



# **Installare una configurazione IP MetroCluster**

ONTAP MetroCluster

NetApp  
April 25, 2024

This PDF was generated from <https://docs.netapp.com/it-it/ontap-metrocluster/install-ip/index.html> on April 25, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Installare una configurazione IP MetroCluster ..... 1
  - Panoramica ..... 1
  - Prepararsi per l'installazione di MetroCluster ..... 1
  - Configurare i componenti hardware di MetroCluster ..... 48
  - Configurare il software MetroCluster in ONTAP ..... 125
  - Configurare il servizio ONTAP Mediator per lo switchover automatico non pianificato ..... 189
  - Test della configurazione MetroCluster ..... 196
  - Considerazioni sulla rimozione delle configurazioni MetroCluster ..... 214
  - Considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster ..... 215
  - Dove trovare ulteriori informazioni ..... 226

# Installare una configurazione IP MetroCluster

## Panoramica

Per installare la configurazione IP di MetroCluster, è necessario eseguire una serie di procedure nell'ordine corretto.

- ["Prepararsi all'installazione e comprendere tutti i requisiti"](#).
- ["Cablare i componenti"](#)
- ["Configurare il software"](#)
- ["Configurare ONTAP mediator"](#) (opzionale)
- ["Verificare la configurazione"](#)

## Prepararsi per l'installazione di MetroCluster

### Differenze tra le configurazioni ONTAP MetroCluster

Le varie configurazioni MetroCluster presentano differenze chiave nei componenti richiesti.

In tutte le configurazioni, ciascuno dei due siti MetroCluster è configurato come cluster ONTAP. In una configurazione MetroCluster a due nodi, ciascun nodo viene configurato come cluster a nodo singolo.

Funzione	Configurazioni IP	Configurazioni fabric attached		Configurazioni di estensione	
		Quattro o otto nodi	Due nodi	Connessione a ponte a due nodi	Direct-attached a due nodi
Numero di controller	Quattro o otto*	Quattro o otto	Due	Due	Due
Utilizza un fabric storage switch FC	No	Sì	Sì	No	No
Utilizza un fabric di storage IP switch	Sì	No	No	No	No
Utilizza bridge FC-SAS	No	Sì	Sì	Sì	No
Utilizza lo storage SAS direct-attached	Sì (solo locale collegato)	No	No	No	Sì

Supporta ADP	Sì (a partire da ONTAP 9.4)	No	No	No	No
Supporta ha locale	Sì	Sì	No	No	No
Supporta lo switchover automatico non pianificato ONTAP (USO)	No	Sì	Sì	Sì	Sì
Supporta aggregati senza mirror	Sì (a partire da ONTAP 9.8)	Sì	Sì	Sì	Sì
Supporta LUN array	No	Sì	Sì	Sì	Sì
Supporta il mediatore ONTAP	Sì (a partire da ONTAP 9.7)	No	No	No	No
Supporta MetroCluster Tiebreaker	Sì (non in combinazione con il mediatore ONTAP)	Sì	Sì	Sì	Sì
Supporta <a href="#">Tutti gli array SAN</a>	Sì	Sì	Sì	Sì	Sì

## Importante

Tenere presente le seguenti considerazioni per le configurazioni IP MetroCluster a otto nodi:

- Le configurazioni a otto nodi sono supportate a partire da ONTAP 9.9.1.
- Sono supportati solo gli switch MetroCluster validati da NetApp (ordinati da NetApp).
- Le configurazioni che utilizzano connessioni backend con routing IP (Layer 3) non sono supportate.
- Le configurazioni che utilizzano reti private Layer 2 condivise non sono supportate.
- Le configurazioni che utilizzano uno switch condiviso Cisco 9336C-FX2 non sono supportate.

## Supporto per tutti i sistemi array SAN nelle configurazioni MetroCluster

Alcuni degli All SAN Array (ASA) sono supportati nelle configurazioni MetroCluster. Nella documentazione MetroCluster, le informazioni relative ai modelli AFF si applicano al sistema ASA corrispondente. Ad esempio, tutti i cavi e altre informazioni per il sistema AFF A400 si applicano anche al sistema ASA AFF A400.

Le configurazioni di piattaforma supportate sono elencate nella ["NetApp Hardware Universe"](#).

## Differenze tra ONTAP Mediator e MetroCluster Tiebreaker

A partire da ONTAP 9.7, è possibile utilizzare il MAUSO (Automatic Unplanned switchover) assistito dal mediatore ONTAP nella configurazione IP di MetroCluster oppure il software MetroCluster Tiebreaker. Non è necessario utilizzare il software MAUSO o Tiebreaker; tuttavia, se si sceglie di non utilizzare uno di questi servizi, è necessario ["eseguire un ripristino manuale"](#) in caso di disastro

Le diverse configurazioni MetroCluster eseguono lo switchover automatico in diverse circostanze:

- **Configurazioni MetroCluster FC che utilizzano la funzionalità AUSO (non presente nelle configurazioni MetroCluster IP)**

In queste configurazioni, AUSO viene avviato se i controller si guastano ma lo storage (e i bridge, se presenti) rimangono operativi.

- **Configurazioni IP MetroCluster che utilizzano il servizio ONTAP Mediator (ONTAP 9.7 e versioni successive)**

In queste configurazioni, MAUSO viene avviato nelle stesse circostanze di AUSO, come descritto sopra, e anche dopo un guasto completo del sito (controller, storage e switch).

["Scoprite in che modo ONTAP Mediator supporta lo switchover non pianificato automatico"](#).

- **Configurazioni MetroCluster IP o FC che utilizzano il software Tiebreaker in modalità attiva**

In queste configurazioni, il Tiebreaker avvia lo switchover non pianificato dopo un guasto completo del sito.

Prima di utilizzare il software Tiebreaker, consultare ["Installazione e configurazione del software MetroCluster Tiebreaker"](#)

## Interoperabilità di ONTAP Mediator con altre applicazioni e appliance

Non è possibile utilizzare applicazioni o appliance di terze parti in grado di attivare uno switchover in combinazione con ONTAP Mediator. Inoltre, il monitoraggio di una configurazione MetroCluster con il software MetroCluster Tiebreaker non è supportato quando si utilizza ONTAP Mediator.

## Considerazioni per le configurazioni MetroCluster IP

È necessario comprendere il modo in cui i controller accedono allo storage remoto e il funzionamento degli indirizzi IP MetroCluster.

### Accesso allo storage remoto nelle configurazioni MetroCluster IP

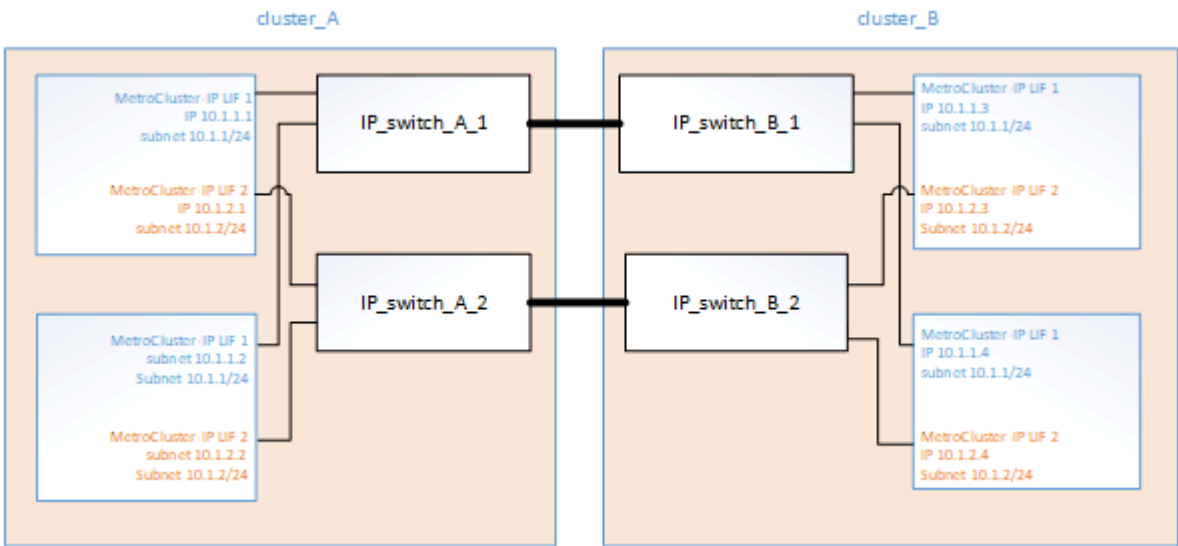
Nelle configurazioni MetroCluster IP, l'unico modo in cui i controller locali possono raggiungere i pool di storage remoti è tramite i controller remoti. Gli switch IP sono collegati alle porte Ethernet dei controller e non dispongono di connessioni dirette agli shelf di dischi. Se il controller remoto non è attivo, i controller locali non possono raggiungere i pool di storage remoti.

Si tratta di configurazioni diverse da quelle FC di MetroCluster, in cui i pool di storage remoti sono collegati ai controller locali tramite il fabric FC o le connessioni SAS. I controller locali hanno ancora accesso allo storage remoto anche se i controller remoti non sono attivi.

Indirizzi IP MetroCluster

È necessario conoscere il modo in cui gli indirizzi IP e le interfacce MetroCluster vengono implementati in una configurazione IP MetroCluster, nonché i requisiti associati.

In una configurazione MetroCluster IP, la replica dello storage e della cache non volatile tra le coppie ha e i partner DR viene eseguita su collegamenti dedicati ad alta larghezza di banda nel fabric IP di MetroCluster. Le connessioni iSCSI vengono utilizzate per la replica dello storage. Gli switch IP vengono utilizzati anche per tutto il traffico intra-cluster all'interno dei cluster locali. Il traffico MetroCluster viene mantenuto separato dal traffico intra-cluster utilizzando sottoreti IP e VLAN separate. Il fabric IP di MetroCluster è distinto e diverso dalla rete di peering del cluster.



La configurazione MetroCluster IP richiede due indirizzi IP su ciascun nodo che sono riservati al fabric MetroCluster IP back-end. Gli indirizzi IP riservati vengono assegnati alle LIF (MetroCluster IP Logical Interface) durante la configurazione iniziale e presentano i seguenti requisiti:



È necessario scegliere attentamente gli indirizzi IP MetroCluster, in quanto non è possibile modificarli dopo la configurazione iniziale.

- Devono rientrare in un intervallo IP univoco.
- Devono risiedere in una delle due subnet IP che le separano da tutto il traffico.

Ad esempio, i nodi potrebbero essere configurati con i seguenti indirizzi IP:

Nodo	Interfaccia	Indirizzo IP	Subnet
Node_A_1	Interfaccia IP MetroCluster 1	10.1.1.1	10.1.1/24
Node_A_1	Interfaccia IP MetroCluster 2	10.1.2.1	10.1.2/24

Node_A_2	Interfaccia IP MetroCluster 1	10.1.1.2	10.1.1/24
Node_A_2	Interfaccia IP MetroCluster 2	10.1.2.2	10.1.2/24
Node_B_1	Interfaccia IP MetroCluster 1	10.1.1.3	10.1.1/24
Node_B_1	Interfaccia IP MetroCluster 2	10.1.2.3	10.1.2/24
Node_B_2	Interfaccia IP MetroCluster 1	10.1.1.4	10.1.1/24
Node_B_2	Interfaccia IP MetroCluster 2	10.1.2.4	10.1.2/24

### Caratteristiche delle interfacce IP MetroCluster

Le interfacce IP di MetroCluster sono specifiche per le configurazioni IP di MetroCluster. Hanno caratteristiche diverse rispetto ad altri tipi di interfaccia ONTAP:

- Vengono creati da `metrocluster configuration-settings interface create` Come parte della configurazione iniziale di MetroCluster.



A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "[Considerazioni per le reti wide-area di livello 3](#)".

Non vengono creati o modificati dai comandi dell'interfaccia di rete.

- Non vengono visualizzati nell'output di `network interface show` comando.
- Non esegue il failover, ma rimangono associati alla porta su cui sono stati creati.
- Le configurazioni IP di MetroCluster utilizzano porte Ethernet specifiche (a seconda della piattaforma) per le interfacce IP di MetroCluster.

### Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive

A partire da ONTAP 9.4, le configurazioni IP di MetroCluster supportano nuove installazioni con ADP (partizione avanzata dei dischi).

Quando si utilizza ADP con le configurazioni IP MetroCluster, è necessario tenere presenti le seguenti considerazioni:

- Per utilizzare ADP con le configurazioni IP di MetroCluster, è necessario ONTAP 9.4 e versioni successive.
- ADPv2 è supportato nelle configurazioni IP di MetroCluster.

- L'aggregato root deve trovarsi nella partizione 3 per tutti i nodi in entrambi i siti.
- Il partizionamento e l'assegnazione dei dischi vengono eseguiti automaticamente durante la configurazione iniziale dei siti MetroCluster.
- Le assegnazioni dei dischi pool 0 vengono eseguite in fabbrica.
- La root senza mirror viene creata in fabbrica.
- L'assegnazione della partizione dei dati viene eseguita presso la sede del cliente durante la procedura di configurazione.
- Nella maggior parte dei casi, l'assegnazione e il partizionamento dei dischi vengono eseguiti automaticamente durante le procedure di installazione.
- Un disco e tutte le sue partizioni devono essere di proprietà dei nodi nella stessa coppia di ha (High Availability). La proprietà di partizioni o dischi all'interno di un singolo disco non può essere combinata tra la coppia ha locale e il partner di disaster recovery (DR) o il partner ausiliario di DR.

Esempio di configurazione supportata:

Disco/partizione	Proprietario
Disco:	ClusterA-Node01
Partizione 1:	ClusterA-Node01
Partizione 2:	ClusterA-Node02
Partizione 3:	ClusterA-Node01



Quando si esegue l'aggiornamento da ONTAP 9.4 a 9.5, il sistema riconosce le assegnazioni dei dischi esistenti.

## Partizione automatica

L'ADP viene eseguito automaticamente durante la configurazione iniziale del sistema.



A partire da ONTAP 9.5, l'assegnazione automatica dei dischi deve essere attivata con `storage disk option modify -autoassign on` comando.

Impostare lo stato ha-config su `mccip` prima del provisioning automatico, per assicurarsi che siano selezionate le dimensioni corrette delle partizioni per consentire le dimensioni appropriate del volume root. Per ulteriori informazioni, vedere ["Verifica dello stato ha-config dei componenti"](#).

Durante l'installazione è possibile partizionare automaticamente un massimo di 96 dischi. È possibile aggiungere dischi aggiuntivi dopo l'installazione iniziale.



Se si utilizzano unità interne ed esterne, è necessario innanzitutto inizializzare MetroCluster con le sole unità interne che utilizzano ADP. Dopo aver completato l'installazione o l'installazione, collegare manualmente lo shelf esterno.

Devi assicurarti che gli shelf interni dispongano del numero minimo di dischi consigliato, come descritto in [Differenze tra ADP e assegnazione del disco per sistema](#).

Per i dischi interni ed esterni, è necessario popolare gli shelf parzialmente pieni, come descritto in [Come popolare gli shelf parzialmente completi](#).



## Come funziona l'assegnazione automatica shelf-by-shelf

Se sono presenti quattro shelf esterni per sito, ogni shelf viene assegnato a un nodo diverso e a un pool diverso, come illustrato nell'esempio seguente:

- Tutti i dischi sul sito\_A-shelf\_1 vengono assegnati automaticamente al pool 0 del nodo\_A\_1
- Tutti i dischi sul sito\_A-shelf\_3 vengono assegnati automaticamente al pool 0 del nodo\_A\_2
- Tutti i dischi sul sito\_B-shelf\_1 vengono assegnati automaticamente al pool 0 del nodo\_B\_1
- Tutti i dischi sul sito\_B-shelf\_3 vengono assegnati automaticamente al pool 0 del nodo\_B\_2
- Tutti i dischi sul sito\_B-shelf\_2 vengono assegnati automaticamente al pool 1 del nodo\_A\_1
- Tutti i dischi sul sito\_B-shelf\_4 vengono assegnati automaticamente al pool 1 del nodo\_A\_2
- Tutti i dischi sul sito\_A-shelf\_2 vengono assegnati automaticamente al pool 1 del nodo\_B\_1
- Tutti i dischi sul sito\_A-shelf\_4 vengono assegnati automaticamente al pool 1 del nodo\_B\_2

## Come popolare gli shelf parzialmente completi

Se la configurazione utilizza shelf non completamente popolati (con alloggiamenti per dischi vuoti), è necessario distribuire i dischi in modo uniforme in tutto lo shelf, a seconda della policy di assegnazione dei dischi. La policy di assegnazione dei dischi dipende dal numero di shelf presenti in ciascun sito MetroCluster.

Se si utilizza un singolo shelf in ogni sito (o solo lo shelf interno in un sistema AFF A800), i dischi vengono assegnati utilizzando una policy di un quarto di shelf. Se lo shelf non è completamente popolato, installare i dischi in parti uguali su tutti i quarter.

La seguente tabella mostra un esempio di come inserire 24 dischi in uno shelf interno da 48 dischi. Viene inoltre mostrata la proprietà dei dischi.

I 48 alloggiamenti per unità sono suddivisi in quattro quarti:	Installare sei dischi nei primi sei alloggiamenti di ogni trimestre...
Quarto 1: Alloggiamenti 0-11	Alloggiamenti 0-5
Secondo trimestre: Alloggiamenti 12-23	Alloggiamenti 12-17
Terzo trimestre: Alloggiamenti 24-35	Alloggiamenti 24-29
Trimestre 4: Baie 36-47	Alloggiamenti 36-41

La tabella seguente mostra un esempio di come posizionare 16 dischi in uno shelf interno di 24 dischi.

Gli alloggiamenti per 24 unità sono divisi in quattro trimestri:	Installare quattro unità nei primi quattro alloggiamenti in ogni trimestre...
Trimestre 1: Baie 0-5	Vani 0-3
Trimestre 2: Baie 6-11	Vani 6-9
Trimestre 3: Baie 12-17	Vani 12-15

Se stai utilizzando due shelf esterni in ciascun sito, i dischi vengono assegnati usando una policy half-shelf. Se gli shelf non sono completamente popolati, installare i dischi in parti uguali da entrambe le estremità dello shelf.

Ad esempio, se si installano 12 dischi in uno shelf da 24 dischi, installare i dischi negli alloggiamenti 0-5 e 18-23.

### Assegnazione manuale del disco (ONTAP 9.5)

In ONTAP 9.5, l'assegnazione manuale dei dischi è necessaria sui sistemi con le seguenti configurazioni di shelf:

- Tre shelf esterni per sito.

Due shelf vengono assegnati automaticamente utilizzando una policy di assegnazione a metà shelf, ma il terzo shelf deve essere assegnato manualmente.

- Più di quattro shelf per sito e il numero totale di shelf esterni non è un multiplo di quattro.

Gli shelf extra sopra il multiplo più vicino di quattro vengono lasciati non assegnati e i dischi devono essere assegnati manualmente. Ad esempio, se nel sito sono presenti cinque shelf esterni, è necessario assegnarli manualmente.

È sufficiente assegnare manualmente un singolo disco su ogni shelf non assegnato. Gli altri dischi sullo shelf vengono quindi assegnati automaticamente.

### Assegnazione manuale del disco (ONTAP 9.4)

In ONTAP 9.4, l'assegnazione manuale dei dischi è necessaria sui sistemi con le seguenti configurazioni di shelf:

- Meno di quattro shelf esterni per sito.

I dischi devono essere assegnati manualmente per garantire un'assegnazione simmetrica dei dischi, con ciascun pool che ha un numero uguale di dischi.

- Più di quattro shelf esterni per sito e il numero totale di shelf esterni non è un multiplo di quattro.

Gli shelf extra sopra il multiplo più vicino di quattro vengono lasciati non assegnati e i dischi devono essere assegnati manualmente.

Quando si assegnano manualmente i dischi, è necessario assegnarli simmetricamente, con un numero uguale di dischi assegnati a ciascun pool. Ad esempio, se la configurazione dispone di due shelf di storage in ogni sito, è necessario uno shelf per la coppia ha locale e uno shelf per la coppia ha remota:

- Assegnare metà dei dischi sul sito\_A-shelf\_1 al pool 0 del nodo\_A\_1.
- Assegnare metà dei dischi sul sito\_A-shelf\_1 al pool 0 del nodo\_A\_2.
- Assegnare metà dei dischi sul sito\_A-shelf\_2 al pool 1 del nodo\_B\_1.
- Assegnare metà dei dischi sul sito\_A-shelf\_2 al pool 1 del nodo\_B\_2.

- Assegnare metà dei dischi sul sito\_B-shelf\_1 al pool 0 del nodo\_B\_1.
- Assegnare metà dei dischi sul sito\_B-shelf\_1 al pool 0 del nodo\_B\_2.
- Assegnare metà dei dischi sul sito\_B-shelf\_2 al pool 1 del nodo\_A\_1.
- Assegnare metà dei dischi sul sito\_B-shelf\_2 al pool 1 del nodo\_A\_2.

### Aggiunta di shelf a una configurazione esistente

L'assegnazione automatica dei dischi supporta l'aggiunta simmetrica di shelf a una configurazione esistente.

Quando vengono aggiunti nuovi shelf, il sistema applica la stessa policy di assegnazione ai nuovi shelf aggiunti. Ad esempio, con un singolo shelf per sito, se viene aggiunto uno shelf aggiuntivo, i sistemi applicano le regole di assegnazione di un quarto di shelf al nuovo shelf.

### Informazioni correlate

["Componenti IP MetroCluster richiesti e convenzioni di denominazione"](#)

["Gestione di dischi e aggregati"](#)

### Differenze di assegnazione dei dischi e ADP in base al sistema nelle configurazioni IP MetroCluster

Il funzionamento della partizione avanzata dei dischi (ADP) e dell'assegnazione automatica dei dischi nelle configurazioni MetroCluster IP varia a seconda del modello di sistema.



Nei sistemi che utilizzano ADP, gli aggregati vengono creati utilizzando partizioni in cui ciascun disco viene partizionato nelle partizioni P1, P2 e P3. L'aggregato root viene creato utilizzando partizioni P3.

È necessario rispettare i limiti MetroCluster per il numero massimo di dischi supportati e altre linee guida.

["NetApp Hardware Universe"](#)


### Assegnazione di ADP e dischi sui sistemi AFF A320


Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
-------------	-----------------	-----------------------------------	-----------------------------------

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	<p>Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota.</p> <p><b>Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni</b></p> <ul style="list-style-type: none"> <li>• Otto partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	<p>Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni:</p> <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>

#### ADP e assegnazione dei dischi sui sistemi AFF A150, ASA A150 e AFF A220

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
-------------	-----------------	-----------------------------------	-----------------------------------

<p>Numero minimo di dischi consigliati (per sito)</p>	<p>Solo dischi interni</p>	<p>I dischi interni sono divisi in quattro gruppi uguali. Ciascun gruppo viene assegnato automaticamente a un pool separato e ciascun pool viene assegnato a un controller separato nella configurazione.</p> <div data-bbox="850 596 902 651">  </div> <p>Metà delle unità interne rimane non assegnata prima della configurazione di MetroCluster.</p>	<p>Due quarti sono utilizzati dalla coppia ha locale. Gli altri due quarti vengono utilizzati dalla coppia ha remota.</p> <p>L'aggregato root include le seguenti partizioni in ogni plex:</p> <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>
---	----------------------------	---	---

Numero minimo di dischi supportati (per sito)	16 dischi interni	<p>I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.</p> <p>Due quarti su uno shelf possono avere lo stesso pool. Il pool viene scelto in base al nodo proprietario del trimestre:</p> <ul style="list-style-type: none"> <li>• Se di proprietà del nodo locale, viene utilizzato pool0.</li> <li>• Se di proprietà del nodo remoto, viene utilizzato pool1.</li> </ul> <p>Ad esempio: Uno shelf con trimestri da Q1 a Q4 può avere le seguenti assegnazioni:</p> <ul style="list-style-type: none"> <li>• Q1: Pool Node_A_1 0</li> <li>• Q2: Pool Node_A_2 0</li> <li>• D3: Pool Node_B_1</li> <li>• D4:pool Node_B_2 1</li> </ul> <div>  <p>Metà delle unità interne rimane non assegnata prima della configurazione di MetroCluster.</p> </div>	<p>Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni:</p> <ul style="list-style-type: none"> <li>• Due partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Nessun ricambio</li> </ul>
---	-------------------	---	---

#### ADP e assegnazione dei dischi su sistemi AFF C250, AFF A250, ASA A250, ASA C250 e FAS500f

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
-------------	-----------------	-----------------------------------	-----------------------------------

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	<p>Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota.</p> <p>Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. L'aggregato root include le seguenti partizioni in ogni plex:</p> <ul style="list-style-type: none"> <li>• Otto partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>
Numero minimo di dischi supportati (per sito)	16 dischi interni	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	<p>Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni:</p> <ul style="list-style-type: none"> <li>• Due partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Nessuna partizione di riserva</li> </ul>

#### Assegnazione di ADP e dischi sui sistemi AFF A300

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
-------------	-----------------	-----------------------------------	-----------------------------------

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	<p>Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota.</p> <p>Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. L'aggregato root include le seguenti partizioni in ogni plex:</p> <ul style="list-style-type: none"> <li>• Otto partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	<p>Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni:</p> <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>

#### ADP e assegnazione dei dischi sui sistemi AFF C400, AFF A400, ASA C400 e ASA A400

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	<p>Ciascuno dei due plessi nell'aggregato root include:</p> <ul style="list-style-type: none"> <li>• 20 partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>



Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>
---	-----------	--	---

#### Assegnazione di ADP e dischi sui sistemi AFF A700

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Ciascuno dei due plessi nell'aggregato root include: <ul style="list-style-type: none"> <li>• 20 partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>

#### ADP e assegnazione dei dischi sui sistemi AFF C800, ASA C800, ASA A800 e AFF A800

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per aggregato root
-------------	-----------------	-----------------------------------	-------------------------------

Numero minimo di dischi consigliati (per sito)	Dischi interni e 96 dischi esterni	Le partizioni interne sono divise in quattro gruppi uguali (quarti). Ogni trimestre viene assegnato automaticamente a un pool separato. I dischi sugli shelf esterni vengono assegnati automaticamente shelf-by-shelf, con tutti i dischi su ogni shelf assegnati a uno dei quattro nodi nella configurazione MetroCluster.	<p>L'aggregato root viene creato con 12 partizioni root sullo shelf interno.</p> <p>Ciascuno dei due plessi nell'aggregato root include:</p> <ul style="list-style-type: none"> <li>• Otto partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>
Numero minimo di dischi supportati (per sito)	24 dischi interni	Le partizioni interne sono divise in quattro gruppi uguali (quarti). Ogni trimestre viene assegnato automaticamente a un pool separato.	<p>L'aggregato root viene creato con 12 partizioni root sullo shelf interno.</p> <p>Ciascuno dei due plessi nell'aggregato root include:</p> <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>

#### ADP e assegnazione dei dischi nei sistemi AFF A900 e ASA A900

Linee guida	Shelf per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	<p>Ciascuno dei due plessi nell'aggregato root include:</p> <ul style="list-style-type: none"> <li>• 20 partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Due partizioni di riserva</li> </ul>

Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: <ul style="list-style-type: none"> <li>• Tre partizioni per i dati</li> <li>• Due partizioni di parità</li> <li>• Una partizione di riserva</li> </ul>
---	-----------	--	---

#### Assegnazione dei dischi sui sistemi FAS2750

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	24 dischi interni e 24 dischi esterni	Gli shelf interni ed esterni sono divisi in due metà uguali. Ogni metà viene assegnata automaticamente a un pool diverso	Non applicabile
Numero minimo di dischi supportati (per sito) (configurazione ha attiva/passiva)	Solo dischi interni	Assegnazione manuale richiesta	Non applicabile

#### Assegnazione dei dischi sui sistemi FAS8200

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi sugli shelf esterni sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	Non applicabile
Numero minimo di dischi supportati (per sito) (configurazione ha attiva/passiva)	24 dischi	Assegnazione manuale richiesta.	Non applicabile

#### Assegnazione dei dischi sui sistemi FAS500f

Le stesse linee guida e regole per l'assegnazione dei dischi per i sistemi AFF C250 e AFF A250 si applicano ai sistemi FAS500f. Per l'assegnazione dei dischi nei sistemi FAS500f, fare riferimento alla [\[ADP\\_FAS500f\]](#) tabella.

### Assegnazione dei dischi sui sistemi FAS9000

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Non applicabile
Numero minimo di dischi supportati (per sito)	48 dischi	I dischi sugli shelf sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	Numero minimo di dischi supportati (per sito) (configurazione ha attiva/passiva)

### Assegnazione dei dischi sui sistemi FAS9500

Linee guida	Shelf per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Non applicabile
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Numero minimo di dischi supportati (per sito) (configurazione ha attiva/passiva)

## Peering dei cluster

Ogni sito MetroCluster viene configurato come peer del sito del partner. È necessario conoscere i prerequisiti e le linee guida per la configurazione delle relazioni di peering. Ciò è importante quando si decide se utilizzare porte condivise o dedicate per tali relazioni.

### Informazioni correlate

["Configurazione rapida del peering di cluster e SVM"](#)

### Prerequisiti per il peering del cluster

Prima di configurare il peering del cluster, è necessario verificare che la connettività tra porta, indirizzo IP, subnet, firewall e i requisiti di denominazione del cluster siano soddisfatti.

## Requisiti di connettività

Ogni LIF di intercluster sul cluster locale deve essere in grado di comunicare con ogni LIF di intercluster sul cluster remoto.

Sebbene non sia necessario, è in genere più semplice configurare gli indirizzi IP utilizzati per le LIF di intercluster nella stessa subnet. Gli indirizzi IP possono risiedere nella stessa sottorete dei file LIF dei dati o in una sottorete diversa. La subnet utilizzata in ciascun cluster deve soddisfare i seguenti requisiti:

- La subnet deve disporre di un numero sufficiente di indirizzi IP da allocare a un LIF intercluster per nodo.

Ad esempio, in un cluster a quattro nodi, la subnet utilizzata per la comunicazione tra cluster deve avere quattro indirizzi IP disponibili.

Ciascun nodo deve disporre di una LIF intercluster con un indirizzo IP sulla rete intercluster.

Le LIF di intercluster possono avere un indirizzo IPv4 o IPv6.



ONTAP 9 consente di migrare le reti peering da IPv4 a IPv6, consentendo la presenza simultanea di entrambi i protocolli nelle LIF dell'intercluster. Nelle versioni precedenti, tutte le relazioni tra cluster per un intero cluster erano IPv4 o IPv6. Ciò significava che la modifica dei protocolli era un evento potenzialmente disgregativo.

## Requisiti delle porte

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Le porte devono soddisfare i seguenti requisiti:

- Tutte le porte utilizzate per comunicare con un determinato cluster remoto devono trovarsi nello stesso IPspace.

È possibile utilizzare più IPspaces per eseguire il peer con più cluster. La connettività full-mesh a coppie è necessaria solo all'interno di un IPspace.

- Il dominio di broadcast utilizzato per la comunicazione tra cluster deve includere almeno due porte per nodo in modo che la comunicazione tra cluster possa eseguire il failover da una porta a un'altra.

Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).

- Tutte le porte devono essere cablate.
- Tutte le porte devono essere in buono stato.
- Le impostazioni MTU delle porte devono essere coerenti.

## Requisiti del firewall

I firewall e i criteri di firewall tra cluster devono consentire i seguenti protocolli:

- Servizio ICMP
- TCP agli indirizzi IP di tutte le LIF dell'intercluster sulle porte 10000, 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

Il criterio predefinito del firewall tra cluster consente l'accesso tramite il protocollo HTTPS e da tutti gli indirizzi

IP (0.0.0.0/0). Se necessario, è possibile modificare o sostituire la policy.

### **Considerazioni sull'utilizzo di porte dedicate**

Quando si determina se l'utilizzo di una porta dedicata per la replica tra cluster è la soluzione di rete tra cluster corretta, è necessario prendere in considerazione configurazioni e requisiti quali tipo di LAN, larghezza di banda WAN disponibile, intervallo di replica, velocità di modifica e numero di porte.

Considerare i seguenti aspetti della rete per determinare se l'utilizzo di una porta dedicata è la migliore soluzione di rete tra cluster:

- Se la quantità di larghezza di banda WAN disponibile è simile a quella delle porte LAN e l'intervallo di replica è tale che la replica si verifica quando esiste un'attività client regolare, è necessario dedicare le porte Ethernet alla replica tra cluster per evitare conflitti tra la replica e i protocolli dati.
- Se l'utilizzo della rete generato dai protocolli dati (CIFS, NFS e iSCSI) è tale che l'utilizzo della rete è superiore al 50%, dedicare le porte per la replica per consentire prestazioni non degradate in caso di failover di un nodo.
- Quando si utilizzano porte fisiche da 10 GbE o superiori per i dati e la replica, è possibile creare porte VLAN per la replica e dedicare le porte logiche per la replica tra cluster.

La larghezza di banda della porta è condivisa tra tutte le VLAN e la porta base.

- Considerare il tasso di cambiamento dei dati e l'intervallo di replica e se la quantità di dati, che devono essere replicati in ciascun intervallo, richiede una larghezza di banda sufficiente. Questo potrebbe causare conflitti con i protocolli dati se si condividono le porte dati.

### **Considerazioni sulla condivisione delle porte dati**

Quando si determina se la condivisione di una porta dati per la replica tra cluster è la soluzione di rete tra cluster corretta, è necessario prendere in considerazione configurazioni e requisiti quali tipo di LAN, larghezza di banda WAN disponibile, intervallo di replica, tasso di cambiamento e numero di porte.

Considerare i seguenti aspetti della rete per determinare se la condivisione delle porte dati è la migliore soluzione di connettività tra cluster:

- Per una rete ad alta velocità, ad esempio una rete 40-Gigabit Ethernet (40-GbE), potrebbe essere disponibile una quantità sufficiente di larghezza di banda LAN locale per eseguire la replica sulle stesse porte 40-GbE utilizzate per l'accesso ai dati.

In molti casi, la larghezza di banda WAN disponibile è di gran lunga inferiore alla larghezza di banda LAN a 10 GbE.

- Tutti i nodi del cluster potrebbero dover replicare i dati e condividere la larghezza di banda WAN disponibile, rendendo più accettabile la condivisione della porta dati.
- La condivisione delle porte per i dati e la replica elimina il numero di porte aggiuntive necessario per dedicare le porte alla replica.
- Le dimensioni massime dell'unità di trasmissione (MTU) della rete di replica saranno le stesse di quelle utilizzate sulla rete dati.
- Considerare il tasso di cambiamento dei dati e l'intervallo di replica e se la quantità di dati, che devono essere replicati in ciascun intervallo, richiede una larghezza di banda sufficiente. Questo potrebbe causare conflitti con i protocolli dati se si condividono le porte dati.
- Quando le porte dati per la replica tra cluster sono condivise, le LIF tra cluster possono essere migrate su

qualsiasi altra porta compatibile con gli intercluster sullo stesso nodo per controllare la porta dati specifica utilizzata per la replica.

## Requisiti ISL

### Panoramica dei requisiti ISL

È necessario verificare che la configurazione IP MetroCluster e la rete soddisfino tutti i requisiti ISL (Inter-Switch link). Sebbene alcuni requisiti potrebbero non essere applicabili alla configurazione in uso, è comunque necessario essere consapevoli di tutti i requisiti ISL per ottenere una migliore comprensione della configurazione complessiva.

La tabella seguente fornisce una panoramica degli argomenti trattati in questa sezione.

Titolo	Descrizione
"Switch NetApp validati e conformi a MetroCluster"	Descrive i requisiti dello switch.  Si applica a tutti gli switch utilizzati nelle configurazioni MetroCluster, compresi gli switch backend.
"Considerazioni per gli ISL"	Descrive i requisiti ISL.  Si applica a tutte le configurazioni MetroCluster, a prescindere dalla topologia di rete e dall'utilizzo di switch validati NetApp o switch conformi a MetroCluster.
"Considerazioni sulla distribuzione di MetroCluster in reti condivise a livello 2 o 3"	Vengono descritti i requisiti per le reti condivise di livello 2 o 3.  Valido per tutte le configurazioni, ad eccezione delle configurazioni MetroCluster che utilizzano switch validati NetApp e ISL connessi direttamente.
"Considerazioni sull'utilizzo di switch compatibili MetroCluster"	Descrive i requisiti per gli switch compatibili con MetroCluster.  Valido per tutte le configurazioni MetroCluster che non utilizzano switch validati NetApp.
"Esempi di topologie di rete MetroCluster"	Vengono forniti esempi di diverse topologie di rete MetroCluster.  Si applica a tutte le configurazioni MetroCluster.

### Switch NetApp validati e conformi a MetroCluster

Tutti gli switch utilizzati nella tua configurazione, inclusi gli switch backend, devono essere validati NetApp o conformi a MetroCluster.

#### Switch validati da NetApp

Uno switch è validato da NetApp se soddisfa i seguenti requisiti:

- Lo switch viene fornito da NetApp come parte della configurazione IP di MetroCluster
- L'interruttore è elencato nella "[NetApp Hardware Universe](#)" Come switch supportato in *MetroCluster-over-IP-Connections*
- Lo switch viene utilizzato solo per collegare controller IP MetroCluster e, in alcune configurazioni, shelf di

dischi NS224

- Lo switch viene configurato utilizzando il file di configurazione di riferimento (RCF) fornito da NetApp

Qualsiasi switch che non soddisfi questi requisiti non è **non** uno switch validato NetApp.

### Switch compatibili con MetroCluster

Uno switch MetroCluster-compliant non è convalidato da NetApp, ma può essere utilizzato in una configurazione MetroCluster IP se soddisfa determinati requisiti e linee guida di configurazione.



NetApp non offre servizi di supporto per la configurazione o il troubleshooting per gli switch non convalidati conformi a MetroCluster.

### Considerazioni per gli ISL

Gli ISL (Inter-Switch Links) che trasportano il traffico MetroCluster su tutte le configurazioni IP di MetroCluster e le topologie di rete hanno determinati requisiti. Questi requisiti si applicano a tutti gli ISL che trasportano traffico MetroCluster, indipendentemente dal fatto che gli ISL siano diretti o condivisi tra gli switch del cliente.

#### Requisiti generali dell'ISL MetroCluster

Quanto segue si applica agli ISL in tutte le configurazioni IP di MetroCluster:

- Entrambi i fabric devono avere lo stesso numero di ISL.
- Gli ISL su un fabric devono essere tutti della stessa velocità e lunghezza.
- Gli ISL in entrambi i fabric devono essere della stessa velocità e lunghezza.
- La differenza massima supportata di distanza tra il tessuto 1 e il tessuto 2 è 20km o 0,2ms.
- Gli ISL devono avere la stessa topologia. Ad esempio, dovrebbero essere tutti collegamenti diretti, o se la configurazione utilizza WDM, devono tutti utilizzare WDM.
- La velocità dell'ISL deve essere di almeno 10Gbps.
- Deve essere presente almeno una porta ISL 10Gbps per fabric.

### Limiti di latenza e perdita di pacchetti negli ISL

Quanto segue si applica al traffico di andata e ritorno tra gli switch IP MetroCluster presso il sito\_A e il sito\_B, con la configurazione MetroCluster in funzionamento stazionario:

- Con l'aumentare della distanza tra due siti MetroCluster, la latenza aumenta, di solito nell'intervallo di 1 ms di ritardo di andata e ritorno per 100 km (62 miglia). La latenza dipende anche dal contratto SLA (Service Level Agreement) della rete in termini di larghezza di banda dei collegamenti ISL, velocità di rilascio dei pacchetti e jitter sulla rete. La bassa larghezza di banda, il jitter elevato e le cadute di pacchetti casuali portano a meccanismi di ripristino differenti tramite gli interruttori, o il motore TCP sui moduli del controller, per una corretta consegna dei pacchetti. Questi meccanismi di recovery possono aumentare la latenza complessiva. Per informazioni specifiche sulla latenza di andata e ritorno e sui requisiti di distanza massima per la configurazione, fare riferimento a. "[Hardware Universe](#)."
- Qualsiasi dispositivo che contribuisca alla latenza deve essere considerato.
- Il "[Hardware Universe](#)." fornisce la distanza in km. Devi assegnare 1ms per ogni 100km. La distanza massima è definita dal raggiungimento del primo valore, ovvero dal tempo massimo di andata e



ritorno (RTT) in ms o dalla distanza in km Ad esempio, se *Hardware Universe* elenca una distanza di 300km, traducendo in 3ms, l'ISL non può essere superiore a 300km e l'RTT massimo non può superare 3ms, a seconda di quale delle due posizioni si raggiunge per prima.

- La perdita di pacchetti deve essere inferiore o uguale al 0,01%. La perdita massima di pacchetti è la somma di tutte le perdite su tutti i collegamenti sul percorso tra i nodi MetroCluster e la perdita sulle interfacce IP MetroCluster locali.
- Il valore di jitter supportato è 3ms per andata e ritorno (o 1,5ms per sola andata).
- La rete dovrebbe allocare e mantenere la quantità di larghezza di banda richiesta per il traffico MetroCluster, indipendentemente dai microbusti e dai picchi del traffico.
- Se si utilizza ONTAP 9,7 o versione successiva, la rete intermedia tra i due siti deve fornire una larghezza di banda minima di 4,5Gbps MHz per la configurazione dell'IP di MetroCluster.

#### Considerazioni sul ricetrasmittitore e sul cavo

Tutti gli SFP o i QSFP supportati dal fornitore dell'apparecchiatura sono supportati per gli MetroCluster ISL. I SFP e i QSFP forniti da NetApp o dal fornitore dell'apparecchiatura devono essere supportati dal firmware dello switch e dello switch.

Per il collegamento dei controller agli switch e agli ISL del cluster locale, è necessario utilizzare i ricetrasmittitori e i cavi forniti da NetApp con MetroCluster.

Quando si utilizza un adattatore QSFP-SFP, la configurazione della porta in modalità breakout o nativa dipende dal modello e dal firmware dello switch. Ad esempio, l'utilizzo di un adattatore QSFP-SFP con switch Cisco 9336C che eseguono il firmware NX-OS 9.x o 10.x richiede la configurazione della porta in modalità di velocità nativa.



Se si configura un RCF, verificare di aver selezionato la modalità di velocità corretta o di utilizzare una porta con una modalità di velocità appropriata.

#### Utilizzando dispositivi di crittografia xWDM, TDM e esterni

Quando si utilizzano dispositivi xWDM/TDM o dispositivi che forniscono la crittografia in una configurazione MetroCluster IP, l'ambiente deve soddisfare i seguenti requisiti:

- Quando si collegano gli switch IP MetroCluster a xWDM/TDM, i dispositivi di crittografia esterni o le apparecchiature xWDM/TDM devono essere certificati dal fornitore per lo switch e il firmware. La certificazione deve riguardare la modalità operativa (ad esempio trunking e crittografia).
- La latenza e il jitter end-to-end complessivi, inclusa la crittografia, non possono superare la quantità massima indicata nel IMT e nella presente documentazione.

#### Numero di ISL e cavi di breakout supportati

La tabella seguente mostra il numero massimo di ISL supportati che è possibile configurare su uno switch IP MetroCluster utilizzando la configurazione del file di configurazione di riferimento (RCF).

Modello di switch IP MetroCluster	Tipo di porta	Numero massimo di ISL
Switch BES-53248 supportati da Broadcom	Porte native	4 ISL utilizzando 10Gbps o 25Gbps

Switch BES-53248 supportati da Broadcom	Porte native (Nota 1)	2 ISL utilizzando 40Gbps o 100Gbps
Cisco 3132Q-V.	Porte native	6 ISL utilizzando 40Gbps
Cisco 3132Q-V.	Cavi di breakout	16 ISL utilizzando 10Gbps
Cisco 3232C	Porte native	6 ISL utilizzando 40Gbps o 100Gbps
Cisco 3232C	Cavi di breakout	16 ISL utilizzando 10Gbps
Cisco 9336C-FX2 (non collegato agli shelf NS224)	Porte native	6 ISL utilizzando 40Gbps o 100Gbps
Cisco 9336C-FX2 (non collegato agli shelf NS224)	Cavi di breakout	16 ISL utilizzando 10
Cisco 9336C-FX2 (collegamento di shelf NS224)	Porte native (Nota 2)	4 ISL utilizzando 40Gbps o 100Gbps
Cisco 9336C-FX2 (collegamento di shelf NS224)	Cavi di breakout (Nota 2)	16 ISL utilizzando 10Gbps
NVIDIA SN2100	Porte native (Nota 2)	2 ISL utilizzando 40Gbps o 100Gbps
NVIDIA SN2100	Cavi di breakout (Nota 2)	8 ISL utilizzando 10Gbps o 25Gbps

**Nota 1:** L'utilizzo di ISL 40Gbps o 100Gbps su uno switch BES-53248 richiede una licenza aggiuntiva.

**Nota 2:** Le stesse porte vengono utilizzate per la velocità nativa e la modalità breakout. È necessario scegliere di utilizzare le porte in modalità velocità nativa o breakout quando si crea il file RCF.

- Tutti gli ISL su uno switch IP MetroCluster devono essere alla stessa velocità. Non è supportato l'utilizzo contemporaneo di una combinazione di porte ISL con velocità diverse.
- Per ottenere prestazioni ottimali, è consigliabile utilizzare almeno un ISL da 40Gbps GB per rete. Non utilizzare un unico ISL 10Gbps per rete per FAS9000, AFF A700 o altre piattaforme ad alta capacità.



NetApp consiglia di configurare un numero ridotto di ISL a elevata larghezza di banda piuttosto che un numero elevato di ISL a bassa larghezza di banda. Ad esempio, è preferibile configurare un ISL 40Gbps invece di quattro ISL 10Gbps. Quando si utilizzano più ISL, il bilanciamento statistico del carico può influire sulla velocità massima. Un bilanciamento non uniforme può ridurre la capacità di trasmissione a quella di un singolo ISL.

### Considerazioni sulla distribuzione di MetroCluster in reti condivise di livello 2 o 3

A seconda dei requisiti, è possibile utilizzare reti condivise di livello 2 o 3 per

## implementare MetroCluster.

A partire da ONTAP 9.6, le configurazioni IP MetroCluster con switch Cisco supportati possono condividere le reti esistenti per i collegamenti interswitch (ISL) invece di utilizzare ISL MetroCluster dedicati. Questa topologia è nota come *reti Layer 2 condivise*.

A partire da ONTAP 9.9.1, le configurazioni IP MetroCluster possono essere implementate con connessioni backend con routing IP (Layer 3). Questa topologia è nota come *reti Layer 3 condivise*.



- È necessario verificare che la capacità di rete sia adeguata e che le dimensioni dell'ISL siano appropriate per la configurazione in uso. La bassa latenza è fondamentale per la replica dei dati tra i siti MetroCluster. I problemi di latenza su queste connessioni possono influire sull'i/o del client
- Tutti i riferimenti agli switch back-end MetroCluster fanno riferimento a switch validati NetApp o conformi a MetroCluster. Vedere ["Switch NetApp validati e conformi a MetroCluster"](#) per ulteriori dettagli.

### Requisiti ISL per le reti Layer 2 e Layer 3

Quanto segue si applica alle reti di livello 2 e 3:

- La velocità e il numero di ISL tra gli switch MetroCluster e gli switch di rete intermedi non devono corrispondere. Analogamente, la velocità tra i commutatori di rete intermedi non deve corrispondere.

Ad esempio, gli switch MetroCluster possono connettersi agli switch intermedi utilizzando un ISL 40Gbps, mentre gli switch intermedi possono collegarsi tra loro utilizzando due ISL 100Gbps.

- Il monitoraggio della rete deve essere configurato sulla rete intermedia in modo da monitorare gli ISL per l'utilizzo, gli errori (cadute, flap di collegamento, danneggiamento e così via), e guasti.
- La dimensione MTU deve essere impostata su 9216 su tutte le porte che trasportano il traffico MetroCluster end-to-end.
- Nessun altro traffico può essere configurato con una priorità maggiore rispetto alla classe di servizio (COS) 5.
- La notifica di congestione esplicita (ECN) deve essere configurata su tutti i percorsi che trasportano traffico MetroCluster end-to-end.
- Gli ISL che trasportano traffico MetroCluster devono essere collegamenti nativi tra gli switch.

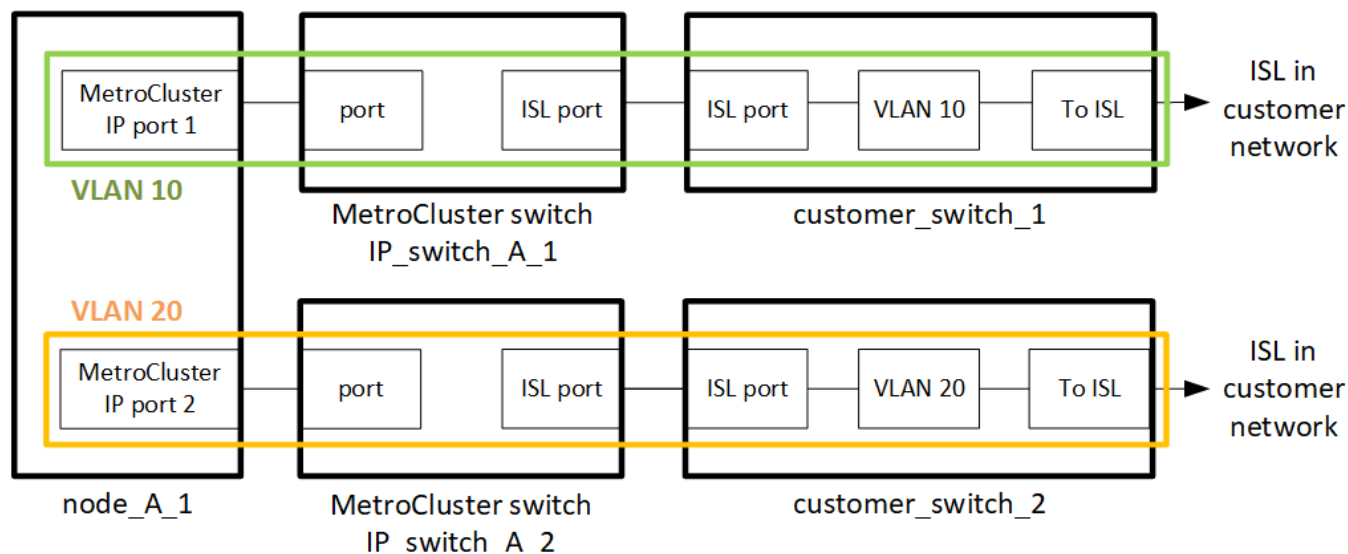
I servizi di condivisione dei collegamenti, ad esempio i collegamenti MPLS (MultiProtocol Label Switching), non sono supportati.

- Le VLAN di livello 2 devono estendersi in modo nativo sui siti. L'overlay VLAN come Virtual Extensible LAN (VXLAN) non è supportato.
- Il numero di interruttori intermedi non è limitato. Tuttavia, NetApp consiglia di mantenere il numero di switch al minimo richiesto.
- Gli ISL sugli switch MetroCluster sono configurati con le seguenti opzioni:
  - Commutare la modalità 'trunk' come parte di un canale-porta LACP
  - La dimensione MTU è 9216
  - Nessuna VLAN nativa configurata
  - Sono consentite solo VLAN con traffico MetroCluster cross-site

- La VLAN predefinita dello switch non è consentita

## Considerazioni per le reti di livello 2

Gli switch backend MetroCluster sono collegati alla rete del cliente.



Gli switch intermedi forniti dal cliente devono soddisfare i seguenti requisiti:

- La rete intermedia deve fornire le stesse VLAN tra i siti. Deve corrispondere alle VLAN MetroCluster impostate nel file RCF.
- RcfFileGenerator non consente la creazione di un file RCF utilizzando VLAN non supportate dalla piattaforma.
- RcfFileGenerator potrebbe limitare l'uso di determinati ID VLAN, ad esempio, se destinati ad un uso futuro. In genere, le VLAN riservate sono fino a 100 incluse.
- Le VLAN di livello 2 con ID corrispondenti agli ID VLAN MetroCluster devono estendersi sulla rete condivisa.

## Configurazione VLAN in ONTAP

È possibile specificare la VLAN solo durante la creazione dell'interfaccia. Una volta create le interfacce MetroCluster, l'ID VLAN non può essere modificato. È possibile configurare altre VLAN durante la creazione dell'interfaccia, ma devono essere comprese nell'intervallo da 10 a 20 o nell'intervallo da 101 a 4096 (o nel numero supportato dal fornitore dello switch, a seconda del numero più basso).



Alcuni fornitori di switch potrebbero riservare l'uso di determinate VLAN.

I seguenti sistemi non richiedono la configurazione VLAN all'interno di ONTAP. La VLAN viene specificata dalla configurazione della porta dello switch:

- FAS8200 e AFF A300
- AFF A320
- FAS9000 e AFF A700
- AFF A800, ASA A800, AFF C800 e ASA C800



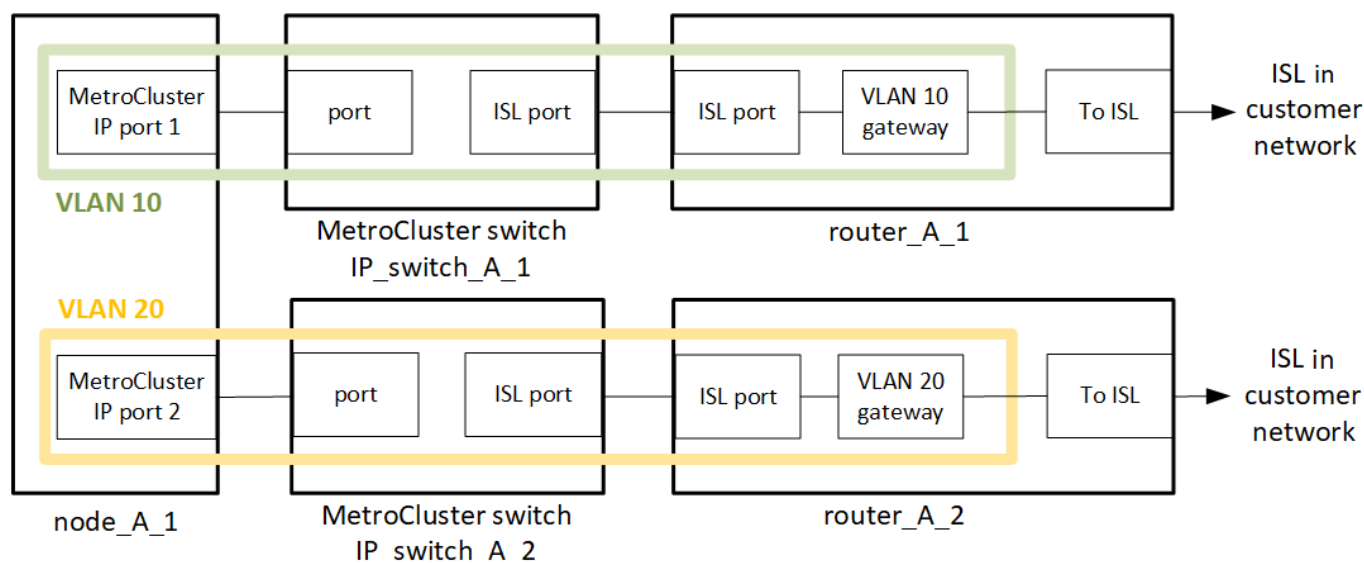
I sistemi sopra elencati potrebbero essere configurati utilizzando VLAN 100 e versioni successive. Tuttavia, alcune VLAN in questo intervallo potrebbero essere riservate ad altri o ad uso futuro.

Per tutti gli altri sistemi, è necessario configurare la VLAN quando si creano le interfacce MetroCluster in ONTAP. Si applicano le seguenti restrizioni:

- La VLAN predefinita è 10 e 20
- Se si esegue ONTAP 9,7 o versioni precedenti, è possibile utilizzare solo le VLAN 10 e 20 predefinite.
- Se si esegue ONTAP 9,8 o versioni successive, è possibile utilizzare la VLAN predefinita 10 e 20 e una VLAN su 100 (101 e versioni successive).

### Considerazioni per le reti di livello 3

Gli switch backend MetroCluster sono collegati alla rete IP instradata, direttamente ai router (come illustrato nell'esempio semplificato seguente) o tramite altri switch interventistici.



L'ambiente MetroCluster viene configurato e cabloato come configurazione standard IP MetroCluster, come descritto in "[Configurare i componenti hardware di MetroCluster](#)". Quando si esegue la procedura di installazione e cablaggio, è necessario eseguire i passaggi specifici per una configurazione di livello 3. Quanto segue si applica alle configurazioni di livello 3:

- È possibile collegare gli switch MetroCluster direttamente al router o a uno o più switch che intervengono.
- È possibile collegare le interfacce IP MetroCluster direttamente al router o a uno dei principali switch.
- La VLAN deve essere estesa al dispositivo gateway.
- Si utilizza `-gateway parameter` Configurare l'indirizzo dell'interfaccia IP MetroCluster con un indirizzo gateway IP.
- Gli ID VLAN per le VLAN MetroCluster devono essere gli stessi in ogni sito. Tuttavia, le subnet possono essere diverse.
- Il routing dinamico non è supportato per il traffico MetroCluster.
- Le seguenti funzioni non sono supportate:
  - Configurazioni MetroCluster a otto nodi

- Aggiornamento di una configurazione MetroCluster a quattro nodi
- Transizione da MetroCluster FC a MetroCluster IP
- Su ciascun sito MetroCluster sono necessarie due subnet, una per ogni rete.
- L'assegnazione Auto-IP non è supportata.

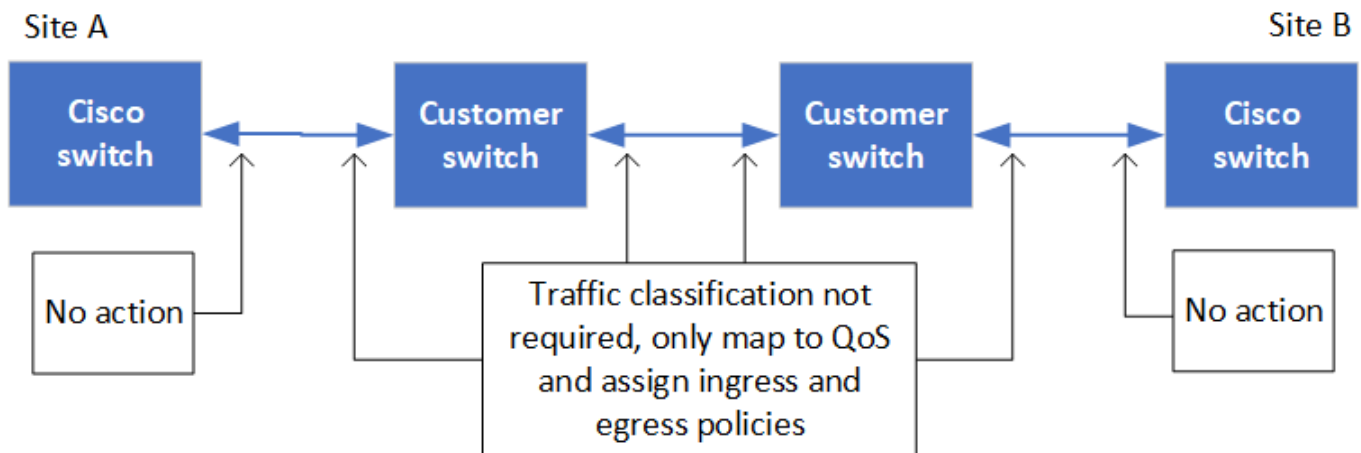
Quando si configurano gli indirizzi IP dei router e dei gateway, sono necessari i seguenti requisiti:

- Due interfacce su un nodo non possono avere lo stesso indirizzo IP del gateway.
- Le interfacce corrispondenti sulle coppie ha su ciascun sito devono avere lo stesso indirizzo IP del gateway.
- Le interfacce corrispondenti su un nodo e i relativi partner DR e AUX non possono avere lo stesso indirizzo IP del gateway.
- Le interfacce corrispondenti su un nodo e i relativi partner DR e AUX devono avere lo stesso ID VLAN.

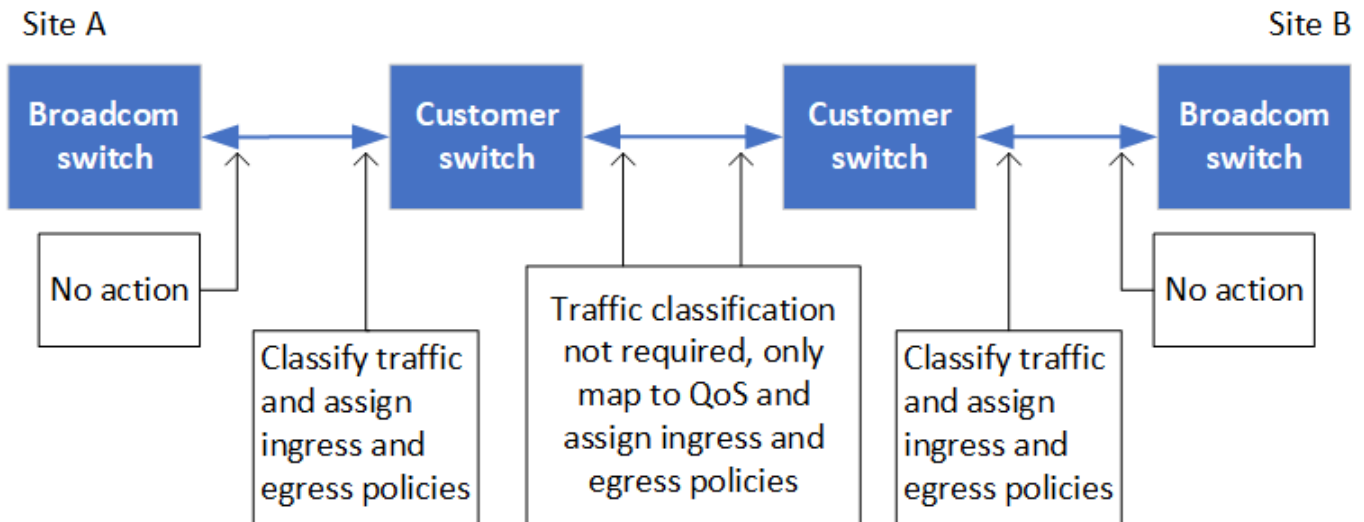
#### Impostazioni richieste per gli interruttori intermedi

Quando il traffico MetroCluster attraversa un ISL in una rete intermedia, è necessario verificare che la configurazione degli switch intermedi assicuri che il traffico MetroCluster (RDMA e storage) soddisfi i livelli di servizio richiesti attraverso l'intero percorso tra i siti MetroCluster.

Il seguente diagramma fornisce una panoramica delle impostazioni richieste quando si utilizzano gli switch Cisco convalidati da NetApp:



Il diagramma seguente offre una panoramica delle impostazioni richieste per una rete condivisa quando gli switch esterni sono switch Broadcom IP.



In questo esempio, vengono creati i seguenti criteri e mappe per il traffico MetroCluster:

- Il `MetroClusterIP_ISL_Ingress` I criteri vengono applicati alle porte dello switch intermedio che si connette agli switch IP MetroCluster.

Il `MetroClusterIP_ISL_Ingress` il criterio associa il traffico con tag in entrata alla coda appropriata sullo switch intermedio.

- `R MetroClusterIP_ISL_Egress` Il criterio viene applicato alle porte dello switch intermedio che si collegano agli ISL tra switch intermedi.
- È necessario configurare gli switch intermedi con mappe di accesso QoS, mappe di classe e policy corrispondenti lungo il percorso tra gli switch IP di MetroCluster. Gli switch intermedi mappano il traffico RDMA su COS5 e il traffico di storage su COS4.

I seguenti esempi si riferiscono agli switch Cisco Nexus 3232C e 9336C-FX2. A seconda del fornitore e del modello dello switch, è necessario verificare che la configurazione degli switch intermedi sia appropriata.

### Configurare la mappa delle classi per la porta ISL dello switch intermedio

Nell'esempio seguente vengono illustrate le definizioni della mappa delle classi a seconda che sia necessario classificare o far corrispondere il traffico in ingresso.

### **Classificare il traffico in ingresso:**

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

### **Corrispondenza del traffico all'ingresso:**

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

### **Creare una mappa dei criteri di ingresso sulla porta ISL dello switch intermedio:**

Gli esempi seguenti mostrano come creare una mappa dei criteri di ingresso a seconda che sia necessario classificare o far corrispondere il traffico in ingresso.



**Classificare il traffico in ingresso:**

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

**Far corrispondere il traffico all'ingresso:**

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

**Configurare il criterio di accodamento in uscita per le porte ISL**

Nell'esempio seguente viene illustrato come configurare il criterio di accodamento in uscita:

```

policy-map type queuing MetroClusterIP_ISL_Egress
  class type queuing c-out-8q-q7
    priority level 1
  class type queuing c-out-8q-q6
    priority level 2
  class type queuing c-out-8q-q5
    priority level 3
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q4
    priority level 4
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q3
    priority level 5
  class type queuing c-out-8q-q2
    priority level 6
  class type queuing c-out-8q-q1
    priority level 7
  class type queuing c-out-8q-q-default
    bandwidth remaining percent 100
    random-detect threshold burst-optimized ecn

```

Queste impostazioni devono essere applicate a tutti gli switch e agli ISL che trasportano traffico MetroCluster.

In questo esempio, Q4 e Q5 sono configurati con `random-detect threshold burst-optimized ecn`. A seconda della configurazione, potrebbe essere necessario impostare le soglie minima e massima, come illustrato nell'esempio seguente:

```

class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
  kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
  kbytes drop-probability 0 weight 0 ecn

```



I valori minimi e massimi variano a seconda dello switch e delle esigenze.

### Esempio 1: Cisco

Se la configurazione in uso dispone di switch Cisco, non è necessario classificarli sulla prima porta di ingresso dello switch intermedio. Quindi, configurare le mappe e i criteri seguenti:

- `class-map type qos match-any c5`
- `class-map type qos match-any c4`

- MetroClusterIP\_ISL\_Ingress\_Match

Viene assegnato il MetroClusterIP\_ISL\_Ingress\_Match Policy map ai porti ISL che trasportano il traffico MetroCluster.

### Esempio 2: Broadcom

Se la configurazione in uso dispone di switch Broadcom, è necessario classificarli sulla prima porta di ingresso dello switch intermedio. Quindi, configurare le mappe e i criteri seguenti:

- ip access-list rdma
- ip access-list storage
- class-map type qos match-all rdma
- class-map type qos match-all storage
- MetroClusterIP\_ISL\_Ingress\_Classify
- MetroClusterIP\_ISL\_Ingress\_Match

Assegnato dall'utente the MetroClusterIP\_ISL\_Ingress\_Classify Mappa dei criteri alle porte ISL sullo switch intermedio che collega lo switch Broadcom.

Viene assegnato il MetroClusterIP\_ISL\_Ingress\_Match La policy viene associata alle porte ISL sullo switch intermedio che trasporta il traffico MetroCluster ma non collega lo switch Broadcom.

### Considerazioni sull'utilizzo di switch compatibili con MetroCluster

#### Requisiti e limitazioni quando si utilizzano switch compatibili con MetroCluster

A partire da ONTAP 9.7, le configurazioni IP di MetroCluster possono utilizzare switch compatibili con MetroCluster. Si tratta di switch non validati da NetApp ma conformi alle specifiche NetApp. Tuttavia, NetApp non fornisce servizi di supporto per la risoluzione dei problemi o la configurazione per nessuno switch non convalidato. È necessario conoscere i requisiti e le limitazioni generali quando si utilizzano gli switch conformi a MetroCluster.

#### Requisiti generali per gli switch compatibili con MetroCluster

Lo switch che collega le interfacce IP MetroCluster deve soddisfare i seguenti requisiti generali:

- Gli switch devono supportare la qualità del servizio (QoS) e la classificazione del traffico.
- Gli switch devono supportare la notifica esplicita di congestione (ECN).
- Gli switch devono supportare una policy di bilanciamento del carico per mantenere l'ordine lungo il percorso.
- Gli switch devono supportare il controllo di flusso L2 (L2FC).
- La porta dello switch deve fornire una velocità dedicata e non deve essere sovraallocata.
- I cavi e i transceiver che collegano i nodi agli switch devono essere forniti da NetApp. Questi cavi devono essere supportati dal fornitore dello switch. Se si utilizza un cablaggio ottico, il ricetrasmittitore nello switch potrebbe non essere fornito da NetApp. È necessario verificare che sia compatibile con il ricetrasmittitore nel controller.

- Gli switch che collegano i nodi MetroCluster possono supportare traffico non MetroCluster.
- Solo le piattaforme che forniscono porte dedicate per le interconnessioni cluster senza switch possono essere utilizzate con uno switch compatibile con MetroCluster. Le piattaforme come FAS2750 e AFF A220 non possono essere utilizzate perché il traffico MetroCluster e il traffico di interconnessione MetroCluster condividono le stesse porte di rete.
- Lo switch compatibile con MetroCluster non deve essere utilizzato per le connessioni cluster locali.
- L'interfaccia IP di MetroCluster può essere collegata a qualsiasi porta dello switch che può essere configurata per soddisfare i requisiti.
- Sono necessari quattro switch IP, due per ciascun fabric dello switch. Se si utilizzano i director, è possibile utilizzare un singolo director su ciascun lato, ma le interfacce IP di MetroCluster devono connettersi a due diversi blade in due diversi domini di errore di tale director.
- Le interfacce MetroCluster da un nodo devono connettersi a due blade o switch di rete. Le interfacce MetroCluster di un nodo non possono essere connesse alla stessa rete, switch o blade.
- La rete deve soddisfare i requisiti indicati nelle seguenti sezioni:
  - ["Considerazioni per gli ISL"](#)
  - ["Considerazioni sulla distribuzione di MetroCluster in reti condivise di livello 2 o 3"](#)
- L'unità di trasmissione massima (MTU) di 9216 deve essere configurata su tutti gli switch che trasportano traffico IP MetroCluster.
- Il ripristino di ONTAP 9,6 o versioni precedenti non è supportato.

Tutti gli switch intermedi utilizzati tra gli switch che collegano le interfacce IP MetroCluster in entrambi i siti devono soddisfare i requisiti e devono essere configurati come descritto nella ["Considerazioni sulla distribuzione di MetroCluster in reti condivise di livello 2 o 3"](#).

### Limitazioni relative all'utilizzo di switch compatibili con MetroCluster

Non è possibile utilizzare alcuna configurazione o funzione che richieda che le connessioni del cluster locale siano connesse a uno switch. Ad esempio, non è possibile utilizzare le seguenti configurazioni e procedure con uno switch conforme a MetroCluster:

- Configurazioni MetroCluster a otto nodi
- Transizione da configurazioni MetroCluster FC a MetroCluster IP
- Aggiornamento di una configurazione IP MetroCluster a quattro nodi
- Piattaforme che condividono un'interfaccia fisica per il cluster locale e il traffico MetroCluster. Fare riferimento a ["Velocità di rete specifiche della piattaforma e modalità di porta dello switch per switch compatibili con MetroCluster"](#) per le velocità supportate.

### Velocità di rete specifiche della piattaforma e modalità di porta dello switch per switch compatibili con MetroCluster

Se si utilizzano switch compatibili MetroCluster, è necessario conoscere le velocità di rete specifiche della piattaforma e i requisiti della modalità porta dello switch.

La tabella seguente fornisce velocità di rete specifiche per piattaforma e modalità di porte switch per gli switch compatibili con MetroCluster. È necessario configurare la modalità della porta dello switch in base alla tabella.



Valori mancanti indicano che la piattaforma non può essere utilizzata con uno switch compatibile con MetroCluster.

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-

#### Esempi di configurazione delle porte dello switch

Informazioni sulle varie configurazioni delle porte dello switch.



Gli esempi seguenti utilizzano i valori decimali e seguono la tabella relativa agli switch Cisco. A seconda del fornitore dello switch, potrebbero essere necessari valori diversi per DSCP. Fare riferimento alla tabella corrispondente del fornitore dello switch per verificare il valore corretto.

Valore DSCP	Decimale	ESA	Significato
101 000	16	0x10	CS2
011 000	24	0x18	CS3

100 000	32	0x20	CS4
101 000	40	0x28	CS5

### Porta dello switch che collega un'interfaccia MetroCluster

- Classificazione per il traffico RDMA (Remote Direct Memory Access):
  - Corrispondenza: Porta TCP 10006, origine, destinazione o entrambe
  - Abbinamento facoltativo: COS 5
  - Abbinamento facoltativo: DSCP 40
  - Impostare DSCP 40
  - Impostare COS 5
  - Opzionale : regolazione della velocità a 20Gbps
- Classificazione per il traffico iSCSI:
  - Corrispondenza: Porta TCP 62500, origine, destinazione o entrambe
  - Abbinamento facoltativo: COS 4
  - Abbinamento facoltativo: DSCP 32
  - Impostare DSCP 32
  - Impostare COS 4
- L2FlowControl (pausa), RX e TX

### Porte ISL

- Classificazione:
  - Corrispondenza con COS 5 o DSCP 40
    - Impostare DSCP 40
    - Impostare COS 5
  - Corrispondenza con COS 4 o DSCP 32
    - Impostare DSCP 32
    - Impostare COS 4
- Uscita in coda
  - Il gruppo COS 4 ha una soglia di configurazione minima di 2000 e una soglia massima di 3000
  - Il gruppo COS 5 ha una soglia di configurazione minima di 3500 e una soglia massima di 6500.



Le soglie di configurazione possono variare a seconda dell'ambiente. È necessario valutare le soglie di configurazione in base al proprio ambiente.

- ECN abilitato per Q4 e Q5
- ROSSO abilitato per Q4 e Q5

### Allocazione della larghezza di banda (porte switch che collegano interfacce MetroCluster e porte ISL)

- RDMA, COS 5 / DSCP 40: 60%

- iSCSI, COS 4/DSCP 32: 40%
- Requisito di capacità minima per rete e configurazione MetroCluster: 10Gbps



Se si utilizzano i limiti di velocità, il traffico dovrebbe essere **modellato** senza introdurre perdite.

## Esempi di configurazione delle porte dello switch che collegano il controller MetroCluster

I comandi di esempio forniti sono validi per gli switch Cisco NX3232 o Cisco NX9336. I comandi variano a seconda del tipo di interruttore.

Se sullo switch non è disponibile una funzione o un suo equivalente, come illustrato negli esempi, lo switch non soddisfa i requisiti minimi e non può essere utilizzato per implementare una configurazione MetroCluster. Questo vale per qualsiasi switch collegato a una configurazione MetroCluster e per tutti gli switch intermedi.



Gli esempi seguenti potrebbero mostrare solo la configurazione di una rete.

### Configurazione di base

È necessario configurare una LAN virtuale (VLAN) in ciascuna rete. Nell'esempio seguente viene illustrato come configurare una VLAN nella rete 10.

#### Esempio:

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

#### Esempio:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

## Esempi di configurazione della classificazione

È necessario configurare le mappe di accesso e di classe per mappare il traffico RDMA e iSCSI alle classi appropriate.

Nell'esempio seguente, tutto il traffico TCP da e verso la porta 65200 viene mappato alla classe di archiviazione (iSCSI). Tutto il traffico TCP da e verso la porta 10006 viene mappato alla classe RDMA. Queste mappe dei criteri vengono utilizzate sulle porte dello switch che collegano le interfacce MetroCluster.

#### Esempio:

```

ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
  match access-group name rdma

```

È necessario configurare un criterio di ingresso. Un criterio di ingresso mappa il traffico come classificato in diversi gruppi COS. In questo esempio, il traffico RDMA viene mappato al gruppo COS 5 e il traffico iSCSI al gruppo COS 4. Il criterio di ingresso viene utilizzato sulle porte degli switch che collegano le interfacce MetroCluster e sulle porte ISL che trasportano il traffico MetroCluster.

#### **Esempio:**

```

policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4

```

NetApp consiglia di modellare il traffico sulle porte dello switch che collegano un'interfaccia MetroCluster, come illustrato nell'esempio seguente:

#### **Esempio:**



```

policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn

```

### Esempi di configurazione delle porte di nodo

Potrebbe essere necessario configurare una porta di nodo in modalità breakout. Nell'esempio seguente, le porte 25 e 26 sono configurate in modalità breakout 4 x 25Gbps.

#### Esempio:

```

interface breakout module 1 port 25-26 map 25g-4x

```

Potrebbe essere necessario configurare la velocità della porta dell'interfaccia MetroCluster. L'esempio seguente mostra come configurare la velocità su **auto** o in modalità 40Gbps:

#### Esempio:

```

speed auto

speed 40000

```

L'esempio seguente mostra una porta dello switch configurata per collegare un'interfaccia MetroCluster. Si tratta di una porta in modalità di accesso nella VLAN 10, con un valore MTU di 9216 e che funziona alla velocità nativa. Ha il controllo di flusso simmetrico (invio e ricezione) (pausa) abilitato e i criteri di ingresso e uscita MetroCluster assegnati.

#### Esempio:

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown
```

Sulle porte 25Gbps, potrebbe essere necessario impostare l'opzione Forward Error Correction (FEC) su "Off", come illustrato nell'esempio seguente.

#### Esempio:

```
fec off
```

### Esempi di configurazione delle porte ISL in tutta la rete

Uno switch conforme a MetroCluster viene considerato uno switch intermedio anche se connette direttamente le interfacce MetroCluster. Le porte ISL che trasportano traffico MetroCluster sullo switch compatibile con MetroCluster devono essere configurate nello stesso modo delle porte ISL su uno switch intermedio. Fare riferimento a ["Impostazioni richieste sugli switch intermedi"](#) per indicazioni ed esempi.



Alcune mappe dei criteri sono identiche per le porte degli switch che collegano interfacce MetroCluster e ISL che trasportano traffico MetroCluster. È possibile utilizzare la stessa mappa dei criteri per entrambi questi utilizzi di porte.

### Esempi di topologie di rete MetroCluster

A partire da ONTAP 9,6, sono supportate alcune configurazioni di rete aggiuntive per le configurazioni IP di MetroCluster. In questa sezione vengono forniti alcuni esempi delle configurazioni di rete supportate. Non sono elencate tutte le topologie supportate.

In queste topologie, si ipotizza che la rete ISL e intermedia sia configurata secondo i requisiti indicati nella ["Considerazioni per gli ISL"](#).

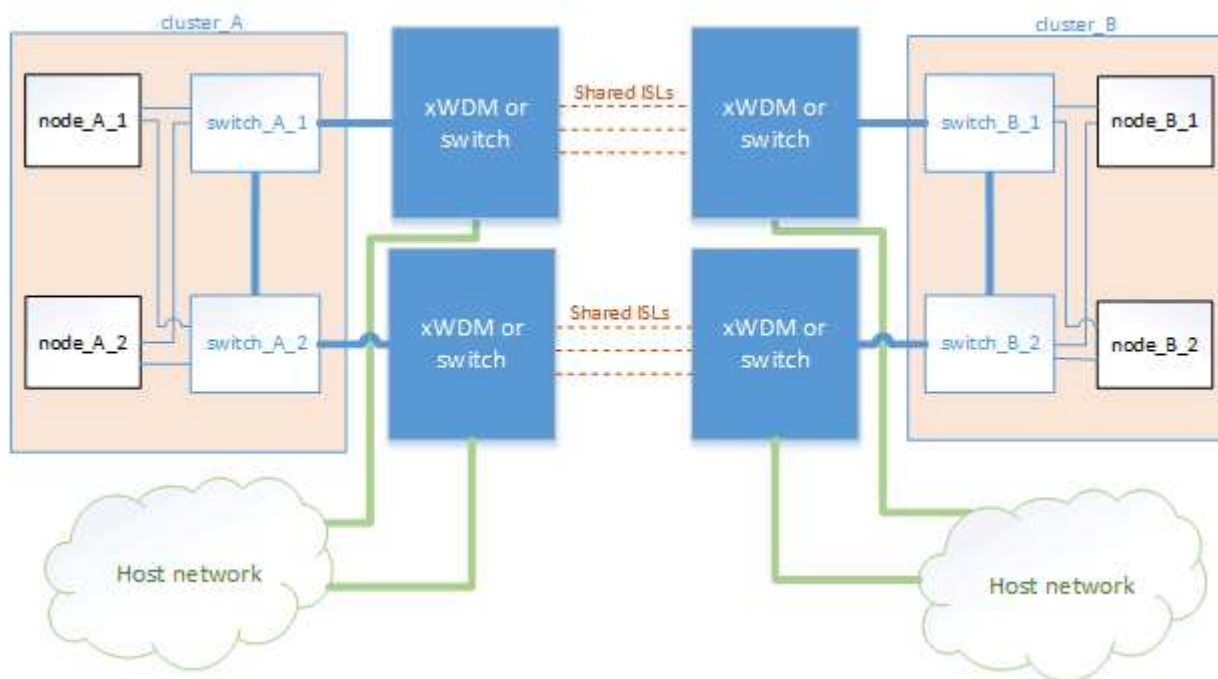


Se si condivide un ISL con traffico non MetroCluster, è necessario verificare che MetroCluster disponga sempre della larghezza di banda minima richiesta.

### Configurazione di rete condivisa con collegamenti diretti

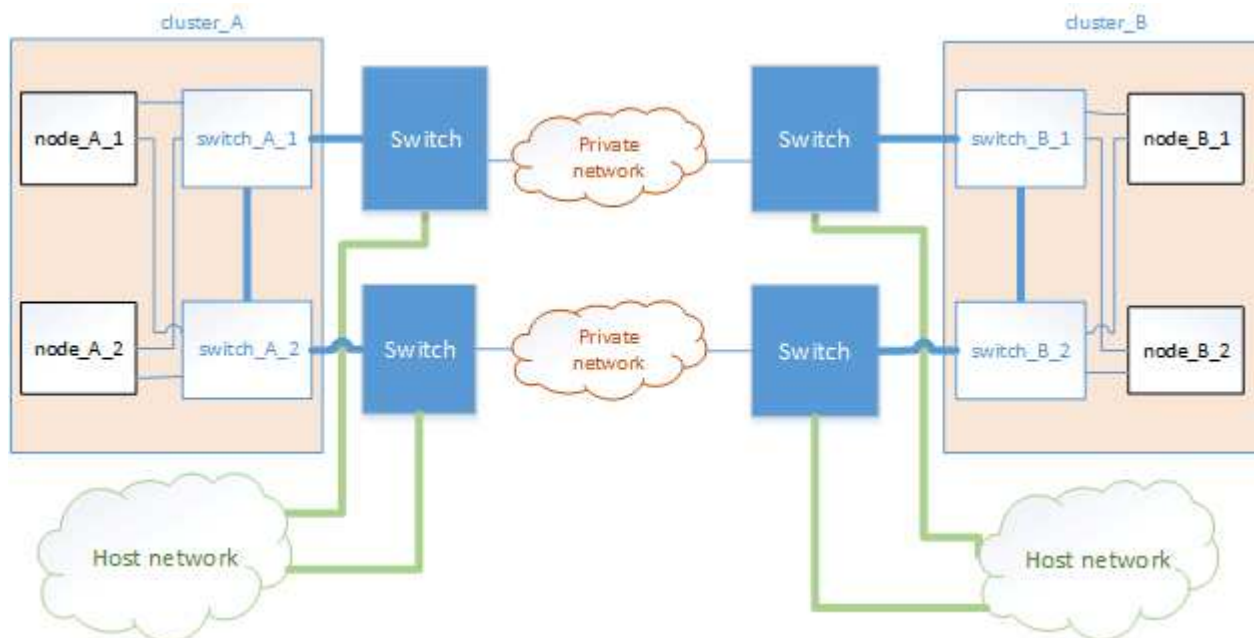
In questa topologia, due siti distinti sono collegati da collegamenti diretti. Questi collegamenti possono essere tra dispositivi o switch xWDM e TDM. La capacità degli ISL non è dedicata al traffico MetroCluster, ma è

condivisa con altro traffico non MetroCluster.



#### Infrastruttura condivisa con reti intermedie

In questa topologia, i siti MetroCluster non sono collegati direttamente, ma MetroCluster e il traffico host viaggiano attraverso una rete. La rete può essere costituita da una serie di xWDM e TDM e switch, ma a differenza della configurazione condivisa con ISL diretti, i collegamenti non sono diretti tra i siti. A seconda dell'infrastruttura tra i siti, è possibile utilizzare qualsiasi combinazione di configurazioni di rete.

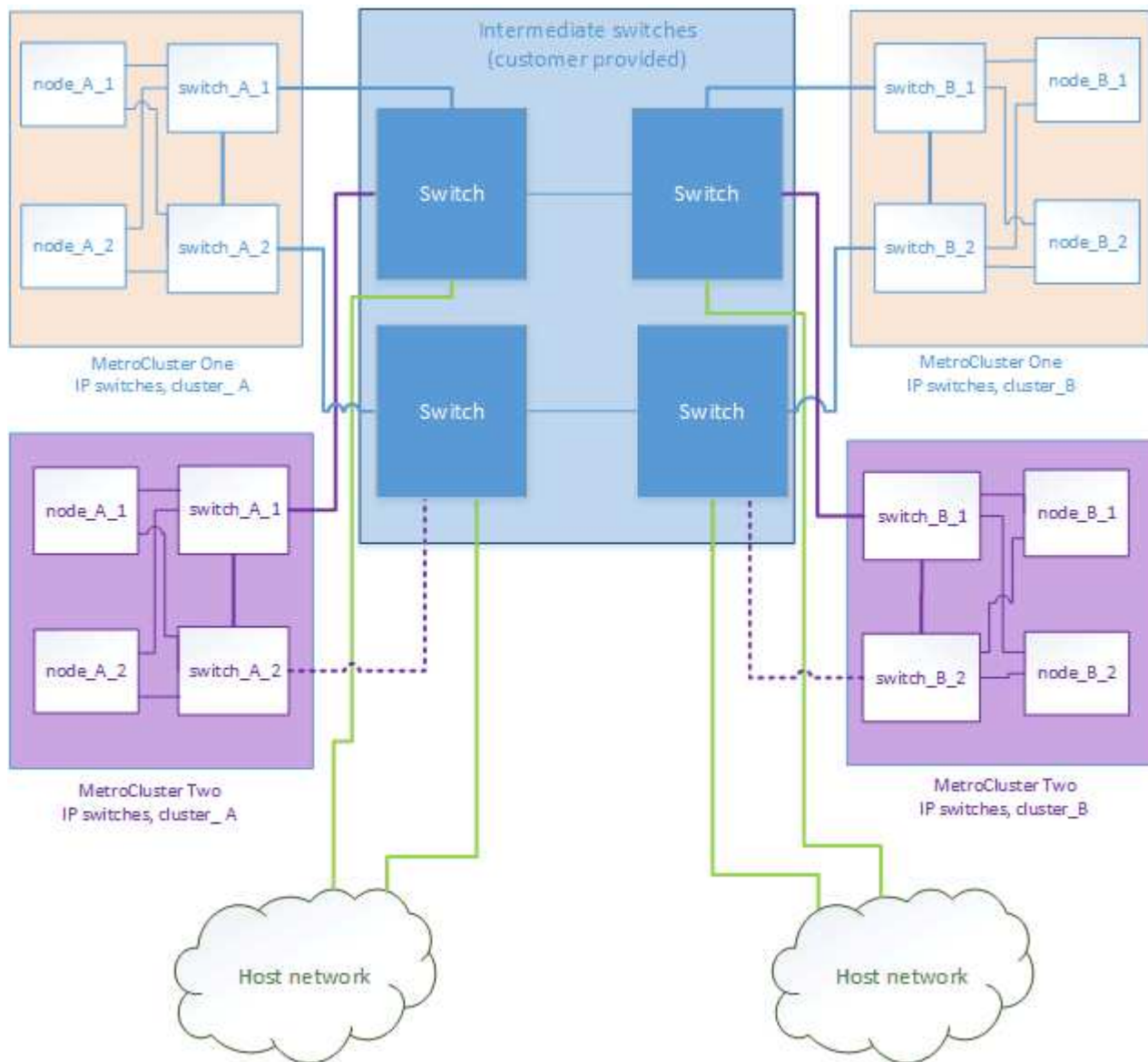


#### Configurazioni MetroCluster multiple che condividono una rete intermedia

In questa topologia, due configurazioni MetroCluster separate condividono la stessa rete intermedia. Nell'esempio, MetroCluster ONE switch\_A\_1 e MetroCluster Two switch\_A\_1, entrambi si collegano allo stesso interruttore intermedio.

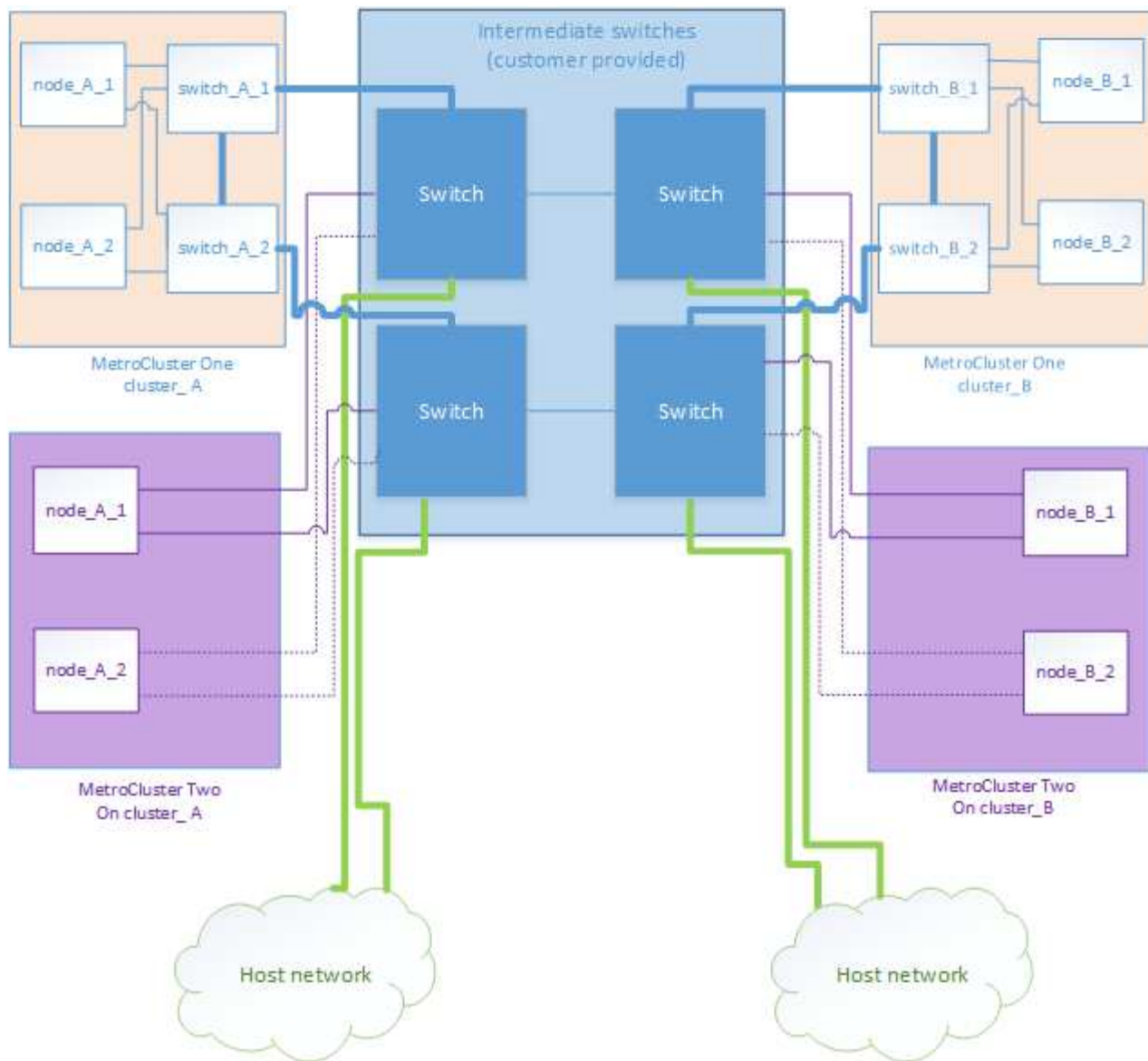


Sia "MetroCluster One" che "MetroCluster Two" possono essere una configurazione MetroCluster a otto nodi o due configurazioni MetroCluster a quattro nodi.



#### **Combinazione di una configurazione MetroCluster con switch validati NetApp e una configurazione con switch compatibili MetroCluster**

Due configurazioni MetroCluster separate condividono lo stesso switch intermedio, dove una MetroCluster viene configurata con switch validati NetApp in una configurazione Layer 2 condivisa (MetroCluster uno) e l'altra MetroCluster con switch compatibili MetroCluster che si collegano direttamente agli switch intermedi (MetroCluster due).



## Utilizzo di aggregati senza mirror

Se la configurazione include aggregati senza mirror, è necessario essere consapevoli dei potenziali problemi di accesso dopo le operazioni di switchover.

### Considerazioni per gli aggregati senza mirror e gli spazi dei nomi gerarchici

Se si utilizzano spazi dei nomi gerarchici, è necessario configurare il percorso di giunzione in modo che tutti i volumi in quel percorso siano solo su aggregati mirrorati o solo su aggregati senza mirror. La configurazione di una combinazione di aggregati senza mirror e mirrorati nel percorso di giunzione potrebbe impedire l'accesso agli aggregati senza mirror dopo l'operazione di switchover.

### Considerazioni per aggregati senza mirror e volumi di metadati CRS e volumi root SVM di dati

Il volume di metadati del servizio di replica della configurazione (CRS) e i volumi radice SVM dei dati devono trovarsi su un aggregato mirrorato. Non è possibile spostare questi volumi in aggregato senza mirror. Se si trovano su aggregato senza mirror, le operazioni di switchover e switchback negoziate vengono vetoed. In questo caso, il comando MetroCluster check fornisce un avviso.

## Considerazioni per aggregati senza mirror e SVM

Le SVM devono essere configurate solo su aggregati mirrorati o solo su aggregati senza mirror. La configurazione di una combinazione di aggregati senza mirror e con mirroring può portare a un'operazione di switchover che supera i 120 secondi e a un'interruzione dei dati se gli aggregati senza mirror non vengono online.

## Considerazioni per aggregati senza mirror e SAN

Prima di ONTAP 9.9.1, un LUN non deve essere posizionato su un aggregato senza mirror. La configurazione di un LUN su un aggregato senza mirror può comportare un'operazione di switchover che supera i 120 secondi e un'interruzione dei dati.

## Considerazioni per l'aggiunta di shelf di storage per aggregati senza mirror



Se si aggiungono shelf che verranno utilizzati per aggregati senza mirror in una configurazione MetroCluster IP, è necessario effettuare le seguenti operazioni:

1. Prima di iniziare la procedura per aggiungere gli shelf, immettere il seguente comando:

```
metrocluster modify -enable-unmirrored-aggr-deployment true
```

2. Verificare che l'assegnazione automatica dei dischi sia disattivata:

```
disk option show
```

3. Seguire i passaggi della procedura per aggiungere lo shelf.

4. Assegnare manualmente tutti i dischi dal nuovo shelf al nodo che sarà proprietario dell'aggregato o degli aggregati senza mirror.

5. Creare gli aggregati:

```
storage aggregate create
```

6. Al termine della procedura, immettere il seguente comando:

```
metrocluster modify -enable-unmirrored-aggr-deployment false
```

7. Verificare che l'assegnazione automatica dei dischi sia attivata:

```
disk option show
```

## Utilizzo del firewall nei siti MetroCluster

Se si utilizza un firewall in un sito MetroCluster, è necessario garantire l'accesso a determinate porte richieste.

### Considerazioni sull'utilizzo del firewall nei siti MetroCluster

Se si utilizza un firewall in un sito MetroCluster, è necessario garantire l'accesso per le porte richieste.

La seguente tabella mostra l'utilizzo della porta TCP/UDP in un firewall esterno posizionato tra due siti MetroCluster.

Tipo di traffico	Porta/servizi
Peering dei cluster	11104 / TCP 11105 / TCP
Gestore di sistema di ONTAP	443 / TCP
MetroCluster IP Intercluster LIF	65200 / TCP 10006 / TCP e UDP
Assistenza hardware	4444 / TCP

## Considerazioni sull'utilizzo del protocollo Virtual IP e Border Gateway con una configurazione MetroCluster

A partire da ONTAP 9.5, ONTAP supporta la connettività Layer 3 utilizzando il protocollo VIP (Virtual IP) e Border Gateway (BGP). La combinazione di VIP e BGP per la ridondanza nella rete front-end con la ridondanza MetroCluster back-end offre una soluzione di disaster recovery Layer 3.

Durante la pianificazione della soluzione Layer 3, consultare le seguenti linee guida e illustrazione. Per ulteriori informazioni sull'implementazione di VIP e BGP in ONTAP, fare riferimento alla seguente sezione:

**"Configurazione di LIF IP virtuali (VIP)"**





## Limitazioni ONTAP

ONTAP non verifica automaticamente che tutti i nodi su entrambi i siti della configurazione MetroCluster siano configurati con il peering BGP.

ONTAP non esegue l'aggregazione di route, ma annuncia tutti i singoli IP LIF virtuali come route host univoche



in qualsiasi momento.

ONTAP non supporta il vero Anycast — solo un singolo nodo nel cluster presenta uno specifico IP LIF virtuale (ma viene accettato da tutte le interfacce fisiche, indipendentemente dal fatto che siano LIF BGP, a condizione che la porta fisica faccia parte dell'IPSpace corretto). Le diverse LIF possono migrare indipendentemente l'una dall'altra in diversi nodi di hosting.

### **Linee guida per l'utilizzo di questa soluzione Layer 3 con una configurazione MetroCluster**

È necessario configurare correttamente BGP e VIP per fornire la ridondanza richiesta.

Si preferiscono scenari di implementazione più semplici rispetto ad architetture più complesse (ad esempio, un router di peering BGP è raggiungibile attraverso un router intermedio non BGP). Tuttavia, ONTAP non applica restrizioni di progettazione o topologia di rete.

Le LIF VIP coprono solo la rete dati/front-end.

A seconda della versione di ONTAP in uso, è necessario configurare le LIF di peering BGP nel nodo SVM, non nel sistema o nei dati SVM. Nel 9.8, le LIF BGP sono visibili nella SVM del cluster (sistema) e le SVM del nodo non sono più presenti.

Ogni SVM di dati richiede la configurazione di tutti i potenziali indirizzi del gateway di primo hop (in genere, l'indirizzo IP di peering del router BGP), in modo che il percorso dei dati di ritorno sia disponibile in caso di migrazione LIF o failover MetroCluster.

Le LIF BGP sono specifiche di un nodo, simili alle LIF di intercluster: Ogni nodo ha una configurazione univoca, che non deve essere replicata nei nodi del sito di DR.

configurato, l'esistenza del v0a (v0b e così via). Convalida continuamente la connettività, garantendo la riuscita di una migrazione LIF o di un failover (a differenza di L2, dove una configurazione giusta è visibile solo dopo l'interruzione).

Una delle principali differenze architetturali consiste nel fatto che i client non devono più condividere la stessa subnet IP del VIP delle SVM di dati. Un router L3 con resilienza di livello Enterprise e funzionalità di ridondanza appropriate attivate (ad esempio, VRRP/HSRP) deve trovarsi sul percorso tra lo storage e i client affinché VIP possa funzionare correttamente.

L'affidabile processo di aggiornamento di BGP consente migrazioni LIF più fluide perché sono marginalmente più veloci e hanno minori probabilità di interruzione per alcuni client

È possibile configurare BGP in modo da rilevare alcune classi di errori di funzionamento della rete o dello switch più velocemente rispetto ai LACP, se configurati di conseguenza.

La BGP esterna (EBGP) utilizza numeri DIVERSI TRA i nodi ONTAP e i router di peering ed è l'implementazione preferita per semplificare l'aggregazione e la ridistribuzione del percorso sui router. Il BGP interno (IBGP) e l'utilizzo dei riflettori di percorso non sono impossibili, ma non rientrano nell'ambito di una semplice configurazione VIP.

Dopo l'implementazione, è necessario verificare che i dati SVM siano accessibili quando la LIF virtuale associata viene migrata tra tutti i nodi di ciascun sito (incluso lo switchover MetroCluster) per verificare la corretta configurazione dei percorsi statici verso gli stessi dati SVM.

VIP funziona con la maggior parte dei protocolli basati su IP (NFS, SMB, iSCSI).

# Configurare i componenti hardware di MetroCluster

## Parti di una configurazione IP MetroCluster

Durante la pianificazione della configurazione IP di MetroCluster, è necessario comprendere i componenti hardware e le modalità di interconnessione.

### Elementi hardware chiave

Una configurazione MetroCluster IP include i seguenti elementi hardware principali:

- Controller di storage

I controller di storage sono configurati come due cluster a due nodi.

- Rete IP

Questa rete IP back-end offre connettività per due utilizzi distinti:

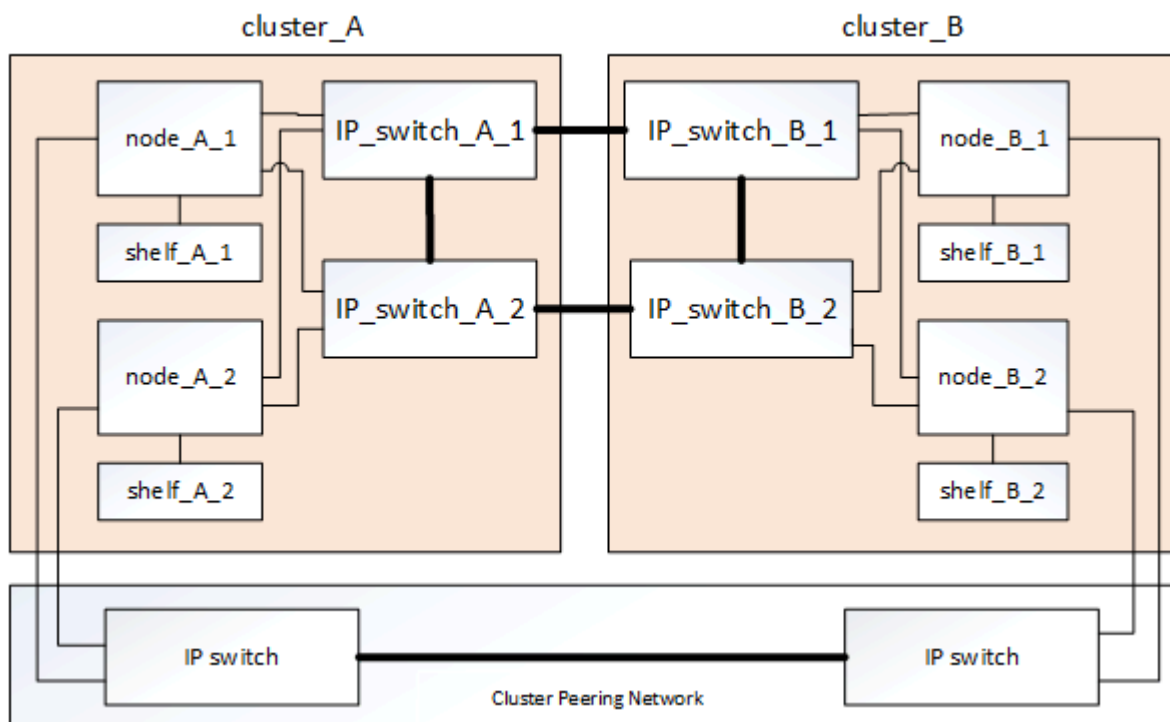
- Connettività cluster standard per comunicazioni intra-cluster.

Si tratta della stessa funzionalità dello switch del cluster utilizzata nei cluster ONTAP con switch non MetroCluster.

- Connettività back-end MetroCluster per la replica dei dati di storage e della cache non volatile.

- Rete di peering del cluster

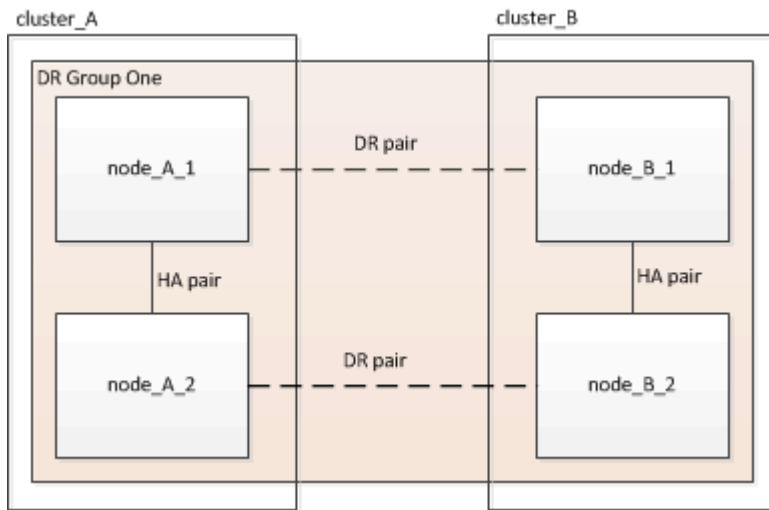
La rete di peering del cluster fornisce la connettività per il mirroring della configurazione del cluster, che include la configurazione di SVM (Storage Virtual Machine). La configurazione di tutte le SVM su un cluster viene sottoposta a mirroring sul cluster partner.



## Gruppi di disaster recovery (DR)

Una configurazione IP MetroCluster è costituita da un gruppo di DR composto da quattro nodi.

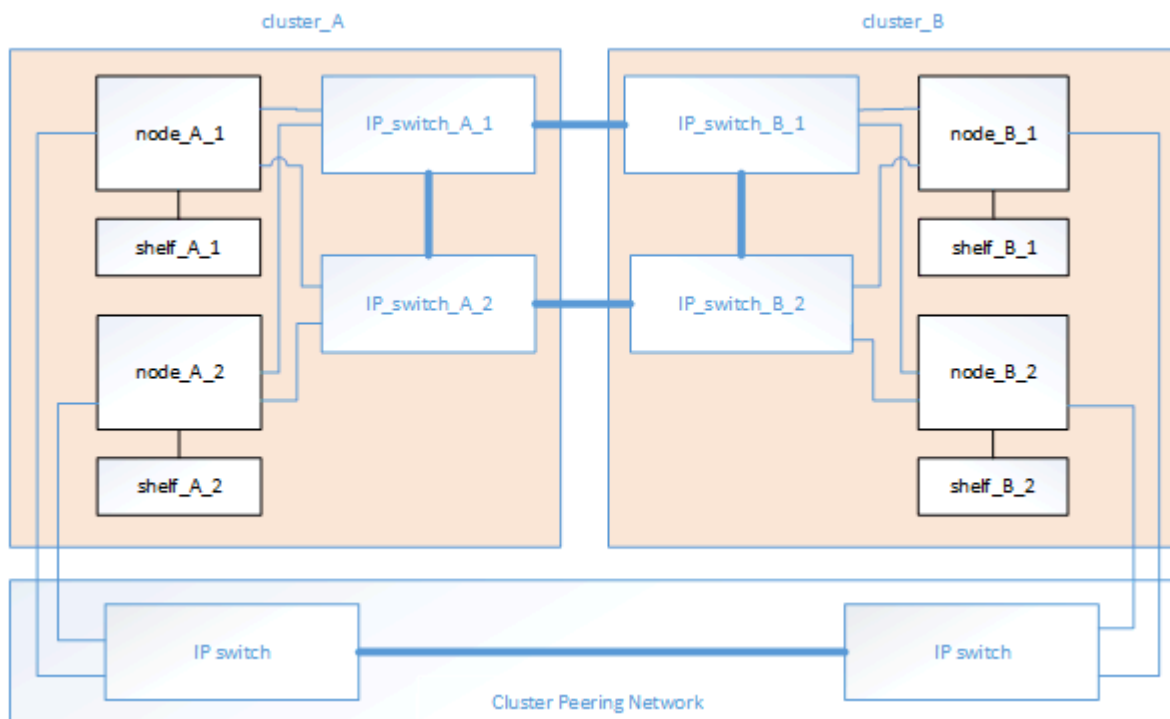
La figura seguente mostra l'organizzazione dei nodi in una configurazione MetroCluster a quattro nodi:



## Immagine delle coppie ha locali in una configurazione MetroCluster

Ogni sito MetroCluster è costituito da controller di storage configurati come coppia ha. Ciò consente la ridondanza locale in modo che, in caso di guasto di uno storage controller, il partner ha locale possa assumere il controllo. Tali guasti possono essere gestiti senza un'operazione di switchover MetroCluster.

Le operazioni di failover e giveback ha locale vengono eseguite con i comandi di failover dello storage, come una configurazione non MetroCluster.

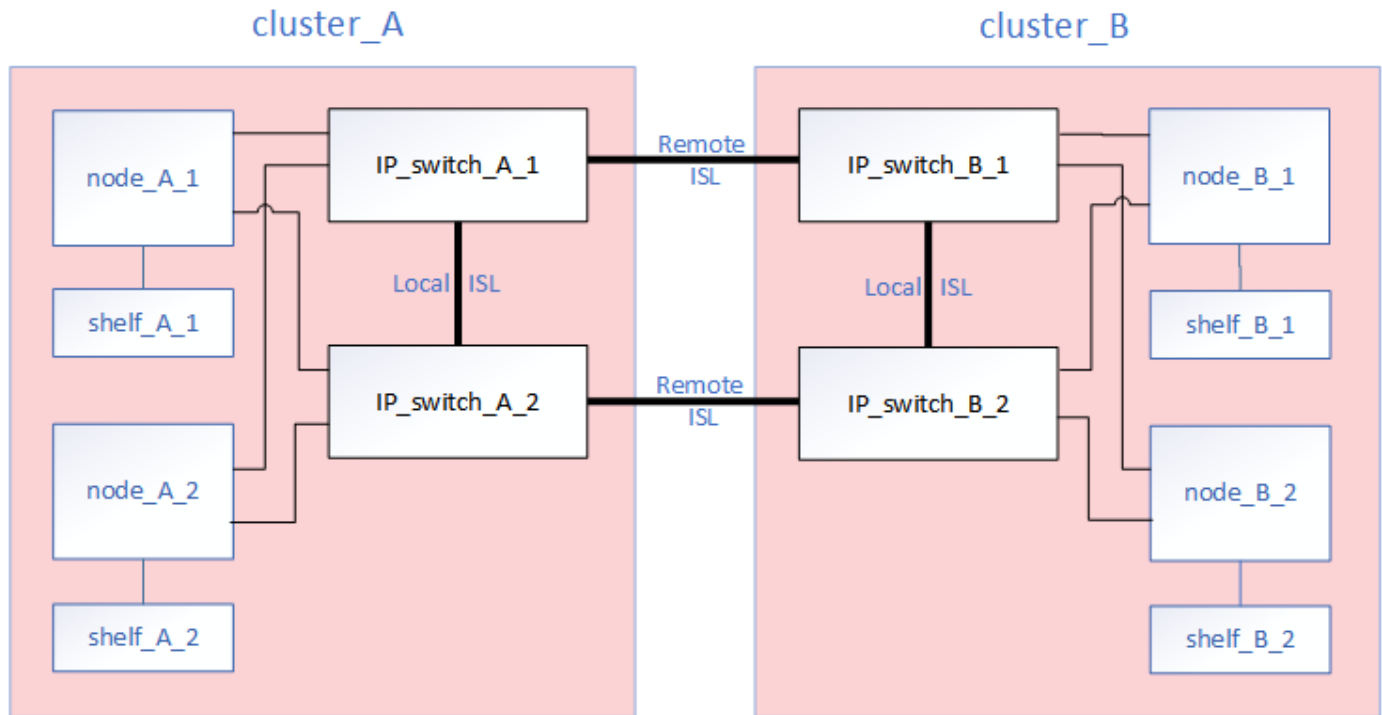


## Informazioni correlate

["Concetti di ONTAP"](#)

## Immagine dell'IP MetroCluster e della rete di interconnessione del cluster

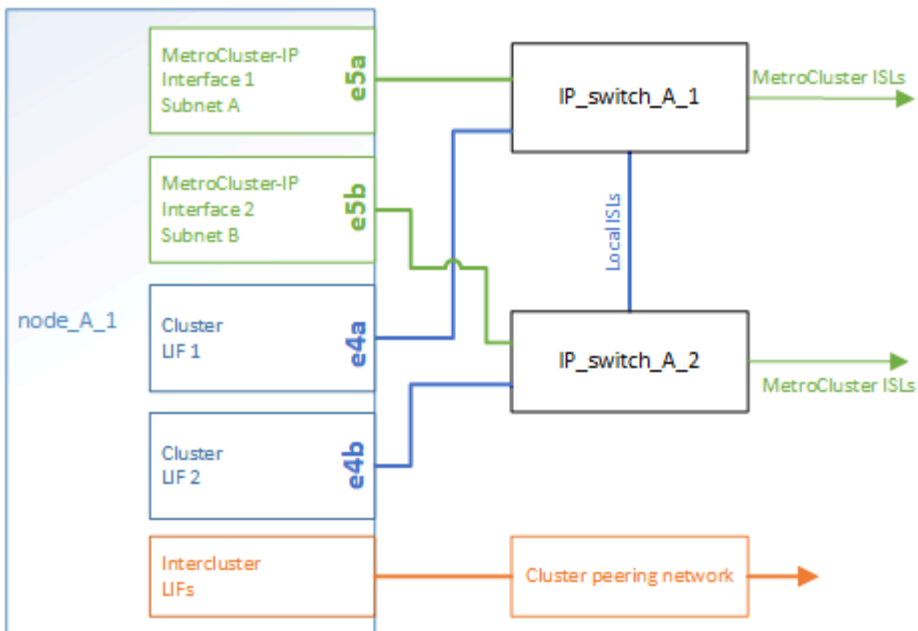
I cluster ONTAP in genere includono una rete di interconnessione cluster per il traffico tra i nodi del cluster. Nelle configurazioni MetroCluster IP, questa rete viene utilizzata anche per trasportare il traffico di replica dei dati tra i siti MetroCluster.



Ogni nodo nella configurazione IP MetroCluster dispone di interfacce dedicate per la connessione alla rete IP back-end:

- Due interfacce IP MetroCluster
- Due interfacce cluster locali

La figura seguente mostra queste interfacce. L'utilizzo delle porte mostrato riguarda un sistema AFF A700 o FAS9000.



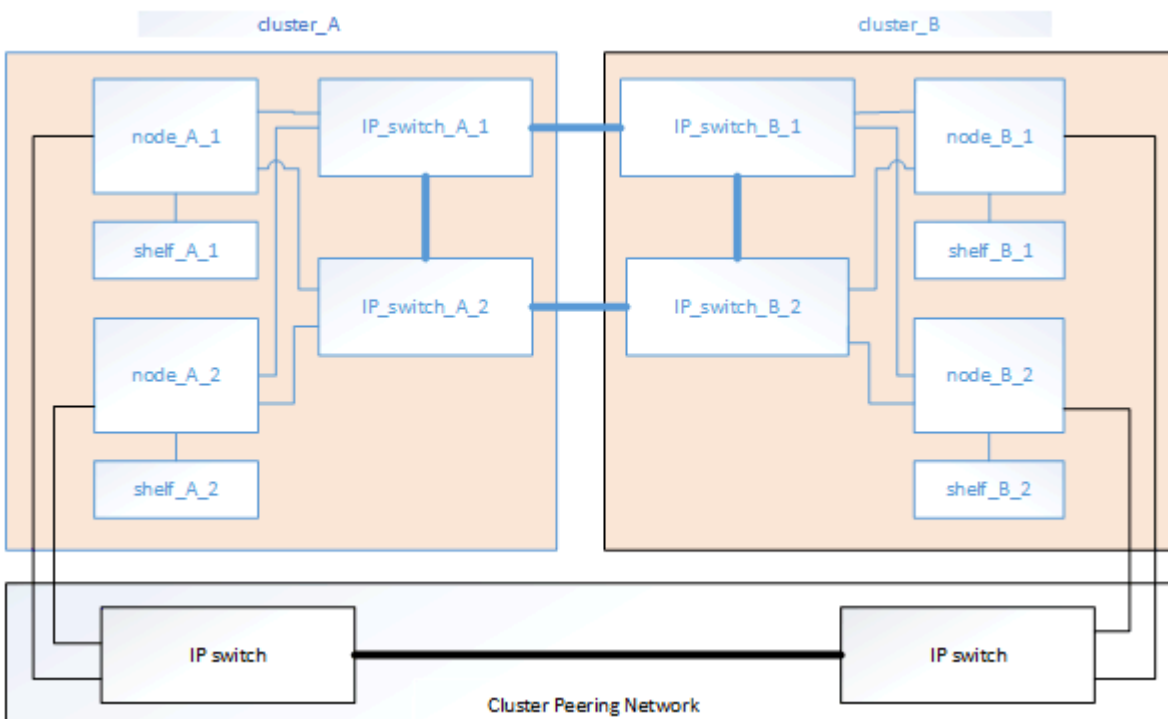
## Informazioni correlate

"Considerazioni per le configurazioni MetroCluster IP"

## Immagine della rete di peering del cluster

I due cluster nella configurazione MetroCluster vengono peering tramite una rete di peering cluster fornita dal cliente. Il peering dei cluster supporta il mirroring sincrono delle macchine virtuali di storage (SVM, precedentemente noto come Vserver) tra i siti.

Le LIF di intercluster devono essere configurate su ciascun nodo della configurazione MetroCluster e i cluster devono essere configurati per il peering. Le porte con le LIF intercluster sono collegate alla rete di peering cluster fornita dal cliente. La replica della configurazione SVM viene eseguita su questa rete attraverso il Servizio di replica della configurazione.



## Informazioni correlate

["Configurazione rapida del peering di cluster e SVM"](#)

["Considerazioni per la configurazione del peering del cluster"](#)

["Cablaggio delle connessioni di peering del cluster"](#)

["Peering dei cluster"](#)

## Componenti IP MetroCluster richiesti e convenzioni di denominazione

Durante la pianificazione della configurazione IP di MetroCluster, è necessario conoscere i componenti hardware e software necessari e supportati. Per comodità e chiarezza, è necessario comprendere anche le convenzioni di denominazione utilizzate per i componenti negli esempi della documentazione.

### Software e hardware supportati

L'hardware e il software devono essere supportati per la configurazione IP di MetroCluster.

["NetApp Hardware Universe"](#)

Quando si utilizzano sistemi AFF, tutti i moduli controller nella configurazione MetroCluster devono essere configurati come sistemi AFF.

### Requisiti di ridondanza dell'hardware in una configurazione MetroCluster IP

A causa della ridondanza hardware nella configurazione IP di MetroCluster, sono presenti due componenti per ogni sito. Ai siti vengono assegnate arbitrariamente le lettere A e B e ai singoli componenti vengono assegnati arbitrariamente i numeri 1 e 2.

### Requisiti del cluster ONTAP in una configurazione IP MetroCluster

Le configurazioni MetroCluster IP richiedono due cluster ONTAP, uno per ciascun sito MetroCluster.

La denominazione deve essere univoca all'interno della configurazione MetroCluster.

Nomi di esempio:

- Sito A: Cluster\_A
- Sito B: Cluster\_B

### Requisiti dello switch IP in una configurazione IP MetroCluster

Le configurazioni IP di MetroCluster richiedono quattro switch IP. I quattro switch formano due fabric storage switch che forniscono l'ISL tra ciascuno dei cluster nella configurazione IP di MetroCluster.

Gli switch IP forniscono anche comunicazioni intra-truste tra i moduli controller di ciascun cluster.

La denominazione deve essere univoca all'interno della configurazione MetroCluster.

Nomi di esempio:

- Sito A: Cluster\_A
  - IP\_switch\_A\_1
  - IP\_switch\_A\_2
- Sito B: Cluster\_B
  - IP\_switch\_B\_1
  - IP\_switch\_B\_2

### Requisiti del modulo controller in una configurazione IP MetroCluster

Le configurazioni MetroCluster IP richiedono quattro o otto moduli controller.

I moduli controller di ogni sito formano una coppia ha. Ogni modulo controller dispone di un partner DR nell'altro sito.

Ogni modulo controller deve eseguire la stessa versione di ONTAP. I modelli di piattaforma supportati dipendono dalla versione di ONTAP:

- Le nuove installazioni MetroCluster IP sui sistemi FAS non sono supportate in ONTAP 9.4.  
Le configurazioni MetroCluster IP esistenti sui sistemi FAS possono essere aggiornate a ONTAP 9.4.
- A partire da ONTAP 9.5, sono supportate le nuove installazioni MetroCluster IP sui sistemi FAS.
- A partire da ONTAP 9.4, sono supportati i moduli controller configurati per ADP.

### Nomi di esempio

Nella documentazione vengono utilizzati i seguenti nomi di esempio:

- Sito A: Cluster\_A
  - Controller\_A\_1
  - Controller\_A\_2
- Sito B: Cluster\_B
  - Controller\_B\_1
  - Controller\_B\_2

### Requisiti dell'adattatore Gigabit Ethernet in una configurazione MetroCluster IP

Le configurazioni IP di MetroCluster utilizzano un adattatore Ethernet da 40/100 Gbps o 10/25 Gbps per le interfacce IP verso gli switch IP utilizzati per il fabric IP di MetroCluster.

Modello di piattaforma	Adattatore Gigabit Ethernet richiesto	Slot richiesto per l'adattatore	Porte
AFF A900, ASA A900 e FAS9500	X91146A	Slot 5, slot 7	e5b, e7b
AFF A700 e FAS9000	X91146A-C.	Slot 5	e5a, e5b

AFF A800, AFF C800, ASA A800 e ASA C800	X1146A/porte integrate	Slot 1	e0b, e1b
FAS8300, AFF A400, ASA A400, ASA C400 e AFF C400	X1146A	Slot 1	e1a, e1b
AFF A300 e FAS8200	X1116A	Slot 1	e1a, e1b
FAS2750, AFF A150, ASA A150 e AFF A220	Porte integrate	Slot 0	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250 e AFF C250	Porte integrate	Slot 0	e0c, e0d
AFF A320	Porte integrate	Slot 0	e0g, e0h

["Scopri l'assegnazione automatica dei dischi e i sistemi ADP nelle configurazioni IP di MetroCluster".](#)

### Requisiti di pool e disco (supporto minimo)

Si consigliano otto shelf di dischi SAS (quattro shelf in ogni sito) per consentire la proprietà dei dischi in base allo shelf.

Una configurazione MetroCluster IP a quattro nodi richiede la configurazione minima per ciascun sito:

- Ogni nodo dispone di almeno un pool locale e di un pool remoto nel sito.
- Almeno sette dischi in ciascun pool.

In una configurazione MetroCluster a quattro nodi con un singolo aggregato di dati mirrorati per nodo, la configurazione minima richiede 24 dischi nel sito.

In una configurazione minima supportata, ciascun pool ha il seguente layout di unità:

- Tre dischi root
- Tre unità dati
- Un disco di riserva

In una configurazione minima supportata, è necessario almeno uno shelf per sito.

Le configurazioni MetroCluster supportano RAID-DP e RAID4.

### Considerazioni sulla posizione dei dischi per gli shelf parzialmente popolati

Per una corretta assegnazione automatica dei dischi quando si utilizzano shelf a metà popolati (12 dischi in uno shelf da 24 dischi), i dischi devono essere posizionati negli slot 0-5 e 18-23.

In una configurazione con uno shelf parzialmente popolato, i dischi devono essere distribuiti uniformemente nei quattro quadranti dello shelf.



## Considerazioni sulla posizione dei dischi interni di AFF A800

Per una corretta implementazione della funzione ADP, gli slot dei dischi del sistema AFF A800 devono essere divisi in quarti e i dischi devono essere posizionati simmetricamente nei quarti.

Un sistema AFF A800 dispone di 48 alloggiamenti per dischi. Gli alloggiamenti possono essere suddivisi in quarti:

- Quarto:
  - Alloggiamenti 0 - 5
  - Alloggiamenti 24 - 29
- Secondo trimestre:
  - Alloggiamenti 6 - 11
  - Alloggiamenti 30 - 35
- Terzo trimestre:
  - Alloggiamenti 12 - 17
  - Alloggiamenti 36 - 41
- Quarto trimestre:
  - Alloggiamenti 18 - 23
  - Alloggiamenti 42 - 47

Se questo sistema è popolato con 16 dischi, devono essere distribuiti simmetricamente tra i quattro quarti:

- Quattro dischi nel primo trimestre: 0, 1, 2, 3
- Quattro dischi nel secondo trimestre: 6, 7, 8, 9
- Quattro dischi nel terzo trimestre: 12, 13, 14, 15
- Quattro dischi nel quarto trimestre: 18, 19, 20, 21

## Combinazione di moduli IOM12 e IOM 6 in uno stack

La tua versione di ONTAP deve supportare la combinazione di shelf. Fare riferimento a. ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#) Per verificare se la versione di ONTAP in uso supporta la combinazione di shelf.

Per ulteriori dettagli sulla miscelazione degli scaffali, vedere ["Shelf hot-adding con moduli IOM12 a uno stack di shelf con moduli IOM6"](#)

## Scaffalatura dei componenti hardware

Se l'apparecchiatura non è già stata installata negli armadi, è necessario installarli in rack.

### A proposito di questa attività

Questa attività deve essere eseguita su entrambi i siti MetroCluster.

### Fasi

1. Pianificare il posizionamento dei componenti di MetroCluster.

Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di stack di shelf di dischi nella configurazione.

2. Mettere a terra l'utente.
3. Installare i moduli controller nel rack o nell'armadietto.

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A220/FAS2700"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A250"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A300"](#)

["Sistemi AFF A320: Installazione e configurazione"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A400"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A700"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi AFF A800"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi FAS500f"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi FAS8200"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi FAS8300 e FAS8700"](#)

["Istruzioni per l'installazione e la configurazione dei sistemi FAS9000"](#)

4. Installare gli switch IP nel rack o nell'armadietto.
5. Installare gli shelf di dischi, accenderli, quindi impostare gli ID degli shelf.
  - È necessario spegnere e riaccendere ogni shelf di dischi.
  - Per agevolare la risoluzione dei problemi, si consiglia di utilizzare ID shelf univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster.



Non utilizzare shelf di dischi per cavi destinati a contenere aggregati senza mirror. È necessario attendere la distribuzione degli shelf destinati agli aggregati senza mirror fino al completamento della configurazione MetroCluster e implementarli solo dopo l'utilizzo di `metrocluster modify -enable-unmirrored-aggr-deployment true` comando.

## Collegare via cavo gli switch IP MetroCluster

### Utilizzo delle tabelle delle porte con lo strumento RcfFileGenerator o di più configurazioni MetroCluster

È necessario comprendere come utilizzare le informazioni nelle tabelle delle porte per generare correttamente i file RCF.

#### Prima di iniziare

Esaminare queste considerazioni prima di utilizzare le tabelle:

- Le seguenti tabelle mostrano l'utilizzo della porta per il sito A. Lo stesso cablaggio viene utilizzato per il sito B.

- Gli switch non possono essere configurati con porte di velocità diverse (ad esempio, una combinazione di porte da 100 Gbps e porte da 40 Gbps).
- Tenere traccia del gruppo di porte MetroCluster (MetroCluster 1, MetroCluster 2, ecc.). Queste informazioni saranno necessarie quando si utilizza lo strumento RcfFileGenerator come descritto più avanti in questa procedura di configurazione.
- Il "[RcfFileGenerator per MetroCluster IP](#)" fornisce inoltre una panoramica del cablaggio per porta per ogni switch. Utilizzare questa panoramica dei cavi per verificare il cablaggio.

### **Cablaggio di configurazioni MetroCluster a otto nodi**

Per la configurazione di MetroCluster con ONTAP 9.8 e versioni precedenti, alcune procedure eseguite per la transizione di un aggiornamento richiedono l'aggiunta di un secondo gruppo di DR a quattro nodi alla configurazione per creare una configurazione temporanea a otto nodi. A partire da ONTAP 9.9.1, sono supportate le configurazioni permanenti di MetroCluster a otto nodi.

### **A proposito di questa attività**

Per tali configurazioni, si utilizza lo stesso metodo descritto in precedenza. Invece di un secondo MetroCluster, si sta cablando un gruppo DR aggiuntivo a quattro nodi.

Ad esempio, la configurazione include quanto segue:

- Switch Cisco 3132Q-V.
- MetroCluster 1: Piattaforme FAS2750
- MetroCluster 2: Piattaforme AFF A700 (queste piattaforme vengono aggiunte come secondo gruppo DR a quattro nodi)

### **Fasi**

1. Per MetroCluster 1, collegare gli switch Cisco 3132Q-V utilizzando la tabella per la piattaforma FAS2750 e le righe per le interfacce MetroCluster 1.
2. Per MetroCluster 2 (il secondo gruppo DR), collegare gli switch Cisco 3132Q-V utilizzando la tabella per la piattaforma AFF A700 e le righe per le interfacce MetroCluster 2.

### **Assegnazioni delle porte della piattaforma per switch Cisco 3132Q-V.**

L'utilizzo della porta in una configurazione IP MetroCluster dipende dal modello dello switch e dal tipo di piattaforma.

Prima di utilizzare le tabelle, rivedere le seguenti linee guida:

- Se si configura lo switch per la transizione da FC MetroCluster a IP, è possibile utilizzare la porta 5, la porta 6, la porta 13 o la porta 14 per connettere le interfacce del cluster locale del nodo FC MetroCluster. Fare riferimento a "[RcfFileGenerator](#)" e i file di cablaggio generati per ulteriori dettagli sul cablaggio di questa configurazione. Per tutte le altre connessioni, è possibile utilizzare le assegnazioni di utilizzo delle porte elencate nelle tabelle.

### **Utilizzo delle porte per i sistemi FAS2750 o AFF A220 e uno switch Cisco 3132Q-V.**

Cabling a FAS2750 or AFF A220 to a Cisco 3132Q-V switch			
Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Utilizzo delle porte per sistemi FAS9000 o AFF A700 e switch Cisco 3132Q-V.

Cabling a FAS9000 or AFF A700 to a Cisco 3132Q-V switch			
Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Utilizzo delle porte per i sistemi AFF A800 o ASA A800 e uno switch Cisco 3132Q-V.

Cabling an AFF A800 or ASA A800 to a Cisco 3132Q-V switch			
Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

### Assegnazioni delle porte della piattaforma per switch Cisco 3232C o Cisco 9336C

L'utilizzo della porta in una configurazione IP MetroCluster dipende dal modello dello switch e dal tipo di piattaforma.

Esaminare queste considerazioni prima di utilizzare le tabelle:

- Le seguenti tabelle mostrano l'utilizzo della porta per il sito A. Lo stesso cablaggio viene utilizzato per il sito B.
- Gli switch non possono essere configurati con porte di velocità diverse (ad esempio, una combinazione di porte da 100 Gbps e porte da 40 Gbps).
- Se si configura un singolo MetroCluster con gli switch, utilizzare il gruppo di porte **MetroCluster 1**.

Tenere traccia del gruppo di porte MetroCluster (MetroCluster 1, MetroCluster 2, MetroCluster 3 o MetroCluster 4). Sarà necessario quando si utilizza lo strumento RcfFileGenerator come descritto più avanti in questa procedura di configurazione.

- RcfFileGenerator per MetroCluster IP fornisce anche una panoramica del cablaggio per porta per ogni switch.

Utilizzare questa panoramica dei cavi per verificare il cablaggio.

- Il file RCF versione v2,10 o successiva è richiesto per la modalità breakout 25g per gli ISL MetroCluster.
- Per utilizzare una piattaforma diversa da FAS8200 o AFF 9.13.1 nel gruppo "MetroCluster 2,00" sono necessari ONTAP A300 o versioni successive e il file RCF versione 4.

#### **Collegamento di due configurazioni MetroCluster agli switch**

Quando si collegano più configurazioni MetroCluster a uno switch Cisco 3132Q-V, è necessario collegare ciascun MetroCluster in base alla tabella appropriata. Ad esempio, se si collegano FAS2750 e AFF A700 allo stesso switch Cisco 3132Q-V. Quindi, collegare il cavo FAS2750 come da "MetroCluster 1" nella Tabella 1 e il cavo AFF A700 come da "MetroCluster 2" o "MetroCluster 3" nella Tabella 2. Non è possibile collegare fisicamente FAS2750 e AFF A700 come "MetroCluster 1".

**Collegamento di un AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, sistema AFF C250, ASA C250, AFF A250 o ASA A250 a uno switch Cisco 3232C o Cisco 9336-FX2C**

Cabling an AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a Cisco 3232C or Cisco 9336-FX2C switch					
Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

**Collegamento di un sistema FAS8200 o AFF A300 a uno switch Cisco 3232C o Cisco 9336C**



Cabling a FAS8200 or AFF A300 to a Cisco 3232C or Cisco 9336C-FX2 switch

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, MetroCluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled	

Se si esegue l'aggiornamento da file RCF meno recenti, la configurazione del cablaggio potrebbe utilizzare porte nel gruppo "MetroCluster 4" (porte 25/26 e 29/30).

**Collegamento di un AFF A320, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900, o dal sistema ASA A900 a uno switch Cisco 3232C o Cisco 9336C-FX2**

Cabling a AFF A320, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 or ASA A900 to a Cisco 3232C or Cisco 9336C-FX2 switch													
Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2													
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4													
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6													
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8													
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
10													
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
12													
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
14													
15													
16	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
17													
18													
19													
20													
21/1-4													
22/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23/1-4													
24/1-4													
25													
26	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
27 - 28	Unused	disabled		disabled		disabled		disabled		disabled		disabled	
29													
30	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
31 - 32	Unused	disabled		disabled		disabled		disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled		disabled		disabled	

**Nota 1:** Se si utilizza un adattatore X91440A (40Gbps), utilizzare le porte e4a e E4E o e4a e E8a. Se si utilizza un adattatore X91153A (100Gbps), utilizzare le porte e4a e e4b o e4a e E8a.



L'uso delle porte nel gruppo "MetroCluster 4" richiede ONTAP 9.13.1 o versione successiva.

**Assegnazione delle porte della piattaforma per uno switch condiviso Cisco 9336C-FX2**

L'utilizzo della porta in una configurazione IP MetroCluster dipende dal modello dello switch e dal tipo di piattaforma.

Esaminare queste considerazioni prima di utilizzare le tabelle:

- Almeno una configurazione MetroCluster o un gruppo di DR deve supportare gli shelf NS224 collegati con switch.
- Le piattaforme che non supportano shelf NS224 con switch possono essere connesse solo come una seconda configurazione MetroCluster o come un secondo gruppo di DR.
- RcfFileGenerator mostra solo le piattaforme idonee quando viene selezionata la prima piattaforma.
- La connessione di una configurazione MetroCluster a otto o due nodi richiede ONTAP 9.14.1 o versione successiva.

**Collegamento di un AFF A320, AFF C400, ASA C400, AFF A400, ASA A400, AFF A700, AFF C800, ASA C800, AFF A800, AFF A900, o dal sistema ASA A900 a uno switch condiviso Cisco 9336C-FX2**

Cabling an AFF A320, AFF C400, ASA C400, AFF A400, ASA A400, AFF A700, AFF C800, ASA C800, AFF A800 , AFF A900, or ASA A900 to a Cisco 9336C-FX2 shared switch													
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400		AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1,	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a
2	Local Cluster interface												Note 1
3	MetroCluster 2,	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a
4	Local Cluster interface												Note 1
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8													
9	MetroCluster 1,	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
10	MetroCluster interface												
11	MetroCluster 2,	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
12	MetroCluster interface												
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14													
15													
16													
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2) e1a (option 3)	e3b (option 1) e10b (option 2) e11b (option 3)
18													
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2) e1a (option 3)	e3b (option 1) e10b (option 2) e11b (option 3)
20													
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

**Nota 1:** Se si utilizza un adattatore X91440A (40Gbps), utilizzare le porte e4a e E4E o e4a e E8a. Se si utilizza un adattatore X91153A (100Gbps), utilizzare le porte e4a e e4b o e4a e E8a.

**Collegamento di un sistema AFF A150, ASA A150, FAS2750 o AFF A220 a uno switch condiviso Cisco 9336C-FX2**

Cabling an AFF A150, ASA A150, FAS2750 or AFF A220 to a Cisco 9336C-FX2 shared switch

Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Collegamento di un sistema FAS500f, AFF C250, ASA C250, AFF A250 o ASA A250 a uno switch condiviso Cisco 9336C-FX2

Cabling a FAS500f, AFF C250, ASA C250, AFF A250, ASA A250 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
9/2-4		disabled	
10/1		e0c	e0d
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
11/2-4		disabled	
12/1		e0c	e0d
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Collegamento di un sistema FAS8200 o AFF A300 a uno switch condiviso Cisco 9336C-FX2

Cabling a FAS8200 or AFF A300 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Collegamento di un sistema FAS8300, FAS8700, FAS9000 o FAS9500 a uno switch condiviso Cisco 9336C-FX2

Cabling a FAS8300, FAS8700, FAS9000, or FAS9500 to a Cisco 9336C-FX2 shared switch							
Switch Port	Port Use	FAS8300 FAS8700		FAS9000		FAS9500	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e4a	e4e / e8a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e4a	e4e / e8a	e4a	e4b(e) / e8a Note 1
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e5a	e5b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e5a	e5b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

**Nota 1:** Se si utilizza un adattatore X91440A (40Gbps), utilizzare le porte e4a e E4E o e4a e E8a. Se si utilizza un adattatore X91153A (100Gbps), utilizzare le porte e4a e e4b o e4a e E8a.

### Assegnazioni delle porte della piattaforma per gli switch IP BES-53248 supportati da Broadcom

L'utilizzo della porta in una configurazione IP MetroCluster dipende dal modello dello switch e dal tipo di piattaforma.

Gli switch non possono essere utilizzati con porte ISL remote di velocità diverse (ad esempio, una porta da 25 Gbps collegata a una porta ISL da 10 Gbps).

#### Leggere queste informazioni prima di utilizzare le tabelle:

- Se si configura lo switch per la transizione da FC MetroCluster a IP, vengono utilizzate le seguenti porte a seconda della piattaforma di destinazione scelta:

Piattaforma di destinazione	Porta
FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, o FAS8700	Porte 1 - 6, 10Gbps
Piattaforme FAS8200 o AFF A300	Porte 3 - 4 e 9 - 12, 10Gbps

- I sistemi AFF A320 configurati con switch Broadcom BES-53248 potrebbero non supportare tutte le funzioni.

Qualsiasi configurazione o funzione che richieda la connessione delle connessioni cluster locali a uno switch non è supportata. Ad esempio, le seguenti configurazioni e procedure non sono supportate:

- Configurazioni MetroCluster a otto nodi
- Transizione da configurazioni MetroCluster FC a MetroCluster IP
- Aggiornamento di una configurazione MetroCluster IP a quattro nodi (ONTAP 9.8 e versioni successive)

#### Note a cui si fa riferimento nelle tabelle:

- Nota 1:** L'utilizzo di queste porte richiede una licenza aggiuntiva.



- **Nota 2:** È possibile collegare allo switch solo un singolo MetroCluster a quattro nodi che utilizza sistemi AFF A320.

Funzionalità che richiedono uno switch cluster non sono supportate in questa configurazione, incluse la transizione da FC a IP MetroCluster e le procedure di tech refresh.

- **Nota 3:** Lo switch BES-53248 richiede che tutte le porte di un gruppo a quattro porte funzionino alla stessa velocità. Per collegare una combinazione di piattaforme AFF 150, ASA A150, FAS2750, AFF A220 e FAS500f, AFF C250, ASA C250, AFF A250 e ASA A250, è necessario utilizzare le porte degli switch situate in gruppi separati a quattro porte. Se si richiede questo tipo di configurazione, si applica quanto segue:
  - In ["RcfFileGenerator per MetroCluster IP"](#), I campi a discesa per "MetroCluster 1" e "MetroCluster 2" vengono compilati solo dopo aver selezionato una piattaforma per MetroCluster 3 o "MetroCluster 4". Fare riferimento a ["Utilizzo delle tabelle delle porte con lo strumento RcfFileGenerator o di più configurazioni MetroCluster"](#) per ulteriori informazioni sull'utilizzo delle tabelle delle porte.
  - Se entrambe le configurazioni MetroCluster utilizzano la stessa piattaforma, NetApp consiglia di selezionare il gruppo "MetroCluster 3" per una configurazione e il gruppo "MetroCluster 4" per l'altra configurazione. Se le piattaforme sono diverse, selezionare "MetroCluster 3" o "MetroCluster 4" per la prima configurazione e selezionare "MetroCluster 1" o "MetroCluster 2" per la seconda configurazione.

#### Collegamento di un AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 o ASA A250 a uno switch Broadcom BES-53248

Cabling an AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a Broadcom BES-53248 switch					
Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled		disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
6					
7	MetroCluster 2, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
8					
9	MetroCluster 3, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
10					
11	MetroCluster 4, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
12					
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 54)				
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

#### Collegamento di un sistema FAS8200, AFF A300 o AFF A320 a uno switch Broadcom BES-53248



Cabling a FAS8200 or AFF A300 to a Broadcom BES-53248 switch			
Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface Not used during Transition	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

Cabling an AFF A320 to a Broadcom BES-53248 switch			
Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (note 2)	e0g	e0h
56			

Cabling a FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 or FAS8700 to a Broadcom BES-53248 switch					
Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

### Assegnazioni delle porte della piattaforma per gli switch IP SN2100 supportati da NVIDIA

L'utilizzo della porta in una configurazione IP MetroCluster dipende dal modello dello switch e dal tipo di piattaforma.

#### Configurazioni supportate

Le seguenti configurazioni non sono attualmente supportate:

- Transizione MetroCluster FC-IP

#### Esaminare queste considerazioni prima di utilizzare le tabelle di configurazione

- La connessione di una configurazione MetroCluster a otto o due nodi richiede ONTAP 9.14.1 o versione successiva e il file RCF versione 2,00 o successiva.
- Se si utilizzano più configurazioni MetroCluster, seguire la tabella corrispondente. Ad esempio:
  - Se si utilizzano due configurazioni MetroCluster a quattro nodi di tipo AFF A700, collegare il primo MetroCluster indicato come "MetroCluster 1" e il secondo MetroCluster indicato come "MetroCluster 2" nella tabella AFF A700.



Le porte 13 e 14 possono essere utilizzate in modalità di velocità nativa che supporta 40 Gbps e 100 Gbps o in modalità breakout per supportare 4 × 25 Gbps o 4 × 10 Gbps. Se utilizzano la modalità di velocità nativa, vengono rappresentate come porte 13 e 14. Se utilizzano la modalità breakout, 4 × 25 Gbps o 4 × 10 Gbps, vengono rappresentate come porte 13s0-3 e 14s0-3.

Le sezioni seguenti descrivono il cablaggio fisico. Fare riferimento anche alla ["RcfFileGenerator"](#) per informazioni dettagliate sul cablaggio.

**Collegamento di un AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, da sistema AFF A250 o ASA A250 a switch NVIDIA SN2100**

Cabling a AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a NVIDIA SN2100 switch					
Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16		ISL, Local Cluster		ISL, Local Cluster	

**Cablaggio a FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, da sistema AFF A800, ASA A800, FAS9500, AFF A900 o ASA A900 a uno switch NVIDIA SN2100**

Cabling a FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 or ASA A900 to a NVIDIA SN2100 switch											
Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2		e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4		e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6		e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
8		e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
10		e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
12		e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	

**Nota 1:** Se si utilizza un adattatore X91440A (40Gbps), utilizzare le porte e4a e E4E o e4a e E8a. Se si utilizza un adattatore X91153A (100Gbps), utilizzare le porte e4a e e4b o e4a e E8a.

## Cablaggio delle porte di peering, dati e gestione del controller

È necessario collegare le porte del modulo controller utilizzate per il peering del cluster, la gestione e la connettività dati.

Questa attività deve essere eseguita su ciascun modulo controller nella configurazione MetroCluster.

Per il peering dei cluster, è necessario utilizzare almeno due porte su ciascun modulo controller.

La larghezza di banda minima consigliata per le porte e la connettività di rete è 1 GbE.

1. Identificare e collegare almeno due porte per il peering del cluster e verificare che dispongano di connettività di rete con il cluster partner.

Il peering del cluster può essere eseguito su porte dedicate o su porte dati. L'utilizzo di porte dedicate offre un throughput più elevato per il traffico di peering del cluster.

["Configurazione rapida del peering di cluster e SVM"](#)

2. Collegare le porte dati e di gestione del controller alle reti dati e di gestione del sito locale.

Seguire le istruzioni di installazione della piattaforma in ["Documentazione dei sistemi hardware ONTAP"](#).



I sistemi MetroCluster IP non dispongono di porte ha (High Availability) dedicate. Quando si utilizza *documentazione dei sistemi hardware ONTAP* per installare la piattaforma, non seguire le istruzioni per collegare il cluster e le porte ha.

## Configurare gli switch IP di MetroCluster

### Configurazione degli switch IP Broadcom

È necessario configurare gli switch IP Broadcom per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.



La configurazione richiede licenze aggiuntive (6 licenze per porte da 100 GB) nei seguenti scenari:

- Le porte 53 e 54 vengono utilizzate come ISL MetroCluster a 40 Gbps o 100 Gbps.
- Si utilizza una piattaforma che connette il cluster locale e le interfacce MetroCluster alle porte 49 - 52.

### Ripristino delle impostazioni predefinite dello switch IP Broadcom

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

#### A proposito di questa attività

- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

#### Fasi

1. Passare al prompt dei comandi con privilegi elevati (#): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Cancellare la configurazione di avvio e rimuovere il banner

a. Cancellare la configurazione di avvio:

**erase startup-config**

```
(IP_switch_A_1) #erase startup-config  
  
Are you sure you want to clear the configuration? (y/n) y  
  
(IP_switch_A_1) #
```

Questo comando non cancella il banner.

b. Rimuovere lo striscione:

**no set clibanner**

```
(IP_switch_A_1) #configure  
(IP_switch_A_1) (Config) # no set clibanner  
(IP_switch_A_1) (Config) #
```

3. Riavviare lo switch:\*(IP\_switch\_A\_1) #reload\*

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



Se il sistema chiede se salvare la configurazione non salvata o modificata prima di ricaricare lo switch, selezionare **No**.

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

L'utente predefinito è "admin" e non è stata impostata alcuna password. Viene visualizzato un prompt simile al seguente:

```
(Routing) >
```

5. Passare al prompt dei comandi con privilegi elevati:

enable

```
Routing) > enable  
(Routing) #
```

6. Impostare il protocollo della porta di servizio su none:

```
serviceport protocol none
```

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Assegnare l'indirizzo IP alla porta di servizio:

```
serviceport ip ip-address netmask gateway
```

L'esempio seguente mostra un indirizzo IP assegnato alla porta di servizio "10.10.10.10" con la subnet "255.255.255.0" e il gateway "10.10.10.1":

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Verificare che la porta di servizio sia configurata correttamente:

```
show serviceport
```

L'esempio seguente mostra che la porta è attiva e che sono stati assegnati gli indirizzi corretti:

```
(Routing) #show serviceport

Interface Status..... Up
IP Address..... 10.10.10.10
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.10.10.1
IPv6 Administrative Mode..... Enabled
IPv6 Prefix is .....
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router..... fe80::222:bdf:fef8:19ff
Configured IPv4 Protocol..... None
Configured IPv6 Protocol..... None
IPv6 AutoConfig Mode..... Disabled
Burned In MAC Address..... D8:C4:97:56:87:D7

(Routing) #
```

9. Se lo si desidera, configurare il server SSH.



Il file RCF disattiva il protocollo Telnet. Se non si configura il server SSH, è possibile accedere al bridge solo utilizzando la connessione alla porta seriale.

a. Generare chiavi RSA.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. Generare chiavi DSA (opzionale)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Se si utilizza la versione conforme a FIPS di EFOS, generare le chiavi ECDSA. Nell'esempio seguente vengono create le chiavi con una lunghezza di 521. I valori validi sono 256, 384 o 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Abilitare il server SSH.

Se necessario, uscire dal contesto di configurazione.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+



Se le chiavi sono già presenti, potrebbe essere richiesto di sovrascriverle.

10. Se lo si desidera, configurare il dominio e il server dei nomi:

configure

Nell'esempio riportato di seguito viene illustrato il `ip domain` e `ip name server` comandi:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Se lo si desidera, configurare il fuso orario e la sincronizzazione dell'ora (SNTP).

Nell'esempio riportato di seguito viene illustrato il `sntp` Che specifica l'indirizzo IP del server SNTP e il relativo fuso orario.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

Per EFOS versione 3.10.0.3 e successive, utilizzare `ntp` comando, come illustrato nell'esempio seguente:

```
> (Config)# ntp ?

authenticate          Enables NTP authentication.
authentication-key     Configure NTP authentication key.
broadcast             Enables NTP broadcast mode.
broadcastdelay         Configure NTP broadcast delay in microseconds.
server               Configure NTP server.
source-interface       Configure the NTP source-interface.
trusted-key           Configure NTP authentication key number for
trusted time source.
vrf                   Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

## 12. Configurare il nome dello switch:

```
hostname IP_switch_A_1
```

Il prompt di switch visualizza il nuovo nome:

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

## 13. Salvare la configurazione:

```
write memory
```

Si ricevono messaggi e output simili al seguente esempio:



```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .

Configuration Saved!

```
(IP_switch_A_1) #
```

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

#### Download e installazione del software EFOS dello switch Broadcom

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

#### A proposito di questa attività

Questa attività deve essere ripetuta su ogni switch nella configurazione IP MetroCluster.

#### Nota:

- Quando si esegue l'aggiornamento da EFOS 3.4.x.x a EFOS 3.7.x.x o versioni successive, lo switch deve eseguire EFOS 3.4.4.6 (o versioni successive 3.4.x.x). Se si esegue una release precedente, aggiornare prima lo switch a EFOS 3.4.4.6 (o versione successiva 3.4.x.x), quindi aggiornare lo switch a EFOS 3.7.x.x o versione successiva.
- La configurazione per EFOS 3.4.x.x e 3.7.x.x o versioni successive è diversa. Se si modifica la versione di EFOS da 3.4.x.x a 3.7.x.x o successiva o viceversa, è necessario ripristinare le impostazioni predefinite dello switch e applicare nuovamente i file RCF per la versione di EFOS corrispondente. Questa procedura richiede l'accesso tramite la porta seriale della console.
- A partire dalla versione EFOS 3.7.x.x o successiva, è disponibile una versione non conforme a FIPS e una conforme a FIPS. Quando si passa da una versione non conforme a FIPS a una versione conforme a FIPS o viceversa, si applicano diverse procedure. Se si cambia EFOS da una versione non conforme a FIPS a una conforme a FIPS o viceversa, si ripristinano le impostazioni predefinite dello switch. Questa procedura richiede l'accesso tramite la porta seriale della console.

#### Fasi

1. Verificare che la versione di EFOS in uso sia conforme a FIPS o non conforme a FIPS utilizzando `show fips status` comando. Negli esempi seguenti, `IP_switch_A_1` Utilizza EFOS conforme a FIPS e `IP_switch_A_2` Utilizza EFOS non conforme a FIPS.

#### Esempio 1

```

IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #

```

## Esempio 2

```

IP_switch_A_2 #show fips status
                ^
% Invalid input detected at ``^` marker.

IP_switch_A_2 #

```

2. Utilizzare la seguente tabella per determinare il metodo da seguire:

Procedura	Versione EFOS corrente	Nuova versione EFOS	Fasi di alto livello
Procedura per l'aggiornamento di EFOS tra due versioni (non conformi a FIPS)	3.4.x.x	3.4.x.x	Installare la nuova immagine EFOS utilizzando il metodo 1) le informazioni di configurazione e licenza vengono conservate
3.4.4.6 (o versione successiva 3.4.x.x)	3.7.x.x o versioni successive non conformi a FIPS	Aggiornare EFOS utilizzando il metodo 1. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.7.x.x o versioni successive	3.7.x.x o versioni successive non conformi a FIPS
3.4.4.6 (o versione successiva 3.4.x.x)	Eseguire il downgrade di EFOS utilizzando il metodo 1. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.4.x.x.	3.7.x.x o versioni successive non conformi a FIPS	

Installare la nuova immagine EFOS utilizzando il metodo 1. Le informazioni di configurazione e licenza vengono conservate	3.7.x.x o successivo conforme a FIPS	3.7.x.x o successivo conforme a FIPS	Installare la nuova immagine EFOS utilizzando il metodo 1. Le informazioni di configurazione e licenza vengono conservate
Procedura per l'aggiornamento a/da una versione EFOS conforme a FIPS	Non conforme a FIPS	Conforme a FIPS	Installazione dell'immagine EFOS con il metodo 2. La configurazione dello switch e le informazioni sulla licenza andranno perse.

- Metodo 1: [Procedura per l'aggiornamento di EFOS con il download dell'immagine software nella partizione di boot di backup](#)
- Metodo 2: [Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE](#)

### Procedura per l'aggiornamento di EFOS con il download dell'immagine software nella partizione di boot di backup

È possibile eseguire i seguenti passaggi solo se entrambe le versioni di EFOS non sono conformi a FIPS o se entrambe le versioni di EFOS sono conformi a FIPS.



Non seguire questa procedura se una versione è conforme a FIPS e l'altra non è conforme a FIPS.

#### Fasi

1. Copiare il software dello switch sullo switch: copy  
`sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

In questo esempio, il file del sistema operativo efos-3.4.4.6.stk viene copiato dal server SFTP all'indirizzo 50.50.50.50 nella partizione di backup. È necessario utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```

(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*****

Mode..... SFTP
Set Server IP..... 50.50.50.50
Path..... /switchsoftware/
Filename..... efos-3.4.4.6.stk
Data Type..... Code
Destination Filename..... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...

File transfer operation completed successfully.

(IP_switch_A_1) #

```

2. Impostare lo switch per l'avvio dalla partizione di backup al successivo riavvio dello switch:

```
boot system backup
```

```

(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #

```

3. Verificare che la nuova immagine di avvio sia attiva al prossimo avvio:

```
show bootvar
```

```
(IP_switch_A_1) #show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.4.2	3.4.4.6	3.4.4.2	3.4.4.6

```
(IP_switch_A_1) #
```

#### 4. Salvare la configurazione:

```
write memory
```

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!

```
(IP_switch_A_1) #
```

#### 5. Riavviare lo switch:

```
reload
```

```
(IP_switch_A_1) #reload
```

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

#### 6. Attendere il riavvio dello switch.



In rari casi, lo switch potrebbe non avviarsi. Seguire la [Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE](#) per installare la nuova immagine.

7. Se si cambia lo switch da EFOS 3.4.x.x a EFOS 3.7.x.x o viceversa, seguire le due procedure seguenti per applicare la configurazione corretta (RCF):
  - a. [Ripristino delle impostazioni predefinite dello switch IP Broadcom](#)
  - b. [Download e installazione dei file RCF Broadcom](#)
8. Ripetere questa procedura sui tre switch IP rimanenti nella configurazione IP MetroCluster.

### Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE

Se una versione di EFOS è conforme a FIPS e l'altra non è conforme a FIPS, eseguire le seguenti operazioni. Questa procedura può essere utilizzata per installare l'immagine EFOS 3.7.x.x non conforme a FIPS o FIPS da ONIE in caso di mancato avvio dello switch.

#### Fasi

1. Avviare lo switch in modalità di installazione ONIE.

Durante l'avvio, selezionare ONIE quando viene visualizzata la seguente schermata:

```
+-----+
| EFOS   |
| *ONIE  |
|        |
|        |
|        |
|        |
|        |
|        |
|        |
|        |
|        |
|        |
|        |
+-----+
```

Dopo aver selezionato "ONIE", lo switch si carica e presenta le seguenti opzioni:

```

+-----+
|*ONIE: Install OS                                     |
| ONIE: Rescue                                         |
| ONIE: Uninstall OS                                   |
| ONIE: Update ONIE                                   |
| ONIE: Embed ONIE                                    |
| DIAG: Diagnostic Mode                               |
| DIAG: Burn-In Mode                                 |
|                                                     |
|                                                     |
|                                                     |
|                                                     |
|                                                     |
+-----+

```

Lo switch si avvia in modalità di installazione ONIE.

## 2. Interrompere il rilevamento ONIE e configurare l'interfaccia ethernet

Una volta visualizzato il seguente messaggio, premere Invio per richiamare la console ONIE:

```

Please press Enter to activate this console. Info: eth0:  Checking
link... up.
ONIE:/ #

```



Il rilevamento ONIE continua e i messaggi vengono stampati sulla console.

```

Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #

```

## 3. Configurare l'interfaccia ethernet e aggiungere il percorso utilizzando `ifconfig eth0 <ipAddress> netmask <netmask> up` e `route add default gw <gatewayAddress>`

```

ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1

```

## 4. Verificare che il server che ospita il file di installazione ONIE sia raggiungibile:

```

ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #

```

## 5. Installare il nuovo software dello switch

```

ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.

```

Il software installerà e riavvierà lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione di EFOS.

## 6. Verificare che il nuovo software dello switch sia installato

### **show bootvar**

```

(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----
unit      active      backup    current-active  next-active
----
1    3.7.0.4    3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #

```



## 7. Completare l'installazione

Lo switch si riavvia senza alcuna configurazione applicata e ripristina le impostazioni predefinite. Seguire le due procedure per configurare le impostazioni di base dello switch e applicare il file RCF come indicato nei due documenti seguenti:

- a. Configurare le impostazioni di base dello switch. Seguire i passaggi 4 e successivi: [Ripristino delle impostazioni predefinite dello switch IP Broadcom](#)
- b. Creare e applicare il file RCF come descritto in [Download e installazione dei file RCF Broadcom](#)

### Download e installazione dei file RCF Broadcom

È necessario scaricare e installare il file RCF dello switch su ogni switch nella configurazione IP MetroCluster.

#### Prima di iniziare

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

#### A proposito di questa attività

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

Sono disponibili quattro file RCF, uno per ciascuno dei quattro switch nella configurazione IP di MetroCluster. È necessario utilizzare i file RCF corretti per il modello di switch in uso.

Switch	File RCF
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt



File RCF per EFOS versione 3.4.4.6 o successiva 3.4.x.x. La release e la versione 3.7.0.4 di EFOS sono diverse. Assicurarsi di aver creato i file RCF corretti per la versione EFOS in esecuzione sullo switch.

Versione EFOS	Versione del file RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

#### Fasi

1. Generare i file RCF Broadcom per l'IP MetroCluster.
  - a. Scaricare il ["RcfFileGenerator per MetroCluster IP"](#)
  - b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.



Le modifiche apportate ai file RCF dopo il download non sono supportate.

## 2. Copiare i file RCF sugli switch:

- a. Copiare i file RCF sul primo switch: 

```
copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt  
nvram:script BES-53248_v1.32_Switch-A1.scr
```

In questo esempio, il file RCF "BES-53248\_v1.32\_Switch-A1.txt" viene copiato dal server SFTP in "50.50.50.50" al bootflash locale. È necessario utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```

(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*****

Mode..... SFTP
Set Server IP..... 50.50.50.50
Path..... /RcfFiles/
Filename..... BES-
53248_v1.32_Switch-A1.txt
Data Type..... Config Script
Destination Filename..... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.

Validating configuration script...

config

set clibanner
"*****
*****

* NetApp Reference Configuration File (RCF)

*

* Switch      : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #

```

b. Verificare che il file RCF sia salvato come script:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name          Size(Bytes)  Date of Modification
-----
BES-53248_v1.32_Switch-A1.scr      852         2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Applicare lo script RCF:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y

config

set clibanner
"*****
*****

* NetApp Reference Configuration File (RCF)

*

* Switch      : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Salvare la configurazione:

```
write memory
```

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Configuration Saved!

```
(IP_switch_A_1) #
```

e. Riavviare lo switch:

```
reload
```

```
(IP_switch_A_1) #reload
```

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

a. Ripetere i passaggi precedenti per ciascuno degli altri tre switch, assicurandosi di copiare il file RCF corrispondente sullo switch corrispondente.

3. Ricaricare lo switch:

```
reload
```

```
IP_switch_A_1# reload
```

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

#### Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari.

1. Identificare le porte ISL e i canali delle porte non utilizzati utilizzando il banner del file RCF:



Se la porta è in modalità breakout, il nome della porta specificato nel comando potrebbe essere diverso dal nome indicato nell'intestazione RCF. È inoltre possibile utilizzare i file di cablaggio RCF per individuare il nome della porta.

**Per informazioni dettagliate sulla porta ISL**

Eseguire il comando `show port all`.

**Per i dettagli del canale della porta**

Eseguire il comando `show port-channel all`.

**2. Disattivare le porte ISL e i canali delle porte non utilizzati.**

È necessario eseguire i seguenti comandi per ogni porta o canale di porta non utilizzato identificato.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1) (Config)# <port_name>
(SwtichA_1) (Interface 0/15)# shutdown
(SwtichA_1) (Interface 0/15)# end
(SwtichA_1)# write memory
```

**Configurare gli switch IP Cisco****Configurazione degli switch IP Cisco**

È necessario configurare gli switch IP Cisco per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.

**A proposito di questa attività**

Molte delle procedure descritte in questa sezione sono procedure indipendenti ed è necessario eseguire solo quelle a cui si è indirizzati o che sono pertinenti al proprio compito.

**Ripristino delle impostazioni predefinite dello switch IP Cisco**

Prima di installare qualsiasi file RCF, è necessario cancellare la configurazione dello switch Cisco ed eseguire la configurazione di base. Questa procedura è necessaria quando si desidera reinstallare lo stesso file RCF dopo un'installazione precedente non riuscita o se si desidera installare una nuova versione di un file RCF.

**A proposito di questa attività**

- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

**Fasi****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]", you should respond `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.

### A proposito di questa attività

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"

#### Fasi

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.

### Download e installazione dei file Cisco IP RCF

È necessario scaricare il file RCF su ogni switch nella configurazione IP MetroCluster.

#### A proposito di questa attività

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"

Sono disponibili quattro file RCF, uno per ciascuno dei quattro switch nella configurazione IP di MetroCluster. È necessario utilizzare i file RCF corretti per il modello di switch in uso.

Switch	File RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

### Fasi

1. Scaricare i file MetroCluster IP RCF.



Le modifiche apportate ai file RCF dopo il download non sono supportate.

2. Copiare i file RCF sugli switch:

- a. Copiare i file RCF sul primo switch:

```
copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
bootflash: vrf management
```

In questo esempio, il file RCF NX3232\_v1.80\_Switch-A1.txt viene copiato dal server SFTP all'indirizzo 10.10.99.99 alla flash di avvio locale. Utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```

IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

a. Ripetere il passaggio precedente per ciascuno degli altri tre switch, assicurandosi di copiare il file RCF corrispondente sullo switch corrispondente.

3. Verificare su ogni switch che il file RCF sia presente 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:
.
.
.
5514   Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
.
.
.

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

```

4. Configurare le regioni TCAM sugli switch Cisco 3132Q-V e Cisco 3232C.



Saltare questo passaggio se non si dispone di switch Cisco 3132Q-V o Cisco 3232C.

a. Sullo switch Cisco 3132Q-V, impostare le seguenti regioni TCAM:



```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- b. Sullo switch Cisco 3232C, impostare le seguenti regioni TCAM:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- c. Dopo aver impostato le regioni TCAM, salvare la configurazione e ricaricare lo switch:

```
copy running-config startup-config
reload
```

5. Copiare il file RCF corrispondente dalla flash di avvio locale alla configurazione in esecuzione su ogni switch:

```
copy bootflash:switch-specific-RCF.txt running-config
```

6. Copiare i file RCF dalla configurazione in esecuzione alla configurazione di avvio su ciascun switch:

```
copy running-config startup-config
```

L'output dovrebbe essere simile a quanto segue:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Ricaricare lo switch:

```
reload
```

```
IP_switch_A_1# reload
```

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

## Impostazione della correzione degli errori di inoltro per i sistemi che utilizzano la connettività a 25 Gbps

Se il sistema è configurato utilizzando la connettività a 25 Gbps, è necessario impostare manualmente il parametro fec (Forward Error Correction) su Off dopo aver applicato il file RCF. Il file RCF non applica questa impostazione.

### A proposito di questa attività

Le porte a 25 Gbps devono essere cablate prima di eseguire questa procedura.

["Assegnazioni delle porte della piattaforma per switch Cisco 3232C o Cisco 9336C"](#)

Questa attività si applica solo alle piattaforme che utilizzano la connettività a 25 Gbps:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Questa attività deve essere eseguita su tutti e quattro gli switch nella configurazione IP di MetroCluster.

### Fasi

1. Impostare il parametro fec su Off su ciascuna porta a 25 Gbps collegata a un modulo controller, quindi copiare la configurazione in esecuzione nella configurazione di avvio:
  - a. Accedere alla modalità di configurazione: `config t`
  - b. Specificare l'interfaccia a 25 Gbps da configurare: `interface interface-ID`
  - c. Impostare fec su Off: `fec off`
  - d. Ripetere i passaggi precedenti per ciascuna porta a 25 Gbps dello switch.
  - e. Uscire dalla modalità di configurazione: `exit`

L'esempio seguente mostra i comandi per l'interfaccia Ethernet1/25/1 sullo switch IP\_switch\_A\_1:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Ripetere il passaggio precedente sugli altri tre switch della configurazione IP MetroCluster.

### Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari.

1. Identificare le porte ISL e i canali delle porte non utilizzati:

```
show interface brief
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati.

È necessario eseguire i seguenti comandi per ogni porta o canale di porta non utilizzato identificato.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

### Configurare la crittografia MACsec sugli switch Cisco 9336C



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

### Configurare la crittografia MACsec sugli switch Cisco 9336C

È necessario configurare la crittografia MACsec solo sulle porte ISL WAN in esecuzione tra i siti. È necessario configurare MACsec dopo aver applicato il file RCF corretto.

### 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"](#)

### Abilitare gli 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.

#### Fasi

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
```

## Configurare una catena di chiavi MACsec e le chiavi

È possibile creare una o più chiavi MACsec nella configurazione.

### Key Lifetime e Hitless Key Rollover

Un portachiavi MACsec può avere più chiavi pre-condivise (PSK), ciascuna configurata con un ID chiave e una durata opzionale. La durata della chiave specifica l'ora di attivazione e scadenza della chiave. In assenza di una configurazione a vita, la durata predefinita è illimitata. Quando viene configurata una vita utile, l'MKA passa alla successiva chiave precondivisa configurata nel portachiavi dopo la scadenza della vita utile. Il fuso orario del tasto può essere locale o UTC. Il fuso orario predefinito è UTC. Un tasto può passare a un secondo tasto all'interno dello stesso portachiavi se configuri il secondo tasto (nel portachiavi) e configuri una durata per il primo tasto. Quando la durata della prima chiave scade, passa automaticamente alla chiave successiva nell'elenco. Se la stessa chiave viene configurata su entrambi i lati del collegamento contemporaneamente, il rollover della chiave è hitless (ovvero, il tasto viene rollover senza interruzione del traffico).

### Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Per nascondere la stringa di ottetti della chiave crittografata, sostituire la stringa con un carattere jolly nell'output di `show running-config` e `show startup-config` comandi:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```



La stringa di ottetti viene nascosta anche quando si salva la configurazione in un file.

Per impostazione predefinita, le chiavi PSK vengono visualizzate in formato crittografato e possono essere facilmente decifrate. Questo comando si applica solo alle catene di chiavi MACsec.

3. Creare una catena di chiavi MACsec per contenere una serie di chiavi MACsec e accedere alla modalità di configurazione della catena di chiavi MACsec:

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

4. Creare una chiave MACsec e accedere alla modalità di configurazione della chiave MACsec:

```
key key-id
```

L'intervallo è compreso tra 1 e 32 caratteri esadecimali e la dimensione massima è di 64 caratteri.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configurare la stringa di ottetti per la chiave:

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```



L'argomento `octet-string` può contenere fino a 64 caratteri esadecimali. La chiave `octet` viene codificata internamente, quindi la chiave in testo non viene visualizzata nell'output di `show running-config macsec` comando.

6. Configurare una durata di invio per la chiave (in secondi):

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

Per impostazione predefinita, il dispositivo considera l'ora di inizio come UTC. L'argomento relativo all'ora di inizio indica l'ora e la data in cui la chiave diventa attiva. L'argomento `duration` è la durata della vita in secondi. La lunghezza massima è di 2147483646 secondi (circa 68 anni).

7. Copiare la configurazione in esecuzione nella configurazione di avvio:

```
copy running-config startup-config
```

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

8. Visualizza la configurazione del portachiavi:

```
show key chain name
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

## Configurare un criterio MACsec

### Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Creare un criterio MACsec:

```
macsec policy name
```

```
IP_switch_A_1(config)# macsec policy abc  
IP_switch_A_1(config-macsec-policy)#
```

3. Configurare una delle seguenti crittografia, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 o GCM-AES-XPN-256:

```
cipher-suite name
```

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configurare la priorità del server chiave per interrompere il legame tra i peer durante uno scambio di chiavi:

```
key-server-priority number
```

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configurare il criterio di protezione per definire la gestione dei dati e dei pacchetti di controllo:

```
security-policy security policy
```

Scegliere una policy di sicurezza tra le seguenti opzioni:

- Must-Secure — i pacchetti che non trasportano intestazioni MACsec vengono eliminati
- Dovrebbe-sicuro — sono consentiti pacchetti che non trasportano intestazioni MACsec (questo è il valore predefinito)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configurare la finestra di protezione dalla riproduzione in modo che l'interfaccia protetta non accetti un pacchetto inferiore alle dimensioni della finestra configurata: `window-size number`



La dimensione della finestra di protezione dalla riproduzione rappresenta il numero massimo di frame fuori sequenza che MACsec accetta e non vengono scartati. L'intervallo va da 0 a 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configurare il tempo in secondi per forzare una riskey SAK:

```
sak-expiry-time time
```

È possibile utilizzare questo comando per impostare la chiave di sessione su un intervallo di tempo prevedibile. Il valore predefinito è 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configurare uno dei seguenti offset di riservatezza nel frame Layer 2 in cui inizia la crittografia:

```
conf-offsetconfidentiality offset
```

Scegliere una delle seguenti opzioni:

- CONF-OFFSET-0.
- CONF-OFFSET-30.
- CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```



Questo comando potrebbe essere necessario affinché gli switch intermedi utilizzino intestazioni di pacchetti (dmac, smac, etype) come tag MPLS.

9. Copiare la configurazione in esecuzione nella configurazione di avvio:

```
copy running-config startup-config
```

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

10. Visualizzare la configurazione del criterio MACsec:

```
show macsec policy
```

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

## Abilitare la crittografia Cisco MACsec sulle interfacce

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Selezionare l'interfaccia configurata con la crittografia 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)#
```

3. Aggiungere il portachiavi e il criterio da configurare sull'interfaccia per aggiungere la configurazione MACsec:

```
macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. Ripetere i passaggi 1 e 2 su tutte le interfacce in cui deve essere configurata la crittografia MACsec.
5. Copiare la configurazione in esecuzione nella configurazione di avvio:

```
copy running-config startup-config
```

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

## Disattivare gli ISL WAN con crittografia Cisco MACsec nelle configurazioni IP di MetroCluster

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

### Fasi

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 e il criterio configurati sull'interfaccia per rimuovere la configurazione MACsec:

```
no macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

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
```

## Verifica della configurazione MACsec

### Fasi

1. Ripetere **tutte** le procedure precedenti sul secondo switch all'interno della configurazione per stabilire una sessione MACsec.
2. Eseguire i seguenti comandi per verificare che entrambi gli switch siano crittografati correttamente:
  - a. Esecuzione: `show macsec mka summary`
  - b. Esecuzione: `show macsec mka session`
  - c. Esecuzione: `show macsec mka statistics`

È possibile verificare la configurazione MACsec utilizzando i seguenti comandi:

Comando	Visualizza informazioni su...
<code>show macsec mka session interface typeslot/port number</code>	La sessione MACsec MKA per un'interfaccia specifica o per tutte le interfacce
<code>show key chain name</code>	La configurazione della catena di chiavi
<code>show macsec mka summary</code>	La configurazione MACsec MKA
<code>show macsec policy policy-name</code>	La configurazione per un criterio MACsec specifico o per tutti i criteri MACsec

### Configurare lo switch NVIDIA IP SN2100

È necessario configurare gli switch IP NVIDIA SN2100 per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.

#### Ripristina le impostazioni predefinite dello switch NVIDIA IP SN2100

Per ripristinare le impostazioni predefinite di uno switch, è possibile scegliere tra i seguenti metodi.

- [Ripristinare lo switch utilizzando l'opzione del file RCF](#)
- [Ripristinare lo switch utilizzando l'opzione di installazione di Cumulus](#)

#### ripristinare lo switch utilizzando l'opzione del file RCF

Prima di installare una nuova configurazione RCF, è necessario ripristinare le impostazioni dello switch NVIDIA.

#### A proposito di questa attività

Per ripristinare le impostazioni predefinite dello switch, eseguire il file RCF con `restoreDefaults` opzione. Questa opzione copia i file di backup originali nella posizione originale e riavvia lo switch. Dopo il riavvio, lo switch viene fornito online con la configurazione originale esistente al momento della prima esecuzione del file RCF per configurare lo switch.

I seguenti dettagli di configurazione non vengono ripristinati:

- Configurazione utente e credenziale
- Configurazione della porta di rete di gestione, eth0



Tutte le altre modifiche di configurazione che si verificano durante l'applicazione del file RCF vengono ripristinate alla configurazione originale.

#### Prima di iniziare

- È necessario configurare lo switch in base a. [Scaricare e installare il file NVIDIA RCF](#). Se la configurazione non è stata eseguita in questo modo o se sono state configurate funzionalità aggiuntive prima di eseguire il file RCF, non è possibile utilizzare questa procedura.

- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere connessi allo switch con una connessione seriale alla console.
- Questa attività ripristina la configurazione della rete di gestione.

#### **Fasi**

1. Verificare che la configurazione RCF sia stata applicata correttamente con la stessa versione del file RCF o compatibile e che i file di backup esistano.



L'output può mostrare file di backup, file conservati o entrambi. Se i file di backup o i file conservati non vengono visualizzati nell'output, non è possibile utilizzare questa procedura.

```

cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
Backup files exist.
Preserved files exist.
Listing completion of the steps:
    Success: Step: 1: Performing Backup and Restore
    Success: Step: 2: updating MOTD file
    Success: Step: 3: Disabling apt-get
    Success: Step: 4: Disabling cdp
    Success: Step: 5: Adding lldp config
    Success: Step: 6: Creating interfaces
    Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
    Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
    Success: Step: 9: Configuring switch basic settings: ecn
    Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
    Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
    Success: Step: 12: Configuring switch basic settings: traffic
classification
    Success: Step: 13: Configuring LAG load balancing policies
    Success: Step: 14: Configuring the VLAN bridge
    Success: Step: 15: Configuring local cluster ISL ports
    Success: Step: 16: Configuring MetroCluster ISL ports
    Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
    Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
    Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
    Success: Step: 20: Configuring L2FC for MetroCluster interfaces
    Success: Step: 21: Configuring the interface to UP
    Success: Step: 22: Final commit
    Success: Step: 23: Final reboot of the switch
Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$

```

2. Eseguire il file RCF con l'opzione per ripristinare le impostazioni predefinite: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_2.py
restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Rispondere "sì" al prompt. Lo switch torna alla configurazione originale e si riavvia.
4. Attendere il riavvio dello switch.

Lo switch viene ripristinato e conserva la configurazione iniziale, ad esempio la configurazione della rete di gestione e le credenziali correnti, così come esistevano prima dell'applicazione del file RCF. Dopo il riavvio, è possibile applicare una nuova configurazione utilizzando la stessa versione o una versione diversa del file RCF.

## reimpostare lo switch utilizzando l'opzione di installazione di Cumulus

### A proposito di questa attività

Seguire questa procedura se si desidera ripristinare completamente lo switch applicando l'immagine Cumulus.

#### Prima di iniziare

- È necessario essere connessi allo switch con una connessione seriale alla console.
- L'immagine software dello switch Cumulus è accessibile tramite HTTP.



Per ulteriori informazioni sull'installazione di Cumulus Linux, vedere ["Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100"](#)

- È necessario disporre della password root per `sudo` accesso ai comandi.

#### Fasi

1. Dalla console di Cumulus scaricare e mettere in coda l'installazione del software dello switch con il comando `onie-install -a -i` seguito dal percorso del file per il software dello switch:

In questo esempio, il file del firmware `cumulus-linux-4.4.2-mlx-amd64.bin` Viene copiato dal server HTTP '50.50.50.50' allo switch locale.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.2-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-
mlx-amd64.bin
#####
# 100.0%
Success: HTTP download complete.
```

```
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
in the future
```

```
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Rispondere `y` alla richiesta di conferma dell'installazione quando l'immagine viene scaricata e verificata.
3. Riavviare lo switch per installare il nuovo software: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```



Lo switch si riavvia e viene avviata l'installazione del software dello switch, operazione che richiede un certo tempo. Al termine dell'installazione, lo switch si riavvia e rimane visualizzato il prompt di accesso.

4. Configurare le impostazioni di base dello switch
  - a. All'avvio dello switch e al prompt di accesso, accedere e modificare la password.



Il nome utente è 'cumulus' e la password predefinita è 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.2u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

## 5. Configurare l'interfaccia di rete di gestione.



L'esempio seguente mostra come configurare il nome host (IP\_switch\_A\_1), l'indirizzo IP (10.10.10.10), la netmask (255.255.255.0 (24)) e il gateway (10.10.10.1) utilizzando i comandi: `net add hostname <hostname>`, `net add interface eth0 ip address <IPAddress/mask>`, e `net add interface eth0 ip gateway <Gateway>`.



```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending
```

```
.
.
.
```

```
cumulus@cumulus:mgmt:~$ net commit
```

```
.
.
.
```

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

User Timestamp Command

```
cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1
```

```
cumulus@cumulus:mgmt:~$
```

6. Riavviare lo switch utilizzando `sudo reboot` comando.

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

Al riavvio dello switch, è possibile applicare una nuova configurazione seguendo la procedura descritta in [Scaricare e installare il file NVIDIA RCF](#).

#### Scarica e installa i file NVIDIA RCF

È necessario scaricare e installare il file RCF dello switch su ogni switch nella configurazione IP MetroCluster.

#### Prima di iniziare

- È necessario disporre della password root per `sudo` accesso ai comandi.
- Il software dello switch è installato e la rete di gestione è configurata.

- È stata eseguita la procedura per installare inizialmente lo switch utilizzando il metodo 1 o il metodo 2.
- Non è stata applicata alcuna configurazione aggiuntiva dopo l'installazione iniziale.



Se si esegue un'ulteriore configurazione dopo aver reimpostato lo switch e prima di applicare il file RCF, non è possibile utilizzare questa procedura.

### A proposito di questa attività

Ripetere questa procedura su ciascuno switch IP nella configurazione MetroCluster IP (nuova installazione) o sullo switch sostitutivo (sostituzione dello switch).

### Fasi

1. Generare i file NVIDIA RCF per MetroCluster IP.
  - a. Scaricare il ["RcfFileGenerator per MetroCluster IP"](#).
  - b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.
  - c. Accedere alla home directory. Se si è registrati come 'cumulo', il percorso del file è /home/cumulus.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

- d. Scaricare il file RCF in questa directory. L'esempio seguente mostra che si utilizza SCP per scaricare il file MSN2100\_v1.0\_IP\_switch\_A\_1.txt dal server '50.50.50.50' alla home directory e salvarlo con nome MSN2100\_v1.0\_IP\_switch\_A\_1.py:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/MSN2100_v1.0_IP_switch_A_1.txt
./MSN2100_v1.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*****
**
Banner of the SCP server
*****
**
username@50.50.50.50's password:
MSN2100_v1.0-X2_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Eseguire il file RCF. Il file RCF richiede un'opzione per applicare uno o più passaggi. Se non richiesto dal supporto tecnico, eseguire il file RCF senza l'opzione della riga di comando. Per verificare lo stato di completamento delle varie fasi del file RCF, utilizzare l'opzione '-1' o 'all' per applicare tutte le fasi (in sospenso).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes

... the steps will apply - this is generating a lot of output ...

Running Step 24: Final reboot of the switch

... The switch will reboot if all steps applied successfully ...
```

#### Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari.

1. Identificare le porte ISL e i canali delle porte non utilizzati utilizzando il banner del file RCF:



Se la porta è in modalità breakout, il nome della porta specificato nel comando potrebbe essere diverso dal nome indicato nell'intestazione RCF. È inoltre possibile utilizzare i file di cablaggio RCF per individuare il nome della porta.

```
net show interface
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati utilizzando il file RCF.

```

cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version   : 5.4.0
    Running RCF file version  : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
    sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
Available commands:
    UP / DOWN the switchport
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
    Set the switch port speed
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
    Set the fec mode on the switch port
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
    Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
    Set the option on the port to support DAC cables. This option
does not support port ranges.
    You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
    This setting requires Cumulus 5.4 or a later 5.x release.
        sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$

```

Il seguente comando di esempio disattiva la porta "swp14":

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Ripetere questo passaggio per ogni porta o canale di porta non utilizzato identificato.

### Configurare gli switch IP MetroCluster per il monitoraggio dello stato

Nelle configurazioni IP di MetroCluster, è possibile configurare SNMPv3 per monitorare lo stato degli switch IP.

### Passaggio 1: Configurare l'utente SNMPv3 sugli switch IP MetroCluster

Per configurare l'utente SNMPv3 sugli switch IP MetroCluster, procedere come segue.



Nei comandi è necessario utilizzare sia i protocolli di autenticazione che quelli di privacy. L'utilizzo dell'autenticazione senza privacy non è supportato.

## Per gli switch IP Broadcom

### Fasi

1. Se il gruppo utenti 'network-admin' non esiste già, crearlo:

```
(IP_switch_1) (Config)# snmp-server group network-admin v3 auth read  
"Default"
```

2. Confermare che il gruppo "network-admin" è stato creato:

```
(IP_switch_1) (Config)# show snmp group
```

3. Configurare l'utente SNMPv3 sugli switch IP Broadcom:

```
(IP_switch_1)# config  
(IP_switch_1) (Config)# snmp-server user <user_name> network-admin  
[auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]  
"<priv_password>"
```

È necessario utilizzare le virgolette intorno alle password di autenticazione e privacy, come illustrato nell'esempio seguente:

```
snmp-server user admin1 network-admin auth-md5 "password" priv-des  
"password"
```

## Per gli switch IP Cisco

### Fasi

1. Eseguire i seguenti comandi per configurare l'utente SNMPv3 su uno switch IP Cisco:

```
IP_switch_A_1 # configure terminal  
IP_switch_A_1 (config) # snmp-server user <user_name> auth  
[md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
```

2. Verificare che l'utente SNMPv3 sia configurato sullo switch:

```
IP_switch_A_1 (config) # show snmp user <user_name>
```

L'output di esempio riportato di seguito mostra che l'utente admin È configurato per SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User          Auth          Priv(enforce) Groups
acl_filter

_____
_____

admin          md5          aes-128(no)   network-admin
```

## Passaggio 2: Configurare l'utente SNMPv3 in ONTAP

Per configurare l'utente SNMPv3 in ONTAP, procedere come segue.

1. Configurare l'utente SNMPv3 in ONTAP:

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

2. Configurare il monitoraggio dello stato dello switch per monitorare lo switch utilizzando il nuovo utente SNMPv3:

```
system switch ethernet modify -device <device_id> -snmp-version SNMPv3
-community-or-username <user_name>
```

3. Verificare che il numero di serie della periferica che verrà monitorato con l'utente SNMPv3 appena creato sia corretto:

- a. Visualizzare il periodo di tempo di polling del monitoraggio dello stato dello switch:

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

- b. Eseguire il comando seguente dopo aver esaurito il tempo di polling:

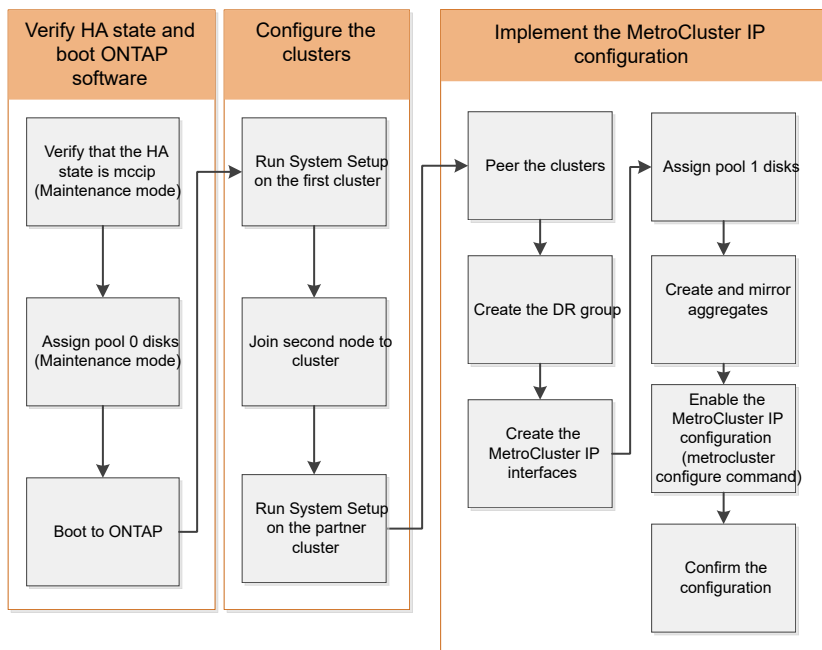
```
system switch ethernet show-all -instance -device <device_serial_number>
```

# Configurare il software MetroCluster in ONTAP

## Configurazione del software MetroCluster in ONTAP

È necessario impostare ciascun nodo nella configurazione MetroCluster in ONTAP, incluse le configurazioni a livello di nodo e la configurazione dei nodi in due siti. È inoltre necessario implementare la relazione MetroCluster tra i due siti.

Se un modulo controller si guasta durante la configurazione, fare riferimento a. ["Scenari di guasto del modulo controller durante l'installazione di MetroCluster"](#).



## Gestione delle configurazioni a otto nodi

Una configurazione a otto nodi è costituita da due gruppi di DR. Configurare il primo gruppo DR utilizzando le attività descritte in questa sezione.

Quindi, eseguire le attività in ["Espansione di una configurazione IP MetroCluster a quattro nodi in una configurazione a otto nodi"](#)

## Raccolta delle informazioni richieste

Prima di iniziare il processo di configurazione, è necessario raccogliere gli indirizzi IP richiesti per i moduli controller.

È possibile utilizzare questi collegamenti per scaricare i file csv e compilare le tabelle con le informazioni specifiche del sito.

["Foglio di lavoro per la configurazione dell'IP MetroCluster, Site\\_A."](#)

["Foglio di lavoro per la configurazione dell'IP MetroCluster, Site\\_B."](#)

## Analogie e differenze tra cluster standard e configurazioni MetroCluster

La configurazione dei nodi in ciascun cluster in una configurazione MetroCluster è simile a quella dei nodi in un cluster standard.

La configurazione di MetroCluster si basa su due cluster standard. Fisicamente, la configurazione deve essere simmetrica, con ciascun nodo con la stessa configurazione hardware e tutti i componenti MetroCluster devono essere cablati e configurati. Tuttavia, la configurazione software di base per i nodi in una configurazione MetroCluster è uguale a quella per i nodi in un cluster standard.



Fase di configurazione	Configurazione standard del cluster	Configurazione di MetroCluster
Configurare le LIF di gestione, cluster e dati su ciascun nodo.	Lo stesso vale per entrambi i tipi di cluster	
Configurare l'aggregato root.	Lo stesso vale per entrambi i tipi di cluster	
Impostare il cluster su un nodo del cluster.	Lo stesso vale per entrambi i tipi di cluster	
Unire l'altro nodo al cluster.	Lo stesso vale per entrambi i tipi di cluster	
Creare un aggregato root mirrorato.	Opzionale	Obbligatorio
Peer dei cluster.	Opzionale	Obbligatorio
Abilitare la configurazione MetroCluster.	Non applicabile	Obbligatorio

## Verifica dello stato ha-config dei componenti

In una configurazione IP MetroCluster non preconfigurata in fabbrica, verificare che lo stato ha-config dei componenti del controller e del telaio sia impostato su “mcip” in modo che si avviino correttamente. Per i sistemi ricevuti dalla fabbrica, questo valore è preconfigurato e non è necessario verificarlo.

### Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

### Fasi

1. Visualizzare lo stato ha del modulo controller e dello chassis:

```
ha-config show
```

Il modulo controller e lo chassis devono visualizzare il valore “mcip”.

2. Se lo stato di sistema visualizzato del controller non è “mccip”, impostare lo stato ha per il controller:

```
ha-config modify controller mccip
```

3. Se lo stato di sistema visualizzato dello chassis non è “mccip”, impostare lo stato ha per lo chassis:

```
ha-config modify chassis mccip
```

4. Ripetere questi passaggi su ciascun nodo della configurazione MetroCluster.

## Ripristino delle impostazioni predefinite di sistema su un modulo controller

Ripristinare le impostazioni predefinite dei moduli controller.

1. Al prompt DEL CARICATORE, riportare le variabili ambientali alle impostazioni predefinite: `set-defaults`
2. Avviare il nodo dal menu di boot: `boot_ontap menu`

Dopo aver eseguito questo comando, attendere che venga visualizzato il menu di avvio.

3. Cancellare la configurazione del nodo:

- Se si utilizzano sistemi configurati per ADP, selezionare l'opzione 9a dal menu di avvio e rispondere no quando richiesto.



Questo processo è disagregativo.

La seguente schermata mostra il prompt del menu di avvio:

```
Please choose one of the following:
```

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a
```

```
...
```

```
##### WARNING: AGGREGATES WILL BE DESTROYED #####
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.
```

```
Before proceeding further, make sure that:
```

```
The aggregates visible from this node do not contain
data that needs to be preserved.
```

```
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
```

```
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
```

```
Do you want to abort this operation (yes/no)? no
```

- Se il sistema non è configurato per ADP, digitare `wipeconfig` Al prompt del menu di avvio, quindi premere Invio.

La seguente schermata mostra il prompt del menu di avvio:

```
Please choose one of the following:
```

- (1) Normal Boot.
- (2) Boot without /etc/rc.
- (3) Change password.
- (4) Clean configuration and initialize all disks.
- (5) Maintenance mode boot.
- (6) Update flash from backup config.
- (7) Install new software first.
- (8) Reboot node.
- (9) Configure Advanced Drive Partitioning.

```
Selection (1-9)? wipeconfig
```

```
This option deletes critical system configuration, including cluster membership.
```

```
Warning: do not run this option on a HA node that has been taken over.
```

```
Are you sure you want to continue?: yes
```

```
Rebooting to finish wipeconfig request.
```

## Assegnazione manuale delle unità al pool 0

Se i sistemi preconfigurati non sono stati ricevuti dalla fabbrica, potrebbe essere necessario assegnare manualmente il pool 0 dischi. A seconda del modello di piattaforma e se il sistema utilizza ADP, è necessario assegnare manualmente le unità al pool 0 per ciascun nodo nella configurazione IP di MetroCluster. La procedura da seguire dipende dalla versione di ONTAP in uso.

### Assegnazione manuale dei dischi per il pool 0 (ONTAP 9.4 e versioni successive)

Se il sistema non è stato preconfigurato in fabbrica e non soddisfa i requisiti per l'assegnazione automatica del disco, è necessario assegnare manualmente il pool 0 dischi.

#### A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.4 o versioni successive.

Per determinare se il sistema richiede l'assegnazione manuale del disco, è necessario esaminare ["Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"](#).

Questa procedura viene eseguita in modalità manutenzione. La procedura deve essere eseguita su ciascun nodo della configurazione.

Gli esempi di questa sezione si basano sui seguenti presupposti:

- Node\_A\_1 e Node\_A\_2 su:
  - Site\_A-shelf\_1 (locale)
  - Site\_B-shelf\_2 (remoto)
- Node\_B\_1 e Node\_B\_2 su:
  - Site\_B-shelf\_1 (locale)
  - Site\_A-shelf\_2 (remoto)

## **Fasi**

1. Visualizzare il menu di avvio:

```
boot_ontap menu
```

2. Selezionare l'opzione 9a e rispondere `no` quando richiesto.

La seguente schermata mostra il prompt del menu di avvio:

Please choose one of the following:

- (1) Normal Boot.
- (2) Boot without /etc/rc.
- (3) Change password.
- (4) Clean configuration and initialize all disks.
- (5) Maintenance mode boot.
- (6) Update flash from backup config.
- (7) Install new software first.
- (8) Reboot node.
- (9) Configure Advanced Drive Partitioning.
- (10) Set Onboard Key Manager recovery secrets.
- (11) Configure node for external key management.

Selection (1-11)? 9a

...

##### WARNING: AGGREGATES WILL BE DESTROYED #####  
This is a disruptive operation that applies to all the disks  
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain  
data that needs to be preserved.

This option (9a) has been executed or will be executed  
on the HA partner node (and DR/DR-AUX partner nodes if  
applicable), prior to reinitializing any system in the  
HA-pair or MetroCluster configuration.

The HA partner node (and DR/DR-AUX partner nodes if  
applicable) is currently waiting at the boot menu.

Do you want to abort this operation (yes/no)? no

3. Al riavvio del nodo, premere Ctrl-C quando richiesto per visualizzare il menu di avvio, quindi selezionare l'opzione **Maintenance mode boot** (Avvio in modalità manutenzione).
4. In modalità Maintenance (manutenzione), assegnare manualmente i dischi per gli aggregati locali sul nodo:

```
disk assign disk-id -p 0 -s local-node-sysid
```

I dischi devono essere assegnati simmetricamente, in modo che ogni nodo abbia un numero uguale di dischi. La procedura seguente riguarda una configurazione con due shelf di storage in ogni sito.

- a. Durante la configurazione di Node\_A\_1, assegnare manualmente le unità dallo slot 0 a 11 al pool 0 del nodo A1 da Site\_A-shelf\_1.
- b. Durante la configurazione di Node\_A\_2, assegnare manualmente le unità dallo slot 12 a 23 al pool 0 del nodo A2 da Site\_A-shelf\_1.

- c. Durante la configurazione di Node\_B\_1, assegnare manualmente le unità dallo slot 0 a 11 al pool 0 del nodo B1 da Site\_B-shelf\_1.
- d. Durante la configurazione di Node\_B\_2, assegnare manualmente le unità dallo slot 12 a 23 al pool 0 del nodo B2 dal sito\_B-shelf\_1.

5. Uscire dalla modalità di manutenzione:

```
halt
```

6. Visualizzare il menu di avvio:

```
boot_ontap menu
```

- 7. Ripetere questa procedura sugli altri nodi nella configurazione IP MetroCluster.
- 8. Selezionare l'opzione **4** dal menu di boot su entrambi i nodi e lasciare che il sistema si avvii.
- 9. Passare a ["Configurazione di ONTAP"](#).

### Assegnazione manuale delle unità per il pool 0 (ONTAP 9.3)

Se si dispone di almeno due shelf di dischi per ciascun nodo, si utilizza la funzionalità di assegnazione automatica di ONTAP per assegnare automaticamente i dischi locali (pool 0).

#### A proposito di questa attività

Mentre il nodo è in modalità manutenzione, è necessario assegnare un singolo disco sugli shelf appropriati al pool 0. ONTAP assegna quindi automaticamente il resto dei dischi sullo shelf allo stesso pool. Questa attività non è richiesta sui sistemi ricevuti dalla fabbrica, che hanno il pool 0 per contenere l'aggregato root preconfigurato.

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.3.

Questa procedura non è necessaria se si riceve la configurazione MetroCluster dalla fabbrica. I nodi della fabbrica sono configurati con pool 0 dischi e aggregati root.

Questa procedura può essere utilizzata solo se si dispone di almeno due shelf di dischi per ciascun nodo, che consente l'assegnazione automatica a livello di shelf dei dischi. Se non è possibile utilizzare l'assegnazione automatica a livello di shelf, è necessario assegnare manualmente i dischi locali in modo che ogni nodo disponga di un pool locale di dischi (pool 0).

Questi passaggi devono essere eseguiti in modalità manutenzione.

Gli esempi di questa sezione presuppongono i seguenti shelf di dischi:

- Node\_A\_1 possiede i dischi su:
  - Site\_A-shelf\_1 (locale)
  - Sito\_B-shelf\_2 (remoto)
- Node\_A\_2 è connesso a:
  - Site\_A-shelf\_3 (locale)
  - Sito\_B-shelf\_4 (remoto)
- Node\_B\_1 è connesso a:
  - Sito\_B-shelf\_1 (locale)

- Site\_A-shelf\_2 (remoto)
- Node\_B\_2 è connesso a:
  - Site\_B-shelf\_3 (locale)
  - Site\_A-shelf\_4 (remoto)

## Fasi

1. Assegnare manualmente un singolo disco per l'aggregato root su ciascun nodo:

```
disk assign disk-id -p 0 -s local-node-sysid
```

L'assegnazione manuale di questi dischi consente alla funzione di assegnazione automatica ONTAP di assegnare il resto dei dischi su ogni shelf.

- a. Sul nodo\_A\_1, assegnare manualmente un disco dal sito locale\_A-shelf\_1 al pool 0.
  - b. Sul nodo\_A\_2, assegnare manualmente un disco dal sito locale\_A-shelf\_3 al pool 0.
  - c. Sul nodo\_B\_1, assegnare manualmente un disco dal sito locale\_B-shelf\_1 al pool 0.
  - d. Sul nodo\_B\_2, assegnare manualmente un disco dal sito locale\_B-shelf\_3 al pool 0.
2. Avviare ciascun nodo nel sito A, utilizzando l'opzione 4 del menu di boot:

Completare questo passaggio su un nodo prima di passare al nodo successivo.

- a. Uscire dalla modalità di manutenzione:

```
halt
```

- b. Visualizzare il menu di avvio:

```
boot_ontap menu
```

- c. Selezionare l'opzione 4 dal menu di avvio e procedere.

3. Avviare ciascun nodo nel sito B, utilizzando l'opzione 4 del menu di boot:

Completare questo passaggio su un nodo prima di passare al nodo successivo.

- a. Uscire dalla modalità di manutenzione:

```
halt
```

- b. Visualizzare il menu di avvio:

```
boot_ontap menu
```

- c. Selezionare l'opzione 4 dal menu di avvio e procedere.

## Configurazione di ONTAP

Dopo aver avviato ciascun nodo, viene richiesto di eseguire la configurazione di base del nodo e del cluster. Dopo aver configurato il cluster, tornare alla CLI ONTAP per creare aggregati e creare la configurazione MetroCluster.

## Prima di iniziare

- La configurazione MetroCluster deve essere cablata.

Se è necessario eseguire il netboot dei nuovi controller, vedere ["Avvio in rete dei nuovi moduli controller"](#).

## A proposito di questa attività

Questa attività deve essere eseguita su entrambi i cluster nella configurazione MetroCluster.

## Fasi

1. Accendere ciascun nodo nel sito locale, se non è già stato fatto, e lasciare che tutti i nodi si avviino completamente.

Se il sistema si trova in modalità manutenzione, è necessario eseguire il comando `halt` per uscire dalla modalità manutenzione, quindi eseguire il comando `boot_ontap` per avviare il sistema e accedere alla configurazione del cluster.

2. Sul primo nodo di ciascun cluster, seguire le istruzioni per configurare il cluster.
  - a. Attivare lo strumento AutoSupport seguendo le istruzioni fornite dal sistema.

L'output dovrebbe essere simile a quanto segue:



Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".

To accept a default or omit a question, do not enter a value.

This system will send event messages and periodic reports to NetApp Technical

Support. To disable this feature, enter  
autosupport modify -support disable  
within 24 hours.

Enabling AutoSupport can significantly speed problem determination and

resolution should a problem occur on your system.

For further information on AutoSupport, see:

<http://support.netapp.com/autosupport/>

Type yes to confirm and continue {yes}: yes

.  
.  
.

b. Configurare l'interfaccia di gestione dei nodi rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Creare il cluster rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
create
```

```
Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no
```

```
Existing cluster interface configuration found:
```

```
Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0
```

```
Do you want to use this configuration? {yes, no} [yes]: no
```

```
System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
```

```
Do you want to use these defaults? {yes, no} [yes]: no
```

```
Enter the cluster administrator's (username "admin") password:
```

```
Retype the password:
```

```
Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.
```

```
List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A
```

```
Creating cluster cluster_A
```

```
Starting cluster support services ...
```

```
Cluster cluster_A has been created.
```

- d. Aggiungere licenze, configurare una SVM di amministrazione cluster e immettere le informazioni DNS rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:

Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.

Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO will be enabled when the partner joins the cluster.

Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

- e. Abilitare il failover dello storage e configurare il nodo rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.
```

```
SFO will be enabled when the partner joins the cluster.
```

```
Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.
```

```
Where is the controller located []: site_A
```

- f. Completare la configurazione del nodo, ma non creare aggregati di dati.

Puoi utilizzare ONTAP System Manager puntando il browser web all'indirizzo IP di gestione del cluster (https://172.17.12.153)., Cluster Management)

["Gestione del cluster con Gestore di sistema \(ONTAP 9.7 e versioni precedenti\)"](#)

["Gestore di sistema ONTAP \(versione 9.7 e successive\)"](#)

- g. Configurare il Service Processor (SP):

["Configurare la rete SP/BMC"](#)

["Utilizza un Service Processor con Gestione di sistema - ONTAP 9.7 e versioni precedenti"](#)

3. Avviare il controller successivo e unirsi al cluster, seguendo le istruzioni.  
4. Verificare che i nodi siano configurati in modalità ad alta disponibilità:

```
storage failover show -fields mode
```

In caso contrario, è necessario configurare la modalità ha su ciascun nodo, quindi riavviare i nodi:

```
storage failover modify -mode ha -node localhost
```



Lo stato di configurazione previsto di ha e failover dello storage è il seguente:

- La modalità HA è configurata ma il failover dello storage non è abilitato.
- La funzionalità HA Takeover è disattivata.
- Le interfacce HA sono offline.
- La modalità HA, il failover dello storage e le interfacce vengono configurati più avanti nel processo.

5. Verificare che siano configurate quattro porte come interconnessioni cluster:

```
network port show
```

Le interfacce IP di MetroCluster non sono attualmente configurate e non vengono visualizzate nell'output del comando.

L'esempio seguente mostra due porte del cluster su Node\_A\_1:

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

Node: node_A_1

Ignore

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

e4a      Cluster      Cluster      up    9000  auto/40000 healthy
false

e4e      Cluster      Cluster      up    9000  auto/40000 healthy
false

Node: node_A_2

Ignore

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

e4a      Cluster      Cluster      up    9000  auto/40000 healthy
false
```

```
e4e      Cluster      Cluster      up      9000      auto/40000 healthy
false

4 entries were displayed.
```

6. Ripetere questi passaggi sul cluster partner.

### Cosa fare in seguito

Tornare all'interfaccia della riga di comando di ONTAP e completare la configurazione di MetroCluster eseguendo le seguenti operazioni.

## Configurazione dei cluster in una configurazione MetroCluster

È necessario eseguire il peer dei cluster, eseguire il mirroring degli aggregati root, creare un aggregato di dati mirrorati e quindi eseguire il comando per implementare le operazioni MetroCluster.

### A proposito di questa attività

Prima di correre `metrocluster configure`, La modalità ha e il mirroring DR non sono abilitati e potrebbe essere visualizzato un messaggio di errore relativo a questo comportamento previsto. La modalità ha e il mirroring del DR vengono successivamente attivate quando si esegue il comando `metrocluster configure` per implementare la configurazione.

### Disattivazione dell'assegnazione automatica del disco (se si esegue l'assegnazione manuale in ONTAP 9.4)

In ONTAP 9.4, se la configurazione MetroCluster IP ha meno di quattro shelf di storage esterni per sito, è necessario disattivare l'assegnazione automatica dei dischi su tutti i nodi e assegnarli manualmente.

### A proposito di questa attività

Questa attività non è richiesta in ONTAP 9.5 e versioni successive.

Questa attività non si applica a un sistema AFF A800 con uno shelf interno e senza shelf esterni.

["Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"](#)

### Fasi

1. Disattivare l'assegnazione automatica dei dischi:

```
storage disk option modify -node node_name -autoassign off
```

2. È necessario eseguire questo comando su tutti i nodi della configurazione IP MetroCluster.

### Verifica dell'assegnazione dei dischi del pool 0

È necessario verificare che i dischi remoti siano visibili ai nodi e che siano stati assegnati correttamente.

### A proposito di questa attività

L'assegnazione automatica dipende dal modello di piattaforma del sistema storage e dalla disposizione degli

shelf di dischi.

"Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"

Fasi

- 1. Verificare che i dischi del pool 0 siano assegnati automaticamente:

```
disk show
```

L'esempio seguente mostra l'output "cluster\_A" per un sistema AFF A800 senza shelf esterni.

Un quarto (8 dischi) è stato assegnato automaticamente a "Node\_A\_1" e un quarto è stato assegnato automaticamente a "Node\_A\_2". I dischi rimanenti saranno unità remote (pool 1) per "Node\_B\_1" e "Node\_B\_2".

cluster\_A::\*> disk show

Disk Owner	Usable Size	Disk Shelf	Bay	Container Type	Type	Container Name
node_A_1:0n.12	1.75TB	0	12	SSD-NVM	shared	aggr0
node_A_1:0n.13	1.75TB	0	13	SSD-NVM	shared	aggr0
node_A_1:0n.14	1.75TB	0	14	SSD-NVM	shared	aggr0
node_A_1:0n.15	1.75TB	0	15	SSD-NVM	shared	aggr0
node_A_1:0n.16	1.75TB	0	16	SSD-NVM	shared	aggr0
node_A_1:0n.17	1.75TB	0	17	SSD-NVM	shared	aggr0
node_A_1:0n.18	1.75TB	0	18	SSD-NVM	shared	aggr0
node_A_1:0n.19	1.75TB	0	19	SSD-NVM	shared	-
node_A_2:0n.0	1.75TB	0	0	SSD-NVM	shared	aggr0_node_A_2_0 node_A_2
node_A_2:0n.1	1.75TB	0	1	SSD-NVM	shared	aggr0_node_A_2_0 node_A_2
node_A_2:0n.2	1.75TB	0	2	SSD-NVM	shared	aggr0_node_A_2_0 node_A_2
node_A_2:0n.3	1.75TB	0	3	SSD-NVM	shared	aggr0_node_A_2_0 node_A_2
node_A_2:0n.4	1.75TB	0	4	SSD-NVM	shared	aggr0_node_A_2_0 node_A_2

```

node_A_2:0n.5      1.75TB      0      5      SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6      1.75TB      0      6      SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7      1.75TB      0      7      SSD-NVM shared      -
node_A_2
node_A_2:0n.24     -            0      24     SSD-NVM unassigned -      -
node_A_2:0n.25     -            0      25     SSD-NVM unassigned -      -
node_A_2:0n.26     -            0      26     SSD-NVM unassigned -      -
node_A_2:0n.27     -            0      27     SSD-NVM unassigned -      -
node_A_2:0n.28     -            0      28     SSD-NVM unassigned -      -
node_A_2:0n.29     -            0      29     SSD-NVM unassigned -      -
node_A_2:0n.30     -            0      30     SSD-NVM unassigned -      -
node_A_2:0n.31     -            0      31     SSD-NVM unassigned -      -
node_A_2:0n.36     -            0      36     SSD-NVM unassigned -      -
node_A_2:0n.37     -            0      37     SSD-NVM unassigned -      -
node_A_2:0n.38     -            0      38     SSD-NVM unassigned -      -
node_A_2:0n.39     -            0      39     SSD-NVM unassigned -      -
node_A_2:0n.40     -            0      40     SSD-NVM unassigned -      -
node_A_2:0n.41     -            0      41     SSD-NVM unassigned -      -
node_A_2:0n.42     -            0      42     SSD-NVM unassigned -      -
node_A_2:0n.43     -            0      43     SSD-NVM unassigned -      -
32 entries were displayed.

```

L'esempio seguente mostra l'output "cluster\_B":

```

cluster_B::> disk show

          Usable      Disk      Container      Container
Disk      Size      Shelf Bay Type      Type      Name
Owner
-----
-----

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12      1.75TB      0      12      SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13      1.75TB      0      13      SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14      1.75TB      0      14      SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15      1.75TB      0      15      SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16      1.75TB      0      16      SSD-NVM shared      aggr0

```



```

node_B_1
node_B_1:0n.17    1.75TB    0    17    SSD-NVM shared    aggr0
node_B_1
node_B_1:0n.18    1.75TB    0    18    SSD-NVM shared    aggr0
node_B_1
node_B_1:0n.19    1.75TB    0    19    SSD-NVM shared    -
node_B_1
node_B_2:0n.0     1.75TB    0    0     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1     1.75TB    0    1     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2     1.75TB    0    2     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3     1.75TB    0    3     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4     1.75TB    0    4     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5     1.75TB    0    5     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6     1.75TB    0    6     SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7     1.75TB    0    7     SSD-NVM shared    -
node_B_2
node_B_2:0n.24    -          0    24    SSD-NVM unassigned -    -
node_B_2:0n.25    -          0    25    SSD-NVM unassigned -    -
node_B_2:0n.26    -          0    26    SSD-NVM unassigned -    -
node_B_2:0n.27    -          0    27    SSD-NVM unassigned -    -
node_B_2:0n.28    -          0    28    SSD-NVM unassigned -    -
node_B_2:0n.29    -          0    29    SSD-NVM unassigned -    -
node_B_2:0n.30    -          0    30    SSD-NVM unassigned -    -
node_B_2:0n.31    -          0    31    SSD-NVM unassigned -    -
node_B_2:0n.36    -          0    36    SSD-NVM unassigned -    -
node_B_2:0n.37    -          0    37    SSD-NVM unassigned -    -
node_B_2:0n.38    -          0    38    SSD-NVM unassigned -    -
node_B_2:0n.39    -          0    39    SSD-NVM unassigned -    -
node_B_2:0n.40    -          0    40    SSD-NVM unassigned -    -
node_B_2:0n.41    -          0    41    SSD-NVM unassigned -    -
node_B_2:0n.42    -          0    42    SSD-NVM unassigned -    -
node_B_2:0n.43    -          0    43    SSD-NVM unassigned -    -
32 entries were displayed.

cluster_B::>

```

## Peering dei cluster

I cluster nella configurazione di MetroCluster devono essere in una relazione peer in modo da poter comunicare tra loro ed eseguire il mirroring dei dati essenziale per il disaster recovery di MetroCluster.

### Informazioni correlate

["Configurazione rapida del peering di cluster e SVM"](#)

["Considerazioni sull'utilizzo di porte dedicate"](#)

["Considerazioni sulla condivisione delle porte dati"](#)

## Configurazione delle LIF di intercluster per il peering dei cluster

È necessario creare LIF intercluster sulle porte utilizzate per la comunicazione tra i cluster di partner MetroCluster. È possibile utilizzare porte o porte dedicate che dispongono anche di traffico dati.

### Configurazione di LIF intercluster su porte dedicate

È possibile configurare le LIF tra cluster su porte dedicate. In genere, aumenta la larghezza di banda disponibile per il traffico di replica.

### Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in "cluster01":

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000

## 2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

```
network interface show -fields home-port,curr-port
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che alle porte "e0e" e "e0f" non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1 e0a       e0a
Cluster cluster01-01_clus2 e0b       e0b
Cluster cluster01-02_clus1 e0a       e0a
Cluster cluster01-02_clus2 e0b       e0b
cluster01
    cluster_mgmt           e0c       e0c
cluster01
    cluster01-01_mgmt1     e0c       e0c
cluster01
    cluster01-02_mgmt1     e0c       e0c
```

## 3. Creare un gruppo di failover per le porte dedicate:

```
network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports
```

Nell'esempio seguente vengono assegnate le porte "e0e" e "e0f" al gruppo di failover "cluster01" sul sistema "SVMcluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verificare che il gruppo di failover sia stato creato:

```
network interface failover-groups show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface failover-groups show
Vserver          Group          Failover
-----
Targets
-----
Cluster
Cluster
cluster01-01:e0a, cluster01-01:e0b,
cluster01-02:e0a, cluster01-02:e0b
cluster01
Default
cluster01-01:e0c, cluster01-01:e0d,
cluster01-02:e0c, cluster01-02:e0d,
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
intercluster01
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Versione di ONTAP	Comando
9.6 e versioni successive	<pre>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask -failover -group failover_group</pre>

9.5 e versioni precedenti	<pre>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group</pre>
---------------------------	--

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF di intercluster "cluster01\_icl01" e "cluster01\_icl02" nel gruppo di failover "intercluster01":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verificare che le LIF dell'intercluster siano state create:

<b>In ONTAP 9.6 e versioni successive:</b>
<pre>network interface show -service-policy default-intercluster</pre>
<b>In ONTAP 9.5 e versioni precedenti:</b>
<pre>network interface show -role intercluster</pre>

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01
true				e0e
	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02
true				e0f

7. Verificare che le LIF dell'intercluster siano ridondanti:

**In ONTAP 9.6 e versioni successive:**

```
network interface show -service-policy default-intercluster -failover
```

**In ONTAP 9.5 e versioni precedenti:**

```
network interface show -role intercluster -failover
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

L'esempio seguente mostra che le LIF dell'intercluster "cluster01\_icl01" e "cluster01\_icl02" sulla porta "SVMe0e" effettueranno il failover sulla porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical	Home	Failover	Failover
	Interface	Node:Port	Policy	Group
cluster01	cluster01_icl01	cluster01-01:e0e	local-only	
intercluster01			Failover Targets: cluster01-01:e0e, cluster01-01:e0f	
	cluster01_icl02	cluster01-02:e0e	local-only	
intercluster01			Failover Targets: cluster01-02:e0e, cluster01-02:e0f	

Informazioni correlate

["Considerazioni sull'utilizzo di porte dedicate"](#)

Configurazione delle LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Fasi

- 1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in "cluster01":

```
cluster01::> network port show
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----						
cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

- 2. Creazione di LIF intercluster sulla SVM di sistema:

<b>In ONTAP 9.6 e versioni successive:</b>
<pre>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service-policy default-intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></pre>
<b>In ONTAP 9.5 e versioni precedenti:</b>
<pre>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></pre>

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF dell'intercluster "cluster01\_icl01" e "cluster01\_icl02":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

**In ONTAP 9.6 e versioni successive:**

```
network interface show -service-policy default-intercluster
```

**In ONTAP 9.5 e versioni precedenti:**

```
network interface show -role intercluster
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
cluster01					
	cluster01_icl01				
		up/up	192.168.1.201/24	cluster01-01	e0c
true					
	cluster01_icl02				
		up/up	192.168.1.202/24	cluster01-02	e0c
true					

4. Verificare che le LIF dell'intercluster siano ridondanti:

**In ONTAP 9.6 e versioni successive:**



```
network interface show -service-policy default-intercluster -failover
```

#### In ONTAP 9.5 e versioni precedenti:

```
network interface show -role intercluster -failover
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

L'esempio seguente mostra che i LIF di intercluster "cluster01\_icl01" e "cluster01\_icl02" sulla porta "e0c" effettueranno il failover sulla porta "e0d".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
-----				
cluster01				
	cluster01_icl01	cluster01-01:e0c	local-only	
	192.168.1.201/24			
		Failover Targets: cluster01-01:e0c,		
		cluster01-01:e0d		
	cluster01_icl02	cluster01-02:e0c	local-only	
	192.168.1.201/24			
		Failover Targets: cluster01-02:e0c,		
		cluster01-02:e0d		

#### Informazioni correlate

["Considerazioni sulla condivisione delle porte dati"](#)

#### Creazione di una relazione peer del cluster

È possibile utilizzare il comando `cluster peer create` per creare una relazione peer tra un cluster locale e un cluster remoto. Una volta creata la relazione peer, è possibile eseguire `cluster peer create` sul cluster remoto per autenticarla nel cluster locale.

#### A proposito di questa attività

- È necessario aver creato le LIF di intercluster su ogni nodo dei cluster che vengono sottoposti a peering.
- I cluster devono eseguire ONTAP 9.3 o versione successiva.

#### Fasi

1. Sul cluster di destinazione, creare una relazione peer con il cluster di origine:

```
cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY
HH:MM:SS|1...7days|1...168hours -peer-addr peer_LIF_IPs -ip-space ip-space
```

Se si specificano entrambi `-generate-passphrase` e `-peer-addr`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addr` può utilizzare la password generata.

È possibile ignorare `-ipspace` Se non si utilizza un IPspace personalizzato. Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creata una relazione `peer` del cluster su un cluster remoto non specificato:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days
```

```
                Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
            Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
            Peer Cluster Name: Clus_7ShR (temporary generated)
```

```
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Nel cluster di origine, autenticare il cluster di origine nel cluster di destinazione:

```
cluster peer create -peer-addr peer_LIF_IPs -ipspace ipspace
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene autenticato il cluster locale nel cluster remoto agli indirizzi IP LIF "192.140.112.101" e "192.140.112.102" dell'intercluster:

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

```
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
```

```
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
```

```
Enter the passphrase:
Confirm the passphrase:
```

```
Clusters cluster02 and cluster01 are peered.
```

Inserire la passphrase per la relazione `peer` quando richiesto.

3. Verificare che la relazione `peer` del cluster sia stata creata:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02
Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101,
192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default
```

#### 4. Verificare la connettività e lo stato dei nodi nella relazione peer:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
```

Node	cluster-Name	Node-Name		
	Ping-Status	RDB-Health	Cluster-Health	Avail...
-----	-----	-----	-----	
cluster01-01				
	cluster02	cluster02-01		
	Data: interface_reachable			
	ICMP: interface_reachable	true	true	true
		cluster02-02		
	Data: interface_reachable			
	ICMP: interface_reachable	true	true	true
cluster01-02				
	cluster02	cluster02-01		
	Data: interface_reachable			
	ICMP: interface_reachable	true	true	true
		cluster02-02		
	Data: interface_reachable			
	ICMP: interface_reachable	true	true	true

### Creazione del gruppo DR

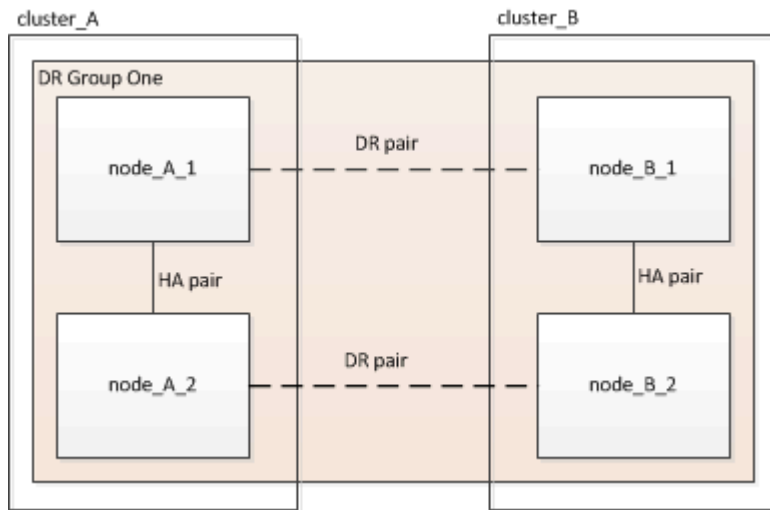
È necessario creare le relazioni del gruppo di disaster recovery (DR) tra i cluster.

#### A proposito di questa attività

Eseguire questa procedura su uno dei cluster nella configurazione MetroCluster per creare le relazioni di DR tra i nodi di entrambi i cluster.



Una volta creati i gruppi DR, non è possibile modificare le relazioni di DR.



## Fasi

1. Verificare che i nodi siano pronti per la creazione del gruppo DR immettendo il seguente comando su ciascun nodo:

```
metrocluster configuration-settings show-status
```

L'output del comando dovrebbe indicare che i nodi sono pronti:

```
cluster_A::> metrocluster configuration-settings show-status
Cluster           Node           Configuration Settings Status
-----
cluster_A         node_A_1      ready for DR group create
                  node_A_2      ready for DR group create
2 entries were displayed.
```

```
cluster_B::> metrocluster configuration-settings show-status
Cluster           Node           Configuration Settings Status
-----
cluster_B         node_B_1      ready for DR group create
                  node_B_2      ready for DR group create
2 entries were displayed.
```

2. Creare il gruppo DR:

```
metrocluster configuration-settings dr-group create -partner-cluster partner-
```

```
cluster-name -local-node local-node-name -remote-node remote-node-name
```

Questo comando viene emesso una sola volta. Non è necessario ripeterlo sul cluster del partner. Nel comando, specificare il nome del cluster remoto e il nome di un nodo locale e di un nodo del cluster partner.

I due nodi specificati vengono configurati come partner DR e gli altri due nodi (non specificati nel comando) vengono configurati come seconda coppia DR nel gruppo DR. Queste relazioni non possono essere modificate dopo aver immesso questo comando.

Il seguente comando crea queste coppie di DR:

- Node\_A\_1 e Node\_B\_1
- Node\_A\_2 e Node\_B\_2

```
Cluster_A::> metrocluster configuration-settings dr-group create  
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1  
[Job 27] Job succeeded: DR Group Create is successful.
```

## Configurazione e connessione delle interfacce IP di MetroCluster

È necessario configurare le interfacce IP MetroCluster utilizzate per la replica dello storage e della cache non volatile di ciascun nodo. Le connessioni vengono quindi stabilite utilizzando le interfacce IP di MetroCluster. In questo modo si creano connessioni iSCSI per la replica dello storage.

### A proposito di questa attività



È necessario scegliere attentamente gli indirizzi IP MetroCluster, in quanto non è possibile modificarli dopo la configurazione iniziale.

- È necessario creare due interfacce per ciascun nodo. Le interfacce devono essere associate alle VLAN definite nel file RCF di MetroCluster.
- È necessario creare tutte le porte "A" dell'interfaccia IP MetroCluster nella stessa VLAN e tutte le porte "B" dell'interfaccia IP MetroCluster nell'altra VLAN. Fare riferimento a. ["Considerazioni sulla configurazione IP di MetroCluster"](#).



- Alcune piattaforme utilizzano una VLAN per l'interfaccia IP di MetroCluster. Per impostazione predefinita, ciascuna delle due porte utilizza una VLAN diversa: 10 e 20. È inoltre possibile specificare una VLAN diversa (non predefinita) superiore a 100 (tra 101 e 4095) utilizzando `-vlan-id parameter` in `metrocluster configuration-settings interface create` comando.
- A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. ["Considerazioni per le reti wide-area di livello 3"](#).

I seguenti modelli di piattaforma possono essere aggiunti alla configurazione MetroCluster esistente se le VLAN utilizzate sono 10/20 o superiori a 100. Se si utilizzano altre VLAN, queste piattaforme non possono essere aggiunte alla configurazione esistente, in quanto l'interfaccia MetroCluster non può essere configurata. Se si utilizza un'altra piattaforma, la configurazione della VLAN non è rilevante in quanto non è richiesta in ONTAP.

Piattaforme AFF	Piattaforme FAS
<ul style="list-style-type: none"> <li>• AFF A220</li> <li>• AFF A250</li> <li>• AFF A400</li> </ul>	<ul style="list-style-type: none"> <li>• FAS2750</li> <li>• FAS500f</li> <li>• FAS8300</li> <li>• FAS8700</li> </ul>

Negli esempi vengono utilizzati i seguenti indirizzi IP e subnet:

Nodo	Interfaccia	Indirizzo IP	Subnet
Node_A_1	Interfaccia IP MetroCluster 1	10.1.1.1	10.1.1/24
Interfaccia IP MetroCluster 2	10.1.2.1	10.1.2/24	Node_A_2
Interfaccia IP MetroCluster 1	10.1.1.2	10.1.1/24	Interfaccia IP MetroCluster 2
10.1.2.2	10.1.2/24	Node_B_1	Interfaccia IP MetroCluster 1
10.1.1.3	10.1.1/24	Interfaccia IP MetroCluster 2	10.1.2.3
10.1.2/24	Node_B_2	Interfaccia IP MetroCluster 1	10.1.1.4
10.1.1/24	Interfaccia IP MetroCluster 2	10.1.2.4	10.1.2/24

Le porte fisiche utilizzate dalle interfacce IP di MetroCluster dipendono dal modello di piattaforma, come mostrato nella tabella seguente.

Modello di piattaforma	Porta IP MetroCluster	Nota
AFF A900 e FAS9500	e5b	
e7b	AFF A800	e0b
	e1b	AFF A700 e FAS9000
e5a		e5b
AFF A400	e1a	

Modello di piattaforma	Porta IP MetroCluster	Nota
e1b	AFF A320	ad esempio
	e0h	AFF A300 e FAS8200
e1a		e1b
AFF A220 e FAS2750	e0a	Su questi sistemi, queste porte fisiche vengono utilizzate anche come interfacce cluster.
e0b	AFF A250 e FAS500f	e0c
	e0d	FAS8300 e FAS8700
e1a		e1b

L'utilizzo delle porte nei seguenti esempi riguarda un sistema AFF A700 o FAS9000.

### Fasi

1. Verificare che ogni nodo abbia attivato l'assegnazione automatica del disco:

```
storage disk option show
```

L'assegnazione automatica del disco assegnerà i dischi del pool 0 e del pool 1 in base a shelf-by-shelf.

La colonna Auto Assign (assegnazione automatica) indica se l'assegnazione automatica del disco è attivata.

```

Node           BKg. FW. Upd.  Auto Copy  Auto Assign  Auto Assign Policy
-----
node_A_1              on           on           on           default
node_A_2              on           on           on           default
2 entries were displayed.
```

2. Verificare che sia possibile creare interfacce IP MetroCluster sui nodi:

```
metrocluster configuration-settings show-status
```

Tutti i nodi devono essere pronti:

Cluster	Node	Configuration Settings Status
-----	-----	-----
cluster_A		
	node_A_1	ready for interface create
	node_A_2	ready for interface create
cluster_B		
	node_B_1	ready for interface create
	node_B_2	ready for interface create
4 entries were displayed.		

### 3. Creare le interfacce su Node\_A\_1.



- L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
- A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. ["Considerazioni per le reti wide-area di livello 3"](#).
- Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

#### a. Configurare l'interfaccia sulla porta "e5a" su "Node\_A\_1":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5a -address ip-address -netmask
netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "node\_A\_1" con indirizzo IP "10.1.1.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

#### b. Configurare l'interfaccia sulla porta "e5b" su "Node\_A\_1":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5b -address ip-address -netmask
netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "node\_A\_1" con indirizzo IP "10.1.2.1":



```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```



È possibile verificare che queste interfacce siano presenti utilizzando `metrocluster configuration-settings interface show` comando.

#### 4. Creare le interfacce su Node\_A\_2.



- L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
- A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. ["Considerazioni per le reti wide-area di livello 3"](#).
- Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

##### a. Configurare l'interfaccia sulla porta "e5a" su "Node\_A\_2":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5a -address ip-address -netmask
netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "node\_A\_2" con indirizzo IP "10.1.1.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
10.1.1.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti. L'esempio seguente mostra il comando per un sistema AFF A220 con un ID VLAN 120:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node\_A\_2":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5b -address ip-address -netmask
netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "node\_A\_2" con indirizzo IP "10.1.2.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
10.1.2.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti. L'esempio seguente mostra il comando per un sistema AFF A220 con un ID VLAN 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Creare le interfacce su "Node\_B\_1".



- L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
- A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. ["Considerazioni per le reti wide-area di livello 3"](#).
- Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

a. Configurare l'interfaccia sulla porta "e5a" su "Node\_B\_1":

```
metrocluster configuration-settings interface create -cluster-name cluster-name -home-node node-name -home-port e5a -address ip-address -netmask netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "Node\_B\_1" con indirizzo IP "10.1.1.3":

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_1 -home-port e5a -address  
10.1.1.3 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node\_B\_1":

```
metrocluster configuration-settings interface create -cluster-name cluster-name -home-node node-name -home-port e5a -address ip-address -netmask netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "Node\_B\_1" con indirizzo IP "10.1.2.3":

```
cluster_A::> metrocluster configuration-settings interface create  
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address  
10.1.2.3 -netmask 255.255.255.0  
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Creare le interfacce su "Node\_B\_2".



- L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
- A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a ["Considerazioni per le reti wide-area di livello 3"](#).
- Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

a. Configurare l'interfaccia sulla porta e5a sul nodo\_B\_2:

```
metrocluster configuration-settings interface create -cluster-name cluster-name -home-node node-name -home-port e5a -address ip-address -netmask netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "Node\_B\_2" con indirizzo IP "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node\_B\_2":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5b -address ip-address -netmask
netmask
```

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "Node\_B\_2" con indirizzo IP "10.1.2.4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Verificare che le interfacce siano state configurate:

```
metrocluster configuration-settings interface show
```

L'esempio seguente mostra che lo stato di configurazione di ciascuna interfaccia è stato completato.

```

cluster_A::> metrocluster configuration-settings interface show
DR
Group Cluster Node      Network Address Netmask      Gateway      Config
-----
-----
1      cluster_A node_A_1
      Home Port: e5a
      10.1.1.1      255.255.255.0    -            completed
      Home Port: e5b
      10.1.2.1      255.255.255.0    -            completed
      node_A_2
      Home Port: e5a
      10.1.1.2      255.255.255.0    -            completed
      Home Port: e5b
      10.1.2.2      255.255.255.0    -            completed
      cluster_B node_B_1
      Home Port: e5a
      10.1.1.3      255.255.255.0    -            completed
      Home Port: e5b
      10.1.2.3      255.255.255.0    -            completed
      node_B_2
      Home Port: e5a
      10.1.1.4      255.255.255.0    -            completed
      Home Port: e5b
      10.1.2.4      255.255.255.0    -            completed
8 entries were displayed.
cluster_A::>

```

#### 8. Verificare che i nodi siano pronti per la connessione alle interfacce MetroCluster:

```
metrocluster configuration-settings show-status
```

L'esempio seguente mostra tutti i nodi nello stato "pronto per la connessione":

```

Cluster      Node      Configuration Settings Status
-----
cluster_A
      node_A_1      ready for connection connect
      node_A_2      ready for connection connect
cluster_B
      node_B_1      ready for connection connect
      node_B_2      ready for connection connect
4 entries were displayed.

```

9. Stabilire le connessioni: `metrocluster configuration-settings connection connect`

Gli indirizzi IP non possono essere modificati dopo aver eseguito questo comando.

L'esempio seguente mostra che il cluster\_A è connesso correttamente:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Verificare che le connessioni siano state stabilite:

`metrocluster configuration-settings show-status`

Lo stato delle impostazioni di configurazione per tutti i nodi deve essere completato:

Cluster	Node	Configuration Settings Status
cluster_A	node_A_1	completed
	node_A_2	completed
cluster_B	node_B_1	completed
	node_B_2	completed

4 entries were displayed.

11. Verificare che le connessioni iSCSI siano state stabilite:

a. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (`*>`).

b. Visualizzare le connessioni:

```
storage iscsi-initiator show
```

Nei sistemi che eseguono ONTAP 9.5, sono presenti otto iniziatori IP MetroCluster su ciascun cluster che dovrebbero essere visualizzati nell'output.

Nei sistemi che eseguono ONTAP 9.4 e versioni precedenti, sono presenti quattro iniziatori IP MetroCluster su ciascun cluster che dovrebbero essere visualizzati nell'output.

L'esempio seguente mostra gli otto iniziatori IP MetroCluster in un cluster che esegue ONTAP 9.5:

```
cluster_A::*> storage iscsi-initiator show
```

Node	Type	Label	Target Portal	Target Name
Admin/Op				
-----				
-----				
cluster_A-01				
		dr_auxiliary		
		mccip-aux-a-initiator	10.227.16.113:65200	prod506.com.company:abab44
up/up				
		mccip-aux-a-initiator2	10.227.16.113:65200	prod507.com.company:abab44
up/up				
		mccip-aux-b-initiator	10.227.95.166:65200	prod506.com.company:abab44
up/up				
		mccip-aux-b-initiator2	10.227.95.166:65200	prod507.com.company:abab44
up/up				
		dr_partner		
		mccip-pri-a-initiator	10.227.16.112:65200	prod506.com.company:cdcd88
up/up				
		mccip-pri-a-initiator2	10.227.16.112:65200	prod507.com.company:cdcd88
up/up				
		mccip-pri-b-initiator	10.227.95.165:65200	prod506.com.company:cdcd88
up/up				
		mccip-pri-b-initiator2	10.227.95.165:65200	prod507.com.company:cdcd88
up/up				
cluster_A-02				
		dr_auxiliary		
		mccip-aux-a-initiator	10.227.16.112:65200	prod506.com.company:cdcd88
up/up				
		mccip-aux-a-initiator2	10.227.16.112:65200	prod507.com.company:cdcd88
up/up				
		mccip-aux-b-initiator	10.227.95.165:65200	prod506.com.company:cdcd88
up/up				
		mccip-aux-b-initiator2	10.227.95.165:65200	prod507.com.company:cdcd88
up/up				

```

dr_partner
    mccip-pri-a-initiator
        10.227.16.113:65200      prod506.com.company:abab44
up/up
    mccip-pri-a-initiator2
        10.227.16.113:65200      prod507.com.company:abab44
up/up
    mccip-pri-b-initiator
        10.227.95.166:65200      prod506.com.company:abab44
up/up
    mccip-pri-b-initiator2
        10.227.95.166:65200      prod507.com.company:abab44
up/up
16 entries were displayed.

```

a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

12. Verificare che i nodi siano pronti per l'implementazione finale della configurazione MetroCluster:

```
metrocluster node show
```

```

cluster_A::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
-----
-      cluster_A
        node_A_1             ready to configure -    -
        node_A_2             ready to configure -    -
2 entries were displayed.
cluster_A::>

```

```

cluster_B::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
-----
-      cluster_B
        node_B_1             ready to configure -    -
        node_B_2             ready to configure -    -
2 entries were displayed.
cluster_B::>

```



## Verifica o esecuzione manuale dell'assegnazione dei dischi del pool 1

A seconda della configurazione dello storage, è necessario verificare l'assegnazione delle unità del pool 1 o assegnare manualmente le unità al pool 1 per ciascun nodo nella configurazione IP di MetroCluster. La procedura da seguire dipende dalla versione di ONTAP in uso.

Tipo di configurazione	Procedura
I sistemi soddisfano i requisiti per l'assegnazione automatica del disco o, se è in esecuzione ONTAP 9.3, sono stati ricevuti dalla fabbrica.	<a href="#">Verifica dell'assegnazione dei dischi per il pool 1</a>
La configurazione include tre shelf oppure, se contiene più di quattro shelf, presenta un multiplo non uniforme di quattro shelf (ad esempio, sette shelf) e utilizza ONTAP 9.5.	<a href="#">Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)</a>
La configurazione non include quattro shelf di storage per sito e utilizza ONTAP 9.4	<a href="#">Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)</a>
I sistemi non sono stati ricevuti dalla fabbrica e utilizzano ONTAP 9.3 i sistemi ricevuti dalla fabbrica sono preconfigurati con i dischi assegnati.	<a href="#">Assegnazione manuale dei dischi per il pool 1 (ONTAP 9.3)</a>

### Verifica dell'assegnazione dei dischi per il pool 1

Verificare che i dischi remoti siano visibili ai nodi e che siano stati assegnati correttamente.

#### Prima di iniziare

Una volta create le interfacce IP MetroCluster e le connessioni con, è necessario attendere almeno dieci minuti per il completamento dell'assegnazione automatica del disco `metrocluster configuration-settings connection connect` comando.

L'output del comando mostra i nomi dei dischi nel formato: Nome-nodo:0m.i1.0L1

["Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"](#)

#### Fasi

1. Verificare che i dischi del pool 1 siano assegnati automaticamente:

```
disk show
```

Il seguente output mostra l'output di un sistema AFF A800 senza shelf esterni.

L'assegnazione automatica dei dischi ha assegnato un quarto (8 dischi) a "node\_A\_1" e un quarto a "node\_A\_2". I dischi rimanenti saranno dischi remoti (pool 1) per "Node\_B\_1" e "Node\_B\_2".

```
cluster_B::> disk show -host-adapter 0m -owner node_B_2
```

	Usable	Disk		Container	Container
Disk	Size	Shelf Bay Type		Type	Name

```

Owner
-----
-----
node_B_2:0m.i0.2L4  894.0GB  0    29  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.2L10 894.0GB  0    25  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L3  894.0GB  0    28  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L9  894.0GB  0    24  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L11 894.0GB  0    26  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L12 894.0GB  0    27  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L15 894.0GB  0    30  SSD-NVM shared  -
node_B_2
node_B_2:0m.i0.3L16 894.0GB  0    31  SSD-NVM shared  -
node_B_2
8 entries were displayed.

cluster_B::> disk show -host-adapter 0m -owner node_B_1
          Usable      Disk          Container  Container
Disk      Size      Shelf Bay Type      Type      Name
Owner
-----
-----
node_B_1:0m.i2.3L19 1.75TB    0    42  SSD-NVM shared  -
node_B_1
node_B_1:0m.i2.3L20 1.75TB    0    43  SSD-NVM spare   Pool1
node_B_1
node_B_1:0m.i2.3L23 1.75TB    0    40  SSD-NVM shared  -
node_B_1
node_B_1:0m.i2.3L24 1.75TB    0    41  SSD-NVM spare   Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB    0    36  SSD-NVM shared  -
node_B_1
node_B_1:0m.i2.3L30 1.75TB    0    37  SSD-NVM shared  -
node_B_1
node_B_1:0m.i2.3L31 1.75TB    0    38  SSD-NVM shared  -
node_B_1
node_B_1:0m.i2.3L32 1.75TB    0    39  SSD-NVM shared  -
node_B_1
8 entries were displayed.

cluster_B::> disk show

```

Disk Owner	Usable Size	Disk Shelf	Bay	Type	Container Type	Container Name
-----	-----	-----	---	-----	-----	-----
node_B_1:0m.i1.0L6 node_A_2	1.75TB	0	1	SSD-NVM	shared	-
node_B_1:0m.i1.0L8 node_A_2	1.75TB	0	3	SSD-NVM	shared	-
node_B_1:0m.i1.0L17 node_A_1	1.75TB	0	18	SSD-NVM	shared	-
node_B_1:0m.i1.0L22	1.75TB	0	17	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.0L25	1.75TB	0	12	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L2	1.75TB	0	5	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L7	1.75TB	0	2	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L14	1.75TB	0	7	SSD-NVM	shared	- node_A_2
node_B_1:0m.i1.2L21	1.75TB	0	16	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L27	1.75TB	0	14	SSD-NVM	shared	- node_A_1
node_B_1:0m.i1.2L28	1.75TB	0	15	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.1L1	1.75TB	0	4	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L5	1.75TB	0	0	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L13	1.75TB	0	6	SSD-NVM	shared	- node_A_2
node_B_1:0m.i2.1L18	1.75TB	0	19	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.1L26	1.75TB	0	13	SSD-NVM	shared	- node_A_1
node_B_1:0m.i2.3L19	1.75TB	0	42	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L20	1.75TB	0	43	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L23	1.75TB	0	40	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L24	1.75TB	0	41	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L29	1.75TB	0	36	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L30	1.75TB	0	37	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L31	1.75TB	0	38	SSD-NVM	shared	- node_B_1
node_B_1:0m.i2.3L32	1.75TB	0	39	SSD-NVM	shared	- node_B_1
node_B_1:0n.12	1.75TB	0	12	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.13	1.75TB	0	13	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.14	1.75TB	0	14	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.15	1.75TB	0	15	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.16	1.75TB	0	16	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.17	1.75TB	0	17	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.18	1.75TB	0	18	SSD-NVM	shared	aggr0 node_B_1
node_B_1:0n.19	1.75TB	0	19	SSD-NVM	shared	- node_B_1
node_B_1:0n.24	894.0GB	0	24	SSD-NVM	shared	- node_A_2
node_B_1:0n.25	894.0GB	0	25	SSD-NVM	shared	- node_A_2
node_B_1:0n.26	894.0GB	0	26	SSD-NVM	shared	- node_A_2
node_B_1:0n.27	894.0GB	0	27	SSD-NVM	shared	- node_A_2
node_B_1:0n.28	894.0GB	0	28	SSD-NVM	shared	- node_A_2
node_B_1:0n.29	894.0GB	0	29	SSD-NVM	shared	- node_A_2

```

node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4   894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3   894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9   894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0        1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

```

```
cluster_B::>
```

```
cluster_A::> disk show
```

```
Usable Disk Container Container
```

```
Disk Size Shelf Bay Type Type Name Owner
```

```

-----
-----
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2

```

```

node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2

```

```
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

### Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)

Se il sistema non è stato preconfigurato in fabbrica e non soddisfa i requisiti per l'assegnazione automatica del disco, è necessario assegnare manualmente i dischi del pool remoto 1.

#### A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.4 o versioni successive.

I dettagli per determinare se il sistema richiede l'assegnazione manuale del disco sono inclusi nella ["Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"](#).

Quando la configurazione include solo due shelf esterni per sito, il pool di 1 unità per ogni sito deve essere condiviso dallo stesso shelf, come mostrato negli esempi seguenti:

- Node\_A\_1 è assegnato ai dischi negli alloggiamenti 0-11 del sito\_B-shelf\_2 (remoto)
- Node\_A\_2 è assegnato ai dischi negli alloggiamenti 12-23 del sito\_B-shelf\_2 (remoto)

#### Fasi

1. Da ciascun nodo della configurazione IP di MetroCluster, assegnare le unità remote al pool 1.

- a. Visualizzare l'elenco delle unità non assegnate:

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
-----	-----	-----	---	-----	-----	-----
6.23.0	-	23	0	SSD	unassigned	-
6.23.1	-	23	1	SSD	unassigned	-
.						
.						
.						
node_A_2:0m.i1.2L51	-	21	14	SSD	unassigned	-
node_A_2:0m.i1.2L64	-	21	10	SSD	unassigned	-
.						
.						
.						

48 entries were displayed.

```
cluster_A::>
```

- b. Assegnare la proprietà dei dischi remoti (0 m) al pool 1 del primo nodo (ad esempio, node\_A\_1):

```
disk assign -disk disk-id -pool 1 -owner owner-node-name
```

*disk-id* deve identificare un disco su uno shelf remoto di *owner-node-name*.

- c. Verificare che le unità siano state assegnate al pool 1:

```
disk show -host-adapter 0m -container-type unassigned
```



La connessione iSCSI utilizzata per accedere ai dischi remoti viene visualizzata come dispositivo 0m.

Il seguente output mostra che i dischi sullo shelf 23 sono stati assegnati perché non compaiono più nell'elenco dei dischi non assegnati:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
          Usable          Disk  Container  Container
Disk      Size Shelf Bay Type   Type      Name
Owner
-----
node_A_2:0m.i1.2L51      -    21   14 SSD    unassigned -    -
node_A_2:0m.i1.2L64      -    21   10 SSD    unassigned -    -
.
.
.
node_A_2:0m.i2.1L90      -    21   19 SSD    unassigned -    -
24 entries were displayed.

cluster_A::>
```

- Ripetere questa procedura per assegnare le unità del pool 1 al secondo nodo sul sito A (ad esempio, "node\_A\_2").
- Ripetere questi passaggi sul sito B.

#### Assegnazione manuale dei dischi per il pool 1 (ONTAP 9.3)

Se si dispone di almeno due shelf di dischi per ciascun nodo, si utilizza la funzionalità di assegnazione automatica di ONTAP per assegnare automaticamente i dischi remoti (pool1).

#### Prima di iniziare

È necessario assegnare un disco sullo shelf al pool 1. ONTAP assegna quindi automaticamente il resto dei dischi sullo shelf allo stesso pool.

#### A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.3.

Questa procedura può essere utilizzata solo se si dispone di almeno due shelf di dischi per ciascun nodo, che consente l'assegnazione automatica dei dischi a livello di shelf.

Se non è possibile utilizzare l'assegnazione automatica a livello di shelf, è necessario assegnare manualmente i dischi remoti in modo che ogni nodo disponga di un pool remoto di dischi (pool 1).

La funzione di assegnazione automatica dei dischi di ONTAP assegna i dischi in base allo shelf-by-shelf. Ad esempio:

- Tutti i dischi sul sito\_B-shelf\_2 vengono assegnati automaticamente al pool 1 del nodo\_A\_1
- Tutti i dischi sul sito\_B-shelf\_4 vengono assegnati automaticamente al pool 1 del nodo\_A\_2
- Tutti i dischi sul sito\_A-shelf\_2 vengono assegnati automaticamente al pool 1 del nodo\_B\_1
- Tutti i dischi sul sito\_A-shelf\_4 vengono assegnati automaticamente al pool 1 del nodo\_B\_2

È necessario "eseguire il seeding" dell'assegnazione automatica specificando un singolo disco su ogni shelf.



## Fasi

1. Da ciascun nodo della configurazione IP MetroCluster, assegnare un disco remoto al pool 1.

- a. Visualizzare l'elenco dei dischi non assegnati:

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
```

Disk Owner	Usable Size	Shelf	Bay	Disk Type	Container Type	Container Name
6.23.0	-	23	0	SSD	unassigned	-
6.23.1	-	23	1	SSD	unassigned	-
.						
.						
.						
node_A_2:0m.i1.2L51	-	21	14	SSD	unassigned	-
node_A_2:0m.i1.2L64	-	21	10	SSD	unassigned	-
.						
.						
.						

48 entries were displayed.

```
cluster_A::>
```

- b. Selezionare un disco remoto (0 m) e assegnare la proprietà del disco al pool 1 del primo nodo (ad esempio, "node\_A\_1"):

```
disk assign -disk disk-id -pool 1 -owner owner-node-name
```

Il *disk-id* deve identificare un disco su uno shelf remoto di *owner-node-name*.

La funzione di assegnazione automatica dei dischi ONTAP assegna tutti i dischi sullo shelf remoto che contengono il disco specificato.

- c. Dopo aver atteso almeno 60 secondi per l'assegnazione automatica del disco, verificare che i dischi remoti sullo shelf siano stati assegnati automaticamente al pool 1:

```
disk show -host-adapter 0m -container-type unassigned
```



La connessione iSCSI utilizzata per accedere ai dischi remoti viene visualizzata come periferica 0m.

Il seguente output mostra che i dischi sullo shelf 23 sono stati assegnati e non vengono più visualizzati:

```

cluster_A::> disk show -host-adapter 0m -container-type unassigned
              Usable          Disk    Container    Container
Disk          Size Shelf Bay Type    Type        Name
Owner
-----
node_A_2:0m.i1.2L51      -      21   14 SSD      unassigned  -      -
node_A_2:0m.i1.2L64      -      21   10 SSD      unassigned  -      -
node_A_2:0m.i1.2L72      -      21   23 SSD      unassigned  -      -
node_A_2:0m.i1.2L74      -      21    1 SSD      unassigned  -      -
node_A_2:0m.i1.2L83      -      21   22 SSD      unassigned  -      -
node_A_2:0m.i1.2L90      -      21    7 SSD      unassigned  -      -
node_A_2:0m.i1.3L52      -      21    6 SSD      unassigned  -      -
node_A_2:0m.i1.3L59      -      21   13 SSD      unassigned  -      -
node_A_2:0m.i1.3L66      -      21   17 SSD      unassigned  -      -
node_A_2:0m.i1.3L73      -      21   12 SSD      unassigned  -      -
node_A_2:0m.i1.3L80      -      21    5 SSD      unassigned  -      -
node_A_2:0m.i1.3L81      -      21    2 SSD      unassigned  -      -
node_A_2:0m.i1.3L82      -      21   16 SSD      unassigned  -      -
node_A_2:0m.i1.3L91      -      21    3 SSD      unassigned  -      -
node_A_2:0m.i2.0L49      -      21   15 SSD      unassigned  -      -
node_A_2:0m.i2.0L50      -      21    4 SSD      unassigned  -      -
node_A_2:0m.i2.1L57      -      21   18 SSD      unassigned  -      -
node_A_2:0m.i2.1L58      -      21   11 SSD      unassigned  -      -
node_A_2:0m.i2.1L59      -      21   21 SSD      unassigned  -      -
node_A_2:0m.i2.1L65      -      21   20 SSD      unassigned  -      -
node_A_2:0m.i2.1L72      -      21    9 SSD      unassigned  -      -
node_A_2:0m.i2.1L80      -      21    0 SSD      unassigned  -      -
node_A_2:0m.i2.1L88      -      21    8 SSD      unassigned  -      -
node_A_2:0m.i2.1L90      -      21   19 SSD      unassigned  -      -
24 entries were displayed.

cluster_A::>

```

- Ripetere questa procedura per assegnare i dischi del pool 1 al secondo nodo del sito A (ad esempio, "node\_A\_2").
- Ripetere questi passaggi sul sito B.

## Abilitazione dell'assegnazione automatica del disco in ONTAP 9.4

### A proposito di questa attività

In ONTAP 9.4, se l'assegnazione automatica del disco è stata disattivata come indicato in precedenza in questa procedura, è necessario riattivarla su tutti i nodi.

["Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"](#)

## Fasi

1. Abilitare l'assegnazione automatica del disco:

```
storage disk option modify -node node_name -autoassign on
```

Questo comando deve essere inviato a tutti i nodi della configurazione IP MetroCluster.

## Mirroring degli aggregati root

È necessario eseguire il mirroring degli aggregati root per garantire la protezione dei dati.

### A proposito di questa attività

Per impostazione predefinita, l'aggregato root viene creato come aggregato di tipo RAID-DP. È possibile modificare l'aggregato root da RAID-DP a aggregato di tipo RAID4. Il seguente comando modifica l'aggregato root per l'aggregato di tipo RAID4:

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```



Nei sistemi non ADP, il tipo RAID dell'aggregato può essere modificato dal RAID-DP predefinito a RAID4 prima o dopo il mirroring dell'aggregato.

## Fasi

1. Eseguire il mirroring dell'aggregato root:

```
storage aggregate mirror aggr_name
```

Il seguente comando esegue il mirroring dell'aggregato root per "controller\_A\_1":

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

Questo esegue il mirroring dell'aggregato, quindi è costituito da un plex locale e da un plex remoto situati nel sito MetroCluster remoto.

2. Ripetere il passaggio precedente per ciascun nodo della configurazione MetroCluster.

## Informazioni correlate

["Gestione dello storage logico"](#)

## Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

### A proposito di questa attività

- Devi sapere quali dischi verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come assicurarsi di selezionare il tipo di disco corretto.
- I dischi sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi in tale aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale per quell'aggregato.

Nei sistemi che utilizzano ADP, gli aggregati vengono creati utilizzando partizioni in cui ciascun disco viene

partizionato nelle partizioni P1, P2 e P3.

- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.

### "Gestione di dischi e aggregati"

#### Fasi

1. Visualizzare un elenco delle parti di ricambio disponibili:

```
storage disk show -spare -owner node_name
```

2. Creare l'aggregato:

```
storage aggregate create -mirror true
```

Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su qualsiasi nodo del cluster. Per assicurarsi che l'aggregato venga creato su un nodo specifico, utilizzare `-node` o specificare i dischi di proprietà di quel nodo.

È possibile specificare le seguenti opzioni:

- Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
- Elenco dei dischi specifici da aggiungere all'aggregato
- Numero di dischi da includere



Nella configurazione minima supportata, in cui è disponibile un numero limitato di dischi, è necessario utilizzare l'opzione `force-Small-aggregate` per consentire la creazione di un aggregato RAID-DP a tre dischi.

- Stile checksum da utilizzare per l'aggregato
- Tipo di dischi da utilizzare
- Dimensioni delle unità da utilizzare
- Velocità del disco da utilizzare
- Tipo RAID per i gruppi RAID sull'aggregato
- Numero massimo di dischi che possono essere inclusi in un gruppo RAID
- Se sono consentiti dischi con diversi RPM per ulteriori informazioni su queste opzioni, consulta la pagina man di creazione degli aggregati di storage.

Il seguente comando crea un aggregato mirrorato con 10 dischi:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

### 3. Verificare il gruppo RAID e i dischi del nuovo aggregato:

```
storage aggregate show-status -aggregate aggregate-name
```

## Implementazione della configurazione MetroCluster

È necessario eseguire `metrocluster configure` Comando per avviare la protezione dei dati in una configurazione MetroCluster.

### A proposito di questa attività

- Su ciascun cluster devono essere presenti almeno due aggregati di dati mirrorati non root.

È possibile verificarlo con `storage aggregate show` comando.



Se si desidera utilizzare un singolo aggregato di dati mirrorato, vedere [Fase 1](#) per istruzioni.

- Lo stato ha-config dei controller e dello chassis deve essere "mccip".

Si emette il `metrocluster configure` Eseguire un comando una volta su uno dei nodi per abilitare la configurazione MetroCluster. Non è necessario eseguire il comando su ciascuno dei siti o nodi e non è importante il nodo o il sito su cui si sceglie di eseguire il comando.

Il `metrocluster configure` Command associa automaticamente i due nodi con gli ID di sistema più bassi in ciascuno dei due cluster come partner di disaster recovery (DR). In una configurazione MetroCluster a quattro nodi, esistono due coppie di partner DR. La seconda coppia di DR viene creata dai due nodi con ID di sistema superiori.



È necessario **non** configurare Onboard Key Manager (OKM) o la gestione delle chiavi esterne prima di eseguire il comando `metrocluster configure`.

### Fasi

1. configurare MetroCluster nel seguente formato:

Se la configurazione di MetroCluster dispone di...	Quindi...
Aggregati di dati multipli	Dal prompt di qualsiasi nodo, configurare MetroCluster:  <code>metrocluster configure node-name</code>

Un singolo aggregato di dati mirrorato

a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:

```
set -privilege advanced
```

Devi rispondere con **y** quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (\*).

b. Configurare MetroCluster con `-allow-with -one-aggregate true` parametro:

```
metrocluster configure -allow-with  
-one-aggregate true node-name
```

c. Tornare al livello di privilegio admin:

```
set -privilege admin
```



La Best practice consiste nell'avere più aggregati di dati. Se il primo gruppo DR dispone di un solo aggregato e si desidera aggiungere un gruppo DR con un aggregato, è necessario spostare il volume di metadati dal singolo aggregato di dati. Per ulteriori informazioni su questa procedura, vedere ["Spostamento di un volume di metadati nelle configurazioni MetroCluster"](#).

Il seguente comando abilita la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene "controller\_A\_1":

```
cluster_A::*> metrocluster configure -node-name controller_A_1  
  
[Job 121] Job succeeded: Configure is successful.
```

2. Verificare lo stato della rete sul sito A:

```
network port show
```

L'esempio seguente mostra l'utilizzo della porta di rete in una configurazione MetroCluster a quattro nodi:

```
cluster_A::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper
-----						
controller_A_1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
controller_A_2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

```
14 entries were displayed.
```

### 3. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster.

#### a. Verificare la configurazione dal sito A:

```
metrocluster show
```

```
cluster_A::> metrocluster show
```

```
Configuration: IP fabric
```

Cluster	Entry Name	State
-----		
Local: cluster_A	Configuration state	configured
	Mode	normal
Remote: cluster_B	Configuration state	configured
	Mode	normal

#### b. Verificare la configurazione dal sito B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
```

Configuration: IP fabric

Cluster	Entry Name	State
Local: cluster_B	Configuration state	configured
	Mode	normal
Remote: cluster_A	Configuration state	configured
	Mode	normal

4. Per evitare possibili problemi con il mirroring della memoria non volatile, riavviare ciascuno dei quattro nodi:

```
node reboot -node node-name -inhibit-takeover true
```

5. Eseguire il `metrocluster show` su entrambi i cluster per verificare nuovamente la configurazione.

### Configurazione del secondo gruppo DR in una configurazione a otto nodi

Ripetere le operazioni precedenti per configurare i nodi nel secondo gruppo di DR.

### Creazione di aggregati di dati senza mirror

È possibile creare aggregati di dati senza mirroring per i dati che non richiedono il mirroring ridondante fornito dalle configurazioni MetroCluster.

#### A proposito di questa attività

- È necessario sapere quali dischi o LUN di array verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come verificare che sia selezionato il tipo di disco corretto.



Nelle configurazioni MetroCluster IP, gli aggregati remoti senza mirror non sono accessibili dopo uno switchover



Gli aggregati senza mirror devono essere locali rispetto al nodo che li possiede.

- I dischi e le LUN degli array sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi dell'aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale dell'aggregato.
- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.
- *Gestione di dischi e aggregati* contiene ulteriori informazioni sugli aggregati di mirroring.

### Fasi

1. Implementazione aggregata senza mirror:

```
metrocluster modify -enable-unmirrored-aggr-deployment true
```



2. Verificare che l'assegnazione automatica del disco sia disattivata:

```
disk option show
```

3. Installare e cablare gli shelf di dischi che conterranno gli aggregati senza mirror.

È possibile utilizzare le procedure descritte nella documentazione di installazione e configurazione per la piattaforma e gli shelf di dischi.

#### ["Documentazione dei sistemi hardware ONTAP"](#)

4. Assegnare manualmente tutti i dischi sul nuovo shelf al nodo appropriato:

```
disk assign -disk disk-id -owner owner-node-name
```

5. Creare l'aggregato:

```
storage aggregate create
```

Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su qualsiasi nodo del cluster. Per verificare che l'aggregato sia creato su un nodo specifico, è necessario utilizzare il parametro `-node` o specificare i dischi di proprietà di quel nodo.

È inoltre necessario assicurarsi di includere nell'aggregato solo i dischi sullo shelf senza mirror.

È possibile specificare le seguenti opzioni:

- Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
- Elenco di unità o LUN di array specifici da aggiungere all'aggregato
- Numero di dischi da includere
- Stile checksum da utilizzare per l'aggregato
- Tipo di dischi da utilizzare
- Dimensioni delle unità da utilizzare
- Velocità del disco da utilizzare
- Tipo RAID per i gruppi RAID sull'aggregato
- Numero massimo di unità o LUN di array che possono essere inclusi in un gruppo RAID
- Se sono consentiti dischi con diversi RPM

Per ulteriori informazioni su queste opzioni, consulta la pagina man di creazione dell'aggregato di storage.

Il seguente comando crea un aggregato senza mirror con 10 dischi:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. Verificare il gruppo RAID e i dischi del nuovo aggregato:

```
storage aggregate show-status -aggregate aggregate-name
```

7. Disattiva implementazione aggregata senza mirror:

```
metrocluster modify -enable-unmirrored-aggr-deployment false
```

8. Verificare che l'assegnazione automatica del disco sia abilitata:

```
disk option show
```

## Informazioni correlate

["Gestione di dischi e aggregati"](#)

## Verifica della configurazione MetroCluster

È possibile verificare che i componenti e le relazioni nella configurazione di MetroCluster funzionino correttamente.

### A proposito di questa attività

Dopo la configurazione iniziale e dopo aver apportato eventuali modifiche alla configurazione MetroCluster, è necessario eseguire un controllo.

È inoltre necessario eseguire un controllo prima di un'operazione di switchover negoziata (pianificata) o di switchback.

Se il `metrocluster check run` il comando viene emesso due volte in un breve periodo di tempo su uno o entrambi i cluster, può verificarsi un conflitto e il comando potrebbe non raccogliere tutti i dati. Successivo `metrocluster check show` i comandi non mostrano l'output previsto.

## Fasi

1. Controllare la configurazione:

```
metrocluster check run
```

Il comando viene eseguito come processo in background e potrebbe non essere completato immediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

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

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	ok
volumes	ok

7 entries were displayed.

## 2. Visualizzare risultati più dettagliati dal comando di esecuzione del controllo MetroCluster più recente:

```
metrocluster check aggregate show

metrocluster check cluster show

metrocluster check config-replication show

metrocluster check lif show

metrocluster check node show
```



Il metrocluster check show i comandi mostrano i risultati dei più recenti metrocluster check run comando. Eseguire sempre il metrocluster check run prima di utilizzare metrocluster check show i comandi in modo che le informazioni visualizzate siano aggiornate.

Nell'esempio riportato di seguito viene illustrato il metrocluster check aggregate show Output di comando per una configurazione MetroCluster a quattro nodi sana:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58
```

Node	Aggregate	Check
Result		
-----	-----	-----
-----		
controller_A_1	controller_A_1_aggr0	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		
	controller_A_1_aggr1	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		
	controller_A_1_aggr2	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		
controller_A_2	controller_A_2_aggr0	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		
	controller_A_2_aggr1	mirroring-status
ok		disk-pool-allocation
ok		ownership-state
ok		
	controller_A_2_aggr2	mirroring-status
ok		disk-pool-allocation
ok		

ok

ownership-state

18 entries were displayed.

L'esempio seguente mostra l'output del comando show del cluster di controllo MetroCluster per una configurazione MetroCluster a quattro nodi sana. Indica che i cluster sono pronti per eseguire uno switchover negoziato, se necessario.

Last Checked On: 9/13/2017 20:47:04

Cluster	Check	Result
-----	-----	-----
mccint-fas9000-0102	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok
mccint-fas9000-0304	negotiated-switchover-ready	not-applicable
	switchback-ready	not-applicable
	job-schedules	ok
	licenses	ok
	periodic-check-enabled	ok

10 entries were displayed.

## Informazioni correlate

["Gestione di dischi e aggregati"](#)

["Gestione di rete e LIF"](#)

## Completamento della configurazione ONTAP

Dopo aver configurato, attivato e verificato la configurazione MetroCluster, è possibile completare la configurazione del cluster aggiungendo ulteriori SVM, interfacce di rete e altre funzionalità ONTAP in base alle necessità.

## Verifica dello switchover, della riparazione e dello switchback

### Fase

1. Utilizzare le procedure per lo switchover negoziato, la riparazione e lo switchback menzionate nella *Guida alla gestione e al disaster recovery di MetroCluster*.

["Gestione MetroCluster e disaster recovery"](#)

## Configurazione del software MetroCluster Tiebreaker o ONTAP Mediator

È possibile scaricare e installare su un terzo sito il software MetroCluster Tiebreaker o, a partire da ONTAP 9.7, il ONTAP Mediator.

### Prima di iniziare

È necessario disporre di un host Linux dotato di connettività di rete per entrambi i cluster nella configurazione MetroCluster. I requisiti specifici sono contenuti nella documentazione di MetroCluster Tiebreaker o ONTAP Mediator.

Se si effettua la connessione a un'istanza di Tiebreaker o ONTAP Mediator esistente, è necessario disporre del nome utente, della password e dell'indirizzo IP del servizio di spareggio o mediatore.

Se è necessario installare una nuova istanza di ONTAP Mediator, seguire le istruzioni per installare e configurare il software.

### "Configurazione del servizio ONTAP Mediator per lo switchover automatico non pianificato"

Se è necessario installare una nuova istanza del software Tiebreaker, seguire la ["istruzioni per installare e configurare il software"](#).

### A proposito di questa attività

Non è possibile utilizzare sia il software MetroCluster Tiebreaker che il mediatore ONTAP con la stessa configurazione MetroCluster.

### "Considerazioni sull'utilizzo di ONTAP Mediator o MetroCluster Tiebreaker"

#### Fase

1. Configurare il servizio ONTAP Mediator o il software Tiebreaker:
  - Se si utilizza un'istanza esistente del mediatore ONTAP, aggiungere il servizio del mediatore ONTAP a ONTAP:

```
metrocluster configuration-settings mediator add -mediator-address ip-  
address-of-mediator-host
```

- Se si utilizza il software Tiebreaker, fare riferimento a. ["Documentazione di Tiebreaker"](#).

## Protezione dei file di backup della configurazione

È possibile fornire una protezione aggiuntiva per i file di backup della configurazione del cluster specificando un URL remoto (HTTP o FTP) in cui verranno caricati i file di backup della configurazione oltre alle posizioni predefinite nel cluster locale.

#### Fase

1. Impostare l'URL della destinazione remota per i file di backup della configurazione:

```
system configuration backup settings modify URL-of-destination
```

Il ["Gestione dei cluster con la CLI"](#) Contiene ulteriori informazioni nella sezione *Gestione dei backup di configurazione*.

# Configurare il servizio ONTAP Mediator per lo switchover automatico non pianificato

## Preparare l'installazione del servizio ONTAP Mediator

L'ambiente deve soddisfare determinati requisiti.

I seguenti requisiti si applicano a un gruppo di disaster recovery (gruppo di DR). Scopri di più ["Gruppi DR"](#).

- Se si prevede di aggiornare la versione di Linux, eseguire questa operazione prima di installare il servizio ONTAP Mediator più recente.
- Il servizio ONTAP Mediator e il software MetroCluster Tiebreaker non devono essere utilizzati con la stessa configurazione MetroCluster.
- Il supporto ONTAP deve essere installato su un host LINUX in una posizione separata dai siti MetroCluster.

La connettività tra il mediatore ONTAP e ciascun sito deve essere composta da due domini di guasto separati.

- Il servizio ONTAP può supportare fino a cinque configurazioni MetroCluster contemporaneamente.
- Lo switchover automatico non pianificato è supportato in ONTAP 9.7 e versioni successive.

## Requisiti di rete per l'utilizzo di Mediator in una configurazione MetroCluster

Per installare il servizio ONTAP Mediator in una configurazione MetroCluster, è necessario assicurarsi che la configurazione soddisfi diversi requisiti di rete.

- Latenza

Latenza massima inferiore a 75 ms (RTT).

Il jitter non deve superare i 5 ms.

- MTU

La dimensione MTU deve essere di almeno 1400.

- Perdita di pacchetti

Per il traffico ICMP (Internet Control message Protocol) e TCP, la perdita di pacchetti deve essere inferiore al 0.01%.

- Larghezza di banda

Il collegamento tra il servizio Mediator e un gruppo DR deve avere almeno 20 Mbps di larghezza di banda.

- Connettività indipendente

È necessaria una connettività indipendente tra ciascun sito e il mediatore ONTAP. Un guasto in un sito non deve interrompere la connettività IP tra gli altri due siti non interessati.

## Requisiti dell'host per il mediatore ONTAP in una configurazione MetroCluster

È necessario assicurarsi che la configurazione soddisfi diversi requisiti dell'host.

- ONTAP Mediator deve essere installato in un sito esterno fisicamente separato dai due cluster ONTAP.
- Il mediatore ONTAP supporta un numero massimo di cinque configurazioni MetroCluster.
- Il mediatore ONTAP non richiede requisiti superiori a quelli minimi del sistema operativo host per CPU e memoria (RAM).
- Oltre ai requisiti minimi del sistema operativo host, devono essere disponibili almeno 30 GB di spazio su disco utilizzabile aggiuntivo.
  - Ogni gruppo di DR richiede fino a 200 MB di spazio su disco.

## Requisiti del firewall per ONTAP Mediator

Il mediatore ONTAP utilizza una serie di porte per comunicare con servizi specifici.

Se si utilizza un firewall di terze parti:

- L'accesso HTTPS deve essere attivato.
- Deve essere configurato per consentire l'accesso alle porte 31784 e 3260.

Quando si utilizza il firewall predefinito Red Hat o CentOS, il firewall viene configurato automaticamente durante l'installazione di Mediator.

La tabella seguente elenca le porte che è necessario consentire nel firewall:



La porta iSCSI è richiesta solo in una configurazione IP MetroCluster.

Porta/servizi	Origine	Destinazione	Scopo
31784/tcp	Interfacce di gestione del cluster ONTAP	Server web di ONTAP Mediator	API REST (HTTPS)
3260/tcp	Cluster ONTAP (LIF per la gestione dei dati o LIF per la gestione dei dati)	Target iSCSI del mediatore ONTAP	Connessione dati iSCSI per caselle postali

## Linee guida per l'aggiornamento del mediatore ONTAP in una configurazione MetroCluster

Se si sta aggiornando il mediatore ONTAP, è necessario soddisfare i requisiti della versione Linux e seguire le linee guida per l'aggiornamento.

- Il servizio Mediator può essere aggiornato da una versione immediatamente precedente alla versione corrente.
- Tutte le versioni di Mediator sono supportate nelle configurazioni MetroCluster IP con ONTAP 9.7 o versioni successive.

["Installare o aggiornare il servizio di supporto ONTAP"](#)



## Dopo l'aggiornamento

Una volta completato l'aggiornamento di Mediator e del sistema operativo, eseguire il `storage iscsi-initiator show` Per confermare che le connessioni del Mediator sono attive.

## Configurare il servizio ONTAP Mediator da una configurazione IP MetroCluster

Il servizio ONTAP Mediator deve essere configurato sul nodo ONTAP per essere utilizzato in una configurazione IP MetroCluster.

### Prima di iniziare

- Il mediatore ONTAP deve essere stato installato correttamente in una posizione di rete raggiungibile da entrambi i siti MetroCluster.

["Installare o aggiornare il servizio di supporto ONTAP"](#)

- È necessario disporre dell'indirizzo IP dell'host che esegue il servizio ONTAP Mediator.
- È necessario disporre del nome utente e della password per il servizio di supporto ONTAP.
- Tutti i nodi della configurazione IP di MetroCluster devono essere in linea.



A partire da ONTAP 9.12.1, è possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster. Questa funzione è un'estensione dello switchover non pianificato assistito dal mediatore. Prima di attivare questa funzione, consultare la ["Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster"](#).

### A proposito di questa attività

- Questa attività attiva lo switchover automatico non pianificato per impostazione predefinita.
- Questa attività può essere eseguita sull'interfaccia ONTAP di qualsiasi nodo della configurazione IP di MetroCluster.
- Una singola installazione del servizio ONTAP può essere configurata con un massimo di cinque configurazioni IP MetroCluster.

### Fasi

1. Aggiungere il servizio ONTAP Mediator a ONTAP:

```
metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
```



Verranno richiesti nome utente e password per l'account utente amministratore di Mediator.

2. Verificare che la funzione di switchover automatico sia attivata:

```
metrocluster show
```

3. Verificare che Mediator sia in esecuzione.

- a. Mostra i dischi virtuali di Mediator:

```
storage disk show -container-type mediator
```

```
cluster_A::> storage disk show -container-type mediator
```

	Usable		Disk		Container	
Container						
Disk	Size	Shelf	Bay	Type	Type	Name
Owner						
NET-1.5	-	-	-	VMDISK	mediator	-
node_A_2						
NET-1.6	-	-	-	VMDISK	mediator	-
node_B_1						
NET-1.7	-	-	-	VMDISK	mediator	-
node_B_2						
NET-1.8	-	-	-	VMDISK	mediator	-
node_A_1						

b. Impostare la modalità dei privilegi su Advanced (avanzata):

```
set advanced
```

```
cluster_A::> set advanced
```

c. Visualizzare gli iniziatori etichettati come mediatore:

```
storage iscsi-initiator show -label mediator
```

```

cluster_A::*> storage iscsi-initiator show -label mediator
(storage iscsi-initiator show)
+
Status
Node Type Label      Target Portal      Target Name
Admin/Op
-----
node_A_1
  mailbox
    mediator 1.1.1.1      iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
node_A_2
  mailbox
    mediator 1.1.1.1      iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up

```

d. Verificare lo stato del dominio dell'errore di switchover non pianificato automatico (AURO):

```
metrocluster show
```



L'output di esempio riportato di seguito è valido per ONTAP 9.13.1 e versioni successive. Per ONTAP 9.12.1 e versioni precedenti, lo stato del dominio di errore AURO dovrebbe essere `auso-on-cluster-disaster`.

```

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

```

4. In alternativa, configurare lo switchover forzato automatico MetroCluster.

È possibile utilizzare il seguente comando solo a livello di privilegi avanzati.



Prima di utilizzare questo comando, rivedere la ["Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster"](#).

```
metrocluster modify -allow-auto-forced-switchover true
```

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

## Disconfigurare il servizio ONTAP Mediator dalla configurazione IP di MetroCluster

È possibile annullare la configurazione del servizio ONTAP Mediator dalla configurazione IP di MetroCluster.

### Prima di iniziare

È necessario aver installato e configurato correttamente il mediatore ONTAP in una posizione di rete raggiungibile da entrambi i siti MetroCluster.

### Fasi

1. Per annullare la configurazione del servizio ONTAP Mediator, utilizzare il seguente comando:

```
metrocluster configuration-settings mediator remove
```

Vengono richiesti il nome utente e la password per l'account utente admin di ONTAP Mediator.



Se il mediatore ONTAP non è attivo, il `metrocluster configuration-settings mediator remove` Il comando richiede comunque di inserire il nome utente e la password per l'account utente amministratore di ONTAP Mediator e rimuove il servizio ONTAP Mediator dalla configurazione MetroCluster.

- a. Controllare se sono presenti dischi rotti utilizzando il seguente comando:

```
disk show -broken
```

### Esempio

```
There are no entries matching your query.
```

2. Verificare che il servizio ONTAP Mediator sia stato rimosso dalla configurazione MetroCluster eseguendo i seguenti comandi su entrambi i cluster:

- a. `metrocluster configuration-settings mediator show`

### Esempio

```
This table is currently empty.
```

- b. `storage iscsi-initiator show -label mediator`

### Esempio

```
There are no entries matching your query.
```

## Connessione di una configurazione MetroCluster a un'istanza diversa di ONTAP Mediator

Se si desidera connettere i nodi MetroCluster a un'altra istanza di ONTAP Mediator, è necessario disconfigurare e riconfigurare la connessione nel software ONTAP.

### Prima di iniziare

Sono necessari il nome utente, la password e l'indirizzo IP della nuova istanza di ONTAP Mediator.

### A proposito di questa attività

Questi comandi possono essere emessi da qualsiasi nodo della configurazione MetroCluster.

### Fasi

1. Rimuovere il mediatore ONTAP corrente dalla configurazione MetroCluster:

```
metrocluster configuration-settings mediator remove
```

2. Stabilire la nuova connessione del mediatore ONTAP alla configurazione MetroCluster:

```
metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
```

## In che modo il mediatore ONTAP supporta lo switchover automatico non pianificato

ONTAP Mediator fornisce i LUN delle cassette postali per memorizzare le informazioni sullo stato dei nodi IP di MetroCluster. Queste LUN sono in co-location con il mediatore ONTAP, che viene eseguito su un host Linux fisicamente separato dai siti MetroCluster. I nodi IP di MetroCluster possono utilizzare le informazioni della cassetta postale per monitorare lo stato dei partner di disaster recovery (DR) e implementare uno switchover non pianificato assistito da Mediator (MAUSO) in caso di emergenza.



MAUSO non è supportato nelle configurazioni MetroCluster FC.

Quando un nodo rileva un guasto di un sito che richiede uno switchover, prende le misure necessarie per confermare che lo switchover è appropriato e, in tal caso, esegue lo switchover. Per impostazione predefinita, viene avviato un MAUSO per i seguenti scenari:

- Il mirroring SyncMirror e il mirroring DR della cache non volatile di ciascun nodo sono in funzione e le cache e i mirror vengono sincronizzati al momento dell'errore.
- Nessuno dei nodi nel sito sopravvissuto è in stato di Takeover.
- In caso di disastro del sito. Un disastro del sito è un errore di *tutti* nodi nello stesso sito.

Un MAUSO viene *non* avviato nei seguenti scenari di arresto:

- Si avvia un arresto. Ad esempio, quando:
  - Arrestare i nodi
  - Riavviare i nodi

A partire da...	Descrizione
ONTAP 9.13.1	<ul style="list-style-type: none"> <li>Un MAUSO viene avviato se un <a href="#">scenario predefinito</a> si verifica e un guasto della ventola o dell'hardware avvia un arresto ambientale. Esempi di guasti hardware includono una temperatura alta o bassa, o un'unità di alimentazione, una batteria NVRAM o un guasto heartbeat del Service Processor.</li> <li>Il valore predefinito per il dominio di errore è impostato su "auso-on-dr-group" in una configurazione IP di MetroCluster. Per ONTAP 9.12.1 e versioni precedenti, il valore predefinito è impostato su "auso-on-cluster-disaster".</li> </ul> <p>In una configurazione IP MetroCluster a otto nodi, "auso-on-dr-group" attiva un MAUSO in caso di errore del cluster o di coppia ha in un gruppo di DR. Per una coppia ha, entrambi i nodi devono guastarsi allo stesso tempo.</p> <p>In alternativa, è possibile modificare l'impostazione del dominio di errore nel dominio "auso-on-cluster-disaster" utilizzando <code>metrocluster modify -auto-switchover -failure-domain auso-on-cluster-disaster</code> Comando che attiva un MAUSO solo in presenza di errori nella coppia di nodi ha in entrambi i gruppi di DR.</p> <ul style="list-style-type: none"> <li>È possibile modificare il comportamento per forzare un MAUSO anche se la NVRAM non è sincronizzata al momento dell'errore.</li> </ul>
ONTAP 9.12.1	<p>È possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster utilizzando il <code>metrocluster modify -allow-auto-forced-switchover true</code> comando.</p> <p>Lo switchover al rilevamento di un guasto di un sito avviene automaticamente quando si attiva la funzione di switchover forzato automatico di MetroCluster. È possibile utilizzare questa funzione per integrare la funzionalità di switchover automatico di MetroCluster IP.</p> <p><b>Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster</b></p> <p>Quando si consente a una configurazione IP di MetroCluster di funzionare in modalità di switchover forzato automatico, il seguente problema noto potrebbe causare la perdita di dati:</p> <ul style="list-style-type: none"> <li>La memoria non volatile negli storage controller non viene mirrorati sul partner di DR remoto sul sito partner,</li> </ul> <p><b>Attenzione:</b> Si potrebbero incontrare scenari non menzionati. NetApp non è responsabile di eventuali danneggiamenti dei dati, perdite di dati o altri danni che potrebbero derivare dall'attivazione della funzione di switchover automatico forzato di MetroCluster. Non utilizzare la funzione di switchover forzato automatico di MetroCluster se i rischi e le limitazioni non sono accettabili per l'utente.</p>

## Test della configurazione MetroCluster

È possibile verificare gli scenari di errore per confermare il corretto funzionamento della configurazione MetroCluster.

## Verifica dello switchover negoziato

È possibile testare l'operazione di switchover negoziata (pianificata) per confermare la disponibilità ininterrotta dei dati.

### A proposito di questa attività

Questo test verifica che la disponibilità dei dati non sia interessata (ad eccezione dei protocolli SMB (Server message Block) di Microsoft e Fibre Channel di Solaris) passando il cluster al secondo data center.

Questo test dovrebbe richiedere circa 30 minuti.

Questa procedura ha i seguenti risultati attesi:

- Il `metrocluster switchover` viene visualizzato un messaggio di avviso.

Se rispondi `yes` al prompt, il sito da cui viene inviato il comando passerà al sito del partner.

Per le configurazioni MetroCluster IP:

- Per ONTAP 9.4 e versioni precedenti:
  - Gli aggregati mirrorati diventeranno degradati dopo lo switchover negoziato.
- Per ONTAP 9.5 e versioni successive:
  - Gli aggregati mirrorati rimarranno in stato normale se lo storage remoto è accessibile.
  - In caso di perdita dell'accesso allo storage remoto, gli aggregati mirrorati diventeranno degradati dopo lo switchover negoziato.
- Per ONTAP 9.8 e versioni successive:
  - Gli aggregati senza mirror che si trovano nel sito di disastro non saranno più disponibili in caso di perdita dell'accesso allo storage remoto. Questo potrebbe causare un'interruzione del controller.

### Fasi

1. Verificare che tutti i nodi si trovino nello stato configurato e nella modalità normale:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
```

Cluster	Configuration State	Mode
-----	-----	
Local: cluster_A	configured	normal
Remote: cluster_B	configured	normal

2. Avviare l'operazione di switchover:

```
metrocluster switchover
```

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Verificare che il cluster locale si trovi nello stato configurato e nella modalità di switchover:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
```

Cluster	Configuration State	Mode
-----	-----	
Local: cluster_A	configured	switchover
Remote: cluster_B	not-reachable	-
configured	normal	

4. Verificare che l'operazione di switchover sia stata eseguita correttamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
    State: successful
  Start Time: 2/6/2016 13:28:50
    End Time: 2/6/2016 13:29:41
    Errors: -
```

5. Utilizzare `vserver show` e `network interface show` Comandi per verificare che le SVM DR e le LIF siano online.

## Verifica della riparazione e dello switchback manuale

È possibile testare le operazioni di riparazione e switchback manuale per verificare che la disponibilità dei dati non sia compromessa (ad eccezione delle configurazioni SMB e Solaris FC), ripristinando il cluster al data center originale dopo uno switchover negoziato.

### A proposito di questa attività

Questo test dovrebbe richiedere circa 30 minuti.

Il risultato previsto di questa procedura è che i servizi devono essere ripristinati nei nodi domestici.



I passaggi di riparazione non sono richiesti nei sistemi che eseguono ONTAP 9.5 o versioni successive, sui quali la riparazione viene eseguita automaticamente dopo uno switchover negoziato. Nei sistemi che eseguono ONTAP 9.6 e versioni successive, la riparazione viene eseguita automaticamente anche dopo uno switchover non pianificato.

## Fasi

1. Se sul sistema è in esecuzione ONTAP 9.4 o versioni precedenti, riparare l'aggregato di dati:

```
metrocluster heal aggregates
```

L'esempio seguente mostra il completamento corretto del comando:

```
cluster_A::> metrocluster heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. Se sul sistema è in esecuzione ONTAP 9.4 o versioni precedenti, riparare l'aggregato root:

```
metrocluster heal root-aggregates
```

Questo passaggio è necessario per le seguenti configurazioni:

- Configurazioni MetroCluster FC.
- Configurazioni IP di MetroCluster con ONTAP 9.4 o versioni precedenti. L'esempio seguente mostra il completamento corretto del comando:

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. Verificare che la riparazione sia completata:

```
metrocluster node show
```

L'esempio seguente mostra il completamento corretto del comando:

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node              State        Mirroring Mode
-----
1      cluster_A
      node_A_1      configured    enabled    heal roots
completed
      cluster_B
      node_B_2      unreachable    -          switched over
42 entries were displayed.metrocluster operation show
```

Se l'operazione di riparazione automatica non riesce per qualsiasi motivo, è necessario eseguire il

metrocluster heal Comandi manuali come nelle versioni di ONTAP precedenti a ONTAP 9.5. È possibile utilizzare metrocluster operation show e metrocluster operation history show -instance comandi per monitorare lo stato di riparazione e determinare la causa di un errore.

4. Verificare che tutti gli aggregati siano mirrorati:

```
storage aggregate show
```

L'esempio seguente mostra che tutti gli aggregati hanno uno stato RAID di mirrored:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size      Available Used% State  #Vols  Nodes  RAID
Status
-----
data_cluster
      4.19TB      4.13TB    2% online    8 node_A_1  raid_dp,
mirrored,
normal

root_cluster
      715.5GB    212.7GB   70% online    1 node_A_1  raid4,
mirrored,
normal

cluster_B Switched Over Aggregates:
Aggregate Size      Available Used% State  #Vols  Nodes  RAID
Status
-----
data_cluster_B
      4.19TB      4.11TB    2% online    5 node_A_1  raid_dp,
mirrored,
normal

root_cluster_B      -          -      - unknown    - node_A_1  -
```

5. Controllare lo stato del ripristino dello switchback:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
```

DR	Group	Cluster	Node	Configuration State	DR Mirroring Mode
1	cluster_A	node_A_1	configured	enabled	heal roots
completed	cluster_B	node_B_2	configured	enabled	waiting for recovery
switchback					

2 entries were displayed.

#### 6. Eseguire lo switchback:

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful. Verify switchback
```

#### 7. Confermare lo stato dei nodi:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
```

DR	Group	Cluster	Node	Configuration State	DR Mirroring Mode
1	cluster_A	node_A_1	configured	enabled	normal
	cluster_B	node_B_2	configured	enabled	normal

2 entries were displayed.

#### 8. Confermare lo stato dell'operazione MetroCluster:

```
metrocluster operation show
```

L'output dovrebbe mostrare uno stato di successo.

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: 2/6/2016 13:54:25
End Time: 2/6/2016 13:56:15
Errors: -
```

## Verifica del funzionamento in seguito a interruzione della linea di alimentazione

È possibile verificare la risposta della configurazione MetroCluster in caso di errore di una PDU.

### A proposito di questa attività

La procedura consigliata consiste nel collegare ciascun alimentatore di un componente a alimentatori separati. Se entrambe le PSU sono collegate alla stessa unità di distribuzione dell'alimentazione (PDU) e si verifica un'interruzione dell'alimentazione elettrica, il sito potrebbe non essere operativo o uno shelf completo potrebbe non essere disponibile. Il guasto di una linea di alimentazione viene testato per verificare che non vi siano incongruenze nel cablaggio che potrebbero causare un'interruzione del servizio.

Questo test dovrebbe richiedere circa 15 minuti.

Questo test richiede lo spegnimento di tutte le PDU di sinistra e quindi di tutte le PDU di destra su tutti i rack contenenti i componenti MetroCluster.

Questa procedura ha i seguenti risultati attesi:

- Gli errori devono essere generati quando le PDU sono disconnesse.
- Non devono verificarsi failover o perdita di servizio.

### Fasi

1. Spegnere le PDU sul lato sinistro del rack contenente i componenti MetroCluster.
2. Monitorare il risultato sulla console:

```
system environment sensors show -state fault
```

```
storage shelf show -errors
```

```

cluster_A::> system environment sensors show -state fault

Node Sensor                      State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
-----
node_A_1
      PSU1                      fault
                                PSU_OFF
      PSU1 Pwr In OK            fault
                                FAULT
node_A_2
      PSU1                      fault
                                PSU_OFF
      PSU1 Pwr In OK            fault
                                FAULT

4 entries were displayed.

cluster_A::> storage shelf show -errors
  Shelf Name: 1.1
  Shelf UID: 50:0a:09:80:03:6c:44:d5
  Serial Number: SHFHU1443000059

Error Type          Description
-----
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1

```

3. Riaccendere le PDU di sinistra.
4. Assicurarsi che ONTAP cancella la condizione di errore.
5. Ripetere i passaggi precedenti con le PDU di destra.

## Verifica del funzionamento dopo la perdita di un singolo shelf di storage

È possibile verificare il guasto di un singolo shelf di storage per verificare che non vi sia un singolo punto di errore.

### A proposito di questa attività

Questa procedura ha i seguenti risultati attesi:

- Il software di monitoraggio dovrebbe segnalare un messaggio di errore.
- Non devono verificarsi failover o perdita di servizio.
- La risincronizzazione del mirror viene avviata automaticamente dopo il ripristino dell'errore hardware.

### Fasi

## 1. Controllare lo stato di failover dello storage:

```
storage failover show
```

```
cluster_A::> storage failover show
```

Node	Partner	Possible	State Description
node_A_1	node_A_2	true	Connected to node_A_2
node_A_2	node_A_1	true	Connected to node_A_1

2 entries were displayed.

## 2. Controllare lo stato dell'aggregato:

```
storage aggregate show
```

```
cluster_A::> storage aggregate show
```

```
cluster Aggregates:
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID
-----------	------	-----------	-------	-------	-------	-------	------

Status	-----	-----	-----	-----	-----	-----	-----
--------	-------	-------	-------	-------	-------	-------	-------

node_A_1data01_mirrored	4.15TB	3.40TB	18%	online	3	node_A_1	
-------------------------	--------	--------	-----	--------	---	----------	--

raid\_dp,

mirrored,

normal

node_A_1root	707.7GB	34.29GB	95%	online	1	node_A_1	
--------------	---------	---------	-----	--------	---	----------	--

raid\_dp,

mirrored,

normal

node_A_2_data01_mirrored	4.15TB	4.12TB	1%	online	2	node_A_2	
--------------------------	--------	--------	----	--------	---	----------	--

raid\_dp,

mirrored,

normal

node_A_2_data02_unmirrored	2.18TB	2.18TB	0%	online	1	node_A_2	
----------------------------	--------	--------	----	--------	---	----------	--

raid\_dp,

normal

node_A_2_root	707.7GB	34.27GB	95%	online	1	node_A_2	
---------------	---------	---------	-----	--------	---	----------	--

raid\_dp,

mirrored,

normal

### 3. Verificare che tutti gli SVM e i volumi di dati siano online e che servano i dati:

```
vserver show -type data
```

```
network interface show -fields is-home false
```

```
volume show !vol0,!MDV*
```

```
cluster_A::> vservers show -type data
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----					
SVM1	data	sync-source		running	SVM1_root
node_A_1_data01_mirrored					
SVM2	data	sync-source		running	SVM2_root
node_A_2_data01_mirrored					

```
cluster_A::> network interface show -fields is-home false
There are no entries matching your query.
```

```
cluster_A::> volume show !vol0,!MDV*
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----					
-----					
SVM1					
	SVM1_root	node_A_1data01_mirrored	online	RW	10GB
9.50GB	5%				
SVM1					
	SVM1_data_vol	node_A_1data01_mirrored	online	RW	10GB
9.49GB	5%				
SVM2					
	SVM2_root	node_A_2_data01_mirrored	online	RW	10GB
9.49GB	5%				
SVM2					
	SVM2_data_vol	node_A_2_data02_unmirrored	online	RW	1GB
972.6MB	5%				

4. Identificare uno shelf nel Pool 1 per il nodo "node\_A\_2" da spegnere per simulare un guasto hardware improvviso:



```
storage aggregate show -r -node node-name !*root
```

Lo shelf selezionato deve contenere dischi che fanno parte di un aggregato di dati mirrorati.

Nell'esempio seguente, l'ID dello shelf "31" è stato selezionato per non riuscire.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
```

					Usable	
Physical						
Position	Disk		Pool	Type	RPM	Size
Size	Status					
-----						
dparity	2.30.3		0	BSAS	7200	827.7GB
828.0GB	(normal)					
parity	2.30.4		0	BSAS	7200	827.7GB
828.0GB	(normal)					
data	2.30.6		0	BSAS	7200	827.7GB
828.0GB	(normal)					
data	2.30.8		0	BSAS	7200	827.7GB
828.0GB	(normal)					
data	2.30.5		0	BSAS	7200	827.7GB
828.0GB	(normal)					

```

Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
```

					Usable	
Physical						
Position	Disk		Pool	Type	RPM	Size
Size	Status					
-----						
dparity	1.31.7		1	BSAS	7200	827.7GB
828.0GB	(normal)					
parity	1.31.6		1	BSAS	7200	827.7GB
828.0GB	(normal)					
data	1.31.3		1	BSAS	7200	827.7GB
828.0GB	(normal)					
data	1.31.4		1	BSAS	7200	827.7GB

```

828.0GB (normal)
      data      1.31.5                1    BSAS      7200    827.7GB
828.0GB (normal)

Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
  RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)

Physical
      Position Disk                Pool Type      RPM      Size
Size Status
-----
-----
      dparity  2.30.12                0    BSAS      7200    827.7GB
828.0GB (normal)
      parity   2.30.22                0    BSAS      7200    827.7GB
828.0GB (normal)
      data     2.30.21                0    BSAS      7200    827.7GB
828.0GB (normal)
      data     2.30.20                0    BSAS      7200    827.7GB
828.0GB (normal)
      data     2.30.14                0    BSAS      7200    827.7GB
828.0GB (normal)
15 entries were displayed.

```

5. Spegner fisicamente lo shelf selezionato.

6. Controllare di nuovo lo stato dell'aggregato:

```
storage aggregate show
```

```
storage aggregate show -r -node node_A_2 !*root
```

L'aggregato con i dischi sullo shelf spento dovrebbe avere uno stato RAID "degradato" e i dischi sul plex interessato dovrebbero avere uno stato "guasto", come mostrato nell'esempio seguente:

```

cluster_A::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes      RAID
Status
-----
-----
node_A_1data01_mirrored
      4.15TB      3.40TB    18% online      3 node_A_1
raid_dp,

```

```

mirrored,

normal
node_A_1root
          707.7GB    34.29GB    95% online        1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
          4.15TB     4.12TB     1% online        2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
          2.18TB     2.18TB     0% online        1 node_A_2
raid_dp,

normal
node_A_2_root
          707.7GB    34.27GB    95% online        1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)

Usable
Physical
Position Disk                                Pool Type    RPM    Size
Size Status
-----
-----
dparity  2.30.3                                0    BSAS    7200  827.7GB
828.0GB (normal)
parity   2.30.4                                0    BSAS    7200  827.7GB

```

```

828.0GB (normal)
    data      2.30.6          0    BSAS    7200    827.7GB
828.0GB (normal)
    data      2.30.8          0    BSAS    7200    827.7GB
828.0GB (normal)
    data      2.30.5          0    BSAS    7200    827.7GB
828.0GB (normal)

```

```

Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)

```

```

RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)

```

					Usable
Physical					
Position	Disk	Pool	Type	RPM	Size
Size	Status				
-----					
dparity	FAILED	-	-	-	827.7GB
- (failed)					
parity	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					
data	FAILED	-	-	-	827.7GB
- (failed)					

```

Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)

```

```

Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)

```

```

RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)

```

					Usable
Physical					
Position	Disk	Pool	Type	RPM	Size
Size	Status				
-----					
dparity	2.30.12	0	BSAS	7200	827.7GB
828.0GB (normal)					
parity	2.30.22	0	BSAS	7200	827.7GB
828.0GB (normal)					
data	2.30.21	0	BSAS	7200	827.7GB

```
828.0GB (normal)
  data      2.30.20                0   BSAS    7200   827.7GB
828.0GB (normal)
  data      2.30.14                0   BSAS    7200   827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Verificare che i dati siano stati forniti e che tutti i volumi siano ancora online:

```
vserver show -type data
```

```
network interface show -fields is-home false
```

```
volume show !vol0,!MDV*
```

```

cluster_A::> vservers show -type data

cluster_A::> vservers show -type data

```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
SVM1	data	sync-source		running	SVM1_root
node_A_1_data01_mirrored					
SVM2	data	sync-source		running	SVM2_root
node_A_1_data01_mirrored					

```

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*

```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
SVM1					
	SVM1_root	node_A_1data01_mirrored	online	RW	10GB
9.50GB	5%				
SVM1					
	SVM1_data_vol	node_A_1data01_mirrored	online	RW	10GB
9.49GB	5%				
SVM2					
	SVM2_root	node_A_1data01_mirrored	online	RW	10GB
9.49GB	5%				
SVM2					
	SVM2_data_vol	node_A_2_data02_unmirrored	online	RW	1GB
972.6MB	5%				

8. Accendere fisicamente lo shelf.

La risincronizzazione viene avviata automaticamente.

9. Verificare che la risincronizzazione sia stata avviata:

```
storage aggregate show
```

L'aggregato interessato deve avere uno stato RAID di "resyncing", come mostrato nell'esempio seguente:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate      Size Available Used% State  #Vols  Nodes      RAID
Status
-----
node_A_1_data01_mirrored
      4.15TB      3.40TB   18% online      3 node_A_1
raid_dp,
mirrored,
normal
node_A_1_root
      707.7GB      34.29GB   95% online      1 node_A_1
raid_dp,
mirrored,
normal
node_A_2_data01_mirrored
      4.15TB      4.12TB    1% online      2 node_A_2
raid_dp,
resyncing
node_A_2_data02_unmirrored
      2.18TB      2.18TB    0% online      1 node_A_2
raid_dp,
normal
node_A_2_root
      707.7GB      34.27GB   95% online      1 node_A_2
raid_dp,
resyncing
```

10. Monitorare l'aggregato per confermare che la risincronizzazione è completa:

```
storage aggregate show
```

L'aggregato interessato deve avere uno stato RAID "normale", come mostrato nell'esempio seguente:

```

cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
node_A_1data01_mirrored
      4.15TB      3.40TB    18% online      3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
      707.7GB      34.29GB    95% online      1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
      4.15TB      4.12TB     1% online      2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
      2.18TB      2.18TB     0% online      1 node_A_2
raid_dp,

normal
node_A_2_root
      707.7GB      34.27GB    95% online      1 node_A_2
raid_dp,

resyncing

```

## Considerazioni sulla rimozione delle configurazioni MetroCluster

Dopo aver rimosso la configurazione MetroCluster, tutte le interconnessioni e la connettività dei dischi devono essere regolate in modo da essere supportate. Per rimuovere la configurazione MetroCluster, contattare il supporto tecnico.





Non è possibile annullare la configurazione di MetroCluster. Questo processo deve essere eseguito solo con l'assistenza del supporto tecnico. Contattare il supporto tecnico NetApp e consultare la guida appropriata per la configurazione dal "[Come rimuovere i nodi da una configurazione MetroCluster - Guida alla risoluzione.](#)"

## Considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster

Quando si utilizza ONTAP in una configurazione MetroCluster, è necessario tenere presente alcune considerazioni relative a licenze, peering ai cluster al di fuori della configurazione MetroCluster, esecuzione di operazioni sui volumi, operazioni NVFAIL e altre operazioni ONTAP.

La configurazione ONTAP dei due cluster, inclusa la rete, deve essere identica, perché la funzionalità MetroCluster si basa sulla capacità di un cluster di fornire dati perfettamente al partner in caso di switchover.

### Considerazioni sulle licenze

- Entrambi i siti devono essere concessi in licenza per le stesse funzionalità concesse in licenza al sito.
- Tutti i nodi devono essere concessi in licenza per le stesse funzioni bloccate dal nodo.

### Considerazione di SnapMirror

- Il disaster recovery di SnapMirror SVM è supportato solo nelle configurazioni MetroCluster con versioni di ONTAP 9.5 o successive.

### Operazioni MetroCluster in Gestore di sistema ONTAP

A seconda della versione di ONTAP in uso, è possibile eseguire alcune operazioni specifiche di MetroCluster utilizzando Gestione di sistema di ONTAP.

Per ulteriori informazioni, fare riferimento alla "[Gestire i siti MetroCluster con Gestione di sistema](#)" documentazione.

### Supporto di FlexCache in una configurazione MetroCluster

A partire da ONTAP 9.7, i volumi FlexCache sono supportati nelle configurazioni MetroCluster. È necessario conoscere i requisiti per l'abrogazione manuale dopo le operazioni di switchover o switchback.

#### **Annullamento della SVM dopo lo switchover quando l'origine e la cache di FlexCache si trovano all'interno dello stesso sito MetroCluster**

Dopo uno switchover negoziato o non pianificato, qualsiasi relazione di peering SVM FlexCache all'interno del cluster deve essere configurata manualmente.

Ad esempio, le SVM vs1 (cache) e vs2 (origine) si trovano sul sito\_A. Questi SVM sono in peering.

Dopo lo switchover, le SVM vs1-mc e vs2-mc vengono attivate presso il sito del partner (Site\_B). Devono essere revocati manualmente perché FlexCache funzioni utilizzando il comando di annullamento peer vserver.

## Annullamento della SVM dopo lo switchover o lo switchback quando una destinazione FlexCache si trova su un terzo cluster e in modalità disconnessa

Per le relazioni FlexCache con un cluster al di fuori della configurazione MetroCluster, il peering deve sempre essere riconfigurato manualmente dopo uno switchover se i cluster coinvolti sono in modalità disconnessa durante lo switchover.

Ad esempio:

- Un'estremità del FlexCache (cache\_1 su vs1) risiede nel sito MetroCluster\_A ha un'estremità del FlexCache
- L'altra estremità del FlexCache (origin\_1 su vs2) risiede sul sito\_C (non nella configurazione MetroCluster)

Quando viene attivato lo switchover e se Site\_A e Site\_C non sono connessi, è necessario revocare manualmente le SVM sul sito\_B (il cluster di switchover) e sul sito\_C utilizzando il comando di peer repeer del vserver dopo lo switchover.

Quando viene eseguito lo switchback, è necessario revocare nuovamente le SVM sul sito\_A (il cluster originale) e sul sito\_C.

### Informazioni correlate

["Gestione dei volumi FlexCache con l'interfaccia CLI"](#)

## Supporto FabricPool nelle configurazioni MetroCluster

A partire da ONTAP 9.7, le configurazioni MetroCluster supportano i Tier di storage FabricPool.

Per informazioni generali sull'utilizzo di FabricPools, vedere ["Gestione di dischi e Tier \(aggregato\)"](#).

### Considerazioni sull'utilizzo di FabricPools

- I cluster devono disporre di licenze FabricPool con limiti di capacità corrispondenti.
- I cluster devono avere IPspaces con nomi corrispondenti.

Può trattarsi dell'IPspace predefinito o di uno spazio IP creato da un amministratore. Questo IPspace verrà utilizzato per le impostazioni di configurazione dell'archivio di oggetti FabricPool.

- Per l'IPspace selezionato, ciascun cluster deve avere una LIF intercluster definita che possa raggiungere l'archivio di oggetti esterno

### Configurazione di un aggregato per l'utilizzo in un FabricPool mirrorato



Prima di configurare l'aggregato, è necessario configurare gli archivi di oggetti come descritto in "impostazione degli archivi di oggetti per FabricPool in una configurazione MetroCluster" in ["Gestione di dischi e aggregati"](#).

### Fasi

Per configurare un aggregato per l'utilizzo in un FabricPool:

1. Creare l'aggregato o selezionare un aggregato esistente.
2. Eseguire il mirroring dell'aggregato come tipico aggregato mirrorato all'interno della configurazione MetroCluster.

3. Creare il mirror FabricPool con l'aggregato, come descritto in ["Gestione di dischi e aggregati"](#)

a. Allegare un archivio di oggetti primario.

Questo archivio di oggetti è fisicamente più vicino al cluster.

b. Aggiungere un archivio di oggetti mirror.

Questo archivio di oggetti è fisicamente più lontano dal cluster rispetto all'archivio di oggetti primario.

## Supporto FlexGroup nelle configurazioni MetroCluster

A partire da ONTAP 9.6, le configurazioni MetroCluster supportano i volumi FlexGroup.

## Pianificazioni dei lavori in una configurazione MetroCluster

In ONTAP 9.3 e versioni successive, le pianificazioni dei processi create dall'utente vengono replicate automaticamente tra i cluster in una configurazione MetroCluster. Se si crea, modifica o elimina una pianificazione di processo su un cluster, la stessa pianificazione viene creata automaticamente sul cluster partner, utilizzando il servizio di replica configurazione (CRS).



Le pianificazioni create dal sistema non vengono replicate ed è necessario eseguire manualmente la stessa operazione sul cluster partner in modo che le pianificazioni dei processi su entrambi i cluster siano identiche.

## Peering dei cluster dal sito MetroCluster a un terzo cluster

Poiché la configurazione di peering non viene replicata, se si esegue il peer di uno dei cluster della configurazione MetroCluster in un terzo cluster esterno a tale configurazione, è necessario configurare anche il peering sul cluster MetroCluster del partner. In questo modo, è possibile mantenere il peering in caso di commutazione.

Il cluster non MetroCluster deve eseguire ONTAP 8.3 o versione successiva. In caso contrario, il peering viene perso se si verifica uno switchover anche se il peering è stato configurato su entrambi i partner MetroCluster.

## Replica della configurazione del client LDAP in una configurazione MetroCluster

Una configurazione del client LDAP creata su una macchina virtuale di storage (SVM) su un cluster locale viene replicata nella SVM dei dati del partner sul cluster remoto. Ad esempio, se la configurazione del client LDAP viene creata sulla SVM amministrativa sul cluster locale, viene replicata su tutti gli SVM dei dati di amministrazione sul cluster remoto. Questa funzione MetroCluster è intenzionale in modo che la configurazione del client LDAP sia attiva su tutte le SVM partner sul cluster remoto.

## Linee guida per il networking e la creazione di LIF per le configurazioni MetroCluster

È necessario conoscere le modalità di creazione e replica delle LIF in una configurazione MetroCluster. È inoltre necessario conoscere i requisiti di coerenza per poter prendere decisioni appropriate durante la configurazione della rete.

### Informazioni correlate

["Gestione di rete e LIF"](#)

"Replica di oggetti IPSpace e requisiti di configurazione della subnet"

"Requisiti per la creazione di LIF in una configurazione MetroCluster"

"Requisiti e problemi di posizionamento e replica LIF"

## **Replica di oggetti IPSpace e requisiti di configurazione della subnet**

È necessario conoscere i requisiti per la replica degli oggetti IPSpace nel cluster partner e per la configurazione di subnet e IPv6 in una configurazione MetroCluster.

### **Replica di IPSpace**

Durante la replica degli oggetti IPSpace nel cluster partner, è necessario prendere in considerazione le seguenti linee guida:

- I nomi IPSpace dei due siti devono corrispondere.
- Gli oggetti IPSpace devono essere replicati manualmente nel cluster partner.

Tutte le macchine virtuali di storage (SVM) create e assegnate a un IPSpace prima della replica di IPSpace non verranno replicate nel cluster partner.

### **Configurazione della subnet**

Durante la configurazione delle subnet in una configurazione MetroCluster, è necessario prendere in considerazione le seguenti linee guida:

- Entrambi i cluster della configurazione MetroCluster devono avere una subnet nello stesso IPSpace con lo stesso nome di subnet, subnet, dominio di trasmissione e gateway.
- Gli intervalli IP dei due cluster devono essere diversi.

Nell'esempio seguente, gli intervalli IP sono diversi:

```
cluster_A::> network subnet show
```

```
IPspace: Default
```

Subnet		Broadcast		Avail/	
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
	192.168.2.11-192.168.2.20				

```
cluster_B::> network subnet show
```

```
IPspace: Default
```

Subnet		Broadcast		Avail/	
Name	Subnet	Domain	Gateway	Total	Ranges
subnet1	192.168.2.0/24	Default	192.168.2.1	10/10	
	192.168.2.21-192.168.2.30				

## Configurazione IPv6

Se IPv6 è configurato su un sito, IPv6 deve essere configurato anche sull'altro sito.

## Informazioni correlate

["Requisiti per la creazione di LIF in una configurazione MetroCluster"](#)

["Requisiti e problemi di posizionamento e replica LIF"](#)

## Requisiti per la creazione di LIF in una configurazione MetroCluster

Quando si configura la rete in una configurazione MetroCluster, è necessario conoscere i requisiti per la creazione di LIF.

Durante la creazione di LIF, è necessario prendere in considerazione le seguenti linee guida:

- Fibre Channel (canale fibra): È necessario utilizzare fabric allungati VSAN o allungati
- IP/iSCSI: È necessario utilizzare la rete con estensione Layer 2
- ARP Broadcasts (trasmissioni ARP): È necessario attivare le trasmissioni ARP tra i due cluster
- LIF duplicati: Non è necessario creare più LIF con lo stesso indirizzo IP (LIF duplicati) in un IPspace
- Configurazioni NFS e SAN: È necessario utilizzare diverse macchine virtuali di storage (SVM) per gli aggregati senza mirror e con mirroring

## Verificare la creazione di LIF

È possibile confermare la creazione di una LIF in una configurazione MetroCluster eseguendo il comando `MetroCluster check lif show`. In caso di problemi durante la creazione del file LIF, è possibile utilizzare il comando `MetroCluster check lif repair-placement` per risolvere i problemi.

## Informazioni correlate

["Replica di oggetti IPspace e requisiti di configurazione della subnet"](#)

["Requisiti e problemi di posizionamento e replica LIF"](#)

## Requisiti e problemi di posizionamento e replica LIF

È necessario conoscere i requisiti di replica LIF in una configurazione MetroCluster. È inoltre necessario conoscere il modo in cui un LIF replicato viene collocato in un cluster di partner e tenere presenti i problemi che si verificano quando la replica LIF o il posizionamento LIF non riesce.

### Replica di LIF nel cluster del partner

Quando si crea una LIF su un cluster in una configurazione MetroCluster, la LIF viene replicata sul cluster partner. I LIF non vengono posizionati in base al nome uno a uno. Per verificare la disponibilità di LIF dopo un'operazione di switchover, il processo di posizionamento LIF verifica che le porte siano in grado di ospitare LIF in base ai controlli di raggiungibilità e attributo delle porte.

Il sistema deve soddisfare le seguenti condizioni per inserire i file LIF replicati nel cluster del partner:

Condizione	Tipo LIF: FC	Tipo LIF: IP/iSCSI
Identificazione del nodo	ONTAP tenta di collocare il LIF replicato nel partner di disaster recovery (DR) del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.	ONTAP tenta di posizionare il LIF replicato sul partner DR del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.
Identificazione della porta	ONTAP identifica le porte di destinazione FC collegate sul cluster DR.	Le porte del cluster DR che si trovano nello stesso IPspace del LIF di origine vengono selezionate per un controllo di raggiungibilità. Se non vi sono porte nel cluster DR nello stesso IPspace, il LIF non può essere posizionato.  Tutte le porte del cluster di DR che ospitano già una LIF nello stesso IPspace e nella stessa subnet vengono automaticamente contrassegnate come raggiungibili e possono essere utilizzate per il posizionamento. Queste porte non sono incluse nel controllo di raggiungibilità.
Controllo della raggiungibilità	La raggiungibilità viene determinata verificando la connettività del WWN del fabric di origine sulle porte del cluster DR. Se lo stesso fabric non è presente nel sito DR, il LIF viene posizionato su una porta casuale del partner DR.	La raggiungibilità è determinata dalla risposta a una trasmissione ARP (Address Resolution Protocol) da ciascuna porta precedentemente identificata sul cluster DR all'indirizzo IP di origine della LIF da posizionare. Per il successo dei controlli di raggiungibilità, è necessario consentire le trasmissioni ARP tra i due cluster.  Ogni porta che riceve una risposta dalla LIF di origine verrà contrassegnata come possibile per il posizionamento.

Selezione della porta	ONTAP classifica le porte in base ad attributi quali tipo di adattatore e velocità, quindi seleziona le porte con attributi corrispondenti. se non viene trovata alcuna porta con attributi corrispondenti, la LIF viene posizionata su una porta connessa in modo casuale sul partner DR.	<p>Dalle porte contrassegnate come raggiungibili durante il controllo di raggiungibilità, ONTAP preferisce le porte che si trovano nel dominio di trasmissione associato alla subnet della LIF. se non sono disponibili porte di rete sul cluster di DR che si trovano nel dominio di trasmissione associato alla subnet della LIF, Quindi, ONTAP seleziona le porte che hanno la raggiungibilità alla LIF di origine.</p> <p>Se non sono presenti porte con raggiungibilità alla LIF di origine, viene selezionata una porta dal dominio di trasmissione associato alla subnet della LIF di origine e, se non esiste tale dominio di trasmissione, viene selezionata una porta casuale.</p> <p>ONTAP classifica le porte in base ad attributi quali tipo di adattatore, tipo di interfaccia e velocità, quindi seleziona le porte con attributi corrispondenti.</p>
Posizionamento LIF	Dalle porte raggiungibili, ONTAP seleziona la porta meno caricata per il posizionamento.	Dalle porte selezionate, ONTAP seleziona la porta meno caricata per il posizionamento.

#### Posizionamento di LIF replicati quando il nodo partner DR non è attivo

Quando viene creato un LIF iSCSI o FC su un nodo il cui partner DR è stato sostituito, il LIF replicato viene posizionato sul nodo del partner ausiliario DR. Dopo una successiva operazione di giveback, i LIF non vengono spostati automaticamente nel partner DR. Ciò può portare alla concentrazione di LIF su un singolo nodo nel cluster del partner. Durante un'operazione di switchover MetroCluster, i tentativi successivi di mappare le LUN appartenenti alla macchina virtuale di storage (SVM) non riescono.

Eseguire il `metrocluster check lif show` Comando dopo un'operazione di Takeover o giveback per verificare che il posizionamento LIF sia corretto. In caso di errori, è possibile eseguire `metrocluster check lif repair-placement` comando per risolvere i problemi.

#### Errori di posizionamento LIF

Errori di posizionamento LIF visualizzati da `metrocluster check lif show` i comandi vengono conservati dopo un'operazione di switchover. Se il `network interface modify`, `network interface rename`, o `network interface delete` Viene inviato un comando per un LIF con un errore di posizionamento, l'errore viene rimosso e non viene visualizzato nell'output di `metrocluster check lif show` comando.

#### Errore di replica LIF

È inoltre possibile verificare se la replica LIF ha avuto esito positivo utilizzando `metrocluster check lif show` comando. Se la replica LIF non riesce, viene visualizzato un messaggio EMS.

È possibile correggere un errore di replica eseguendo `metrocluster check lif repair-placement` Comando per qualsiasi LIF che non riesce a trovare una porta corretta. È necessario risolvere al più presto eventuali errori di replica LIF per verificare la disponibilità di LIF durante un'operazione di switchover MetroCluster.



Anche se la SVM di origine non è disponibile, il posizionamento LIF potrebbe procedere normalmente se esiste una LIF appartenente a una SVM diversa in una porta con lo stesso IPspace e la stessa rete nella SVM di destinazione.

#### Informazioni correlate

["Replica di oggetti IPspace e requisiti di configurazione della subnet"](#)

["Requisiti per la creazione di LIF in una configurazione MetroCluster"](#)

#### Creazione di un volume su un aggregato root

Il sistema non consente la creazione di nuovi volumi nell'aggregato root (un aggregato con un criterio ha di CFO) di un nodo in una configurazione MetroCluster.

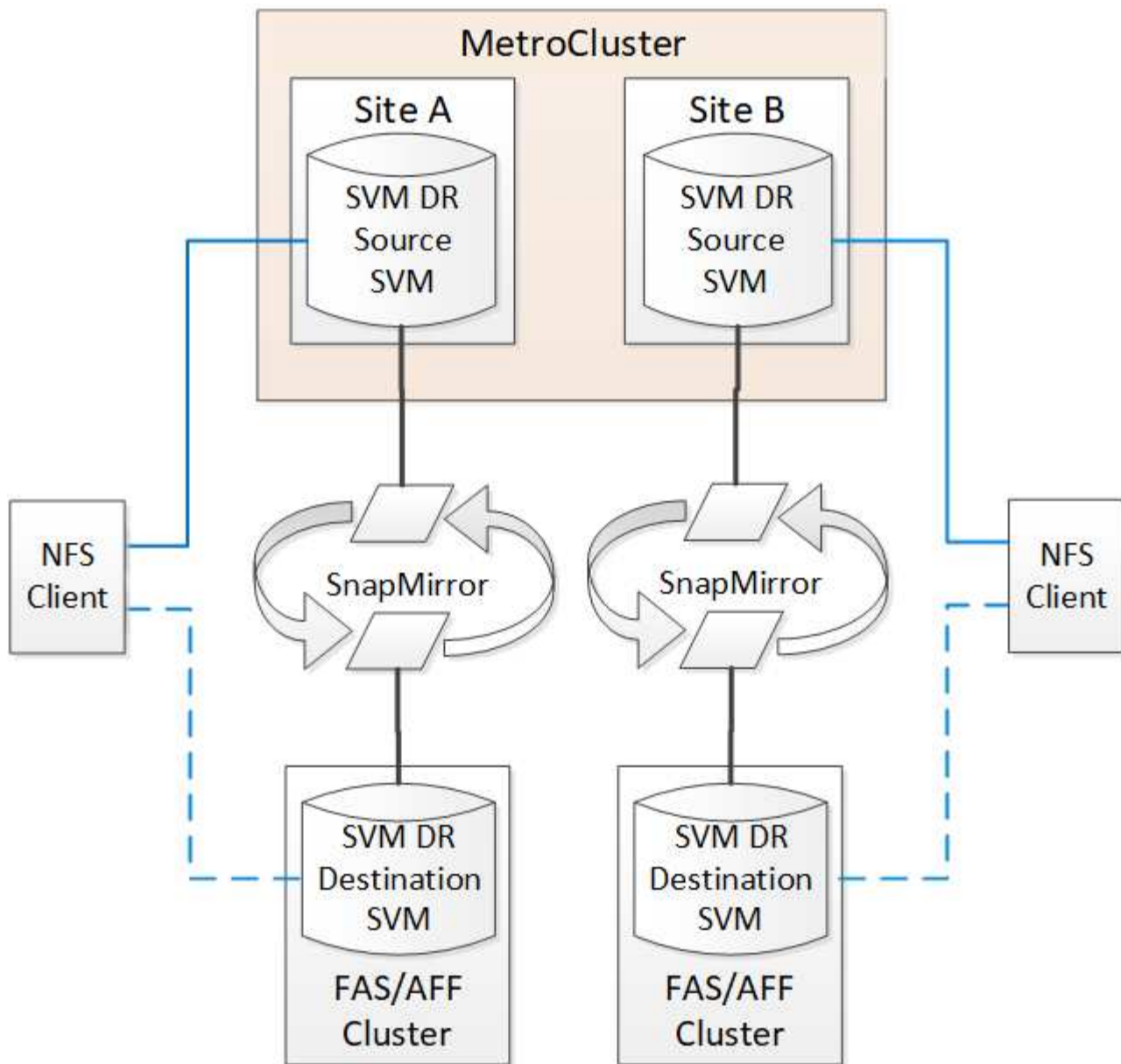
A causa di questa restrizione, non è possibile aggiungere aggregati root a una SVM utilizzando `vserver add-aggregates` comando.

#### Disaster recovery SVM in una configurazione MetroCluster

A partire da ONTAP 9.5, le macchine virtuali con storage attivo (SVM) in una configurazione MetroCluster possono essere utilizzate come origini con la funzione di disaster recovery di SnapMirror SVM. La SVM di destinazione deve trovarsi sul terzo cluster al di fuori della configurazione MetroCluster.

A partire da ONTAP 9.11.1, entrambi i siti all'interno di una configurazione MetroCluster possono essere l'origine di una relazione DR SVM con un cluster di destinazione FAS o AFF, come mostrato nell'immagine seguente.





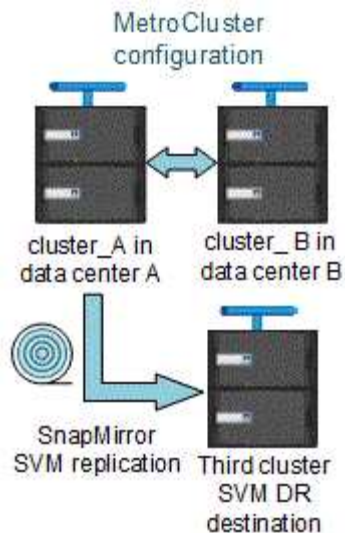
È necessario conoscere i seguenti requisiti e limitazioni dell'utilizzo di SVM con il disaster recovery SnapMirror:

- Solo una SVM attiva all'interno di una configurazione MetroCluster può essere l'origine di una relazione di disaster recovery SVM.

Un'origine può essere una SVM di origine della sincronizzazione prima dello switchover o una SVM di destinazione della sincronizzazione dopo lo switchover.

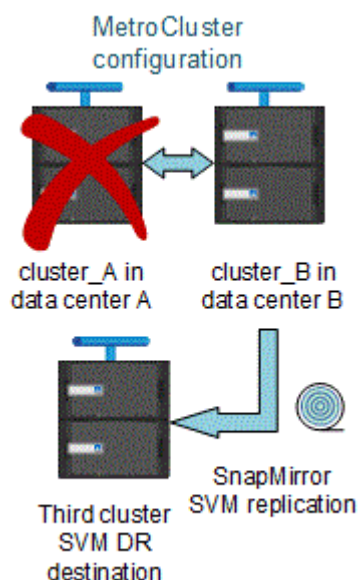
- Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.

La seguente immagine mostra il comportamento del disaster recovery SVM in uno stato stabile:



- Quando la SVM di origine della sincronizzazione è l'origine di una relazione DR con SVM, le informazioni di relazione DR con SVM di origine vengono replicate nel partner MetroCluster.

In questo modo, gli aggiornamenti DR di SVM possono continuare dopo uno switchover, come mostrato nell'immagine seguente:



- Durante i processi di switchover e switchback, la replica alla destinazione DR SVM potrebbe non riuscire.

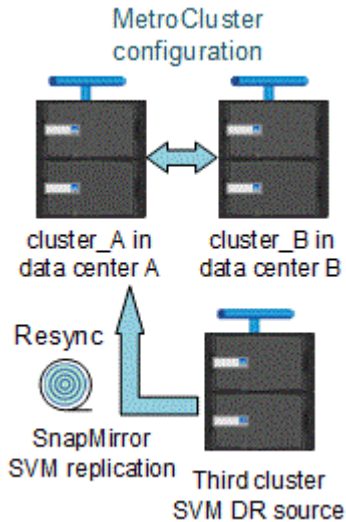
Tuttavia, una volta completato il processo di switchover o switchback, gli aggiornamenti pianificati per il DR SVM successivi avranno esito positivo.

Vedere “Replica della configurazione SVM” in ["Protezione dei dati"](#) Per informazioni dettagliate sulla configurazione di una relazione DR SVM.

### Risincronizzazione SVM in un sito di disaster recovery

Durante la risincronizzazione, l'origine del disaster recovery (DR) delle macchine virtuali dello storage sulla configurazione MetroCluster viene ripristinata dalla SVM di destinazione sul sito non MetroCluster.

Durante la risincronizzazione, la SVM di origine (cluster\_A) agisce temporaneamente come SVM di destinazione, come mostrato nell'immagine seguente:



#### Se durante la risincronizzazione si verifica uno switchover non pianificato

Gli switchover non pianificati che si verificano durante la risincronizzazione arrestano il trasferimento di risincronizzazione. Se si verifica uno switchover non pianificato, sono soddisfatte le seguenti condizioni:

- La SVM di destinazione sul sito MetroCluster (che era una SVM di origine prima della risincronizzazione) rimane come SVM di destinazione. La SVM del cluster partner continuerà a conservare il sottotipo e rimarrà inattiva.
- La relazione SnapMirror deve essere ricreata manualmente con la SVM di destinazione della sincronizzazione come destinazione.
- La relazione di SnapMirror non viene visualizzata nell'output di SnapMirror dopo uno switchover nel sito superstite, a meno che non venga eseguita un'operazione di creazione di SnapMirror.

#### Esecuzione dello switchback dopo uno switchover non pianificato durante la risincronizzazione

Per eseguire correttamente il processo di switchback, la relazione di risincronizzazione deve essere interrotta ed eliminata. Lo switchback non è consentito se sono presenti SVM di destinazione DR SnapMirror nella configurazione MetroCluster o se il cluster dispone di una SVM di sottotipo "dp-destination".

### L'output per il comando di visualizzazione plesso dell'aggregato di storage è indeterminato dopo uno switchover MetroCluster

Quando si esegue il comando show dell'aggregato di storage dopo uno switchover MetroCluster, lo stato di plex0 dell'aggregato root commutato è indeterminato e viene visualizzato come failed (non riuscito). Durante questo periodo, la root commutata non viene aggiornata. Lo stato effettivo di questo plex può essere determinato solo dopo la fase di riparazione MetroCluster.

### Modifica dei volumi per impostare il flag NVFAIL in caso di switchover

È possibile modificare un volume in modo che il flag NVFAIL venga impostato sul volume in caso di switchover MetroCluster. Il flag NVFAIL disattiva il volume da qualsiasi modifica. Ciò è necessario per i volumi che devono essere gestiti come se le scritture assegnate al volume fossero perse dopo il passaggio.



Nelle versioni di ONTAP precedenti alla 9.0, il flag NVFAIL viene utilizzato per ogni switchover. In ONTAP 9.0 e versioni successive, viene utilizzato lo switchover non pianificato (USO).

## Fase

1. Abilitare la configurazione MetroCluster per attivare NVFAIL allo switchover impostando `vol -dr-force -nvfail` parametro su on:

```
vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
```

## Dove trovare ulteriori informazioni

Scopri di più sulla configurazione di MetroCluster.

### MetroCluster e informazioni varie

Informazioni	Soggetto
<a href="#">"Installazione e configurazione di Fabric-Attached MetroCluster"</a>	<ul style="list-style-type: none"><li>• Architettura Fabric-Attached MetroCluster</li><li>• Cablaggio della configurazione</li><li>• Configurazione dei bridge FC-SAS</li><li>• Configurazione degli switch FC</li><li>• Configurazione di MetroCluster in ONTAP</li></ul>
<a href="#">"Estensione dell'installazione e della configurazione di MetroCluster"</a>	<ul style="list-style-type: none"><li>• Estendi l'architettura MetroCluster</li><li>• Cablaggio della configurazione</li><li>• Configurazione dei bridge FC-SAS</li><li>• Configurazione di MetroCluster in ONTAP</li></ul>
<a href="#">"Gestione di MetroCluster"</a>	<ul style="list-style-type: none"><li>• Informazioni sulla configurazione di MetroCluster</li><li>• Switchover, healing e switchback</li></ul>
<a href="#">"Disaster recovery"</a>	<ul style="list-style-type: none"><li>• Disaster recovery</li><li>• Switchover forzato</li><li>• Ripristino da un errore di storage o multi-controller</li></ul>

"Manutenzione MetroCluster"	<ul style="list-style-type: none"> <li>• Linee guida per la manutenzione in una configurazione MetroCluster FC</li> <li>• Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC</li> <li>• Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch</li> <li>• Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch</li> <li>• Sostituzione dell'hardware in un sito di emergenza in una configurazione FC MetroCluster Fabric-Attached o Stretch</li> <li>• Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi.</li> <li>• Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.</li> </ul>
"Upgrade ed espansione di MetroCluster"	<ul style="list-style-type: none"> <li>• Aggiornamento o aggiornamento di una configurazione MetroCluster</li> <li>• Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi</li> </ul>
"Transizione MetroCluster"	<ul style="list-style-type: none"> <li>• Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP</li> </ul>
"Upgrade, transizione ed espansione di MetroCluster"	<ul style="list-style-type: none"> <li>• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker</li> </ul>
<p>"Documentazione dei sistemi hardware ONTAP"</p> <p><b>Nota:</b> le procedure standard di manutenzione dello shelf storage possono essere utilizzate con le configurazioni MetroCluster IP.</p>	<ul style="list-style-type: none"> <li>• Aggiunta a caldo di uno shelf di dischi</li> <li>• Rimozione a caldo di uno shelf di dischi</li> </ul>
"Transizione basata sulla copia"	<ul style="list-style-type: none"> <li>• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster</li> </ul>
"Concetti di ONTAP"	<ul style="list-style-type: none"> <li>• Come funzionano gli aggregati mirrorati</li> </ul>

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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