Cisco Nexus 92300YC

Cluster and storage switches

NetApp
April 25, 2024

Sommario

Cisco Nexus 92300YC . . . 1
Panoramica . . . 1
Installare l’hardware . . . 5
Configurare il software . . . 15
Migrare gli switch . . . 59
Sostituire gli interruttori . . . 96

Cisco Nexus 92300YC

Panoramica

Panoramica dell'installazione e della configurazione degli switch Cisco Nexus 92300YC

Prima di configurare gli switch Cisco Nexus 92300YC, consultare la panoramica della procedura.

Per configurare inizialmente uno switch Cisco Nexus 92300YC sui sistemi che eseguono ONTAP, attenersi alla seguente procedura:

1. "Completa il foglio di lavoro per il cablaggio di Cisco Nexus 92300YC". Il foglio di lavoro di esempio relativo ai cavi fornisce esempi di assegnazione delle porte consigliate dagli switch ai controller. Il foglio di lavoro vuoto fornisce un modello che è possibile utilizzare per la configurazione del cluster.
2. "Configurare lo switch Cisco Nexus 92300YC". Configurare e configurare lo switch Cisco Nexus 92300YC.
3. "Preparazione all'installazione del software NX-OS e del file di configurazione di riferimento (RCF)". Prepararsi all'installazione del software NX-OS e del file di configurazione di riferimento (RCF).
4. "Installare il software NX-OS". Installare il software NX-OS sullo switch Nexus 92300YC. NX-OS è un sistema operativo di rete per la serie Nexus di switch Ethernet e la serie MDS di switch Fibre Channel (FC) storage area network forniti da Cisco Systems.
5. "Installazione del file di configurazione di riferimento (RCF)". Installare RCF dopo aver configurato lo switch Nexus 92300YC per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.
6. "Installare il file di configurazione di Cluster Switch Health Monitor (CSHM)". Installare il file di configurazione applicabile per il monitoraggio dello stato degli switch del cluster Nexus 92300YC.

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 Cisco Nexus 92300YC

Per l'installazione e la manutenzione dello switch Cisco Nexus 92300YC, verificare tutti i requisiti di configurazione e di rete.

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.

Requisiti di configurazione

Per configurare il cluster, sono necessari 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 A700, l'interfaccia e0M utilizza una porta Ethernet dedicata.

Fare riferimento a. "Hardware Universe" per informazioni aggiornate.

Componenti per switch Cisco Nexus 92300YC

Per l'installazione e la manutenzione dello switch Cisco Nexus 92300YC, assicurarsi di esaminare tutti i componenti e i numeri di parte dello switch. Vedere "Hardware Universe" per ulteriori informazioni.

La seguente tabella elenca il codice ricambio e la descrizione dello switch, delle ventole e degli alimentatori 92300YC:

Codice del ricambio	Descrizione
190003	Cisco 92300YC, CLSW, 48Pt10/25 GB, 18Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25 GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-FAN-35CFM-B.	Ventola, flusso d'aria di aspirazione laterale della porta Cisco N9K
X-NXA-FAN-35CFM-F.	Ventola, flusso d'aria di scarico lato porta Cisco N9K
X-NXA-PAC-650W-B.	Alimentatore, Cisco 650 W - presa lato porta
X-NXA-PAC-650 W-F.	Alimentatore, Cisco 650 W - scarico lato porta

Dettagli sul flusso d'aria dello switch Cisco Nexus 92300YC:

- Flusso d'aria di scarico lato porta (aria standard) — l'aria fredda entra nel telaio attraverso i moduli della ventola e dell'alimentatore nel corridoio freddo e viene erogata attraverso l'estremità della porta del telaio nel corridoio caldo. Flusso d'aria di scarico lato porta con colorazione blu.
- Flusso d'aria di aspirazione lato porta (aria inversa) — l'aria fredda entra nel telaio attraverso l'estremità della porta nel corridoio freddo e si scarica attraverso i moduli della ventola e dell'alimentatore nel corridoio

caldo. Flusso d'aria di aspirazione lato porta con colorazione bordeaux.

Requisiti della documentazione per gli switch Cisco Nexus 92300YC

Per l'installazione e la manutenzione dello switch Cisco Nexus 92300YC, consultare tutta la documentazione consigliata.

Documentazione dello switch

Per configurare gli switch Cisco Nexus 92300YC, è necessario disporre della seguente documentazione dal "Supporto degli switch Cisco Nexus serie 9000" pagina:

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

Documentazione sui sistemi ONTAP

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

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

Kit di guide e documentazione del cabinet

Per installare uno switch Cisco Nexus 92300YC 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 Nexus 92300YC in un cabinet NetApp"	Descrive come installare uno switch Cisco Nexus 92300YC 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

Completa il foglio di lavoro per il cablaggio di Cisco Nexus 92300YC

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

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

Esempio di foglio di lavoro per il cablaggio

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

Switch del cluster A		**Switch del cluster B**	
Porta dello switch	Utilizzo di nodi e porte	Porta dello switch	Utilizzo di nodi e porte
1	Nodo 10/25 GbE	1	Nodo 10/25 GbE
2	Nodo 10/25 GbE	2	Nodo 10/25 GbE
3	Nodo 10/25 GbE	3	Nodo 10/25 GbE
4	Nodo 10/25 GbE	4	Nodo 10/25 GbE
5	Nodo 10/25 GbE	5	Nodo 10/25 GbE
6	Nodo 10/25 GbE	6	Nodo 10/25 GbE
7	Nodo 10/25 GbE	7	Nodo 10/25 GbE
8	Nodo 10/25 GbE	8	Nodo 10/25 GbE
9	Nodo 10/25 GbE	9	Nodo 10/25 GbE
10	Nodo 10/25 GbE	10	Nodo 10/25 GbE
11	Nodo 10/25 GbE	11	Nodo 10/25 GbE
12	Nodo 10/25 GbE	12	Nodo 10/25 GbE
13	Nodo 10/25 GbE	13	Nodo 10/25 GbE
14	Nodo 10/25 GbE	14	Nodo 10/25 GbE

Switch del cluster A		Switch del cluster B	
15	Nodo 10/25 GbE	15	Nodo 10/25 GbE
16	Nodo 10/25 GbE	16	Nodo 10/25 GbE
17	Nodo 10/25 GbE	17	Nodo 10/25 GbE
18	Nodo 10/25 GbE	18	Nodo 10/25 GbE
19	Nodo 10/25 GbE	19	Nodo 10/25 GbE
20	Nodo 10/25 GbE	20	Nodo 10/25 GbE
21	Nodo 10/25 GbE	21	Nodo 10/25 GbE
22	Nodo 10/25 GbE	22	Nodo 10/25 GbE
23	Nodo 10/25 GbE	23	Nodo 10/25 GbE
24	Nodo 10/25 GbE	24	Nodo 10/25 GbE
25	Nodo 10/25 GbE	25	Nodo 10/25 GbE
26	Nodo 10/25 GbE	26	Nodo 10/25 GbE
27	Nodo 10/25 GbE	27	Nodo 10/25 GbE
28	Nodo 10/25 GbE	28	Nodo 10/25 GbE
29	Nodo 10/25 GbE	29	Nodo 10/25 GbE
30	Nodo 10/25 GbE	30	Nodo 10/25 GbE
31	Nodo 10/25 GbE	31	Nodo 10/25 GbE
32	Nodo 10/25 GbE	32	Nodo 10/25 GbE
33	Nodo 10/25 GbE	33	Nodo 10/25 GbE
34	Nodo 10/25 GbE	34	Nodo 10/25 GbE
35	Nodo 10/25 GbE	35	Nodo 10/25 GbE
36	Nodo 10/25 GbE	36	Nodo 10/25 GbE

Switch del cluster A		Switch del cluster B	
37	Nodo 10/25 GbE	37	Nodo 10/25 GbE
38	Nodo 10/25 GbE	38	Nodo 10/25 GbE
39	Nodo 10/25 GbE	39	Nodo 10/25 GbE
40	Nodo 10/25 GbE	40	Nodo 10/25 GbE
41	Nodo 10/25 GbE	41	Nodo 10/25 GbE
42	Nodo 10/25 GbE	42	Nodo 10/25 GbE
43	Nodo 10/25 GbE	43	Nodo 10/25 GbE
44	Nodo 10/25 GbE	44	Nodo 10/25 GbE
45	Nodo 10/25 GbE	45	Nodo 10/25 GbE
46	Nodo 10/25 GbE	46	Nodo 10/25 GbE
47	Nodo 10/25 GbE	47	Nodo 10/25 GbE
48	Nodo 10/25 GbE	48	Nodo 10/25 GbE
49	Nodo 40/100 GbE	49	Nodo 40/100 GbE
50	Nodo 40/100 GbE	50	Nodo 40/100 GbE
51	Nodo 40/100 GbE	51	Nodo 40/100 GbE
52	Nodo 40/100 GbE	52	Nodo 40/100 GbE
53	Nodo 40/100 GbE	53	Nodo 40/100 GbE
54	Nodo 40/100 GbE	54	Nodo 40/100 GbE
55	Nodo 40/100 GbE	55	Nodo 40/100 GbE
56	Nodo 40/100 GbE	56	Nodo 40/100 GbE
57	Nodo 40/100 GbE	57	Nodo 40/100 GbE
58	Nodo 40/100 GbE	58	Nodo 40/100 GbE

Switch del cluster A		Switch del cluster B	
59	Nodo 40/100 GbE	59	Nodo 40/100 GbE
60	Nodo 40/100 GbE	60	Nodo 40/100 GbE
61	Nodo 40/100 GbE	61	Nodo 40/100 GbE
62	Nodo 40/100 GbE	62	Nodo 40/100 GbE
63	Nodo 40/100 GbE	63	Nodo 40/100 GbE
64	Nodo 40/100 GbE	64	Nodo 40/100 GbE
65	100 GbE ISL alla porta B dello switch 65	65	100 GbE ISL per lo switch Di Una porta 65
66	100 GbE ISL alla porta B dello switch 66	66	100 GbE ISL per lo switch Di Una porta 65

Foglio di lavoro di cablaggio vuoto

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

Switch del cluster A		Switch del cluster B	
Porta dello switch	Utilizzo di nodo/porta	Porta dello switch	Utilizzo di nodo/porta
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	

Switch del cluster A		Switch del cluster B	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	

Switch del cluster A		Switch del cluster B	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	

Switch del cluster A		Switch del cluster B	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	Da ISL a switch B porta 65	65	ISL per lo switch Di Una porta 65
66	Da ISL a switch B porta 66	66	ISL per lo switch Di Una porta 66

Configurare lo switch Cisco Nexus 92300YC

Seguire questa procedura per configurare lo switch Cisco Nexus 92300YC.

Fasi

1. Collegare la porta seriale a una porta host o seriale.
2. Collegare la porta di gestione (sul lato diverso dalla porta dello switch) alla stessa rete in cui si trova il server SFTP.
3. Nella console, impostare le impostazioni seriali lato host:
    - 9600 baud
    - 8 bit di dati
    - 1 bit di stop
    - parità: nessuna
    - controllo di flusso: nessuno

4. Quando si avvia per la prima volta o si riavvia dopo aver cancellato la configurazione in esecuzione, lo switch Nexus 92300YC esegue un ciclo di boot. Interrompere questo ciclo digitando **yes** per interrompere il provisioning automatico all'accensione.

   Viene visualizzata la finestra System Admin account Setup (Configurazione account amministratore di sistema).

   Mostra esempio

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no)[no]: y
Disabling POAP.......Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

          ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Digitare **y** per applicare lo standard di password sicura:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Inserire e confermare la password per l'amministratore utente:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Digitare **yes** per accedere alla finestra di dialogo Basic System Configuration (Configurazione di base del sistema).

Mostra esempio

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

8. Creare un altro account di accesso:

```
Create another login account (yes/no) [n]:
```

9. Configurare le stringhe di comunità SNMP di sola lettura e di lettura/scrittura:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Configurare il nome dello switch del cluster:

```
Enter the switch name : cs2
```

11. Configurare l'interfaccia di gestione out-of-band:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Configurare le opzioni IP avanzate:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Configurare i servizi Telnet:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Configurare i servizi SSH e le chiavi SSH:

```
Enable the ssh service? (yes/no) [y]: y

       Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

       Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Configurare altre impostazioni:

```
Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L2]: L2

  Configure default switchport interface state (shut/noshut) [noshut]:
noshut

  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Confermare le informazioni sullo switch e salvare la configurazione:

```
Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Quali sono le prossime novità?

"Preparare l'installazione del software NX-OS e RCF".

Esaminare le considerazioni relative al cablaggio e alla configurazione

Prima di configurare lo switch Cisco 92300YC, esaminare le seguenti considerazioni.

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

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

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

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

Configurare il software

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

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

Di cosa hai bisogno

- Un cluster completamente funzionante (nessun errore nei log o problemi simili).
- Le guide appropriate per il software e l'aggiornamento, disponibili all'interno del sito "Switch Cisco Nexus serie 9000".

A proposito degli esempi

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

Gli 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 `node1` e. `node2`.
- I nomi LIF del cluster sono `node1_clus1` e. `node1_clus2` per il node1 e. `node2_clus1` e. `node2_clus2` per il node2.
- 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. Gli output dei comandi possono variare a seconda delle diverse versioni di ONTAP.

Fasi

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato (`*>`).

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

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

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

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

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

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

3. Visualizza quante interfacce di interconnessione cluster sono configurate in ciascun nodo per ogni switch di interconnessione cluster: `network device-discovery show -protocol cdp`

Mostra esempio

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

 Node/      Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2           N9K-
C92300YC
            e0b    cs2                       Eth1/2           N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1           N9K-
C92300YC
            e0b    cs2                       Eth1/1           N9K-
C92300YC

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: node2
                                                      Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: node1
                                                      Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Visualizzare le informazioni sui LIF: `network interface show -vserver Cluster`

Mostra esempio

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

5. Ping delle LIF del cluster remoto:

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

Mostra esempio

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

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

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

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor di stato dello switch del cluster per la raccolta dei file di log relativi allo switch utilizzando i comandi seguenti:

   `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 Nexus 92300YC.

NX-OS è un sistema operativo di rete per la serie Nexus di switch Ethernet e la serie MDS di switch Fibre Channel (FC) storage area network forniti da Cisco Systems.

Verifica dei requisiti

Porte e connessioni di nodi supportate

- I collegamenti Inter-Switch (ISL) supportati per gli switch Nexus 92300YC sono le porte 1/65 e 1/66.
- Le connessioni dei nodi supportate per gli switch Nexus 92300YC sono le porte da 1/1 a 1/66.

Di cosa hai bisogno

- Software NetApp Cisco NX-OS applicabile per i tuoi switch dal sito di supporto NetApp, disponibile all'interno del sito "mysupport.netapp.com"
- 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.

Installare il software

Gli esempi di questa procedura utilizzano due nodi, ma è possibile includere fino a 24 nodi in un cluster.

A proposito degli esempi

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

- I nomi degli switch Nexus 92300YC sono `cs1` e. `cs2`.
- L'esempio utilizzato in questa procedura avvia l'aggiornamento sul secondo switch, **cs2*.*
- I nomi LIF del cluster sono `node1_clus1` e. `node1_clus2` per il node1, e. `node2_clus1` e. `node2_clus2` per il node2.
- Il nome IPSpace è `Cluster`.
- Il `cluster1::*>` prompt indica il nome del cluster.
- Le porte del cluster su ciascun nodo sono denominate `e0a` e. `e0b`.

  Vedere "*Hardware Universe*^" per le porte cluster effettivamente supportate sulla piattaforma.

Fasi

1. Collegare lo switch del cluster alla rete di gestione.
2. Utilizzare `ping` Comando 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 92300YC.

Mostra esempio

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.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.9.2.2.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.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.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) 2002-2018, 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 05.31
  NXOS: version 9.2(1)
  BIOS compile time:  05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time:  7/17/2018 16:00:00 [07/18/2018 00:21:19]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.2(1)
  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.9.2.2.bin

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

Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.2.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                                  9.2(1)
9.2(2)         yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)       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
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

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) 2002-2018, 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 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)

Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

```
  Reason: Reset due to upgrade
  System version: 9.2(1)
  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.9.2.2.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
```

Quali sono le prossime novità?

"Installare il file di configurazione di riferimento"

Installazione del file di configurazione di riferimento (RCF)

È possibile installare RCF dopo aver configurato lo switch Nexus 92300YC per la prima volta. È inoltre possibile utilizzare questa procedura per aggiornare la versione di RCF.

A proposito di questa attività

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 `node1` e. `node2`.
- I nomi LIF del cluster sono `node1_clus1`, `node1_clus2`, `node2_clus1`, e. `node2_clus2`.
- Il `cluster1::*>` prompt indica il nome del cluster.

- La procedura richiede l'utilizzo di entrambi i comandi ONTAP e. "Switch Cisco Nexus serie 9000"; I comandi ONTAP vengono utilizzati se non diversamente indicato.
- Prima di eseguire questa procedura, assicurarsi di disporre di un backup corrente della configurazione dello switch.
- 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.

Fasi

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
----------- ------ ------------------------- ----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/1     N9K-
C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/2     N9K-
C92300YC
cluster1::*>
```

2. Controllare lo stato amministrativo e operativo di ciascuna porta del cluster.
   a. Verificare che tutte le porte del cluster siano funzionanti: `network port show -ipspace Cluster`

Mostra esempio

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

Node: node1

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: node2

Ignore
                                                      Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
cluster1::*>
```

b. Verificare che tutte le interfacce del cluster (LIF) siano sulla porta home: `network interface show -vserver Cluster`

Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            node1_clus1        up/up      169.254.3.4/23    node1
e0c     true
            node1_clus2        up/up      169.254.3.5/23    node1
e0d     true
            node2_clus1        up/up      169.254.3.8/23    node2
e0c     true
            node2_clus2        up/up      169.254.3.9/23    node2
e0d     true
cluster1::*>
```

c. Verificare che il cluster visualizzi le informazioni per entrambi gli switch del cluster: `system cluster-switch show -is-monitoring-enabled-operational true`

Mostra esempio

```
cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.233.205.92
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.93
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Disattiva l'autorevert sulle LIF del cluster.

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

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

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Verificare che le porte del cluster siano migrate alle porte ospitate sullo switch del cluster cs1. Questa operazione potrebbe richiedere alcuni secondi. `network interface show -vserver Cluster`

Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1       up/up      169.254.3.4/23     node1
e0c     true
            node1_clus2       up/up      169.254.3.5/23     node1
e0c     false
            node2_clus1       up/up      169.254.3.8/23     node2
e0c     true
            node2_clus2       up/up      169.254.3.9/23     node2
e0c     false
cluster1::*>
```

6. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

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

7. 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`

8. 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
```

9. 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 "Switch Cisco Nexus serie 9000" guide.

   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: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp 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:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. Applicare l'RCF precedentemente scaricato al bootflash.

    Per ulteriori informazioni sui comandi Cisco, consultare la guida appropriata in "Switch Cisco Nexus serie 9000" guide.

Questo esempio mostra il file RCF `Nexus_92300YC_RCF_v1.0.2.txt` in fase di installazione sullo switch cs2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands

Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits)......
generated ecdsa key

Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a
single
 host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
 Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
 have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...
Copy complete.
```

11. Verificare sullo switch che l'RCF sia stato Unito correttamente:

    ```
    show running-config
    ```

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*
```

Quando si applica RCF per la prima volta, il messaggio **ERROR: Failed to write VSH comands** (ERRORE: Impossibile scrivere i comandi VSH) è previsto e può essere ignorato.

1. 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.

2. 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 "Switch Cisco Nexus serie 9000" guide.

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

3. Riavviare lo switch cs2. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

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

4. 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 -ipspace Cluster`

Mostra esempio

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

Node: node1

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

Node: node2

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

b. Verificare 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
----------- ------ ------------------------- -----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1
N9K-C92300YC
            e0b    cs2                       Ethernet1/1
N9K-C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/2
N9K-C92300YC
            e0b    cs2                       Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

A seconda della versione RCF precedentemente caricata sullo switch, è possibile osservare i seguenti output sulla console dello switch cs1

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

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

   Nell'esempio seguente viene utilizzato l'output dell'esempio di interfaccia del passo 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

6. Verificare che le LIF del cluster siano migrate alle porte ospitate sullo switch cs2. Questa operazione potrebbe richiedere alcuni secondi. `network interface show -vserver Cluster`

   Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
            Logical          Status     Network            Current
Current Is
Vserver     Interface        Admin/Oper Address/Mask       Node
Port    Home
----------- ---------------- ---------- ------------------
----------------- ------- ----
Cluster
            node1_clus1      up/up      169.254.3.4/23     node1
e0d     false
            node1_clus2      up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1      up/up      169.254.3.8/23     node2
e0d     false
            node2_clus2      up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

7. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

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

8. Ripetere i passaggi da 7 a 14 sullo switch cs1.
9. Abilitare il ripristino automatico sulle LIF del cluster.

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

10. Riavviare lo switch cs1. Questa operazione consente di attivare le LIF del cluster per ripristinare le porte home. È possibile ignorare gli eventi di "interruzione delle porte del cluster" riportati sui nodi durante il riavvio dello switch.

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

11. Verificare che le porte dello switch collegate alle porte del cluster siano in funzione.

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1       eth  access up      none
10G(D) --
Ethernet1/2      1       eth  access up      none
10G(D) --
Ethernet1/3      1       eth  trunk  up      none
100G(D) --
Ethernet1/4      1       eth  trunk  up      none
100G(D) --
.
.
```

12. Verificare che l'ISL tra cs1 e cs2 funzioni correttamente: `show port-channel summary`

Mostra esempio

```
cs1# *show port-channel summary*
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
----------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
----------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
cs1#
```

13. Verificare che le LIF del cluster siano tornate alla porta home: `network interface show -vserver Cluster`

Mostra esempio

```
cluster1::*> *network interface show -vserver Cluster*
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
------------- ------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/23     node1
e0d     true
            node1_clus2   up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1   up/up      169.254.3.8/23     node2
e0d     true
            node2_clus2   up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

14. Verificare che il cluster funzioni correttamente: `cluster show`

Mostra esempio

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

15. 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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Per ONTAP 9.8 e versioni successive

Per ONTAP 9.8 e versioni successive, attivare la funzione di raccolta dei log del monitor dello stato dello switch del cluster 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`

Inserire: `system switch ethernet log setup-password`

```
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>
```

Seguito da: `system switch ethernet log enable-collection`

```
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::*>
```

Per ONTAP 9.4 e versioni successive

Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor di stato dello switch del cluster per la raccolta dei file di log relativi allo switch utilizzando i comandi seguenti:

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

Inserire: `system cluster-switch log setup-password`

```
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>
```

Seguito da: `system cluster-switch log enable-collection`

```
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.

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.

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. 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.

Risolvere i 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 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 92300YC:

- 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: cshm1!
                                  Model Number: N9K-C92300YC
                                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-C92300YC
                               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::*>
```

Migrare gli switch

Migrare a un cluster con switch a due nodi con uno switch Cisco Nexus 92300YC

Se si dispone di un ambiente di cluster *switchless* a due nodi, è possibile migrare a un ambiente di cluster *switched* a due nodi utilizzando gli switch Cisco Nexus 92300YC per consentire la scalabilità oltre due nodi nel cluster.

La procedura da seguire dipende dalla presenza di due porte cluster-network dedicate su ciascun controller o di una singola porta cluster su ciascun controller. Il processo documentato funziona per tutti i nodi che utilizzano porte ottiche o twinax, ma non è supportato su questo switch se i nodi utilizzano porte RJ45 10GB BASE-T integrate per le porte di rete del cluster.

La maggior parte dei sistemi richiede due porte cluster-network dedicate su ciascun controller.

> Al termine della migrazione, potrebbe essere necessario installare il file di configurazione richiesto per supportare il monitoraggio dello stato di salute dello switch cluster (CSHM) per gli switch cluster 92300YC. Vedere"Installazione del Cluster Switch Health Monitor (CSHM)".

Verifica dei requisiti

Di cosa hai bisogno

Per una configurazione senza switch a due nodi, assicurarsi che:

- La configurazione senza switch a due nodi è configurata e funziona correttamente.
- I nodi eseguono ONTAP 9.6 e versioni successive.
- Tutte le porte del cluster si trovano nello stato **up**.
- Tutte le interfacce logiche del cluster (LIFF) si trovano nello stato **up** e nelle porte home.

Per la configurazione dello switch Cisco Nexus 92300YC:

- Entrambi gli switch dispongono di connettività di rete di gestione.
- Gli switch del cluster sono accessibili dalla console.
- Le connessioni switch nodo-nodo e switch-to-switch Nexus 92300YC utilizzano cavi twinax o in fibra.

  "Hardware Universe - Switch" contiene ulteriori informazioni sul cablaggio.

- I cavi ISL (Inter-Switch link) sono collegati alle porte 1/65 e 1/66 su entrambi gli switch 92300YC.
- La personalizzazione iniziale di entrambi gli switch 92300YC è stata completata. In modo che:
  - Gli switch 92300YC utilizzano la versione più recente del software
  - I file di configurazione di riferimento (RCF) vengono applicati agli switch. Qualsiasi personalizzazione del sito, ad esempio SMTP, SNMP e SSH, viene configurata sui nuovi switch.

Migrare lo switch

A proposito degli esempi

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

- I nomi degli switch 92300YC sono cs1 e cs2.
- I nomi delle SVM del cluster sono node1 e node2.
- I nomi delle LIF sono rispettivamente node1_clus1 e node1_clus2 sul nodo 1 e node2_clus1 e node2_clus2 sul nodo 2.
- Il `cluster1::*>` prompt indica il nome del cluster.
- Le porte del cluster utilizzate in questa procedura sono e0a e e0b.

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

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato (`*>`).

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

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

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

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

   Mostra esempio

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

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

Fase 2: Configurazione di cavi e porte

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

   Non è necessario disattivare le porte ISL.

   Mostra esempio

   L'esempio seguente mostra che le porte rivolte al nodo da 1 a 64 sono disattivate sullo switch cs1:

   ```
   cs1# config
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e/1-64
   cs1(config-if-range)# shutdown
   ```

2. Verificare che le porte ISL e fisiche dell'ISL tra i due switch 92300YC cs1 e cs2 siano installate sulle porte 1/65 e 1/66:

   ```
   show port-channel summary
   ```

Mostra esempio

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

```
cs1# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

+ il seguente esempio mostra che le porte ISL sono installate sullo switch cs2 :

+

```
(cs2)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

3. Visualizzare l’elenco dei dispositivi vicini:

   ```
   show cdp neighbors
   ```

   Questo comando fornisce informazioni sui dispositivi collegati al sistema.

Mostra esempio

Nell'esempio riportato di seguito sono elencati i dispositivi adiacenti sullo switch cs1:

```
cs1# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

+ nell'esempio seguente sono elencati i dispositivi adiacenti sullo switch cs2:

+

```
cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1(FDO220329KU)    Eth1/65        177    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)    Eth1/66        177    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

4. Verificare che tutte le porte del cluster siano installate:

   `network port show -ipspace Cluster`

Ogni porta deve essere visualizzata per `Link` e sano per `Health Status`.

Mostra esempio

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

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

   `network interface show -vserver Cluster`

   Ogni LIF del cluster dovrebbe visualizzare true per `Is Home` e hanno un `Status Admin/Oper` di up/up

Mostra esempio

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Verificare che l'autorevert sia attivato su tutte le LIF del cluster:

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

   Mostra esempio

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

7. Scollegare il cavo dalla porta del cluster e0a sul nodo 1, quindi collegare e0a alla porta 1 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch 92300YC.

Il "*Hardware Universe - Switch*" contiene ulteriori informazioni sul cablaggio.

8. Scollegare il cavo dalla porta del cluster e0a sul nodo 2, quindi collegare e0a alla porta 2 sullo switch del cluster cs1, utilizzando il cablaggio appropriato supportato dagli switch 92300YC.
9. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs1.

Mostra esempio

L'esempio seguente mostra che le porte da 1/1 a 1/64 sono attivate sullo switch cs1:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

10. Verificare che tutte le LIF del cluster siano funzionanti, operative e visualizzate come vere per `Is Home`:

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

Mostra esempio

L'esempio seguente mostra che tutte le LIF sono in su su node1 e node2 e questo `Is Home` i risultati sono veri:

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

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node        Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1       e0a
true
         node1_clus2  up/up      169.254.49.125/16  node1       e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2       e0a
true
         node2_clus2  up/up      169.254.19.183/16  node2       e0b
true

4 entries were displayed.
```

11. Visualizza informazioni sullo stato dei nodi nel cluster:

```
cluster show
```

Mostra esempio

Nell'esempio seguente vengono visualizzate informazioni sullo stato e sull'idoneità dei nodi nel cluster:

```
cluster1::*> cluster show

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

2 entries were displayed.
```

12. Scollegare il cavo dalla porta del cluster e0b sul nodo 1, quindi collegare e0b alla porta 1 sullo switch del cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch 92300YC.
13. Scollegare il cavo dalla porta del cluster e0b sul nodo 2, quindi collegare e0b alla porta 2 sullo switch del cluster cs2, utilizzando il cablaggio appropriato supportato dagli switch 92300YC.
14. Abilitare tutte le porte rivolte ai nodi sullo switch cluster cs2.

Mostra esempio

L'esempio seguente mostra che le porte da 1/1 a 1/64 sono attivate sullo switch cs2:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

Fase 3: Verificare la configurazione

1. Verificare che tutte le porte del cluster siano installate:

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

Mostra esempio

L'esempio seguente mostra che tutte le porte del cluster sono su node1 e node2:

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

2. Verificare che tutte le interfacce visualizzino true per `Is Home`:

   `network interface show -vserver Cluster`

   Il completamento di questa operazione potrebbe richiedere alcuni minuti.

Mostra esempio

L'esempio seguente mostra che tutte le LIF sono in su su node1 e node2 e questo `Is Home` i risultati sono veri:

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true

4 entries were displayed.
```

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

   `show cdp neighbors`

Mostra esempio

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

```
(cs1)# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0a
node2               Eth1/2         133    H         FAS2980
e0a
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4


(cs2)# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0b
node2               Eth1/2         133    H         FAS2980
e0b
cs1(FDO220329KU)
                    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

4. Visualizzare le informazioni relative ai dispositivi di rete rilevati nel cluster:

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

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.
```

5. Verificare che le impostazioni siano disattivate:

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

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

Mostra esempio

L'output falso nell'esempio seguente mostra che le impostazioni di configurazione sono disattivate:

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

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

```
cluster show
```

Mostra esempio

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

```
cluster1::*> cluster show

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

7. Verificare che la rete del cluster disponga di connettività completa:

   `cluster ping-cluster -node node-name`

   Mostra esempio

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

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

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

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

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

Mostra esempio

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

9. Modificare nuovamente il livello di privilegio in admin:

   ```
   set -privilege admin
   ```

10. Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor dello stato dello switch del cluster per la raccolta dei file di log relativi allo switch, utilizzando i comandi seguenti:

    `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.

Migrare da uno switch Cisco a uno switch Cisco Nexus 92300YC

È possibile migrare senza interruzioni gli switch cluster Cisco meno recenti per un cluster

ONTAP agli switch di rete del cluster Cisco Nexus 92300YC.

> Al termine della migrazione, potrebbe essere necessario installare il file di configurazione richiesto per supportare il monitoraggio dello stato di salute dello switch cluster (CSHM) per gli switch cluster 92300YC. Vedere"Installazione del Cluster Switch Health Monitor (CSHM)".

Verifica dei requisiti

Di cosa hai bisogno

- Un cluster esistente completamente funzionale.
- Connettività 10 GbE e 40 GbE dai nodi agli switch di cluster Nexus 92300YC.
- Tutte le porte del cluster sono in stato attivo per garantire operazioni senza interruzioni.
- Versione corretta di NX-OS e file di configurazione di riferimento (RCF) installati sugli switch cluster Nexus 92300YC.
- 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.

Migrare lo switch

A proposito degli esempi

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

- Gli switch cluster Cisco Nexus 5596UP esistenti sono c1 e c2.
- I nuovi switch in cluster Nexus 92300YC sono cs1 e cs2.
- I nodi sono node1 e node2.
- I LIF del cluster sono rispettivamente node1_clus1 e node1_clus2 sul nodo 1, e node2_clus1 e node2_clus2 sul nodo 2.
- Lo switch c2 viene sostituito prima dallo switch cs2, quindi lo switch c1 viene sostituito dallo switch cs1.
  - Un ISL temporaneo è costruito su cs1 che collega c1 a cs1.
  - Il cablaggio tra i nodi e c2 viene quindi scollegato da c2 e ricollegato a cs2.
  - Il cablaggio tra i nodi e c1 viene quindi scollegato da c1 e ricollegato a cs1.
  - L'ISL temporaneo tra c1 e cs1 viene quindi rimosso.

Porte utilizzate per le connessioni

- Alcune porte sono configurate su switch Nexus 92300YC per funzionare a 10 GbE o 40 GbE.
- Gli switch del cluster utilizzano le seguenti porte per le connessioni ai nodi:
  - Porte e1/1-48 (10/25 GbE), e1/49-64 (40/100 GbE): Nexus 92300YC
  - Porte e1/1-40 (10 GbE): Nexus 5596UP
  - Porte e1/1-32 (10 GbE): Nexus 5020
  - Porte e1/1-12, e2/1-6 (10 GbE): Nexus 5010 con modulo di espansione

- Gli switch del cluster utilizzano le seguenti porte ISL (Inter-Switch link):
  - Porte e1/65-66 (100 GbE): Nexus 92300YC
  - Porte e1/41-48 (10 GbE): Nexus 5596UP
  - Porte e1/33-40 (10 GbE): Nexus 5020
  - Porte e1/13-20 (10 GbE): Nexus 5010
- "Hardware Universe - Switch" contiene informazioni sul cablaggio supportato per tutti gli switch del cluster.
- Le versioni di ONTAP e NX-OS supportate in questa procedura sono disponibili in "Switch Ethernet Cisco" pagina.

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

   Viene visualizzato il prompt Advanced (*>).

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

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

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

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

   Mostra esempio

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

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

3. Verificare che l'autorevert sia attivato su tutte le LIF del cluster:

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

Mostra esempio

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_clus2   true

4 entries were displayed.
```

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

   Ogni porta deve essere visualizzata per `Link` e sano per `Health Status`.

   a. Visualizzare gli attributi della porta di rete:

      `network port show -ipspace Cluster`

Mostra esempio

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

b. Visualizzare le informazioni sulle interfacce logiche e sui relativi nodi principali designati:

   `network interface show -vserver Cluster`

   Ogni LIF deve visualizzare UP/UP per `Status Admin/Oper` e vero per `Is Home`.

Mostra esempio

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true

4 entries were displayed.
```

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

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

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    c1                        0/2               N5K-
C5596UP
            e0b    c2                        0/2               N5K-
C5596UP
node1      /cdp
            e0a    c1                        0/1               N5K-
C5596UP
            e0b    c2                        0/1               N5K-
C5596UP

4 entries were displayed.
```

6. Verificare che le porte del cluster e gli switch siano collegati nel modo seguente (dal punto di vista degli switch) utilizzando il comando:

   `show cdp neighbors`

Mostra esempio

```
c1# show cdp neighbors

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


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
c2(FOX2025GEFC)     Eth1/41        179    S I s     N5K-C5596UP
Eth1/41

c2(FOX2025GEFC)     Eth1/42        175    S I s     N5K-C5596UP
Eth1/42

c2(FOX2025GEFC)     Eth1/43        179    S I s     N5K-C5596UP
Eth1/43

c2(FOX2025GEFC)     Eth1/44        175    S I s     N5K-C5596UP
Eth1/44

c2(FOX2025GEFC)     Eth1/45        179    S I s     N5K-C5596UP
Eth1/45

c2(FOX2025GEFC)     Eth1/46        179    S I s     N5K-C5596UP
Eth1/46

c2(FOX2025GEFC)     Eth1/47        175    S I s     N5K-C5596UP
Eth1/47

c2(FOX2025GEFC)     Eth1/48        179    S I s     N5K-C5596UP
Eth1/48

Total entries displayed: 10


c2# show cdp neighbors
```

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


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0b
node2               Eth1/2         124    H         FAS2750
e0b
c1(FOX2025GEEX)     Eth1/41        175    S I s     N5K-C5596UP
Eth1/41

c1(FOX2025GEEX)     Eth1/42        175    S I s     N5K-C5596UP
Eth1/42

c1(FOX2025GEEX)     Eth1/43        175    S I s     N5K-C5596UP
Eth1/43

c1(FOX2025GEEX)     Eth1/44        175    S I s     N5K-C5596UP
Eth1/44

c1(FOX2025GEEX)     Eth1/45        175    S I s     N5K-C5596UP
Eth1/45

c1(FOX2025GEEX)     Eth1/46        175    S I s     N5K-C5596UP
Eth1/46

c1(FOX2025GEEX)     Eth1/47        176    S I s     N5K-C5596UP
Eth1/47

c1(FOX2025GEEX)     Eth1/48        176    S I s     N5K-C5596UP
Eth1/48
```

7. Verificare che la rete del cluster disponga della connettività completa utilizzando il comando:

   `cluster ping-cluster -node node-name`

Mostra esempio

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Fase 2: Configurazione di cavi e porte

1. Configurare un ISL temporaneo su cs1sulle porte e1/41-48, tra c1 e cs1.

Mostra esempio

L'esempio seguente mostra come il nuovo ISL viene configurato su c1 e cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP
and Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range)# no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config)# interface port-channel 101
cs1(config-if)# switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

2. Rimuovere i cavi ISL dalle porte e1/41-48 da c2 e collegarli alle porte e1/41-48 su cs1.
3. Verificare che le porte ISL e il port-channel siano operativi collegando c1 e cs1:

   ```
   show port-channel summary
   ```

Mostra esempio

Nell’esempio seguente viene illustrato il comando Cisco show port-channel summary utilizzato per verificare che le porte ISL siano operative su c1 e cs1:

```
c1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)


cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
101   Po101(SU)   Eth      LACP      Eth1/41(P)   Eth1/42(P)
Eth1/43(P)
                                     Eth1/44(P)   Eth1/45(P)
Eth1/46(P)
                                     Eth1/47(P)   Eth1/48(P)
```

4. Per il nodo 1, scollegare il cavo da e1/1 su c2, quindi collegarlo a e1/1 su cs2, utilizzando il cablaggio appropriato supportato da Nexus 92300YC.
5. Per il nodo 2, scollegare il cavo da e1/2 su c2, quindi collegarlo a e1/2 su cs2, utilizzando il cablaggio appropriato supportato da Nexus 92300YC.
6. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel seguente modo, dal punto di vista dei nodi:

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

   Mostra esempio

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

   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID)  Interface
   Platform
   ----------- ------ ------------------------- ----------------
   ----------------
   node2      /cdp
               e0a    c1                        0/2               N5K-
   C5596UP
               e0b    cs2                       0/2               N9K-
   C92300YC
   node1      /cdp
               e0a    c1                        0/1               N5K-
   C5596UP
               e0b    cs2                       0/1               N9K-
   C92300YC

   4 entries were displayed.
   ```

7. Per il nodo 1, scollegare il cavo da e1/1 su c1, quindi collegarlo a e1/1 su cs1, utilizzando il cablaggio appropriato supportato da Nexus 92300YC.
8. Per il nodo 2, scollegare il cavo da e1/2 su c1, quindi collegarlo a e1/2 su cs1, utilizzando il cablaggio appropriato supportato da Nexus 92300YC.
9. Le porte del cluster su ciascun nodo sono ora collegate agli switch del cluster nel seguente modo, dal punto di vista dei nodi:

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

Mostra esempio

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC
4 entries were displayed.
```

10. Eliminare l'ISL temporaneo tra cs1 e c1.

Mostra esempio

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

Fase 3: Completare la migrazione

1. Verificare la configurazione finale del cluster:

   `network port show -ipspace Cluster`

   Ogni porta deve essere visualizzata per `Link` e sano per `Health Status`.

Mostra esempio

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

Node: node1

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

Node: node2

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

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
```

```
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.


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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0a
node2               Eth1/2         124    H         FAS2750
e0a
cs2(FDO220329V5)    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
```

```
cs2(FDO220329V5)    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66


cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         124    H         FAS2750
e0b
node2               Eth1/2         124    H         FAS2750
e0b
cs1(FDO220329KU)
                    Eth1/65        179    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        179    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

2. Verificare che la rete del cluster disponga di connettività completa:

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

Mostra esempio

```
cluster1::*> set -priv advanced

Warning: These advanced commands are potentially dangerous; use them
only when
         directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)


cluster1::*> set -privilege admin
cluster1::*>
```

3. Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log del monitor dello stato dello switch del cluster per la raccolta dei file di log relativi allo switch, utilizzando i comandi seguenti:

   `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.

Sostituire gli interruttori

Sostituire uno switch Cisco Nexus 92300YC

La sostituzione di uno switch Nexus 92300YC difettoso in una rete cluster è una procedura senza interruzioni (NDU).

Verifica dei requisiti

Di cosa hai bisogno

Prima di sostituire lo switch, assicurarsi che:

- Nel cluster e nell'infrastruttura di rete esistenti:
  - Il cluster esistente viene verificato come completamente funzionale, con almeno uno switch del cluster completamente connesso.
  - Tutte le porte del cluster sono installate.
  - Tutte le interfacce logiche del cluster (LIFF) sono installate sulle porte domestiche.
  - Il comando ping-cluster -node node1 del cluster ONTAP deve indicare che la connettività di base e le comunicazioni di dimensioni superiori a quelle di PMTU hanno esito positivo su tutti i percorsi.
- Per lo switch sostitutivo Nexus 92300YC:
  - La connettività di rete di gestione sullo switch sostitutivo è funzionale.
  - L'accesso della console allo switch sostitutivo è in posizione.
  - Le connessioni dei nodi sono le porte da 1/1 a 1/64.
  - Tutte le porte ISL (Inter-Switch link) sono disattivate sulle porte 1/65 e 1/66.
  - Il file di configurazione di riferimento desiderato (RCF) e lo switch dell'immagine del sistema operativo NX-OS vengono caricati sullo switch.
  - La personalizzazione iniziale dello switch è completa, come descritto in: "Configurare lo switch Cisco Nexus 92300YC".

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

Sostituire lo switch

A proposito degli esempi

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

- I nomi degli switch Nexus 92300YC esistenti sono cs1 e cs2.
- Il nome del nuovo switch Nexus 92300YC è newcs2.
- I nomi dei nodi sono node1 e node2.
- Le porte del cluster su ciascun nodo sono denominate e0a e e0b.
- I nomi LIF del cluster sono node1_clus1 e node1_clus2 per node1 e node2_clus1 e node2_clus2 per node2.
- Il prompt per le modifiche a tutti i nodi del cluster è cluster1:*>

A proposito di questa attività

È necessario eseguire il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.

La seguente procedura si basa sulla seguente topologia di rete del cluster:

Mostra topologia

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

Node: node1

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

Node: node2

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



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C92300YC
            e0b    cs2                       Eth1/2            N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C92300YC
            e0b    cs2                       Eth1/1            N9K-
C92300YC
4 entries were displayed.



cs1# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2(FDO220329V5)   Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
cs2(FDO220329V5)   Eth1/66        176    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

```
cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

Fase 1: Preparazione per la sostituzione

1. Installare l'RCF e l'immagine appropriati sullo switch, newcs2, ed eseguire le operazioni necessarie per la preparazione del sito.

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

   a. Accedere alla *pagina Descrizione del file di configurazione di riferimento per gli switch di rete di gestione e cluster NetApp* sul sito del supporto NetApp.
   b. Fare clic sul link per la *matrice di compatibilità della rete di gestione e di rete del cluster*, quindi annotare la versione del software dello switch richiesta.
   c. Fare clic sulla freccia indietro del browser per tornare alla pagina **Descrizione**, fare clic su **CONTINUA**, accettare il contratto di licenza, quindi passare alla pagina **Download**.
   d. Seguire la procedura riportata nella pagina di download per scaricare i file RCF e NX-OS corretti per la versione del software ONTAP che si sta installando.
2. Sul nuovo switch, accedere come admin e chiudere tutte le porte che verranno collegate alle interfacce del cluster di nodi (porte da 1/1 a 1/64).

   Se lo switch che si sta sostituendo non funziona e viene spento, passare alla fase 4. Le LIF sui nodi del cluster dovrebbero essere già riuscite a eseguire il failover sull'altra porta del cluster per ciascun nodo.

Mostra esempio

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Verificare che tutte le LIF del cluster abbiano attivato l'autorevert:

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

Mostra esempio

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

             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

4. Verificare che tutte le LIF del cluster siano in grado di comunicare:

```
cluster ping-cluster
```

Mostra esempio

```
cluster1::*> cluster ping-cluster node1

Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Fase 2: Configurazione di cavi e porte

1. Spegnere le porte ISL 1/65 e 1/66 sullo switch Nexus 92300YC cs1:

   Mostra esempio

   ```
   cs1# configure
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/65-66
   cs1(config-if-range)# shutdown
   cs1(config-if-range)#
   ```

2. Rimuovere tutti i cavi dallo switch Nexus 92300YC cs2, quindi collegarli alle stesse porte dello switch Nexus 92300YC newcs2.

3. Richiamare le porte ISL 1/65 e 1/66 tra gli switch cs1 e newcs2, quindi verificare lo stato di funzionamento del canale della porta.

   Port-Channel deve indicare PO1(su) e Member Ports deve indicare eth1/65(P) e eth1/66(P).

   Mostra esempio

   Questo esempio abilita le porte ISL 1/65 e 1/66 e visualizza il riepilogo del canale delle porte sullo switch cs1:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)

cs1(config-if-range)#
```

4. Verificare che la porta e0b sia attiva su tutti i nodi:

   `network port show ipspace Cluster`

Mostra esempio

L'output dovrebbe essere simile a quanto segue:

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

5. Sullo stesso nodo utilizzato nella fase precedente, ripristinare la LIF del cluster associata alla porta nella fase precedente utilizzando il comando di revert dell'interfaccia di rete.

Mostra esempio

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

I seguenti comandi restituiscono LIF `node1_clus2` acceso `node1` alla porta home `e0a` E visualizza le informazioni sui LIF su entrambi i nodi. L'attivazione del primo nodo ha esito positivo se la colonna is Home è vera per entrambe le interfacce del cluster e mostra le assegnazioni di porta corrette, in questo esempio `e0a` e. `e0b` al nodo1.

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Visualizzare le informazioni sui nodi di un cluster:

   `cluster show`

   Mostra esempio

   Questo esempio mostra che l'integrità del nodo per node1 e node2 in questo cluster è vera:

```
cluster1::*> cluster show

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

7. Verificare che tutte le porte del cluster fisico siano installate:

   ```
   network port show ipspace Cluster
   ```

   Mostra esempio

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

   Node: node1

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

   Node: node2

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

   4 entries were displayed.
   ```

Fase 3: Completare la procedura

1. Verificare che tutte le LIF del cluster siano in grado di comunicare:

   ```
   cluster ping-cluster
   ```

Mostra esempio

```
cluster1::*> cluster ping-cluster -node node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

2. Confermare la seguente configurazione di rete del cluster:

```
network port show
```

Mostra esempio

```
cluster1::*> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    newcs2                    0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    newcs2                    0/1               N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

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

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     N9K-C92300YC
```

```
Eth1/66


Total entries displayed: 4


cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e0b
node2              Eth1/2         124    H           FAS2980
e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

3. Per ONTAP 9.4 e versioni successive, attivare la funzione di raccolta dei log di monitoraggio dello stato dello switch del cluster per la raccolta dei file di log relativi allo switch, utilizzando gthe commamds:

   `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.

Sostituire gli switch cluster Cisco Nexus 92300YC con connessioni senza switch

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

sono collegati direttamente per ONTAP 9.3 e versioni successive.

Verifica dei requisiti

Linee guida

Consultare le seguenti linee guida:

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

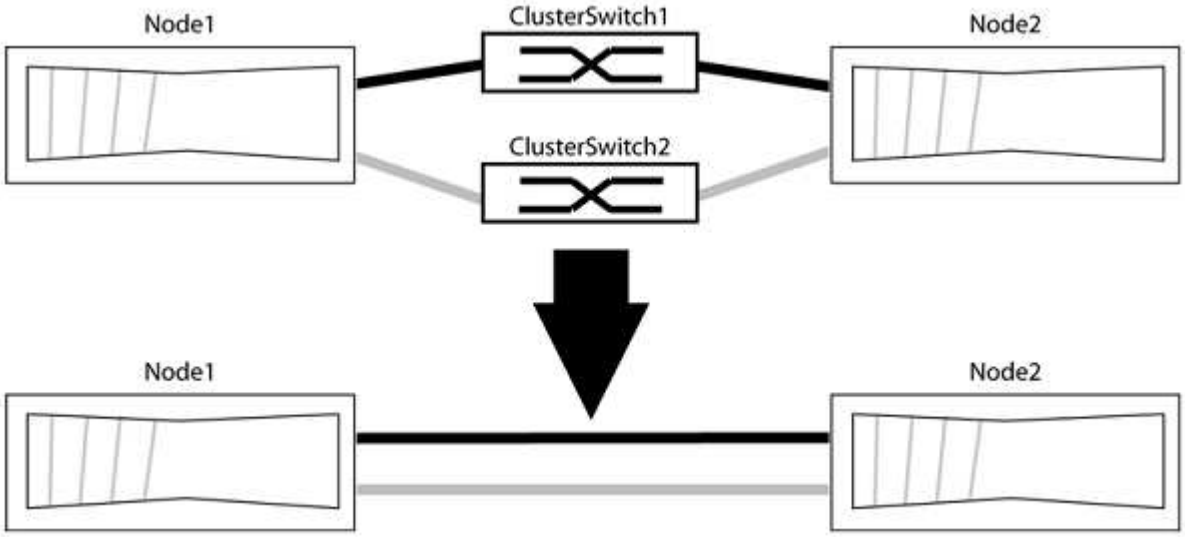
Di cosa hai bisogno

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

Migrare gli switch

A proposito di questa attività

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



A proposito degli esempi

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

Fase 1: Preparazione per la migrazione

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

   ```
   set -privilege advanced
   ```

   Il prompt avanzato `*>` viene visualizzato.

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

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

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

   Mostra esempio

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

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

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

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

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

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

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

   Mostra esempio

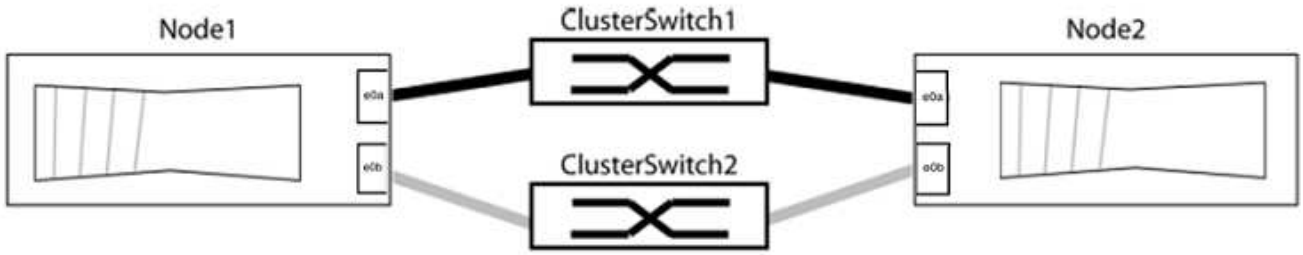
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Fase 2: Configurare le porte e il cablaggio

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

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

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

   Verificare che il valore delle porte sia di `up` Per la colonna "link" e un valore di `healthy` Per la colonna "Health Status" (Stato salute).

Mostra esempio

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

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

Node: node2

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

3. Verificare che tutte le LIF del cluster si trovino sulle porte home.

   Verificare che la colonna "is-home" sia `true` Per ciascuna LIF del cluster:

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

Mostra esempio

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

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

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

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

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

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

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

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

Mostra esempio

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

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

6. Verificare la connettività del cluster:

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

7. Verificare che il cluster funzioni correttamente:

```
cluster ring show
```

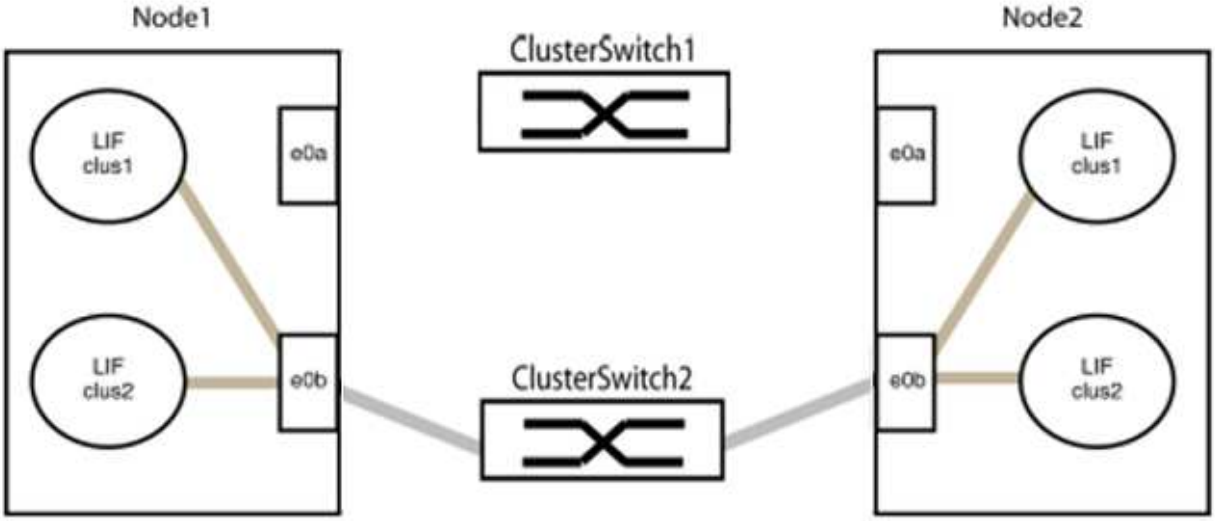
Tutte le unità devono essere master o secondarie.

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

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

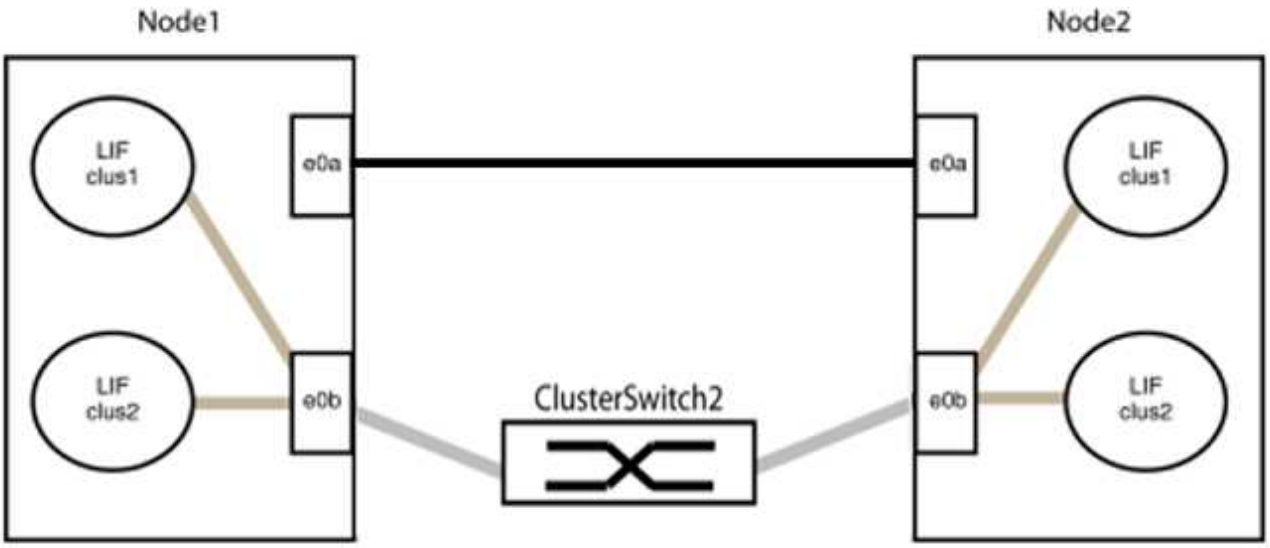
a. Scollegare tutti i cavi dalle porte del raggruppo1 contemporaneamente.

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



b. Collegare le porte del gruppo 1 da una parte all'altro.

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



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

   `network options switchless-cluster show`

   Il seguente esempio mostra che il cluster senza switch è abilitato:

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

10. Verificare che la rete del cluster non venga interrotta:

    `cluster ping-cluster -node local`

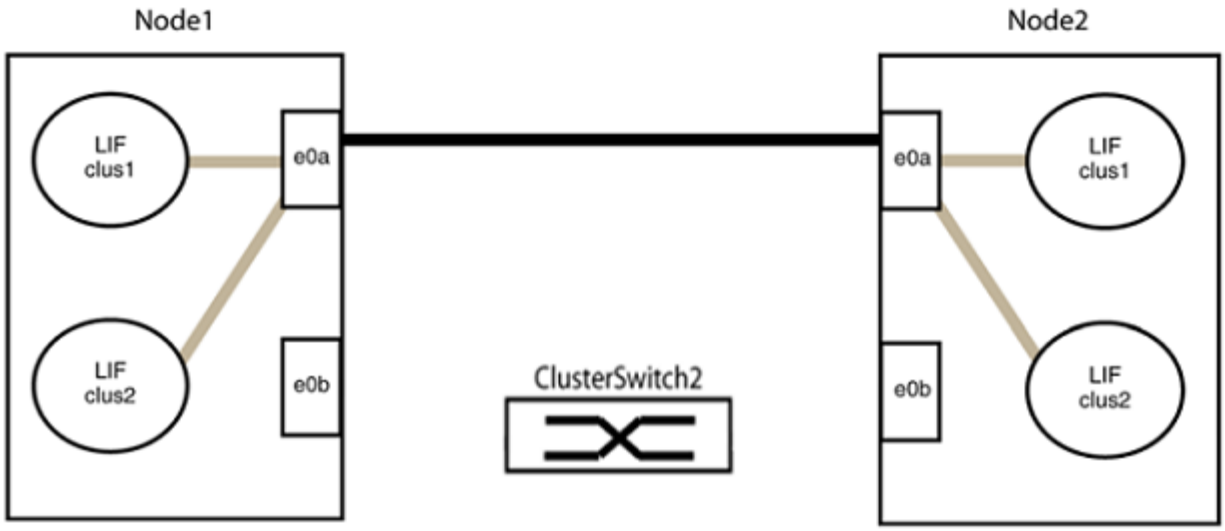
    > Prima di passare alla fase successiva, è necessario attendere almeno due minuti per confermare una connessione back-to-back funzionante sul gruppo 1.

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

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

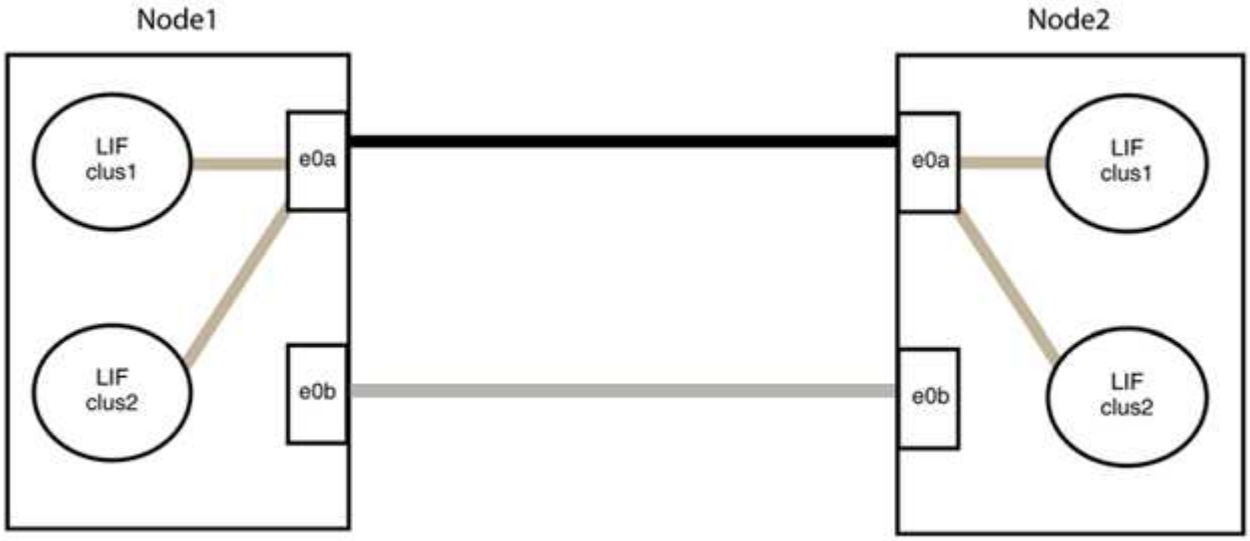
    a. Scollegare tutti i cavi dalle porte del raggruppo2 contemporaneamente.

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



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

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



Fase 3: Verificare la configurazione

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

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

Mostra esempio

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

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

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

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

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

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

Mostra esempio

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

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

Se uno dei cluster LIFS non è tornato alle porte home, ripristinarli manualmente dal nodo locale:

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

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

   `cluster show`

   Mostra esempio

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

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

5. Verificare la connettività tra le porte del cluster:

   `cluster ping-cluster local`

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

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

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

7. Modificare nuovamente il livello di privilegio in admin:

```
set -privilege admin
```