Procedure di manutenzione per le configurazioni IP di MetroCluster

ONTAP MetroCluster

NetApp
September 06, 2024

Sommario

Procedure di manutenzione per le configurazioni IP di MetroCluster

Modificare le proprietà di un'interfaccia IP MetroCluster

A partire da ONTAP 9.10.1, è possibile modificare le seguenti proprietà di un'interfaccia IP MetroCluster: Indirizzo IP, maschera e gateway. È possibile utilizzare qualsiasi combinazione di parametri per l'aggiornamento.

Potrebbe essere necessario aggiornare queste proprietà, ad esempio, se viene rilevato un indirizzo IP duplicato o se un gateway deve essere modificato in caso di rete di livello 3 a causa di modifiche alla configurazione del router.

A proposito di questa attività

- È possibile modificare solo un'interfaccia alla volta. L'interfaccia verrà rallentata fino a quando le altre interfacce non saranno aggiornate e le connessioni non verranno ristabilita.
- Utilizzare `metrocluster configuration-settings interface modify` Per modificare qualsiasi proprietà dell'interfaccia IP di MetroCluster.

> Questi comandi modificano la configurazione di un nodo specifico per una determinata porta. Per ripristinare la connettività di rete completa, sono necessari comandi simili su altre porte. Analogamente, anche gli switch di rete devono aggiornare la configurazione. Ad esempio, se il gateway viene aggiornato, idealmente viene modificato su entrambi i nodi di una coppia ha, poiché sono identici. Inoltre, anche lo switch connesso a tali nodi deve aggiornare il gateway.

- Utilizzare i `metrocluster configuration-settings interface show`comandi , , `metrocluster connection check`e `metrocluster connection show` per verificare che tutta la connettività funzioni in tutte le interfacce.

Modificare l'indirizzo IP, la netmask e il gateway

Eseguire i seguenti passaggi per modificare l'indirizzo IP, la netmask e il gateway di un'interfaccia IP MetroCluster.

Fasi

1. Aggiornare l'indirizzo IP, la netmask e il gateway per un singolo nodo e interfaccia: `metrocluster configuration-settings interface modify`

   Il comando seguente mostra come aggiornare l'indirizzo IP, la netmask e il gateway:

```
cluster_A::* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsi13:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsi14:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsi15:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsi16:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful
```

2. verificare che la connettività funzioni per tutte le interfacce: `metrocluster configuration-settings interface show`

Il seguente comando mostra come verificare che tutte le connessioni funzionino per tutte le interfacce:

```
cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR              Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.12.201  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.200  255.255.255.0   192.168.20.1
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.12.101  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.101  255.255.255.0   192.168.20.1
completed
      cluster_B node_B_1
                 Home Port: e0a-10
                      192.168.11.151  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.150  255.255.255.0   192.168.21.1
completed
                node_B_2
                 Home Port: e0a-10
                      192.168.11.250  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.250  255.255.255.0   192.168.21.1
completed
8 entries were displayed.
```

3. verificare che tutte le connessioni funzionino:

   `metrocluster configuration-settings connection show`

   Il seguente comando mostra come verificare che tutte le connessioni funzionino:

```
cluster_A::*> metrocluster configuration-settings connection show
  (metrocluster configuration-settings connection show)
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A node_A_2
                  Home Port: e0a-10
                       192.168.10.200  192.168.10.101  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.250  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.200  192.168.11.151  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.20.100  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.250  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.200  192.168.21.150  DR Auxiliary
completed
                 node_A_1
                  Home Port: e0a-10
                       192.168.10.101  192.168.10.200  HA Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.151  DR Partner
completed
                  Home Port: e0a-10
                       192.168.10.101  192.168.11.250  DR Auxiliary
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.20.200  HA Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.150  DR Partner
completed
                  Home Port: e0b-20
                       192.168.20.100  192.168.21.250  DR Auxiliary
completed
```

Manutenzione e sostituzione dello switch IP

Sostituire uno switch IP o modificare l'utilizzo degli switch IP MetroCluster esistenti

Potrebbe essere necessario sostituire uno switch guasto, aggiornare o eseguire il downgrade di uno switch o modificare l'utilizzo degli switch IP MetroCluster esistenti.

A proposito di questa attività

Questa procedura si applica quando si utilizzano switch validati da NetApp. Se si utilizzano switch compatibili con MetroCluster, rivolgersi al fornitore dello switch.

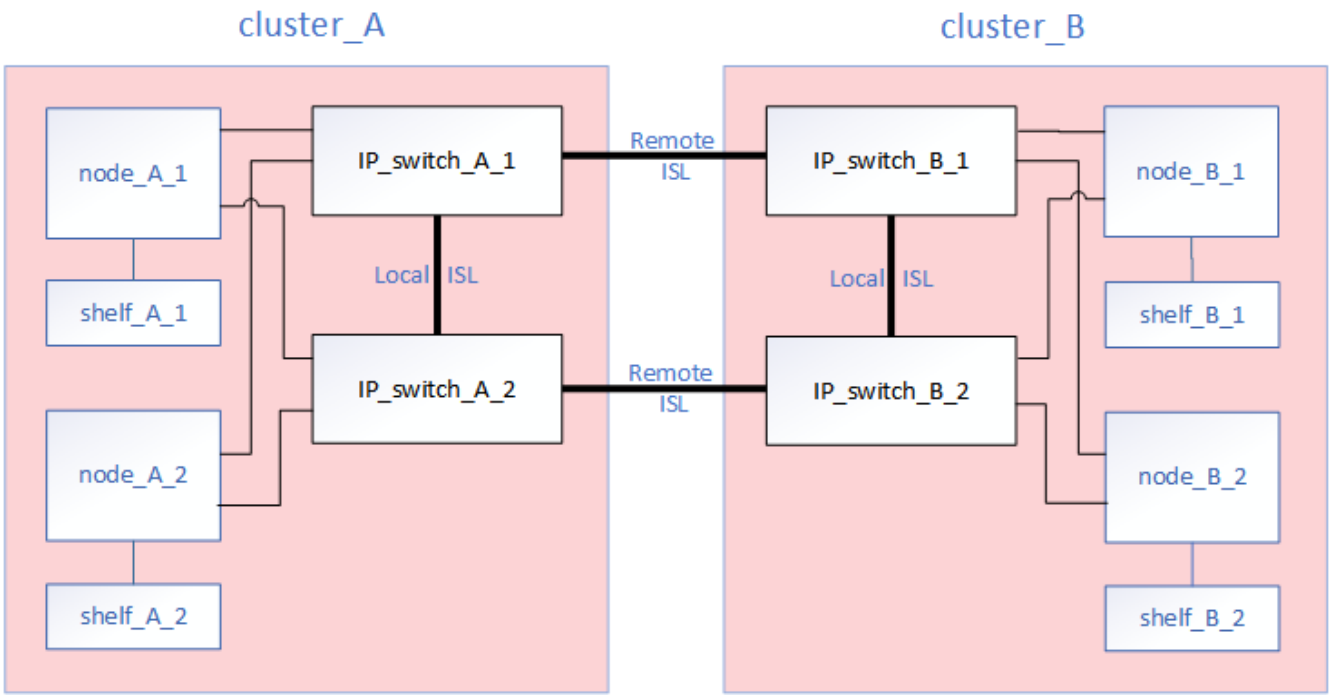
"Attivare la registrazione della console" prima di eseguire questa attività.

Questa procedura supporta le seguenti conversioni:

- Modifica del vendor, del tipo o di entrambi gli switch. Il nuovo switch può essere lo stesso del vecchio switch in caso di guasto oppure è possibile modificare il tipo di switch (aggiornare o eseguire il downgrade dello switch).

  Ad esempio, per espandere una configurazione MetroCluster IP da una singola configurazione a quattro nodi utilizzando controller AFF A400 e switch BES-53248 a una configurazione a otto nodi utilizzando controller AFF A400, è necessario modificare gli switch in un tipo supportato per la configurazione, in quanto gli switch BES-53248 non sono supportati nella nuova configurazione.

  Se si desidera sostituire uno switch guasto con lo stesso tipo di switch, sostituire solo lo switch guasto. Se si desidera aggiornare o eseguire il downgrade di uno switch, è necessario regolare due switch che si trovano nella stessa rete. Due switch si trovano nella stessa rete quando sono collegati con un collegamento inter-switch (ISL) e non si trovano nello stesso sito. Ad esempio, la rete 1 include IP_switch_A_1 e IP_switch_B_1, mentre la rete 2 include IP_switch_A_2 e IP_switch_B_2, come mostrato nel diagramma seguente:



Se si sostituisce uno switch o si esegue l'aggiornamento a switch diversi, è possibile preconfigurare gli switch installando il firmware dello switch e il file RCF.

- Convertire una configurazione IP MetroCluster in una configurazione IP MetroCluster utilizzando switch MetroCluster di storage condiviso.

  Ad esempio, se si dispone di una configurazione MetroCluster IP regolare utilizzando i controller AFF A700 e si desidera riconfigurare MetroCluster per collegare gli shelf NS224 agli stessi switch.

  - Se si aggiungono o rimuovono shelf in una configurazione MetroCluster IP utilizzando switch MetroCluster IP storage condiviso, seguire la procedura descritta in "Aggiunta di shelf a un MetroCluster IP utilizzando switch MetroCluster per lo storage condiviso"
  - La configurazione IP di MetroCluster potrebbe già essere collegata direttamente agli shelf NS224 o a switch di storage dedicati.

Foglio di lavoro sull'utilizzo delle porte

Di seguito viene riportato un esempio di foglio di lavoro per la conversione di una configurazione MetroCluster IP in una configurazione storage condivisa che collega due shelf NS224 utilizzando gli switch esistenti.

Definizioni dei fogli di lavoro:

- Configurazione esistente: Il cablaggio della configurazione MetroCluster esistente.
- Nuova configurazione con shelf NS224: La configurazione di destinazione in cui gli switch sono condivisi tra lo storage e MetroCluster.

I campi evidenziati in questo foglio di lavoro indicano quanto segue:

- Verde: Non è necessario modificare il cablaggio.
- Giallo: È necessario spostare le porte con la stessa configurazione o con una configurazione diversa.
- Blu: Porte nuove connessioni.

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

Fasi

1. controllare lo stato della configurazione.

   a. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster: **metrocluster show**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verificare che il mirroring sia attivato su ciascun nodo: **metrocluster node show**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Verificare che i componenti di MetroCluster siano in buone condizioni: **metrocluster check run**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Verificare che non siano presenti avvisi sullo stato di salute: **`system health alert show`**

2. Configurare il nuovo switch prima dell'installazione.

   Se si stanno riutilizzando gli switch esistenti, passare a. Fase 4.

   > Se si stanno aggiornando o eseguendo il downgrade degli switch, è necessario configurare tutti gli switch della rete.

   Seguire le istruzioni della sezione *Configurazione degli switch IP* in "Installazione e configurazione di MetroCluster IP."

   Assicurarsi di applicare il file RCF corretto per lo switch _A_1, _A_2, _B_1 o _B_2. Se il nuovo switch è lo stesso del vecchio switch, è necessario applicare lo stesso file RCF.

   Se si esegue l'aggiornamento o il downgrade di uno switch, applicare il file RCF più recente supportato per il nuovo switch.

3. Eseguire il comando port show per visualizzare le informazioni relative alle porte di rete:

   `network port show`

   a. Modifica tutte le LIF del cluster per disattivare l'indirizzamento automatico:

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. Disconnetti le connessioni dal vecchio switch.

Si scollegano solo le connessioni che non utilizzano la stessa porta nelle configurazioni precedenti e nuove. Se si utilizzano nuovi switch, è necessario scollegare tutte le connessioni.

Rimuovere i collegamenti nel seguente ordine:

a. Scollegare le interfacce del cluster locale
b. Disconnettere gli ISL del cluster locale
c. Scollegare le interfacce IP di MetroCluster
d. Disconnettere gli ISL MetroCluster

Nell'esempio [port_usage_worksheet], gli switch non cambiano. Gli ISL MetroCluster vengono ricollocati e devono essere disconnessi. Non è necessario scollegare le connessioni contrassegnate in verde sul foglio di lavoro.

5. Se si utilizzano nuovi switch, spegnere il vecchio switch, rimuovere i cavi e rimuovere fisicamente il vecchio switch.

Se si stanno riutilizzando gli switch esistenti, passare a. Fase 6.

Non collegare * i nuovi switch ad eccezione dell'interfaccia di gestione (se utilizzata).

6. Configura gli switch esistenti.

Se gli switch sono già stati preconfigurati, è possibile saltare questo passaggio.

Per configurare gli switch esistenti, seguire la procedura per installare e aggiornare il firmware e i file RCF:

- "Aggiornamento del firmware sugli switch IP MetroCluster"
- "Aggiornare i file RCF sugli switch IP MetroCluster"

7. Collegare gli switch.

Seguire la procedura descritta nella sezione *collegamento degli switch IP* di "Installazione e configurazione di MetroCluster IP".

Collegare gli switch nel seguente ordine (se necessario):

a. Collegare gli ISL al sito remoto.
b. Collegare le interfacce IP di MetroCluster.
c. Collegare le interfacce del cluster locale.

- Se il tipo di switch è diverso, le porte utilizzate potrebbero essere diverse da quelle del vecchio switch. Se si stanno aggiornando o eseguendo il downgrade degli switch, **NON** collegare gli ISL locali. Collegare gli ISL locali solo se si aggiornano o si esegue il downgrade degli switch nella seconda rete e entrambi gli switch in un sito sono dello stesso tipo e del medesimo cablaggio.
- Se si sta aggiornando Switch-A1 e Switch-B1, eseguire i passaggi da 1 a 6 per gli switch Switch-A2 e Switch-B2.

8. Finalizzare il cablaggio del cluster locale.

a. Se le interfacce del cluster locale sono collegate a uno switch:

   i. Collegare via cavo gli ISL del cluster locale.

b. Se le interfacce del cluster locale sono **non** collegate a uno switch:

   i. Utilizzare "Migrare a un ambiente cluster NetApp con switch" procedura per convertire un cluster senza switch in un cluster con switch. Utilizzare le porte indicate nella "Installazione e configurazione di MetroCluster IP" Oppure i file di cablaggio RCF per collegare l'interfaccia cluster locale.

9. Accendere lo switch o gli switch.

   Se il nuovo switch è lo stesso, accendere il nuovo switch. Se si stanno aggiornando o eseguendo il downgrade degli switch, accendere entrambi gli switch. La configurazione può funzionare con due switch diversi in ogni sito fino all'aggiornamento della seconda rete.

10. Verificare che la configurazione di MetroCluster sia corretta ripetendo la configurazione Fase 1.

    Se si aggiornano o si esegue il downgrade degli switch nella prima rete, potrebbero essere visualizzati alcuni avvisi relativi al clustering locale.

    Se si esegue l'aggiornamento o il downgrade delle reti, ripetere tutti i passaggi per la seconda rete.

11. Modifica tutte le LIF del cluster per riattivare l'indirizzamento automatico:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. In alternativa, spostare gli shelf NS224.

    Se si sta riconfigurando una configurazione IP MetroCluster che non collega gli shelf NS224 agli switch IP MetroCluster, utilizzare la procedura appropriata per aggiungere o spostare gli shelf NS224:

    - "Aggiunta di shelf a un MetroCluster IP utilizzando switch MetroCluster per lo storage condiviso"
    - "Migrazione da un cluster senza switch con storage direct-attached"
    - "Migrare da una configurazione senza switch con storage collegato a switch riutilizzando gli switch storage"

Porte di interfaccia IP MetroCluster online o offline

Quando si eseguono attività di manutenzione, potrebbe essere necessario portare una porta di interfaccia IP MetroCluster offline o online.

A proposito di questa attività

"Attivare la registrazione della console" prima di eseguire questa attività.

Fasi

È possibile utilizzare la seguente procedura per portare una porta di interfaccia IP di MetroCluster online o offline.

1. Impostare il livello di privilegio su Advanced (avanzato).

```
set -privilege advanced
```

Esempio di output

```
Cluster A_1::> set -privilege 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
```

2. Portare la porta di interfaccia IP MetroCluster offline.

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

Esempio di output

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

a. Verificare che l'interfaccia IP MetroCluster non sia in linea.

```
Cluster_A1::*> system ha interconnect port show
```

Esempio di output

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1         off
                             0  disabled  down              4          3
false
                             1  linkup    active            4          2
true
node-a2         off
                             0  linkup    active            4          2
true
                             1  linkup    active            4          2
true
2 entries were displayed.
```

3. Portare online la porta di interfaccia IP MetroCluster.

```
system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>
```

Esempio di output

```
Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0
```

a. Verificare che la porta di interfaccia IP MetroCluster sia in linea.

```
Cluster_A1::*> system ha interconnect port show
```

Esempio di output

```
Cluster_A1::*> system ha interconnect port show
                                Physical  Link
                 Link           Layer     Layer      Physical   Physical
Active
Node             Monitor  Port  State     State       Link Up  Link Down
Link
--------------  -------  ----  --------  ---------  --------  ---------
------
node-a1        off
                              0  linkup    active            5          3
true
                              1  linkup    active            4          2
true
node-a2        off
                              0  linkup    active            4          2
true
                              1  linkup    active            4          2
true
2 entries were displayed.
```

Aggiornamento del firmware sugli switch IP MetroCluster

Potrebbe essere necessario aggiornare il firmware su uno switch IP MetroCluster.

A proposito di questa attività

È necessario ripetere questa attività su ciascuno switch in successione.

"Attivare la registrazione della console" prima di eseguire questa attività.

Fasi

1. Controllare lo stato della configurazione.

   a. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster:

      ```
      metrocluster show
      ```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Verificare che il mirroring sia attivato su ciascun nodo:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Verificare che i componenti di MetroCluster siano in buone condizioni:

`metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

a. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Installare il software sul primo switch.

> È necessario installare il software dello switch sugli switch nel seguente ordine: Switch_A_1, switch_B_1, switch_A_2, switch_B_2.

Seguire la procedura per l'installazione del software switch nell'argomento pertinente, a seconda che il tipo di switch sia Broadcom, Cisco o NVIDIA:

- "Scaricare e installare il software Broadcom switch EFOS"
- "Scaricare e installare il software Cisco switch NX-OS"
- "Scaricare e installare il software Cumulus switch NVIDIA SN2100"

3. Ripetere il passaggio precedente per ciascuno degli switch.
4. Ripetere Fase 1 per controllare lo stato di salute della configurazione.

Aggiornare i file RCF sugli switch IP MetroCluster

Potrebbe essere necessario aggiornare un file RCF su uno switch IP MetroCluster. Ad esempio, se la versione del file RCF in esecuzione sugli switch non è supportata dalla versione ONTAP, dalla versione firmware dello switch o da entrambe.

Verificare che il file RCF sia supportato

Se si sta modificando la versione di ONTAP o la versione del firmware dello switch, è necessario verificare di disporre di un file RCF supportato per tale versione. Se si utilizza il generatore RCF, viene generato il file RCF corretto.

Fasi

1. Utilizzare i seguenti comandi degli switch per verificare la versione del file RCF:

Da questo switch…	Eseguire questo comando…
Switch Broadcom	`(IP_switch_A_1) # show clibanner`
Switch Cisco	`IP_switch_A_1# show banner motd`

   Per entrambi gli switch, individuare la riga nell'output che indica la versione del file RCF. Ad esempio, il seguente output proviene da uno switch Cisco, che indica che la versione del file RCF è "v1.80".

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Per controllare quali file sono supportati per una versione, uno switch e una piattaforma ONTAP specifici, utilizzare RcfFileGenerator. Se è possibile generare il file RCF per la configurazione in uso o a cui si desidera eseguire l'aggiornamento, il file è supportato.
3. Per verificare che il firmware dello switch sia supportato, fare riferimento a quanto segue:
   - "Hardware Universe"
   - "Matrice di interoperabilità NetApp"

Aggiornare i file RCF

Se si sta installando un nuovo firmware dello switch, è necessario installare il firmware dello switch prima di aggiornare il file RCF.

A proposito di questa attività

- Questa procedura interrompe il traffico sullo switch in cui viene aggiornato il file RCF. Il traffico riprenderà una volta applicato il nuovo file RCF.
- Eseguire le operazioni su un interruttore alla volta, nell'ordine seguente: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.
- "Attivare la registrazione della console" prima di eseguire questa attività.

Fasi

1. Verificare lo stato della configurazione.

   a. Verificare che i componenti di MetroCluster siano integri:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

      L'operazione viene eseguita in background.

   b. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id 38
```

b. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire la procedura per il fornitore dello switch:

   - "Ripristinare l'interruttore Broadcom IP alle impostazioni predefinite"
   - "Ripristinare lo switch IP Cisco alle impostazioni predefinite"
   - "Ripristinare le impostazioni predefinite dello switch NVIDIA IP SN2100"

3. Scaricare e installare il file RCF IP, a seconda del fornitore dello switch.
   - "Scaricare e installare i file Broadcom IP RCF"
   - "Scaricare e installare i file RCF IP di Cisco"
   - "Scaricare e installare i file RCF NVIDIA IP"

   > Se si dispone di una configurazione di rete L2 condivisa o L3, potrebbe essere necessario regolare le porte ISL sugli switch intermedi/clienti. La modalità switchport potrebbe passare dalla modalità 'access' alla modalità 'trunk'. Procedere all'aggiornamento della seconda coppia di switch (A_2, B_2) solo se la connettività di rete tra gli switch A_1 e B_1 è completamente operativa e la rete funziona correttamente.

Aggiornare i file RCF sugli switch IP Cisco utilizzando CleanUpFiles

Potrebbe essere necessario aggiornare un file RCF su uno switch IP Cisco. Ad esempio,

un aggiornamento ONTAP o un aggiornamento del firmware dello switch richiedono un nuovo file RCF.

A proposito di questa attività

- A partire dalla versione 1.4a di RcfFileGenerator, è disponibile una nuova opzione per modificare (aggiornare, eseguire il downgrade o sostituire) la configurazione dello switch sugli switch IP Cisco senza eseguire una "cancellazione in scrittura".
- "Attivare la registrazione della console" prima di eseguire questa attività.
- Lo switch Cisco 9336C-FX2 è dotato di due tipi di storage di switch diversi con nomi diversi nell'RCF. Utilizzare la tabella seguente per determinare il tipo di storage Cisco 9336C-FX2 corretto per la propria configurazione:

Se si sta collegando il seguente dispositivo di archiviazione…	Scegliere il tipo di storage Cisco 9336C-FX2…	Banner/MOTD file RCF di esempio
• Shelf SAS collegati direttamente • Shelf NVMe connessi direttamente • Shelf NVMe connessi a switch storage dedicati	9336C-FX2 - solo archiviazione diretta	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• Shelf SAS collegati direttamente • Shelf NVMe connessi agli switch IP MetroCluster ⓘ È richiesto almeno uno shelf NVMe connesso a Ethernet	9336C-FX2 – Storage SAS ed Ethernet	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

Prima di iniziare

È possibile utilizzare questo metodo se la configurazione soddisfa i seguenti requisiti:

- Viene applicata la configurazione RCF standard.
- Il "RcfFileGenerator" Deve essere in grado di creare lo stesso file RCF applicato, con la stessa versione e configurazione (piattaforme, VLAN).
- Il file RCF applicato non è stato fornito da NetApp per una configurazione speciale.
- Il file RCF non è stato modificato prima dell'applicazione.
- Prima di applicare il file RCF corrente, sono state seguite le procedure per ripristinare le impostazioni predefinite dello switch.
- Non sono state apportate modifiche alla configurazione dello switch (porta) dopo l'applicazione dell'RCF.

  Se non si soddisfano questi requisiti, non è possibile utilizzare i CleanUpFiles creati durante la generazione dei file RCF. Tuttavia, è possibile sfruttare la funzione per creare file CleanUpFiles generici — la pulitura che utilizza questo metodo deriva dall'output di `show running-config` ed è la best

practice.

> È necessario aggiornare gli switch nel seguente ordine: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. In alternativa, è possibile aggiornare gli switch Switch_A_1 e Switch_B_1 contemporaneamente, seguiti dagli switch Switch_A_2 e Switch_B_2.

Fasi

1. Determinare la versione corrente del file RCF e le porte e le VLAN utilizzate: `IP_switch_A_1# show banner motd`

   > È necessario ottenere queste informazioni da tutti e quattro gli switch e completare la seguente tabella di informazioni.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*

#
IP_switch_A_1#
```

   Da questo output, è necessario raccogliere le informazioni mostrate nelle due tabelle seguenti.

Informazioni generiche	MetroCluster	Dati

Versione del file RCF		1.81
Tipo di switch		NX9336
Tipologia di rete		Reti L2, ISL diretto
Tipo di storage		Storage SAS
Piattaforme	1	AFF A400
	2	FAS9000

Informazioni sulla VLAN	Rete	Configurazione di MetroCluster	Switchport	Sito A	Sito B
Cluster locale VLAN	Rete 1	1	1, 2	111	222
		2	3, 4	151	251
	Rete 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN MetroCluster	Rete 1	1	9, 10	119	119
		2	11, 12	159	159
	Rete 2	1	9, 10	219	219
		2	11, 12	259	259

2. Crea i file RCF e CleanUpFiles oppure crea file generici per la configurazione corrente.

   Se la configurazione soddisfa i requisiti indicati nei prerequisiti, selezionare **opzione 1**. Se la configurazione **non** soddisfa i requisiti indicati nei prerequisiti, selezionare **opzione 2**.

Opzione 1: Creare i file RCF e CleanUpFiles

Utilizzare questa procedura se la configurazione soddisfa i requisiti.

Fasi

a. Utilizzare RcfFileGenerator 1.4a (o versione successiva) per creare i file RCF con le informazioni recuperate nel passaggio 1. La nuova versione di RcfFileGenerator crea un set aggiuntivo di CleanUpFiles che è possibile utilizzare per ripristinare alcune configurazioni e preparare lo switch ad applicare una nuova configurazione RCF.

b. Confrontare il motd del banner con i file RCF attualmente applicati. I tipi di piattaforma, il tipo di switch, la porta e l'utilizzo della VLAN devono essere identici.

> È necessario utilizzare CleanUpFiles della stessa versione del file RCF e per la stessa configurazione. L'utilizzo di CleanUpFile non funziona e potrebbe richiedere un ripristino completo dello switch.

> La versione di ONTAP per la quale viene creato il file RCF non è rilevante. È importante solo la versione del file RCF.

> Il file RCF (anche se è della stessa versione) potrebbe elencare un numero inferiore o superiore di piattaforme. Assicurarsi che la piattaforma sia presente nell'elenco.

Opzione 2: Creazione di file CleanUpFiles generici

Utilizzare questa procedura se la configurazione **non** soddisfa tutti i requisiti.

Fasi

a. Recuperare l'output di `show running-config` da ogni switch.

b. Aprire lo strumento RcfFileGenerator e fare clic su "Create generic CleanUpFiles" (Crea file di pulizia generici) nella parte inferiore della finestra

c. Copiare l'output recuperato al punto 1 dal commutatore 'uno' nella finestra superiore. È possibile rimuovere o lasciare l'output predefinito.

d. Fare clic su "Create CUF Files" (Crea file CUF).

e. Copiare l'output dalla finestra inferiore in un file di testo (questo file è CleanUpFile).

f. Ripetere i passaggi c, d ed e per tutti gli switch della configurazione.

   Al termine di questa procedura, si dovrebbero avere quattro file di testo, uno per ogni switch. È possibile utilizzare questi file nello stesso modo dei CleanUpFiles che è possibile creare utilizzando l'opzione 1.

3. Crea i "nuovi" file RCF per la nuova configurazione. Creare questi file nello stesso modo in cui sono stati creati nel passaggio precedente, ad eccezione della scelta della versione del file ONTAP e RCF corrispondente.

   Dopo aver completato questo passaggio, si dovrebbero avere due set di file RCF, ciascuno costituito da dodici file.

4. Scaricare i file sul bootflash.

   a. Scaricare i CleanUpFiles creati in Creare i file RCF e CleanUpFiles oppure creare file CleanUpFiles generici per la configurazione corrente

      Questo file CleanUpFile si applica al file RCF corrente e **NON** al nuovo RCF a cui si desidera eseguire l'aggiornamento.

      Esempio di CleanUpFile per Switch-A1: `Cleanup_NX9336_v1.81_Switch-A1.txt`

   b. Scarica i "nuovi" file RCF creati in Creare i "nuovi" file RCF per la nuova configurazione.

      Esempio di file RCF per Switch-A1: `NX9336_v1.90_Switch-A1.txt`

   c. Scaricare i CleanUpFiles creati in Creare i "nuovi" file RCF per la nuova configurazione. Questo passaggio è facoltativo: È possibile utilizzare il file in futuro per aggiornare la configurazione dello switch. Corrisponde alla configurazione attualmente applicata.

      Esempio di CleanUpFile per Switch-A1: `Cleanup_NX9336_v1.90_Switch-A1.txt`

      Utilizzare CleanUpFile per la versione RCF corretta (corrispondente). Se si utilizza un CleanUpFile per una versione RCF diversa o per una configurazione diversa, la pulizia della configurazione potrebbe non funzionare correttamente.

      Il seguente esempio copia i tre file nella flash di avvio:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

   Viene richiesto di specificare Virtual Routing and Forwarding (VRF).

5. Applicare il file CleanUpFile o il file CleanUpFile generico.

   Alcune configurazioni vengono ripristinate e gli switchport vengono "offline".

   a. Verificare che non vi siano modifiche in sospeso alla configurazione di avvio: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Se viene visualizzato l'output di sistema, salvare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

   L'output del sistema indica che la configurazione di avvio e la configurazione in esecuzione sono diverse e in sospeso. Se non si salvano le modifiche in sospeso, non è possibile eseguire il rollback utilizzando un ricaricamento dello switch.

   a. Applicare il comando CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

   Lo script potrebbe impiegare del tempo per tornare al prompt dello switch. Nessun output previsto.

7. Visualizzare la configurazione in esecuzione per verificare che la configurazione sia stata cancellata: `show running-config`

   La configurazione corrente dovrebbe mostrare:

   - Non sono configurate mappe di classe ed elenchi di accesso IP
   - Non sono configurate mappe di policy
   - Nessuna policy di servizio configurata
   - Nessun profilo porta configurato
   - Tutte le interfacce Ethernet (ad eccezione di mgmt0 che non devono mostrare alcuna configurazione e deve essere configurata solo la VLAN 1).

     Se uno degli elementi sopra indicati è configurato, potrebbe non essere possibile applicare una nuova configurazione del file RCF. Tuttavia, è possibile tornare alla configurazione precedente ricaricando lo switch **senza** salvare la configurazione in esecuzione nella configurazione di avvio. Lo switch verrà configurato in precedenza.

8. Applicare il file RCF e verificare che le porte siano in linea.

   a. Applicare i file RCF.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

Durante l'applicazione della configurazione vengono visualizzati alcuni messaggi di avviso. I messaggi di errore generalmente non sono previsti. Tuttavia, se si è connessi con SSH, potrebbe essere visualizzato il seguente errore: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. Una volta applicata la configurazione, verificare che il cluster e le porte MetroCluster siano in linea con uno dei seguenti comandi: `show interface brief`, `show cdp neighbors`, o. `show lldp neighbors`

Se è stata modificata la VLAN per il cluster locale e si è aggiornato il primo switch del sito, il monitoraggio dello stato del cluster potrebbe non riportare lo stato come "integro" perché le VLAN delle configurazioni precedenti e nuove non corrispondono. Dopo l'aggiornamento del secondo switch, lo stato dovrebbe tornare a essere integro.

Se la configurazione non viene applicata correttamente o non si desidera mantenere la configurazione, è possibile tornare alla configurazione precedente ricaricando lo switch **senza** salvare la configurazione in esecuzione nella configurazione di avvio. Lo switch verrà configurato in precedenza.

9. Salvare la configurazione e ricaricare lo switch.

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Ridenominazione di uno switch IP Cisco

Potrebbe essere necessario rinominare uno switch IP Cisco per fornire un nome coerente per tutta la configurazione.

A proposito di questa attività

- Negli esempi di questa attività, il nome dello switch viene modificato da `myswitch` a. `IP_switch_A_1`.
- "Attivare la registrazione della console" prima di eseguire questa attività.

Fasi

1. Accedere alla modalità di configurazione globale:

   `configure terminal`

   L'esempio seguente mostra il prompt della modalità di configurazione. Entrambi i prompt mostrano il nome dello switch di `myswitch`.

   ```
   myswitch# configure terminal
   myswitch(config)#
   ```

2. Rinominare lo switch:

   `switchname new-switch-name`

Se si stanno rinominando entrambi gli switch nel fabric, utilizzare lo stesso comando su ogni switch.

Il prompt CLI cambia per riflettere il nuovo nome:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Uscire dalla modalità di configurazione:

   exit

   Viene visualizzato il prompt di livello superiore:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Copiare la configurazione corrente in esecuzione nel file di configurazione di avvio:

   copy running-config startup-config

5. Verificare che la modifica del nome dello switch sia visibile dal prompt del cluster ONTAP.

   Si noti che viene visualizzato il nuovo nome dello switch e il vecchio nome dello switch (`myswitch`) non viene visualizzato.

   a. Accedere alla modalità avanzata dei privilegi, premendo **y** quando richiesto:
      set -privilege advanced
   b. Visualizzare i dispositivi collegati:
      network device-discovery show
   c. Tornare alla modalità privilegi di amministratore:
      set -privilege admin

      L'esempio seguente mostra che lo switch viene visualizzato con il nuovo nome, `IP_switch_A_1`:

```
cluster_A::storage show> set 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

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Aggiunta, rimozione o modifica delle porte ISL senza interruzioni sugli switch IP Cisco

Potrebbe essere necessario aggiungere, rimuovere o modificare le porte ISL sugli switch IP Cisco. È possibile convertire porte ISL dedicate in porte ISL condivise o modificare la velocità delle porte ISL su uno switch IP Cisco.

A proposito di questa attività

Se si stanno convertendo porte ISL dedicate in porte ISL condivise, assicurarsi che le nuove porte soddisfino il "Requisiti per le porte ISL condivise".

Per garantire la connettività ISL, è necessario completare tutti i passaggi su entrambi gli switch.

La seguente procedura presuppone la sostituzione di un ISL da 10 GB collegato alla porta dello switch eth1/24/1 con due ISL da 100 GB collegati alle porte dello switch 17 e 18.

> Se si utilizza uno switch Cisco 9336C-FX2 in una configurazione condivisa che collega NS224 shelf, la modifica degli ISL potrebbe richiedere un nuovo file RCF. Non è necessario un nuovo file RCF se la velocità attuale e quella nuova dell'ISL è 40Gbps e 100Gbps. Tutte le altre modifiche alla velocità ISL richiedono un nuovo file RCF. Ad esempio, la modifica della velocità ISL da 40Gbps a 100Gbps non richiede un nuovo file RCF, ma la modifica della velocità ISL da 10Gbps a 40Gbps richiede un nuovo file RCF.

Prima di iniziare

Fare riferimento alla sezione **interruttori** della "NetApp Hardware Universe" per verificare i ricetrasmettitori supportati.

"Attivare la registrazione della console" prima di eseguire questa attività.

Fasi

1. Disattivare le porte ISL degli ISL su entrambi gli switch del fabric che si desidera modificare.

   > Le porte ISL correnti devono essere disattivate solo se vengono spostate su un'altra porta o se la velocità dell'ISL cambia. Se si aggiunge una porta ISL con la stessa velocità degli ISL esistenti, passare alla fase 3.

   Immettere un solo comando di configurazione per ogni riga e premere Ctrl-Z dopo aver immesso tutti i comandi, come illustrato nell'esempio seguente:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#
```

2. Rimuovere i cavi e i ricetrasmettitori esistenti.
3. Modificare la porta ISL secondo necessità.

> Se si utilizzano gli switch Cisco 9336C-FX2 in una configurazione condivisa che collega gli shelf NS224 ed è necessario aggiornare il file RCF e applicare la nuova configurazione per le nuove porte ISL, seguire i passaggi da a. "Aggiornare i file RCF sugli switch IP MetroCluster."

Opzione	Fase
Per modificare la velocità di una porta ISL…	Collegare i nuovi ISL alle porte designate in base alla velocità. Assicurarsi che le porte ISL dello switch siano elencate nella sezione *Installazione e configurazione IP MetroCluster*.
Per aggiungere un ISL…	Inserire i QFSP nelle porte che si stanno aggiungendo come porte ISL. Assicurarsi che siano elencati nella sezione *Installazione e configurazione IP MetroCluster* e cablarli di conseguenza.

4. Abilitare tutte le porte ISL (se non attivate) su entrambi gli switch del fabric iniziando dal seguente comando:

   ```
   switch_A_1# conf t
   ```

   Immettere un solo comando di configurazione per riga e premere Ctrl-Z dopo aver immesso tutti i comandi:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Verificare che gli ISL e i canali delle porte per gli ISL siano stabiliti tra entrambi gli switch:

   ```
   switch_A_1# show int brief
   ```

   Le interfacce ISL dovrebbero essere visualizzate nell'output del comando, come mostrato nell'esempio seguente:

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. Ripetere la procedura per il fabric 2.

Identificazione dello storage in una configurazione MetroCluster IP

Se è necessario sostituire un disco o un modulo shelf, è necessario prima identificare la posizione.

Identificazione degli shelf locali e remoti

Quando si visualizzano le informazioni sugli shelf da un sito MetroCluster, tutti i dischi remoti si trovano su 0 m, l'adattatore host iSCSI virtuale. Ciò significa che l'accesso ai dischi avviene tramite le interfacce IP di MetroCluster. Tutti gli altri dischi sono locali.

Dopo aver identificato se uno shelf è remoto (su 0 m), è possibile identificare ulteriormente l'unità o lo shelf in base al numero di serie o, in base alle assegnazioni degli shelf ID nella configurazione, in base all'ID dello shelf.

Nelle configurazioni MetroCluster IP che eseguono ONTAP 9.4, l'ID shelf non deve essere univoco tra i siti MetroCluster. Questo include sia shelf interni (0) che shelf esterni. Il numero di serie è coerente se visualizzato da qualsiasi nodo su uno dei siti MetroCluster.

Gli shelf ID devono essere univoci all'interno del gruppo di disaster recovery (DR), ad eccezione dello shelf interno.

Una volta identificato il modulo del disco o dello shelf, è possibile sostituire il componente utilizzando la procedura appropriata.

"Manutenzione degli shelf di dischi DS460C DS224C e DS212C"

Esempio di output sysconfig -A.

Nell'esempio riportato di seguito viene utilizzato il `sysconfig -a` Per visualizzare i dispositivi su un nodo nella configurazione IP MetroCluster. Questo nodo ha i seguenti shelf e dispositivi collegati:

- Slot 0: Dischi interni (dischi locali)
- Slot 3: ID shelf esterno 75 e 76 (dischi locali)
- Slot 0: Virtual iSCSI host adapter 0m (dischi remoti)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
```

```
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
```

```
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

Aggiunta di shelf a un MetroCluster IP utilizzando switch Storage MetroCluster condivisi

Potrebbe essere necessario aggiungere shelf NS224 a un MetroCluster utilizzando switch Storage MetroCluster condivisi.

A partire da ONTAP 9.10.1, è possibile aggiungere shelf NS224 da un MetroCluster utilizzando gli switch storage/MetroCluster condivisi. È possibile aggiungere più shelf alla volta.

Prima di iniziare

- I nodi devono eseguire ONTAP 9.9.1 o versione successiva.
- Tutti gli shelf NS224 attualmente connessi devono essere collegati agli stessi switch di MetroCluster (configurazione storage condiviso/switch MetroCluster).
- Questa procedura non può essere utilizzata per convertire una configurazione con shelf NS224 collegati direttamente o shelf NS224 collegati a switch Ethernet dedicati in una configurazione che utilizza switch storage/MetroCluster condivisi.
- "Attivare la registrazione della console" prima di eseguire questa attività.

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per

indicare che l'aggiornamento è in corso.

a. Immettere il seguente comando:

```
system node autosupport invoke -node * -type all -message "Maint=10h Adding
or Removing NS224 shelves"_
```

Questo esempio specifica una finestra di manutenzione di 10 ore. A seconda del piano, potrebbe essere necessario dedicare più tempo.

Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

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

a. Ripetere il comando sul cluster partner.

Verifica dello stato della configurazione MetroCluster

Prima di eseguire la transizione, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

```
node run -node node-name sysconfig -a
```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

```
system health alert show
```

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

```
metrocluster show
```

   d. Eseguire un controllo MetroCluster:

```
metrocluster check run
```

   e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

   f. Eseguire Config Advisor.

   "Download NetApp: Config Advisor"

   g. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.
2. Verificare che il cluster funzioni correttamente:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1    true    true          false
node_A_2    true    true          false

cluster_A::>
```

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

   `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  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: node_A_2-old

                                                  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.

cluster_A::>
```

4. 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 avere uno stato Admin/Oper di up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

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

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

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Applicazione del nuovo file RCF agli switch

Se lo switch è già configurato correttamente, è possibile saltare queste sezioni successive e passare direttamente a. Configurazione della crittografia MACsec sugli switch Cisco 9336C, se applicabile o a. Collegamento del nuovo shelf NS224.

- È necessario modificare la configurazione dello switch per aggiungere shelf.
- Consultare i dettagli del cablaggio all'indirizzo "Assegnazioni delle porte della piattaforma".
- È necessario utilizzare lo strumento **RcfFileGenerator** per creare il file RCF per la configurazione. Il "RcfFileGenerator" fornisce inoltre una panoramica del cablaggio per porta per ogni switch. Assicurarsi di scegliere il numero corretto di shelf. Insieme al file RCF vengono creati file aggiuntivi che forniscono un layout di cablaggio dettagliato corrispondente alle opzioni specifiche. Utilizzare questa panoramica dei cavi per verificare il cablaggio durante il cablaggio dei nuovi shelf.

Aggiornamento dei file RCF sugli switch IP MetroCluster

Se si sta installando un nuovo firmware dello switch, è necessario installare il firmware dello switch prima di aggiornare il file RCF.

Questa procedura interrompe il traffico sullo switch in cui viene aggiornato il file RCF. Il traffico riprenderà una volta applicato il nuovo file RCF.

Fasi

1. Verificare lo stato della configurazione.

   a. Verificare che i componenti di MetroCluster siano integri:

      metrocluster check run

```
cluster_A::*> metrocluster check run
```

L'operazione viene eseguita in background.

b. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Per verificare lo stato dell'operazione MetroCluster check in corso, utilizzare il comando: **`metrocluster operation history show -job-id 38`**

b. Verificare che non siano presenti avvisi sullo stato di salute: **`system health alert show`**

2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

Ripristino delle impostazioni predefinite dello switch IP Cisco

Prima di installare una nuova versione software e gli RCF, è necessario cancellare la configurazione dello switch Cisco ed eseguire la configurazione di base.

È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.

1. Ripristinare le impostazioni predefinite dello switch:

a. Cancellare la configurazione esistente: `write erase`

b. Ricaricare il software dello switch: `reload`

Il sistema viene riavviato e viene avviata la configurazione guidata. Durante l'avvio, se viene visualizzato il messaggio Interrompi provisioning automatico e continua con la normale configurazione?(sì/no)[n], dovresti rispondere `yes` per procedere.

c. Nella configurazione guidata, immettere le impostazioni di base dello switch:

- Password amministratore
- Nome dello switch
- Configurazione della gestione fuori banda
- Gateway predefinito
- Servizio SSH (RSA) al termine della configurazione guidata, lo switch si riavvia.

d. Quando richiesto, immettere il nome utente e la password per accedere allo switch.

L'esempio seguente mostra i prompt e le risposte del sistema durante la configurazione dello switch. Le staffe angolari (<<<) mostra dove inserire le informazioni.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

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 Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 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.
```

Inserire le informazioni di base nel successivo set di prompt, inclusi nome dello switch, indirizzo di gestione e gateway, quindi selezionare SSH con RSA.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  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]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

L’ultimo set di prompt completa la configurazione:

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

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

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Salvare la configurazione:

```
IP_switch-A-1# copy running-config startup-config
```

3. Riavviare lo switch e attendere che lo switch si ricarichi:

```
IP_switch-A-1# reload
```

4. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Download e installazione del software NX-OS dello switch Cisco

È necessario scaricare il file del sistema operativo dello switch e il file RCF su ciascun switch nella configurazione IP MetroCluster.

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per copiare i file sui centralini.

Questa procedura deve essere ripetuta su ciascuno switch IP nella configurazione IP di MetroCluster.

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

1. Scaricare il file software NX-OS supportato.

   "Download del software Cisco"

2. Copiare il software dello switch sullo switch: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In questo esempio, il file nxos.7.0.3.I4.6.bin viene copiato dal server SFTP 10.10.99.99 al bootflash locale:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verificare su ogni switch che i file NX-OS dello switch siano presenti nella directory bootflash di ogni switch: `dir bootflash:`

   Il seguente esempio mostra che i file sono presenti su IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installare il software dello switch: `install all nxos bootflash:nxos.version-number.bin`

   Lo switch viene ricaricato (riavviato) automaticamente dopo l'installazione del software dello switch.

   L'esempio seguente mostra l'installazione del software su IP_switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 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                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


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


Install is in progress, please wait.

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

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

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

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


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Attendere che lo switch si ricarichi, quindi accedere allo switch.

   Una volta riavviato lo switch, viene visualizzato il prompt di login:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verificare che il software dello switch sia stato installato: `show version`

   L'esempio seguente mostra l'output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Ripetere questa procedura sui tre switch IP rimanenti nella configurazione IP MetroCluster.

Configurazione della crittografia MACsec sugli switch Cisco 9336C

Se lo si desidera, è possibile configurare la crittografia MACsec sulle porte ISL WAN che vengono eseguite tra i siti. È necessario configurare MACsec dopo aver applicato il file RCF corretto.

La crittografia MACsec può essere applicata solo alle porte ISL WAN.

Requisiti di licenza per MACsec

MACsec richiede una licenza di sicurezza. Per una spiegazione completa dello schema di licenza di Cisco NX-OS e su come ottenere e richiedere le licenze, consultare la "Guida alle licenze di Cisco NX-OS"

Abilitazione degli ISL WAN con crittografia Cisco MACsec nelle configurazioni IP di MetroCluster

È possibile attivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

1. Accedere alla modalità di configurazione globale: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Abilitare MACsec e MKA sul dispositivo: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copiare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Disattivazione della crittografia Cisco MACsec

Potrebbe essere necessario disattivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

Se si disattiva la crittografia, è necessario eliminare anche le chiavi.

1. Accedere alla modalità di configurazione globale: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disattivare la configurazione MACsec sul dispositivo: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

Selezionando l'opzione no si ripristina la funzione MACsec.

3. Selezionare l'interfaccia già configurata con MACsec.

È possibile specificare il tipo di interfaccia e l'identità. Per una porta Ethernet, utilizzare slot/porta ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Rimuovere il portachiavi, il criterio e il portachiavi fallback configurati sull'interfaccia per rimuovere la configurazione MACsec: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Ripetere i passaggi 3 e 4 su tutte le interfacce in cui è configurato MACsec.
6. Copiare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configurazione di una catena di chiavi MACsec e delle chiavi

Per ulteriori informazioni sulla configurazione di una catena di chiavi MACsec, consultare la documentazione Cisco relativa allo switch.

Collegamento del nuovo shelf NS224

Fasi

1. Installare il kit per il montaggio su guida fornito con lo shelf utilizzando il volantino di installazione fornito nella confezione del kit.
2. Installare e fissare lo shelf sulle staffe di supporto e sul rack o sull'armadietto utilizzando il volantino di installazione.
3. Collegare i cavi di alimentazione allo shelf, fissarli con il fermo del cavo di alimentazione, quindi collegare i cavi di alimentazione a diverse fonti di alimentazione per garantire la resilienza.

   Uno shelf si accende quando viene collegato a una fonte di alimentazione; non dispone di interruttori di alimentazione. Quando funziona correttamente, il LED bicolore di un alimentatore si illumina di verde.

4. Impostare l'ID dello shelf su un numero univoco all'interno della coppia ha e nella configurazione.
5. Collegare le porte dello shelf nel seguente ordine:
   a. Collegare NSM-A, e0a allo switch (Switch-A1 o Switch-B1)
   b. Collegare NSM-B, e0a allo switch (Switch-A2 o Switch-B2)
   c. Collegare NSM-A, e0b allo switch (Switch-A1 o Switch-B1)
   d. Collegare NSM-B, e0b allo switch (Switch-A2 o Switch-B2)
6. Utilizzare il layout di cablaggio generato dallo strumento **RcfFileGenerator** per collegare lo shelf alle porte

appropriate.

Una volta collegato correttamente il nuovo shelf, ONTAP lo rileva automaticamente sulla rete.

Configurare la crittografia end-to-end in una configurazione IP MetroCluster

A partire da ONTAP 9.15.1, è possibile configurare la crittografia end-to-end per crittografare il traffico back-end, ad esempio NVlog e i dati di replica dello storage, tra i siti in una configurazione IP di MetroCluster.

A proposito di questa attività

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Prima di poter configurare la crittografia end-to-end, è necessario "Configurare la gestione esterna delle chiavi".
- Esaminare i sistemi supportati e la versione ONTAP minima richiesta per configurare la crittografia end-to-end in una configurazione IP di MetroCluster:

Release ONTAP minima	Sistemi supportati
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700

Attiva la crittografia end-to-end

Per attivare la crittografia end-to-end, procedere come segue.

Fasi

1. Verificare lo stato della configurazione MetroCluster.

   a. Verificare che i componenti di MetroCluster siano integri:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   L'operazione viene eseguita in background.

   b. Dopo il `metrocluster check run` l'operazione è completata, eseguire:

   ```
   metrocluster check show
   ```

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id <id>
```

b. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Verificare che la gestione delle chiavi esterne sia configurata su entrambi i cluster:

```
security key-manager external show-status
```

3. Abilita la crittografia end-to-end per ogni gruppo di DR:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Esempio

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Ripetere questa operazione per ciascun gruppo DR nella configurazione.

4. Verificare che la crittografia end-to-end sia abilitata:

```
metrocluster node show -fields is-encryption-enabled
```

Esempio

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

Disattiva la crittografia end-to-end

Per disattivare la crittografia end-to-end, procedere come segue.

Fasi

1. Verificare lo stato della configurazione MetroCluster.

   a. Verificare che i componenti di MetroCluster siano integri:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   L'operazione viene eseguita in background.

b. Dopo il `metrocluster check run` l'operazione è completata, eseguire:

```
metrocluster check show
```

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id <id>
```

b. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Verificare che la gestione delle chiavi esterne sia configurata su entrambi i cluster:

```
security key-manager external show-status
```

3. Disattivare la crittografia end-to-end per ogni gruppo di DR:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Esempio

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Ripetere questa operazione per ciascun gruppo DR nella configurazione.

4. Verificare che la crittografia end-to-end sia disattivata:

```
metrocluster node show -fields is-encryption-enabled
```

Esempio

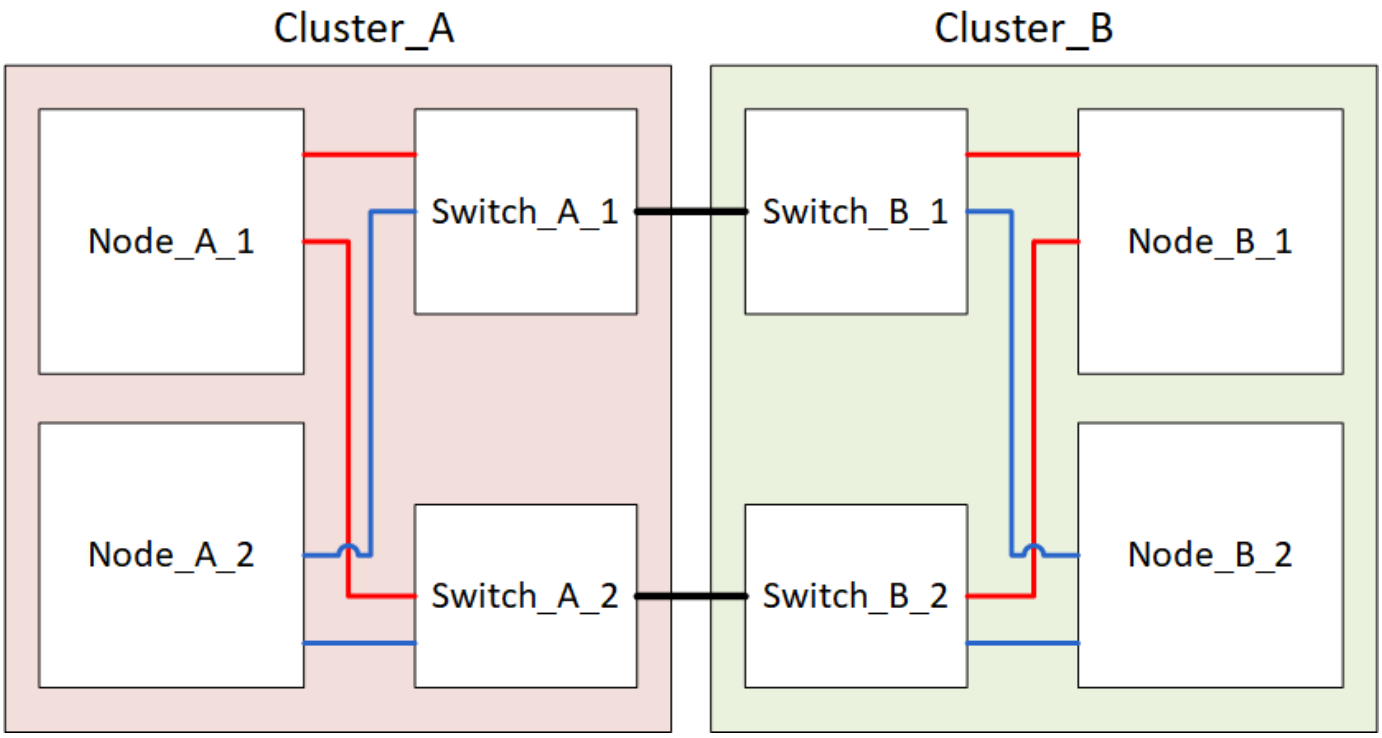
```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Spegnere e riaccendere un singolo sito in una configurazione IP di MetroCluster

Se è necessario eseguire la manutenzione del sito o spostare un singolo sito in una configurazione IP MetroCluster, è necessario sapere come spegnere e riaccendere il sito.

Per spostare e riconfigurare un sito (ad esempio per l'espansione da un cluster a quattro nodi a uno a otto nodi), non è possibile completare contemporaneamente le attività. Questa procedura descrive solo le fasi necessarie per eseguire la manutenzione del sito o per spostare un sito senza modificarne la configurazione.

Il seguente diagramma mostra una configurazione MetroCluster. Il cluster_B è spento per la manutenzione.



Spegnere un sito MetroCluster

È necessario spegnere un sito e tutte le apparecchiature prima di iniziare la manutenzione o il trasferimento del sito.

A proposito di questa attività

Tutti i comandi dei seguenti passaggi vengono emessi dal sito che rimane acceso.

Fasi

1. Prima di iniziare, verificare che gli aggregati non mirrorati nel sito siano offline.
2. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      `node run -node node-name sysconfig -a`

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      `system health alert show`

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      `metrocluster show`

   d. Eseguire un controllo MetroCluster:
      `metrocluster check run`
   e. Visualizzare i risultati del controllo MetroCluster:

      `metrocluster check show`

f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

```
storage switch show
```

g. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

3. Dal sito in cui si desidera rimanere attivi, implementare lo switchover:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Il completamento dell'operazione può richiedere alcuni minuti.

4. Monitorare e verificare il completamento dello switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Se si dispone di una configurazione MetroCluster IP con ONTAP 9.6 o versione successiva, attendere che i plex del sito di emergenza siano online e che le operazioni di riparazione vengano completate automaticamente.

Nelle configurazioni IP di MetroCluster che eseguono ONTAP 9,5 o versione precedente, i nodi del sito di disastro non si avviano automaticamente su ONTAP e i plex rimangono offline.

6. Spostare offline tutti i volumi e le LUN che appartengono agli aggregati senza mirror.

a. Spostare i volumi offline.

```
cluster_A::* volume offline <volume name>
```

b. Spostare i LUN offline.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Sposta aggregati senza mirror offline: `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. A seconda della configurazione e della versione di ONTAP, identificare e spostare offline i plex interessati che si trovano nel sito di emergenza (Cluster_B).

   Devi spostare i seguenti plessi offline:

   - Plessi non mirrorati che risiedono su dischi situati nel sito di disastro.

     Se non si spostano offline i plex non di mirroring del sito di disastro, potrebbe verificarsi un'interruzione quando il sito di disastro viene successivamente spento.

   - Plessi mirrorati che risiedono su dischi situati nel sito di disastro per il mirroring aggregato. Una volta spostati offline, i plex non sono accessibili.

   a. Identificare i plessi interessati.

      I plex di proprietà dei nodi nel sito sopravvissuto sono costituiti da dischi Pool1. I plex di proprietà dei nodi nel sito di disastro sono costituiti da dischi Pool0.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------ --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

I plex interessati sono quelli remoti al cluster A. La seguente tabella indica se i dischi sono locali o remoti rispetto al cluster A:

Nodo	Dischi nel pool	I dischi devono essere impostati offline?	Esempio di plessi da spostare offline
Nodo _A_1 e nodo _A_2	Dischi nel pool 0	No I dischi sono locali nel cluster A.	-
Dischi nel pool 1	Sì. I dischi sono remoti nel cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nodo _B_1 e nodo _B_2

Dischi nel pool 0	Sì. I dischi sono remoti nel cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Dischi nel pool 1

b. Sposta i plessi interessati offline:

`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

Eseguire questa operazione per tutti i plessi che hanno dischi remoti a Cluster_A.

9. Le porte dello switch ISL sono costantemente offline in base al tipo di switch.
10. Arrestare i nodi eseguendo il seguente comando su ciascun nodo:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Spegnere l'apparecchiatura in caso di disastro.

È necessario spegnere le seguenti apparecchiature nell'ordine indicato:

- Storage controller: Gli storage controller devono trovarsi attualmente nella `LOADER` è necessario spegnerli completamente.
- Switch IP MetroCluster
- Shelf di storage

Spostamento del sito spento di MetroCluster

Una volta spento il sito, è possibile iniziare il lavoro di manutenzione. La procedura è la stessa sia che i componenti MetroCluster vengano ricollocati all'interno dello stesso data center sia che vengano ricollocati in un data center diverso.

- Il cavo dell'hardware deve essere identico a quello del sito precedente.
- Se la velocità, la lunghezza o il numero di InterSwitch link (ISL) sono stati modificati, è necessario riconfigurare tutti.

Fasi

1. Verificare che il cablaggio di tutti i componenti sia registrato attentamente in modo che possa essere ricollegato correttamente nella nuova posizione.
2. Spostare fisicamente tutto l'hardware, i controller di storage, gli switch IP, i FibreBridge e gli shelf di storage.
3. Configurare le porte ISL e verificare la connettività tra siti.

a. Accendere gli switch IP.

Non * accendere altre apparecchiature.

4. Utilizzare gli strumenti sugli switch (se disponibili) per verificare la connettività tra siti.

Procedere solo se i collegamenti sono correttamente configurati e stabili.

5. Disattivare nuovamente i collegamenti se risultano stabili.

Accensione della configurazione MetroCluster e ripristino del normale funzionamento

Una volta completata la manutenzione o spostato il sito, è necessario accendere il sito e ripristinare la configurazione MetroCluster.

A proposito di questa attività

Tutti i comandi descritti di seguito vengono emessi dal sito di accensione.

Fasi

1. Accendere gli interruttori.

   Accendere prima gli interruttori. Potrebbero essere stati accesi durante la fase precedente se il sito è stato trasferito.

   a. Riconfigurare il collegamento interswitch (ISL) se necessario o se non è stato completato come parte del trasferimento.
   b. Abilitare l'ISL se la scherma è stata completata.
   c. Verificare l'ISL.

2. Accendere i controller di archiviazione e attendere che venga visualizzato `LOADER` prompt. I controller non devono essere completamente avviati.

   Se l'avvio automatico è attivato, premere `Ctrl+C` per interrompere l'avvio automatico dei controller.

3. Accendere gli scaffali, lasciando abbastanza tempo per accenderli completamente.
4. Verificare che lo spazio di archiviazione sia visibile.
   a. Verificare che lo storage sia visibile dal sito sopravvissuto. Riportare i plesso offline in linea per riavviare l'operazione di risincronizzazione e ristabilire la SyncMirror.
   b. Verificare che la memoria locale sia visibile dal nodo in modalità manutenzione:

      ```
      disk show -v
      ```

5. Ristabilire la configurazione MetroCluster.

   Seguire le istruzioni riportate in "Verificare che il sistema sia pronto per lo switchback" Per eseguire operazioni di healing e switchback in base alla configurazione MetroCluster.

Spegnimento di un'intera configurazione IP MetroCluster

Prima di iniziare la manutenzione o il trasferimento, è necessario spegnere l'intera configurazione IP di MetroCluster e tutte le apparecchiature.

A partire da ONTAP 9.8, la **`storage switch`** il comando viene sostituito con **`system switch`**. La procedura riportata di seguito mostra **`storage switch`** Ma se si utilizza ONTAP 9.8 o versione successiva, il comando **`system switch`** è preferibile utilizzare il comando.

1. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster.
   a. Verificare che la configurazione e la modalità operativa di MetroCluster siano normali.
      `metrocluster show`
   b. Eseguire il seguente comando:
      `metrocluster interconnect show`
   c. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:
      `run local sysconfig -v`
   d. Eseguire il seguente comando:
      `storage port show`
   e. Eseguire il seguente comando:
      `storage switch show`
   f. Eseguire il seguente comando:
      `network interface show`
   g. Eseguire il seguente comando:
      `network port show`
   h. Eseguire il seguente comando:
      `network device-discovery show`
   i. Eseguire un controllo MetroCluster:
      `metrocluster check run`
   j. Visualizzare i risultati del controllo MetroCluster:
      `metrocluster check show`
   k. Eseguire il seguente comando:
      `metrocluster configuration-settings interface show`
2. Se necessario, disattivare AUSO modificando IL dominio di errore AUSO in

   `auso-disabled`

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

In una configurazione IP MetroCluster, il dominio di errore AUSODISABLED è già impostato su 'ausodisabled', a meno che la configurazione non sia configurata con il supporto ONTAP.

3. Verificare la modifica utilizzando il comando

   metrocluster operation show

   ```
   cluster_A_site_A::*> metrocluster operation show
      Operation: modify
          State: successful
     Start Time: 4/25/2020 20:20:36
       End Time: 4/25/2020 20:20:36
         Errors: -
   ```

4. Arrestare i nodi:

   halt

   ```
   system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
   -warnings true
   ```

5. Spegnere le seguenti apparecchiature presso il sito:
   - Controller di storage
   - Switch IP MetroCluster
   - Shelf di storage
6. Attendere trenta minuti, quindi accendere tutti gli shelf di storage, gli switch IP MetroCluster e i controller di storage.
7. Dopo aver acceso i controller, verificare la configurazione MetroCluster da entrambi i siti.

   Per verificare la configurazione, ripetere il passaggio 1.

8. Eseguire i controlli del ciclo di alimentazione.
   a. Verificare che tutte le SVM di origine della sincronizzazione siano online:
   vserver show
   b. Avviare tutte le SVM di origine della sincronizzazione non in linea:
   vserver start

Informazioni sul copyright

Informazioni sul marchio commerciale