituisce un errore o se la raccolta dei log non viene completata, contattare il supporto NetApp.

Risoluzione dei problemi

Se si verifica uno dei seguenti stati di errore segnalati dalla funzione di raccolta registri (visibile nell'output di `system switch ethernet log show`), provare i passi di debug corrispondenti:

Stato errore raccolta log	Risoluzione
Chiavi RSA non presenti	Rigenerare le chiavi SSH ONTAP. Contattare l'assistenza NetApp.
errore password cambio	Verificare le credenziali, verificare la connettività SSH e rigenerare le chiavi SSH ONTAP. Per istruzioni, consultare la documentazione dello switch o contattare l'assistenza NetApp.
Chiavi ECDSA non presenti per FIPS	Se la modalità FIPS è attivata, le chiavi ECDSA devono essere generate sullo switch prima di riprovare.

trovato log preesistente	Rimuovere il file di raccolta del registro precedente sullo switch.
errore registro dump switch	Assicurarsi che l'utente dello switch disponga delle autorizzazioni per la raccolta dei registri. Fare riferimento ai prerequisiti riportati sopra.

Configurare SNMPv3

Seguire questa procedura per configurare SNMPv3, che supporta il monitoraggio dello stato dello switch Ethernet (CSHM).

A proposito di questa attività

I seguenti comandi configurano un nome utente SNMPv3 sugli switch Cisco 9336C-FX2:

- Per **nessuna autenticazione**:

```
snmp-server user SNMPv3_USER NoAuth
```

- Per l'autenticazione **MD5/SHA**:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
show snmp user
```

Mostra esempio

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config)# show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config)#
```

2. Impostare l'utente SNMPv3 sul lato ONTAP:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Mostra esempio

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1" -instance
```


Mostra esempio

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Verificare che il numero seriale da sottoporre a query con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente dopo il completamento del periodo di polling CSHM.

```
system switch ethernet polling-interval show
```

Mostra esempio

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Sostituire uno switch storage Cisco Nexus 9336C-FX2

È possibile sostituire uno switch Nexus 9336C-FX2 difettoso in una rete cluster. Si tratta di una procedura senza interruzioni.

Di cosa hai bisogno

Prima di installare il software NX-OS e gli RCF su uno switch di storage Cisco Nexus 9336C-FX2, assicurarsi che:

- Il sistema supporta gli switch storage Cisco Nexus 9336C-FX2.
- Per le versioni supportate di ONTAP, NX-OS e RCF, consultare la tabella di compatibilità degli switch nella pagina Switch Ethernet Cisco.
- Hai fatto riferimento alle guide appropriate per il software e l'aggiornamento disponibili sul sito Web di Cisco.

Switch Cisco Nexus serie 3000:

- Hai scaricato gli RCF applicabili.
- La configurazione di rete esistente presenta le seguenti caratteristiche:

- La pagina Cisco Ethernet Switches (Switch Ethernet Cisco) contiene le ultime versioni RCF e NX-OS sugli switch.
- La connettività di gestione deve esistere su entrambi gli switch.
- Lo switch Cisco Nexus 9336C-FX2 sostitutivo presenta le seguenti caratteristiche:
 - La connettività di rete per la gestione è funzionale.
 - L'accesso della console allo switch sostitutivo è in posizione.
 - Sullo switch viene caricata l'immagine appropriata del sistema operativo RCF e NX-OS.
 - La fiducia iniziale dello switch è stata completata.

A proposito di questa attività

Questa procedura sostituisce il secondo switch di storage Nexus 9336C-FX2 S2 con il nuovo switch NS2 9336C-FX. I due nodi sono node1 e node2.

Procedura da completare:

- Verificare che l'interruttore da sostituire sia S2.
- Scollegare i cavi dallo switch S2.
- Ricollegare i cavi allo switch NS2.
- Verificare tutte le configurazioni del dispositivo sullo switch NS2.



Nelle versioni RCF e NX-OS possono esserci dipendenze tra la sintassi dei comandi.

Fasi

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

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

x è la durata della finestra di manutenzione in ore.

2. Controllare lo stato delle porte dei nodi di storage per verificare che vi sia una connessione allo switch di storage S1:

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

Mostra esempio

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

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

```
storage::*>
```

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

```
network device-discovery show
```

Mostra esempio

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e3a    S1                        Ethernet1/1 NX9336C
           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 NX9336C
           e4a    node1                     e4a         AFF-A700
           e4e    node1                     e4e         AFF-A700
node2/lldp
           e3a    S1                        Ethernet1/2 -
           e4a    node1                     e4a         -
           e4e    node1                     e4e         -
storage::*>
```

4. Eseguire lo spettacolo `lldp neighbors` comando sull'interruttore funzionante per confermare che è possibile visualizzare sia i nodi che tutti gli shelf:

```
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
```

5. Verificare le porte dello shelf nel sistema storage:

```
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  -            -
storage::*>
```

6. Rimuovere tutti i cavi collegati allo switch di storage S2.

7. Ricollegare tutti i cavi allo switch NS2 sostitutivo.

8. Controllare nuovamente lo stato di salute delle porte del nodo di storage:

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

Mostra esempio

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

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

```
storage::*>
```

9. Verificare che entrambi gli switch siano disponibili:

```
network device-discovery show
```

Mostra esempio

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e3a  S1                        Ethernet1/1 NX9336C
          e4a  node2                     e4a         AFF-A700
          e4e  node2                     e4e         AFF-A700
          e7b  NS2                      Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                        Ethernet1/1 -
          e4a  node2                     e4a         -
          e4e  node2                     e4e         -
          e7b  NS2                      Ethernet1/1 -
node2/cdp
          e3a  S1                        Ethernet1/2 NX9336C
          e4a  node1                     e4a         AFF-A700
          e4e  node1                     e4e         AFF-A700
          e7b  NS2                      Ethernet1/2 NX9336C
node2/lldp
          e3a  S1                        Ethernet1/2 -
          e4a  node1                     e4a         -
          e4e  node1                     e4e         -
          e7b  NS2                      Ethernet1/2 -
storage::*>
```

10. Verificare le porte dello shelf nel sistema storage:

```
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  
storage::*>
```

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

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

NVIDIA SN2100

Panoramica

Panoramica del processo di configurazione per gli switch storage NVIDIA SN2100

NVIDIA SN2100 è uno switch storage che consente di instradare i dati tra server e storage array in una SAN (Storage Area Network).

Panoramica della configurazione iniziale

Per configurare uno switch NVIDIA SN2100 sui sistemi che eseguono ONTAP, attenersi alla seguente procedura:

1. ["Installare l'hardware per lo switch NVIDIA SN2100"](#).

Le istruzioni sono disponibili nella *Guida all'installazione dello switch NVIDIA*.

2. ["Configurare lo switch"](#).

Le istruzioni sono disponibili nella documentazione NVIDIA.

3. ["Esaminare le considerazioni relative al cablaggio e alla configurazione"](#).

Esaminare i requisiti per le connessioni ottiche, l'adattatore QSA e la velocità di switchport.

4. ["Cablare gli shelf NS224 come storage collegato allo switch"](#).

Seguire queste procedure se si dispone di un sistema in cui gli shelf di dischi NS224 devono essere cablati come storage collegato allo switch (non come storage collegato direttamente).

5. ["Installare Cumulus Linux in modalità Cumulus"](#) oppure ["Installare Cumulus Linux in modalità ONIE"](#).

È possibile installare il sistema operativo Cumulus Linux (CL) quando lo switch esegue Cumulus Linux o ONIE.

6. ["Installare lo script del file di configurazione di riferimento"](#).

Sono disponibili due script RCF per le applicazioni di clustering e storage.

7. ["Configurare SNMPv3 per la raccolta dei log dello switch"](#).

Questa versione include il supporto per SNMPv3 per la raccolta dei log degli switch e per Switch Health Monitoring (SHM).

Le procedure utilizzano Network Command Line Utility (NCLU), un'interfaccia a riga di comando che garantisce l'accesso completo a Cumulus Linux. Il comando net è l'utility wrapper utilizzata per eseguire azioni da un terminale.

Ulteriori informazioni

Prima di iniziare l'installazione o la manutenzione, verificare quanto segue:

- ["Requisiti di configurazione"](#)
- ["Componenti e numeri di parte"](#)
- ["Documentazione richiesta"](#)

Requisiti di configurazione per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, verificare tutti i requisiti.

Requisiti di installazione

Se si desidera creare cluster ONTAP con più di due nodi, sono necessari due switch di rete cluster supportati. È possibile utilizzare switch di gestione aggiuntivi, opzionali.

Lo switch NVIDIA SN2100 (X190006/X190106) viene installato nel cabinet doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Per le linee guida relative al cablaggio, vedere ["Considerazioni sul cablaggio e sulla configurazione"](#).

Supporto di ONTAP e Linux

Lo switch NVIDIA SN2100 è uno switch Ethernet da 10/25/40/100 GB con Cumulus Linux. Lo switch supporta quanto segue:

- ONTAP 9.10.1P3. Lo switch SN2100 serve applicazioni cluster e storage in ONTAP 9.10.1P3 su diverse coppie di switch. A partire da ONTAP 9.10.1P3, è possibile utilizzare gli switch NVIDIA SN2100 per combinare funzionalità di storage e cluster in una configurazione di switch condivisa.
- Sistema operativo Cumulus Linux (CL) versione 4.4.3. Per informazioni aggiornate sulla compatibilità,

consultare ["Switch Ethernet NVIDIA"](#) pagina informativa.

- È possibile installare Cumulus Linux quando lo switch esegue Cumulus Linux o ONIE.

Componenti e codici ricambio per switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, consultare l'elenco dei componenti e i codici del cabinet e del kit di guide.

Dettagli del cabinet

Lo switch NVIDIA SN2100 (X190006/X190106) viene installato nel cabinet doppio/singolo NVIDIA con le staffe standard incluse con lo switch.

Dettagli del kit ferroviario

La seguente tabella elenca il codice ricambio e la descrizione degli switch e dei kit di guide MSN2100:

Codice del ricambio	Descrizione
X190006-PE	Switch cluster, NVIDIA SN2100, 16 PUNTI 100G, PTSX
X190006-PI	Switch cluster, NVIDIA SN2100, 16 PUNTI 100G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16PT 100G, PTSX, front-end
X190106-FE-PI	Switch, NVIDIA SN2100, 16PT 100G, PSIN, front-end
X-MTEF-KIT-D	Kit di guide, NVIDIA Dual Switch fianco a fianco
X-MTEF-KIT-E	Kit di guide, NVIDIA Single Switch a breve profondità



Consultare la documentazione NVIDIA per ulteriori informazioni su ["Installazione dello switch SN2100 e del kit guida"](#).

Requisiti della documentazione per gli switch NVIDIA SN2100

Per l'installazione e la manutenzione dello switch NVIDIA SN2100, consultare tutta la documentazione consigliata.

La seguente tabella elenca la documentazione disponibile per gli switch NVIDIA SN2100.

Titolo	Descrizione
"Configurazione e configurazione degli switch NVIDIA SN2100"	Descrive come configurare e configurare gli switch NVIDIA SN2100, inclusa l'installazione di Cumulus Linux e degli RCF applicabili.
"Eseguire la migrazione da uno switch cluster Cisco a uno switch cluster NVIDIA SN2100"	Descrive come eseguire la migrazione da ambienti che utilizzano switch cluster Cisco a ambienti che utilizzano switch cluster NVIDIA SN2100.

Titolo	Descrizione
"Migrare da uno switch di storage Cisco a uno switch di storage NVIDIA"	Descrive come eseguire la migrazione da ambienti che utilizzano switch di storage Cisco a ambienti che utilizzano switch di storage NVIDIA SN2100.
"Eseguire la migrazione a un cluster con switch a due nodi con switch cluster NVIDIA SN2100"	Descrive come migrare a un ambiente con switch a due nodi utilizzando gli switch cluster NVIDIA SN2100.
"Sostituire uno switch cluster NVIDIA SN2100"	Descrive la procedura per sostituire uno switch NVIDIA SN2100 difettoso in un cluster e scaricare Cumulus Linux e il file di configurazione di riferimento.
"Sostituire uno switch di storage NVIDIA SN2100"	Descrive la procedura per sostituire uno switch di storage NVIDIA SN2100 difettoso e scaricare Cumulus Linux e il file di configurazione di riferimento.

Installare l'hardware

Installare l'hardware per lo switch NVIDIA SN2100

Per installare l'hardware SN2100, consultare la documentazione di NVIDIA.

Fasi

1. Esaminare ["requisiti di configurazione"](#).
2. Seguire le istruzioni riportate in ["Guida all'installazione dello switch NVIDIA"](#).

Quali sono le prossime novità?

["Configurare lo switch"](#).

Configurare lo switch NVIDIA SN2100

Per configurare lo switch SN2100, consultare la documentazione di NVIDIA.

Fasi

1. Esaminare ["requisiti di configurazione"](#).
2. Seguire le istruzioni riportate in ["Sistema NVIDIA Bring-Up"](#).

Quali sono le prossime novità?

["Esaminare le considerazioni relative al cablaggio e alla configurazione"](#).

Esaminare le considerazioni relative al cablaggio e alla configurazione

Prima di configurare lo switch NVIDIA SN2100, fare riferimento alle seguenti considerazioni.

Dettagli della porta NVIDIA

Porte switch	Utilizzo delle porte
swp1s0-3	10/40 nodi di porta del cluster
swp2s0-3	25/100 nodi di porta del cluster
nodì porta cluster swp3-14 40/100	Porte ISL (Inter-Switch link) swp15-16 40/100

Vedere ["Hardware Universe"](#) per ulteriori informazioni sulle porte dello switch.

Connessioni ottiche

Solo le connessioni ottiche sono supportate sugli switch SN2100 con NIC X1151A, NIC X1146A o porte 100GbE integrate. Ad esempio:

- AFF A800 sulle porte e0a e e0b
- AFF A320 sulle porte e0g e e0h

Adpater QSA

Quando si utilizza un adattatore QSA per connettersi alle porte cluster Intel integrate su una piattaforma, non vengono visualizzati tutti i collegamenti. Le piattaforme di esempio sono: FAS2750, AFF A300 e FAS8200 (tutti 10G) e AFF A250 (25G).

Per risolvere il problema, procedere come segue:

1. Per Intel 10G, impostare manualmente la velocità di collegamento swp1s0-3 su 10000 e impostare la negoziazione automatica su Off.
2. Per Chelsio 25G, impostare manualmente la velocità di collegamento swp2s0-3 su 25000 e impostare la negoziazione automatica su Off.



Utilizzando QSA 10G/25G, utilizzare le porte 40/100G senza interruzione. Non inserire l'adattatore QSA nelle porte configurate per la breakout.

Velocità switchport

A seconda del ricetrasmittitore in switchport, potrebbe essere necessario impostare la velocità su una porta fissa. Se si utilizzano porte di breakout 10G e 25G, assicurarsi che la negoziazione automatica sia disattivata e impostare a fondo la velocità della porta sullo switch. Ad esempio:

```

cumulus@cumulus:mgmt:~$ net add int swpls3 link autoneg off && net com
--- /etc/network/interfaces      2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swpls3
iface swpls3
    alias 10G Intra-Cluster Node
-   link-autoneg off
+   link-autoneg on
    link-speed 10000 <---- port speed set
    mstpctl-bpduguard yes
    mstpctl-portadminedge yes
    mtu 9216

auto swp2s0
iface swp2s0
    alias 25G Intra-Cluster Node
    link-autoneg off
    link-speed 25000 <---- port speed set

```

Quali sono le prossime novità?

["Cablare gli shelf NS224 come storage collegato allo switch".](#)

Cablare gli shelf NS224 come storage collegato allo switch

Se si dispone di un sistema in cui gli shelf di dischi NS224 devono essere cablati come storage collegato allo switch (non come storage collegato direttamente), utilizzare le informazioni fornite qui.

- Cablare gli shelf di dischi NS224 attraverso gli switch di storage:

["Informazioni per il cablaggio degli shelf di dischi NS224 collegati allo switch"](#)

- Installare gli switch storage:

["Documentazione switch AFF e FAS"](#)

- Verificare l'hardware supportato, ad esempio switch e cavi storage, per il modello di piattaforma in uso:

Configurare il software

Workflow di installazione del software per switch storage NVIDIA SN2100

Per installare e configurare il software per uno switch NVIDIA SN2100, attenersi alla seguente procedura:

1. ["Installare Cumulus Linux in modalità Cumulus"](#) oppure ["Installare Cumulus Linux in modalità ONIE"](#).

È possibile installare il sistema operativo Cumulus Linux (CL) quando lo switch esegue Cumulus Linux o ONIE.

2. ["Installare lo script del file di configurazione di riferimento"](#).

Sono disponibili due script RCF per le applicazioni di clustering e storage.

3. ["Configurare SNMPv3 per la raccolta dei log dello switch"](#).

Questa versione include il supporto per SNMPv3 per la raccolta dei log degli switch e per Switch Health Monitoring (SHM).

Le procedure utilizzano Network Command Line Utility (NCLU), un'interfaccia a riga di comando che garantisce l'accesso completo a Cumulus Linux. Il comando net è l'utility wrapper utilizzata per eseguire azioni da un terminale.

Installare Cumulus Linux in modalità Cumulus

Seguire questa procedura per installare il sistema operativo Cumulus Linux (CL) quando lo switch è in esecuzione in modalità Cumulus.



Il sistema operativo Cumulus Linux (CL) può essere installato quando lo switch esegue Cumulus Linux o ONIE (vedere ["Installare in modalità ONIE"](#)).

Di cosa hai bisogno

- Conoscenza di livello intermedio di Linux.
- Familiarità con la modifica di base del testo, le autorizzazioni dei file UNIX e il monitoraggio dei processi. Sono preinstallati diversi editor di testo, tra cui `vi` e `nano`.
- Accesso a una shell Linux o UNIX. Se si utilizza Windows, utilizzare un ambiente Linux come strumento della riga di comando per interagire con Cumulus Linux.
- Il requisito di velocità di trasmissione deve essere impostato su 115200 sullo switch della console seriale per l'accesso alla console dello switch NVIDIA SN2100, come segue:
 - 115200 baud
 - 8 bit di dati
 - 1 bit di stop
 - parità: nessuna
 - controllo di flusso: nessuno

A proposito di questa attività

Tenere presente quanto segue:



Ogni volta che Cumulus Linux viene installato, l'intera struttura del file system viene cancellata e ricostruita.



La password predefinita per l'account utente cumulus è **cumulus**. La prima volta che si accede a Cumulus Linux, è necessario modificare questa password predefinita. Assicurarsi di aggiornare gli script di automazione prima di installare una nuova immagine. Cumulus Linux offre opzioni della riga di comando per modificare automaticamente la password predefinita durante il processo di installazione.

Fasi

1. Accedere allo switch.

La prima volta che si accede allo switch, è necessario specificare il nome utente/la password **cumulus** /**cumulus** con sudo privilegi.

Mostra esempio

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Controllare la versione di Cumulus Linux:

```
net show system
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Configurare il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito. Il nuovo nome host diventa effettivo solo dopo il riavvio della sessione console/SSH.



Uno switch Cumulus Linux fornisce almeno una porta di gestione Ethernet dedicata chiamata `eth0`. Questa interfaccia è specificamente per l'utilizzo della gestione fuori banda. Per impostazione predefinita, l'interfaccia di gestione utilizza DHCPv4 per l'indirizzamento.



Non utilizzare caratteri di sottolineatura (`_`), apostrofo (`'`) o non ASCII nel nome host.

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Questo comando modifica entrambi `/etc/hostname` e `/etc/hosts` file.

4. Verificare che il nome host, l'indirizzo IP, la subnet mask e il gateway predefinito siano stati aggiornati.

Mostra esempio

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.233.204.71 netmask 255.255.254.0 broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6 prefixlen 64 scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6 txqueuelen 1000 (Ethernet)
RX packets 75364 bytes 23013528 (21.9 MiB)
RX errors 0 dropped 7 overruns 0 frame 0
TX packets 4053 bytes 827280 (807.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Configurare il fuso orario utilizzando la modalità interattiva NTP.

- a. Su un terminale, eseguire il seguente comando:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- b. Seguire le opzioni del menu a schermo per selezionare l'area geografica e la regione.
- c. Per impostare il fuso orario per tutti i servizi e i daemon, riavviare lo switch.
- d. Verificare che la data e l'ora dello switch siano corrette e, se necessario, aggiornarle.

6. Installare Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-  
server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

Il programma di installazione avvia il download. Digitare **y** quando richiesto.

7. Riavviare lo switch NVIDIA SN2100:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. L'installazione viene avviata automaticamente e vengono visualizzate le seguenti schermate di GRUB. Non * effettuare selezioni:

- Cumulus-Linux GNU/Linux
- ONIE: Installare il sistema operativo
- INSTALLAZIONE DI CUMULUS
- Cumulus-Linux GNU/Linux

9. Ripetere i passaggi da 1 a 4 per accedere.

10. Verificare che la versione di Cumulus Linux sia 4.4.3:

```
net show version
```

Mostra esempio

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Creare un nuovo utente e aggiungerlo al sudo gruppo. Questo utente diventa effettivo solo dopo il riavvio della sessione console/SSH.

```
sudo adduser --ingroup netedit admin
```

Mostra esempio

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user `admin' ...
Adding new user `admin' (1001) with group `netedit' ...
Creating home directory `/home/admin' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

Quali sono le prossime novità?

["Installare lo script RCF".](#)

Installare Cumulus Linux in modalità ONIE

Seguire questa procedura per installare il sistema operativo Cumulus Linux (CL) quando lo switch è in esecuzione in modalità ONIE.



Il sistema operativo Cumulus Linux (CL) può essere installato quando lo switch esegue Cumulus Linux o ONIE (vedere ["Installare in modalità Cumulus"](#)).

A proposito di questa attività

È possibile installare Cumulus Linux utilizzando Open Network Install Environment (ONIE) che consente il rilevamento automatico dell'immagine di un programma di installazione di rete. Questo semplifica il modello di sistema per la protezione degli switch con una scelta di sistemi operativi, come Cumulus Linux. Il modo più semplice per installare Cumulus Linux con ONIE consiste nel rilevamento HTTP locale.



Se l'host è abilitato per IPv6, assicurarsi che sia in esecuzione un server Web. Se l'host è abilitato per IPv4, assicurarsi che sia in esecuzione DHCP oltre a un server Web.

Questa procedura illustra come aggiornare Cumulus Linux dopo l'avvio dell'amministratore in ONIE.

Fasi

1. Scaricare il file di installazione di Cumulus Linux nella directory principale del server Web. Rinominare il file `onie-installer`.
2. Collegare l'host alla porta Ethernet di gestione dello switch utilizzando un cavo Ethernet.
3. Accendere lo switch. Lo switch scarica il programma di installazione dell'immagine ONIE e si avvia. Al termine dell'installazione, nella finestra del terminale viene visualizzato il prompt di accesso di Cumulus Linux.



Ogni volta che Cumulus Linux viene installato, l'intera struttura del file system viene cancellata e ricostruita.

4. Riavviare lo switch SN2100:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Premere il tasto **Esc** nella schermata di GNU GRUB per interrompere il normale processo di avvio, selezionare **ONIE** e premere **Invio**.
6. Nella schermata successiva, selezionare **ONIE: Install OS**.
7. Il processo di ricerca del programma di installazione di ONIE esegue la ricerca dell'installazione automatica. Premere **Invio** per interrompere temporaneamente il processo.
8. Quando il processo di rilevamento si è arrestato:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process 427:
No such process done.
```

9. Se il servizio DHCP è in esecuzione sulla rete, verificare che l'indirizzo IP, la subnet mask e il gateway predefinito siano assegnati correttamente:

```
ifconfig eth0
```

Mostra esempio

```
ONIE:/ # ifconfig eth0
eth0    Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
        inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
        inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
        TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
        Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref
Use Iface

default            10.233.204.1      0.0.0.0           UG    0      0
0 eth0
10.233.204.0       *                  255.255.254.0     U      0      0
0 eth0
```

10. Se lo schema di indirizzamento IP viene definito manualmente, procedere come segue:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Ripetere il passaggio 9 per verificare che le informazioni statiche siano inserite correttamente.
12. Installare Cumulus Linux:

```
ONIE:/ # route
```

```
Kernel IP routing table
```

```
ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

```
Stopping: discover... done.
```

```
Info: Attempting
```

```
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-mlx-amd64.bin ...
```

```
Connecting to 10.60.132.97 (10.60.132.97:80)
```

```
installer          100% |*|    552M  0:00:00 ETA
```

```
...
```

```
...
```

13. Una volta completata l'installazione, accedere allo switch:

Mostra esempio

```
cumulus login: cumulus
```

```
Password: cumulus
```

```
You are required to change your password immediately (administrator enforced)
```

```
Changing password for cumulus.
```

```
Current password: cumulus
```

```
New password: <new_password>
```

```
Retype new password: <new_password>
```

14. Verificare la versione di Cumulus Linux:

```
net show version
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show version
```

```
NCLU_VERSION=1.0-cl4.4.3u4
```

```
DISTRIB_ID="Cumulus Linux"
```

```
DISTRIB_RELEASE=4.4.3
```

```
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

Quali sono le prossime novità?

["Installare lo script RCF".](#)

Installare lo script RCF

Seguire questa procedura per installare lo script RCF.

Di cosa hai bisogno

Prima di installare lo script RCF, assicurarsi che sullo switch siano disponibili le seguenti informazioni:

- Cumulus Linux 4.4.3 è installato.
- Indirizzo IP, subnet mask e gateway predefinito definiti tramite DHCP o configurati manualmente.

Versioni correnti degli script RCF

Sono disponibili due script RCF per le applicazioni di clustering e storage. La procedura per ciascuno di essi è la stessa.

- Clustering: **MSN2100-RCF-v1.8-Cluster**
- Storage: **MSN2100-RCF-v1.8-Storage**



La seguente procedura di esempio mostra come scaricare e applicare lo script RCF per gli switch del cluster.



L'output di comando di esempio utilizza l'indirizzo IP di gestione dello switch 10.233.204.71, la netmask 255.255.254.0 e il gateway predefinito 10.233.204.1.

Fasi

1. Visualizzare le interfacce disponibili sullo switch SN2100:

```
net show interface all
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	---	-----	-----	-----	-----

...						
...						
ADMDN	swp1	N/A	9216	NotConfigured		
ADMDN	swp2	N/A	9216	NotConfigured		
ADMDN	swp3	N/A	9216	NotConfigured		
ADMDN	swp4	N/A	9216	NotConfigured		
ADMDN	swp5	N/A	9216	NotConfigured		
ADMDN	swp6	N/A	9216	NotConfigured		
ADMDN	swp7	N/A	9216	NotConfigure		
ADMDN	swp8	N/A	9216	NotConfigured		
ADMDN	swp9	N/A	9216	NotConfigured		
ADMDN	swp10	N/A	9216	NotConfigured		
ADMDN	swp11	N/A	9216	NotConfigured		
ADMDN	swp12	N/A	9216	NotConfigured		
ADMDN	swp13	N/A	9216	NotConfigured		
ADMDN	swp14	N/A	9216	NotConfigured		
ADMDN	swp15	N/A	9216	NotConfigured		
ADMDN	swp16	N/A	9216	NotConfigured		

2. Copiare lo script python RCF sullo switch:

```
cumulus@cumulus:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt: /tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster          100% 8607    111.2KB/s
00:00
```

3. Applicare lo script python RCF **MSN2100-RCF-v1.8-Cluster**:


```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Lo script RCF completa le istruzioni elencate sopra.



Per qualsiasi problema di script RCF python che non può essere corretto, contatta ["Supporto NetApp"](#) per assistenza.

4. Verificare la configurazione dopo il riavvio:

```
net show interface all
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	-----	-----	-----	-----	-----
...						
...						
DN	swp1s0	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s1	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s2	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp1s3	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s0	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s1	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s2	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp2s3	N/A	9216	Trunk/L2		Master:
bridge (UP)						
UP	swp3	100G	9216	Trunk/L2		Master:
bridge (UP)						
UP	swp4	100G	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp5	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp6	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp7	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp8	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp9	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp10	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp11	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp12	N/A	9216	Trunk/L2		Master:
bridge (UP)						
DN	swp13	N/A	9216	Trunk/L2		Master:
bridge (UP)						

```

DN      swp14      N/A    9216    Trunk/L2      Master:
bridge(UP)
UP      swp15      N/A    9216    BondMember    Master:
bond_15_16(UP)
UP      swp16      N/A    9216    BondMember    Master:
bond_15_16(UP)
...
...

```

```
cumulus@cumulus:mgmt:~$ net show roce config
```

```
RoCE mode..... lossless
```

```
Congestion Control:
```

```
Enabled SPs.... 0 2 5
```

```
Mode..... ECN
```

```
Min Threshold.. 150 KB
```

```
Max Threshold.. 1500 KB
```

```
PFC:
```

```
Status..... enabled
```

```
Enabled SPs.... 2 5
```

```
Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9
```

DSCP	802.1p	switch-priority
-----	-----	-----
0 1 2 3 4 5 6 7	0	0
8 9 10 11 12 13 14 15	1	1
16 17 18 19 20 21 22 23	2	2
24 25 26 27 28 29 30 31	3	3
32 33 34 35 36 37 38 39	4	4
40 41 42 43 44 45 46 47	5	5
48 49 50 51 52 53 54 55	6	6
56 57 58 59 60 61 62 63	7	7

switch-priority	TC	ETS
-----	--	-----
0 1 3 4 6 7	0	DWRR 28%
2	2	DWRR 28%
5	5	DWRR 43%

5. Verificare le informazioni relative al ricetrasmittitore nell'interfaccia:

```
net show interface pluggables
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
```

Interface	Identifier	Vendor	Name	Vendor PN	Vendor SN
Vendor	Rev				
swp3	0x11 (QSFP28)	Amphenol		112-00574	
APF20379253516	B0				
swp4	0x11 (QSFP28)	AVAGO		332-00440	AF1815GU05Z
A0					
swp15	0x11 (QSFP28)	Amphenol		112-00573	
APF21109348001	B0				
swp16	0x11 (QSFP28)	Amphenol		112-00573	
APF21109347895	B0				

6. Verificare che i nodi dispongano di una connessione a ciascuno switch:

```
net show lldp
```

Mostra esempio

```
cumulus@cumulus:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw1	e3a
swp4	100G	Trunk/L2	sw2	e3b
swp15	100G	BondMember	sw13	swp15
swp16	100G	BondMember	sw14	swp16

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

a. Verificare che le porte e0d siano in buone condizioni su tutti i nodi del cluster:

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

Mostra esempio

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

Node: node1

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

Node: node2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e3a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e3b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

- a. Verificare lo stato dello switch dal cluster (potrebbe non essere visualizzato lo switch sw2, poiché i LIF non sono presenti su e0d).

Mostra esempio

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
-----	-----	-----	-----	-----
node1/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-


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

Switch	Type	Address
Model		
-----	-----	-----
sw1	cluster-network	10.233.205.90
MSN2100-CB2RC		
Serial Number: MNXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on		
Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		
sw2	cluster-network	10.233.205.91
MSN2100-CB2RC		
Serial Number: MNCXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on		
Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		

Quali sono le prossime novità?

"Configurare la raccolta dei log degli switch".

Raccolta registro monitoraggio stato switch Ethernet

Il monitor dello stato degli switch Ethernet (CSHM) ha la responsabilità di garantire lo stato operativo degli switch del cluster e della rete di storage e di raccogliere i registri degli switch a scopo di debug. Questa procedura guida l'utente attraverso il processo di impostazione e avvio della raccolta di registri **supporto** dettagliati dal centralino e avvia una raccolta oraria di dati **periodici** raccolti da AutoSupport.

Prima di iniziare

- È necessario specificare l'utente per la raccolta di log quando viene applicato il file di configurazione di riferimento (RCF). Per impostazione predefinita, questo utente è impostato su 'admin'. Se si desidera utilizzare un altro utente, è necessario specificarlo nella sezione `*# SHM User*s` di RCF.
- L'utente deve avere accesso ai comandi **nv show**. Questo può essere aggiunto eseguendo `sudo adduser USER nv show` E sostituendo l'utente con l'utente per la raccolta dei log.
- Il monitoraggio dello stato dello switch deve essere abilitato per lo switch. Verificare questo assicurandosi che `Is Monitored:` il campo è impostato su **true** nell'output di `system switch ethernet show` comando.

Fasi

1. Per impostare la raccolta di log, eseguire il comando seguente per ogni switch. Viene richiesto di immettere il nome dello switch, il nome utente e la password per la raccolta del registro.

```
system switch ethernet log setup-password
```

Mostra esempio

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Per avviare la raccolta dei log, eseguire il comando seguente, sostituendo DEVICE con lo switch utilizzato nel comando precedente. In questo modo vengono avviati entrambi i tipi di raccolta di log: Il dettagliato Support registri e una raccolta oraria di Periodic dati.

```
system switch ethernet log modify -device <switch-name> -log-request true
```


Mostra esempio

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Attendere 10 minuti, quindi verificare che la raccolta dei log sia completa:

```
system switch ethernet log show
```



Se uno di questi comandi restituisce un errore o se la raccolta dei log non viene completata, contattare il supporto NetApp.

Risoluzione dei problemi

Se si verifica uno dei seguenti stati di errore segnalati dalla funzione di raccolta registri (visibile nell'output di `system switch ethernet log show`), provare i passi di debug corrispondenti:

Stato errore raccolta log	Risoluzione
Chiavi RSA non presenti	Rigenerare le chiavi SSH ONTAP. Contattare l'assistenza NetApp.
errore password cambio	Verificare le credenziali, verificare la connettività SSH e rigenerare le chiavi SSH ONTAP. Consultare la documentazione dello switch o contattare il supporto NetApp per le istruzioni.
Chiavi ECDSA non presenti per FIPS	Se la modalità FIPS è attivata, le chiavi ECDSA devono essere generate sullo switch prima di riprovare.
trovato log preesistente	Rimuovere la directory di raccolta dei log precedente e il file '.tar' che si trova in <code>/tmp/shm_log</code> sull'interruttore.

errore registro dump switch	Assicurarsi che l'utente dello switch disponga delle autorizzazioni per la raccolta dei registri. Fare riferimento ai prerequisiti riportati sopra.
------------------------------------	---

Configurare SNMPv3

Seguire questa procedura per configurare SNMPv3, che supporta il monitoraggio dello stato dello switch Ethernet (CSHM).

A proposito di questa attività

I seguenti comandi configurano un nome utente SNMPv3 sugli switch NVIDIA SN2100:

- Per **nessuna autenticazione**:

```
net add snmp-server username SNMPv3_USER auth-none
```
- Per l'autenticazione **MD5/SHA**:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
```
- Per l'autenticazione **MD5/SHA con crittografia AES/DES**:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
[encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Il seguente comando configura un nome utente SNMPv3 sul lato ONTAP:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Il seguente comando stabilisce il nome utente SNMPv3 con CSHM:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Fasi

1. Impostare l'utente SNMPv3 sullo switch per l'utilizzo dell'autenticazione e della crittografia:

```
net show snmp status
```

Mostra esempio

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status                active (running)
Reload Status                 enabled
Listening IP Addresses        all vrf mgmt
Main snmpd PID                4318
Version 1 and 2c Community String Configured
Version 3 Usernames           Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
```

```

rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syssservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

=====

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username
SNMPv3User	auth-md5 <password>	encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames     Configured    <---- Configured
here
-----
cumulus@sw1:~$

```

2. Impostare l'utente SNMPv3 sul lato ONTAP:

```

security login create -user-or-group-name SNMPv3User -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212

```

Mostra esempio

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Configurare CSHM per il monitoraggio con il nuovo utente SNMPv3:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)" -instance
```

Mostra esempio

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Verificare che il numero seriale da interrogare con l'utente SNMPv3 appena creato sia lo stesso descritto nel passaggio precedente una volta completato il periodo di polling CSHM.

```
system switch ethernet polling-interval show
```

Mostra esempio

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Migrare gli switch

Migrare da uno switch storage Cisco a uno switch storage NVIDIA SN2100

È possibile migrare gli switch Cisco meno recenti per un cluster ONTAP agli switch storage NVIDIA SN2100. Si tratta di una procedura senza interruzioni.

Verifica dei requisiti

Sono supportati i seguenti switch storage:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Vedere "[Hardware Universe](#)" per informazioni dettagliate sulle porte supportate e sulle relative configurazioni.

Di cosa hai bisogno

Assicurarsi che:

- Il cluster esistente è configurato e funziona correttamente.
- Tutte le porte di storage sono in stato attivo per garantire operazioni senza interruzioni.
- Gli switch storage NVIDIA SN2100 sono configurati e funzionano con la versione corretta di Cumulus Linux installata con il file di configurazione di riferimento (RCF) applicato.
- La configurazione della rete di storage esistente prevede quanto segue:
 - Un cluster NetApp ridondante e completamente funzionale che utilizza entrambi gli switch Cisco meno recenti.
 - Connettività di gestione e accesso alla console sia agli switch Cisco meno recenti che ai nuovi switch.
 - Tutte le LIF del cluster in stato up con le LIF del cluster si trovano sulle porte home.
 - Porte ISL abilitate e cablate tra i vecchi switch Cisco e tra i nuovi switch.
- Vedere ["Hardware Universe"](#) per informazioni dettagliate sulle porte supportate e sulle relative configurazioni.
- Alcune porte sono configurate sugli switch NVIDIA SN2100 per funzionare a 100 GbE.
- Hai pianificato, migrato e documentato la connettività 100 GbE dai nodi agli switch storage NVIDIA SN2100.

Migrare gli switch

A proposito degli esempi

In questa procedura, gli switch storage Cisco Nexus 9336C-FX2 vengono utilizzati, ad esempio, comandi e output.

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

- Gli switch storage Cisco Nexus 9336C-FX2 esistenti sono *S1* e *S2*.
- I nuovi switch storage NVIDIA SN2100 sono *sw1* e *sw2*.
- I nodi sono *node1* e *node2*.
- I LIF del cluster sono *node1_clus1* e *node1_clus2* sul nodo 1, e *node2_clus1* e *node2_clus2* rispettivamente sul nodo 2.
- Il `cluster1 : *` prompt indica il nome del cluster.
- Le porte di rete utilizzate in questa procedura sono *e5a* e *e5b*.
- Le porte breakout hanno il formato: *swp1s0-3*. Ad esempio, quattro porte di breakout su *swp1* sono *swp1s0*, *swp1s1*, *swp1s2* e *swp1s3*.
- L'interruttore *S2* viene sostituito dall'interruttore *sw2*, quindi l'interruttore *S1* viene sostituito dall'interruttore *sw1*.
 - Il cablaggio tra i nodi e *S2* viene quindi scollegato da *S2* e ricollegato a *sw2*.
 - Il cablaggio tra i nodi e *S1* viene quindi scollegato da *S1* e ricollegato a *sw1*.

Fase 1: Preparazione per la migrazione

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

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


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

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

```
set -privilege advanced
```

Viene visualizzato il prompt Advanced (*>).

3. Determinare lo stato amministrativo o operativo di ciascuna interfaccia di storage:

Ogni porta deve visualizzare Enabled per Status.

Fase 2: Configurazione di cavi e porte

1. Visualizzare gli attributi della porta di rete:

```
storage port show
```

Mostra esempio

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

2. Verificare che le porte di storage su ciascun nodo siano collegate agli switch di storage esistenti nel seguente modo (dal punto di vista dei nodi) utilizzando il comando:

```
network device-discovery show -protocol lldp
```

Mostra esempio

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

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

node1	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1 -
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/1 -
node2	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2 -
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/2 -

3. Sugli switch S1 e S2, assicurarsi che le porte e gli switch di storage siano collegati nel modo seguente (dal punto di vista degli switch) utilizzando il comando:

```
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 Port ID	Local Intf	Holdtime	Capability
node1 e0c	Eth1/1	121	S
node2 e0c	Eth1/2	121	S
SHFGD1947000186 e0a	Eth1/10	120	S
SHFGD1947000186 e0a	Eth1/11	120	S
SHFGB2017000269 e0a	Eth1/12	120	S
SHFGB2017000269 e0a	Eth1/13	120	S

S2# **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 Port ID	Local Intf	Holdtime	Capability
node1 e5b	Eth1/1	121	S
node2 e5b	Eth1/2	121	S
SHFGD1947000186 e0b	Eth1/10	120	S
SHFGD1947000186 e0b	Eth1/11	120	S
SHFGB2017000269 e0b	Eth1/12	120	S
SHFGB2017000269 e0b	Eth1/13	120	S

4. Sullo switch sw2, spegnere le porte collegate alle porte di storage e ai nodi degli shelf di dischi.

Mostra esempio

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Spostare le porte di storage dei nodi del controller e degli shelf di dischi dal vecchio switch S2 al nuovo switch sw2, utilizzando il cablaggio appropriato supportato da NVIDIA SN2100.
6. Sullo switch sw2, richiamare le porte collegate alle porte di storage dei nodi e degli shelf di dischi.

Mostra esempio

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Verificare che le porte di storage su ciascun nodo siano ora collegate agli switch nel modo seguente, dal punto di vista dei nodi:

```
network device-discovery show -protocol lldp
```

Mostra esempio

```
cluster1::~*> network device-discovery show -protocol lldp
```

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

node1	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

8. Verificare gli attributi della porta di rete:

```
storage port show
```

Mostra esempio

```
cluster1::*> storage port show
```

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

node1	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

9. Sullo switch sw2, verificare che tutte le porte di storage dei nodi siano in funzione:

```
net show interface
```

Mostra esempio

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					
-----	-----	----	-----	-----	-----

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

10. Sullo switch sw1, spegnere le porte collegate alle porte di storage dei nodi e degli shelf di dischi.

Mostra esempio

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Spostare le porte di storage dei nodi del controller e degli shelf di dischi dal vecchio switch S1 al nuovo switch sw1, utilizzando il cablaggio appropriato supportato da NVIDIA SN2100.
12. Sullo switch sw1, richiamare le porte collegate alle porte di storage dei nodi e degli shelf di dischi.

Mostra esempio

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Verificare che le porte di storage su ciascun nodo siano ora collegate agli switch nel modo seguente, dal punto di vista dei nodi:

```
network device-discovery show -protocol lldp
```

Mostra esempio

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

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

node1	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

14. Verificare la configurazione finale:

```
storage port show
```

Ogni porta deve visualizzare Enabled per State e abilitato per Status.

Mostra esempio

```
cluster1::*> storage port show
```

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

node1	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

15. Sullo switch sw2, verificare che tutte le porte di storage dei nodi siano in funzione:

```
net show interface
```


Mostra esempio

```
cumulus@sw2:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e5b)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e5b)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

16. Verificare che entrambi i nodi dispongano di una connessione a ciascuno switch:

```
net show lldp
```

Mostra esempio

L'esempio seguente mostra i risultati appropriati per entrambi gli switch:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
...				
swp1	100G	Trunk/L2	node1	e0c
swp2	100G	Trunk/L2	node2	e0c
swp3	100G	Trunk/L2	SHFFG1826000112	e0a
swp4	100G	Trunk/L2	SHFFG1826000112	e0a
swp5	100G	Trunk/L2	SHFFG1826000102	e0a
swp6	100G	Trunk/L2	SHFFG1826000102	e0a

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
...				
swp1	100G	Trunk/L2	node1	e5b
swp2	100G	Trunk/L2	node2	e5b
swp3	100G	Trunk/L2	SHFFG1826000112	e0b
swp4	100G	Trunk/L2	SHFFG1826000112	e0b
swp5	100G	Trunk/L2	SHFFG1826000102	e0b
swp6	100G	Trunk/L2	SHFFG1826000102	e0b

Fase 3: Completare la procedura

1. Attivare la funzione di raccolta dei log dello switch Ethernet per la raccolta dei file di log relativi allo switch, utilizzando i due comandi:

```
system switch ethernet log setup-password e.system switch ethernet log enable-collection
```

Inserire: system switch ethernet log setup-password

Mostra esempio

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Seguito da:

```
system switch ethernet log enable-collection
```

Mostra esempio

```
cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Se uno di questi comandi restituisce un errore, contattare il supporto NetApp.

2. Avviare la funzione di raccolta dei log dello switch:

```
system switch ethernet log collect -device *
```

Attendere 10 minuti, quindi verificare che la raccolta dei log sia stata eseguita correttamente utilizzando il comando:

```
system switch ethernet log show
```

Mostra esempio

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	sw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete

3. Modificare nuovamente il livello di privilegio in admin:

```
set -privilege admin
```

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

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

Sostituire uno switch di storage NVIDIA SN2100

Quando si sostituiscono gli switch di storage NVIDIA SN2100, è necessario conoscere alcune informazioni di configurazione, i collegamenti delle porte e i requisiti di cablaggio.

Prima di iniziare

Prima di installare il software Cumulus e gli RCF su uno switch di storage NVIDIA SN2100, verificare che sussistano le seguenti condizioni:

- Il sistema supporta gli switch storage NVIDIA SN2100.
- È necessario aver scaricato gli RCF applicabili.
- Il ["Hardware Universe"](#) fornisce informazioni dettagliate sulle porte supportate e sulle relative configurazioni.

A proposito di questa attività

La configurazione di rete esistente deve avere le seguenti caratteristiche:

- Assicurarsi che tutte le fasi di risoluzione dei problemi siano state completate per confermare che lo switch deve essere sostituito.
- La connettività di gestione deve esistere su entrambi gli switch.



Assicurarsi che tutte le fasi di risoluzione dei problemi siano state completate per confermare che lo switch deve essere sostituito.

Lo switch NVIDIA SN2100 sostitutivo deve avere le seguenti caratteristiche:

- La connettività della rete di gestione deve essere funzionale.
- L'accesso della console allo switch sostitutivo deve essere in posizione.
- Sullo switch deve essere caricata l'immagine appropriata del sistema operativo RCF e Cumulus.
- La personalizzazione iniziale dello switch deve essere completata.

Riepilogo della procedura

Questa procedura sostituisce il secondo switch di storage NVIDIA SN2100 sw2 con il nuovo switch NVIDIA SN2100 nsw2. I due nodi sono node1 e node2.

Procedura da completare:

- Verificare che lo switch da sostituire sia sw2.
- Scollegare i cavi dallo switch sw2.
- Ricollegare i cavi allo switch nsw2.
- Verificare tutte le configurazioni del dispositivo sullo switch nsw2.

Fasi

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

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

x è la durata della finestra di manutenzione in ore.

2. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare: `set -privilege advanced`
3. Controllare lo stato delle porte dei nodi di storage per verificare che vi sia una connessione allo switch di storage S1:

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

Mostra esempio

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN 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	100	enabled	online	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	100	enabled	online	30

```
cluster1::*>
```

4. Verificare che lo switch di storage sw1 sia disponibile:

```
network device-discovery show
```

Mostra esempio

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1/lldp				
	e3a	sw1 (b8:ce:f6:19:1b:42)	swp3	-
node2/lldp				
	e3a	sw1 (b8:ce:f6:19:1b:42)	swp4	-

```
cluster1::*>
```

5. Eseguire

```
net show interface comando sull'interruttore funzionante per confermare che è possibile visualizzare sia i nodi che tutti gli shelf:
```

```
net show interface
```

Mostra esempio

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e3a)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e3a)
Master: bridge(UP)					
UP	swp3	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp4	100G	9216	Trunk/L2	SHFFG1826000112 (e0b)
Master: bridge(UP)					
UP	swp5	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
UP	swp6	100G	9216	Trunk/L2	SHFFG1826000102 (e0b)
Master: bridge(UP)					
...					
...					

6. Verificare le porte dello shelf nel sistema storage:

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

Mostra esempio

```
cluster1::*> storage shelf port show -fields remote-device, remote-  
port  
shelf    id  remote-port  remote-device  
-----  --  -  
3.20     0   swp3         sw1  
3.20     1   -           -  
3.20     2   swp4         sw1  
3.20     3   -           -  
3.30     0   swp5         sw1  
3.20     1   -           -  
3.30     2   swp6         sw1  
3.20     3   -           -  
cluster1::*>
```

7. Rimuovere tutti i cavi collegati allo switch di storage sw2.
8. Ricollegare tutti i cavi allo switch sostitutivo nsw2.
9. Controllare nuovamente lo stato di salute delle porte del nodo di storage:
storage port show -port-type ENET

Mostra esempio

```
cluster1::*> storage port show -port-type ENET  
  
Node      Port Type  Mode   Speed      State   Status   VLAN  
-----  -  
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 100   enabled online   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 100   enabled online   30  
cluster1::*>
```

10. Verificare che entrambi gli switch siano disponibili:
net device-discovery show

Mostra esempio

```
cluster1::*> network device-discovery show protocol lldp
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/lldp
          e3a  sw1 (b8:ce:f6:19:1b:96)   swp1       -
          e7b  nsw2 (b8:ce:f6:19:1a:7e)  swp1       -
node2/lldp
          e3a  sw1 (b8:ce:f6:19:1b:96)   swp2       -
          e7b  nsw2 (b8:ce:f6:19:1a:7e)  swp2       -
cluster1::*>
```

11. Verificare le porte dello shelf nel sistema storage:

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

Mostra esempio

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf  id  remote-port  remote-device
-----  --  -
3.20   0   swp3         sw1
3.20   1   swp3         nsw2
3.20   2   swp4         sw1
3.20   3   swp4         nsw2
3.30   0   swp5         sw1
3.20   1   swp5         nsw2
3.30   2   swp6         sw1
3.20   3   swp6         nsw2
cluster1::*>
```

12. Creare una password per la funzione di raccolta dei log dello switch Ethernet Health monitor:

```
system switch ethernet log setup-password
```

Mostra esempio

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
nsw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: csw1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: nsw2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

13. Attivare la funzione di raccolta dei log dello switch Ethernet.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Mostra esempio

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

Attendere 10 minuti, quindi verificare che la raccolta dei log sia completa:

```
system switch ethernet log show
```

Mostra esempio

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	nsw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Se uno di questi comandi restituisce un errore o se la raccolta dei log non viene completata, contattare il supporto NetApp.

14. Modificare nuovamente il livello di privilegio in admin: `set -privilege admin`
15. Se è stata eliminata la creazione automatica del caso, riattivarla richiamando un messaggio AutoSupport:
`system node autosupport invoke -node * -type all -message MAINT=END`

Informazioni sul copyright

Copyright © 2024 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.