



# **Installare un MetroCluster collegato al fabric**

## **ONTAP MetroCluster**

NetApp  
April 25, 2024

# Sommario

Installare un MetroCluster collegato al fabric .....	1
Panoramica .....	1
Prepararsi per l'installazione di MetroCluster .....	1
Scelta della procedura di installazione corretta per la configurazione .....	11
Collegare una configurazione MetroCluster collegata al fabric .....	12
Configurare l'hardware per la condivisione di un fabric FC Brocade 6510 durante la transizione .....	210
Configurazione del software MetroCluster in ONTAP .....	219
Considerazioni sull'utilizzo del protocollo Virtual IP e Border Gateway con una configurazione MetroCluster .....	278
Test della configurazione MetroCluster .....	281
Considerazioni sulla rimozione delle configurazioni MetroCluster .....	300
Pianificare e installare una configurazione MetroCluster con LUN array .....	301
Come utilizzare Active IQ Unified Manager e Gestore di sistema di ONTAP per ulteriori configurazioni e monitoraggi .....	354
Considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster .....	355
Dove trovare ulteriori informazioni .....	367

# Installare un MetroCluster collegato al fabric

## Panoramica

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

- ["Prepararsi all'installazione e comprendere tutti i requisiti"](#).
- ["Scegliere la procedura di installazione corretta"](#)
- ["Cablare i componenti"](#)
- ["Configurare il software"](#)
- ["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"](#).

## 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.

## **Considerazioni per le configurazioni MetroCluster con shelf di dischi nativi o LUN di array**

La configurazione MetroCluster supporta installazioni solo con shelf di dischi nativi (NetApp), solo LUN di array o una combinazione di entrambi.

I sistemi AFF non supportano i LUN degli array.

### **Informazioni correlate**

["Cablaggio di una configurazione MetroCluster collegata al fabric"](#)

["Pianificazione e installazione di una configurazione MetroCluster con LUN array"](#)

["Requisiti e riferimenti per l'installazione della virtualizzazione FlexArray"](#)

## **Considerazioni per la transizione da 7-Mode a ONTAP**

Prima di utilizzare gli strumenti di transizione per spostare i dati da una configurazione MetroCluster 7-Mode a una configurazione ONTAP, è necessario che la nuova configurazione MetroCluster sia completamente configurata e funzionante. Se la configurazione 7-Mode utilizza switch Brocade 6510, la nuova configurazione può condividere i fabric esistenti per ridurre i requisiti hardware.

Se si dispone di switch Brocade 6510 e si prevede di condividere le fabric dello switch tra 7-Mode Fabric MetroCluster e MetroCluster in esecuzione in ONTAP, è necessario utilizzare la procedura specifica per la configurazione dei componenti MetroCluster.

["Configurazione dell'hardware MetroCluster per la condivisione di un fabric FC Brocade 6510 7-Mode durante la transizione"](#)

## Considerazioni per gli ISL

È necessario determinare il numero di ISL necessari per ciascun fabric di switch FC nella configurazione MetroCluster. A partire da ONTAP 9.2, in alcuni casi, invece di dedicare switch FC e ISL a ogni singola configurazione MetroCluster, è possibile condividere gli stessi quattro switch.

### Considerazioni sulla condivisione ISL (ONTAP 9.2)

A partire da ONTAP 9.2, è possibile utilizzare la condivisione ISL nei seguenti casi:

- Una configurazione MetroCluster a due nodi e una a quattro nodi
- Due configurazioni MetroCluster separate a quattro nodi
- Due configurazioni MetroCluster separate a due nodi
- Due gruppi di DR in una configurazione MetroCluster a otto nodi

Il numero di ISL richiesti tra gli switch condivisi dipende dalla larghezza di banda dei modelli di piattaforma collegati agli switch condivisi.

Per determinare il numero di ISL necessari, considerare i seguenti aspetti della configurazione.

- I dispositivi non MetroCluster non devono essere collegati a nessuno degli switch FC che forniscono la connettività MetroCluster back-end.
- La condivisione ISL è supportata su tutti gli switch, ad eccezione degli switch Cisco 9250i e Cisco 9148.
- Tutti i nodi devono eseguire ONTAP 9.2 o versione successiva.
- Il cablaggio dello switch FC per la condivisione ISL è lo stesso del cablaggio MetroCluster a otto nodi.
- I file RCF per la condivisione ISL sono gli stessi del cablaggio MetroCluster a otto nodi.
- Verificare che tutte le versioni hardware e software siano supportate.

#### "NetApp Hardware Universe"

- La velocità e il numero di ISL devono essere dimensionati per supportare il carico del client su entrambi i sistemi MetroCluster.
- Gli ISL back-end e i componenti back-end devono essere dedicati solo alla configurazione MetroCluster.
- L'ISL deve utilizzare una delle velocità supportate: 4 Gbps, 8 Gbps, 16 Gbps o 32 Gbps.
- Gli ISL su un fabric devono essere tutti della stessa velocità e lunghezza.
- Gli ISL su un fabric devono avere tutti la stessa topologia. Ad esempio, dovrebbero essere tutti collegamenti diretti o, se il sistema utilizza WDM, dovrebbero utilizzare tutti WDM.

### Considerazioni ISL specifiche per la piattaforma

Il numero di ISL consigliati è specifico per il modello di piattaforma. La seguente tabella mostra i requisiti ISL per ciascun fabric in base al modello di piattaforma. Si presume che ogni ISL abbia una capacità di 16 Gbps.

Modello di piattaforma	Numero consigliato di ISL per gruppo DR a quattro nodi (per fabric switch)
------------------------	--



AFF A900 e FAS9500	Otto
AFF A700	Sei
FAS9000	Sei
8080	Quattro
Tutti gli altri	Due

Se il fabric dello switch supporta otto nodi (parte di una singola configurazione MetroCluster a otto nodi o due configurazioni a quattro nodi che condividono gli ISL), il numero totale consigliato di ISL per il fabric è la somma di quello richiesto per ciascun gruppo DR a quattro nodi. Ad esempio:

- Se il gruppo DR 1 include quattro sistemi AFF A700, sono necessari sei ISL.
- Se il gruppo di DR 2 include quattro sistemi FAS8200, sono necessari due ISL.
- Il numero totale di ISL consigliati per il fabric dello switch è otto.

## Considerazioni sull'utilizzo di apparecchiature TDM/WDM con configurazioni MetroCluster collegate al fabric

Il tool Hardware Universe fornisce alcune note sui requisiti che le apparecchiature TDM (Time Division Multiplexing) o WDM (Wavelength Division Multiplexing) devono soddisfare per funzionare con una configurazione Fabric-Attached MetroCluster. Queste note includono anche informazioni sulle varie configurazioni, che possono aiutare a determinare quando utilizzare la distribuzione in-order (IOD) dei frame o la distribuzione out-of-order (OOD) dei frame.

Un esempio di tali requisiti è che l'apparecchiatura TDM/WDM deve supportare la funzionalità di aggregazione dei collegamenti (trunking) con criteri di routing. L'ordine di consegna (IOD o OOOD) dei frame viene mantenuto all'interno di uno switch ed è determinato dalla policy di routing in vigore.

["NetApp Hardware Universe"](#)

La seguente tabella fornisce i criteri di routing per le configurazioni contenenti switch Brocade e switch Cisco:

Switch	Configurazione delle configurazioni MetroCluster per IOD	Configurazione delle configurazioni MetroCluster per OOD
Brocade	<ul style="list-style-type: none"> <li>• AptPolicy deve essere impostato su 1</li> <li>• DLS deve essere impostato su Off</li> <li>• IOD deve essere impostato su ON</li> </ul>	<ul style="list-style-type: none"> <li>• AptPolicy deve essere impostato su 3</li> <li>• DLS deve essere impostato su ON</li> <li>• IOD deve essere impostato su Off</li> </ul>

Cisco	<p>Policy per il VSAN designato da FCVI:</p> <ul style="list-style-type: none"> <li>• Policy per il bilanciamento del carico: Srcid e dstid</li> <li>• IOD deve essere impostato su ON</li> </ul> <p>Policy per il VSAN designato per lo storage:</p> <ul style="list-style-type: none"> <li>• Policy per il bilanciamento del carico: Srcid, dstid e oxid</li> <li>• VSAN non deve avere l'opzione di garanzia in-order impostata</li> </ul>	Non applicabile
-------	---	-----------------

### Quando utilizzare IOD

Si consiglia di utilizzare IOD se supportato dai collegamenti. Le seguenti configurazioni supportano IOD:

- Un singolo ISL
- L'ISL e il link (e l'apparecchiatura di collegamento, come TDM/WDM, se utilizzata) supportano la configurazione per IOD.
- Un singolo trunk, gli ISL e i link (e l'apparecchiatura di collegamento, come TDM/WDM, se utilizzata) supportano la configurazione per IOD.

### Quando utilizzare OOD

- È possibile utilizzare OOD per tutte le configurazioni che non supportano IOD.
- È possibile utilizzare OOD per configurazioni che non supportano la funzionalità trunking.

### Utilizzo di dispositivi di crittografia

Quando si utilizzano dispositivi di crittografia dedicati sull'ISL o la crittografia sui dispositivi WDM nella configurazione MetroCluster, è necessario soddisfare i seguenti requisiti:

- I dispositivi di crittografia esterni o le apparecchiature WDM sono stati certificati dal vendor con lo switch FC in questione.

L'autocertificazione deve riguardare la modalità operativa (ad esempio trunking e crittografia).

- La latenza aggiunta dovuta alla crittografia non deve superare i 10 microsecondi.

### Requisiti per l'utilizzo di uno switch Brocade DCX 8510-8

Durante la preparazione all'installazione di MetroCluster, è necessario conoscere l'architettura hardware di MetroCluster e i componenti richiesti.

- Gli switch DCX 8510-8 utilizzati nelle configurazioni MetroCluster devono essere acquistati da NetApp.

- Per la scalabilità, è necessario lasciare un blocco di porte tra le configurazioni MetroCluster se si collegano solo due MetroClusters in moduli a 4 porte. Ciò consente di espandere l'utilizzo delle porte nelle configurazioni MetroCluster senza doverlo riabilitare.
- Ogni switch Brocade DCX 8510-8 nella configurazione MetroCluster deve essere configurato correttamente per le porte ISL e le connessioni storage. Per l'utilizzo delle porte, consultare la seguente sezione: ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#).
- Gli MetroCluster non possono essere condivisi e ogni ISL richiede due ISL per ogni fabric.
- Lo switch DCX 8510-8 utilizzato per la connettività MetroCluster back-end non deve essere utilizzato per altre connessioni.

I dispositivi non MetroCluster non devono essere collegati a questi switch e il traffico non MetroCluster non deve passare attraverso gli switch DCX 8510-8.

- Una scheda di linea può essere collegata a MetroClusters \* ONTAP o \* MetroClusters 7-Mode ONTAP.



I file RCF non sono disponibili per questo switch.

Di seguito sono riportati i requisiti per l'utilizzo di due switch Brocade DCX 8510-8:

- È necessario disporre di uno switch DCX 8510-8 in ogni sito.
- È necessario utilizzare almeno due blade a 48 porte che contengono 16 GB di SFP in ogni switch.

Di seguito sono riportati i requisiti per l'utilizzo di quattro switch DCX 8510-8 in ogni sito in una configurazione MetroCluster:

- È necessario disporre di due switch DCX 8510-8 per ciascun sito.
- È necessario utilizzare almeno un blade a 48 porte per ogni switch DCX 8510-8.
- Ogni blade viene configurato come switch virtuale utilizzando fabric virtuali.

Gli switch Brocade DCX 8510-8 non supportano i seguenti prodotti NetApp:

- Config Advisor
- Fabric Health Monitor
- MyAutoSupport (i rischi del sistema potrebbero mostrare falsi positivi)
- Active IQ Unified Manager (in precedenza Unified Manager di OnCommand)



Assicurarsi che tutti i componenti necessari per questa configurazione si trovino in ["Tool di matrice di interoperabilità NetApp"](#). Per informazioni sulle configurazioni supportate, consultare la sezione delle note del tool Interoperability Matrix.

## Considerazioni sull'utilizzo di aggregati senza mirror

### Considerazioni sull'utilizzo di aggregati senza mirror

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

## **Considerazioni per gli aggregati senza mirror quando si eseguono interventi di manutenzione che richiedono lo spegnimento dell'alimentazione**

Se si esegue uno switchover negoziato per motivi di manutenzione che richiedono uno spegnimento dell'alimentazione a livello di sito, è necessario prima portare manualmente fuori linea gli aggregati senza mirror di proprietà del sito di disastro.

Se non si offline alcun aggregato senza mirror, i nodi del sito sopravvissuto potrebbero andare in stato di inattività a causa di una panica su più dischi. Questo potrebbe verificarsi se gli aggregati senza mirror passano offline o mancano, a causa della perdita di connettività allo storage nel sito di disastro. Questo è il risultato di un arresto dell'alimentazione o di una perdita degli ISL.

## **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 un aggregato senza mirror. Se si trovano su un 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**

Nelle versioni di ONTAP precedenti alla 9.9.1, un LUN non deve trovarsi in 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.

## **Utilizzo del firewall nei siti MetroCluster**

### **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.

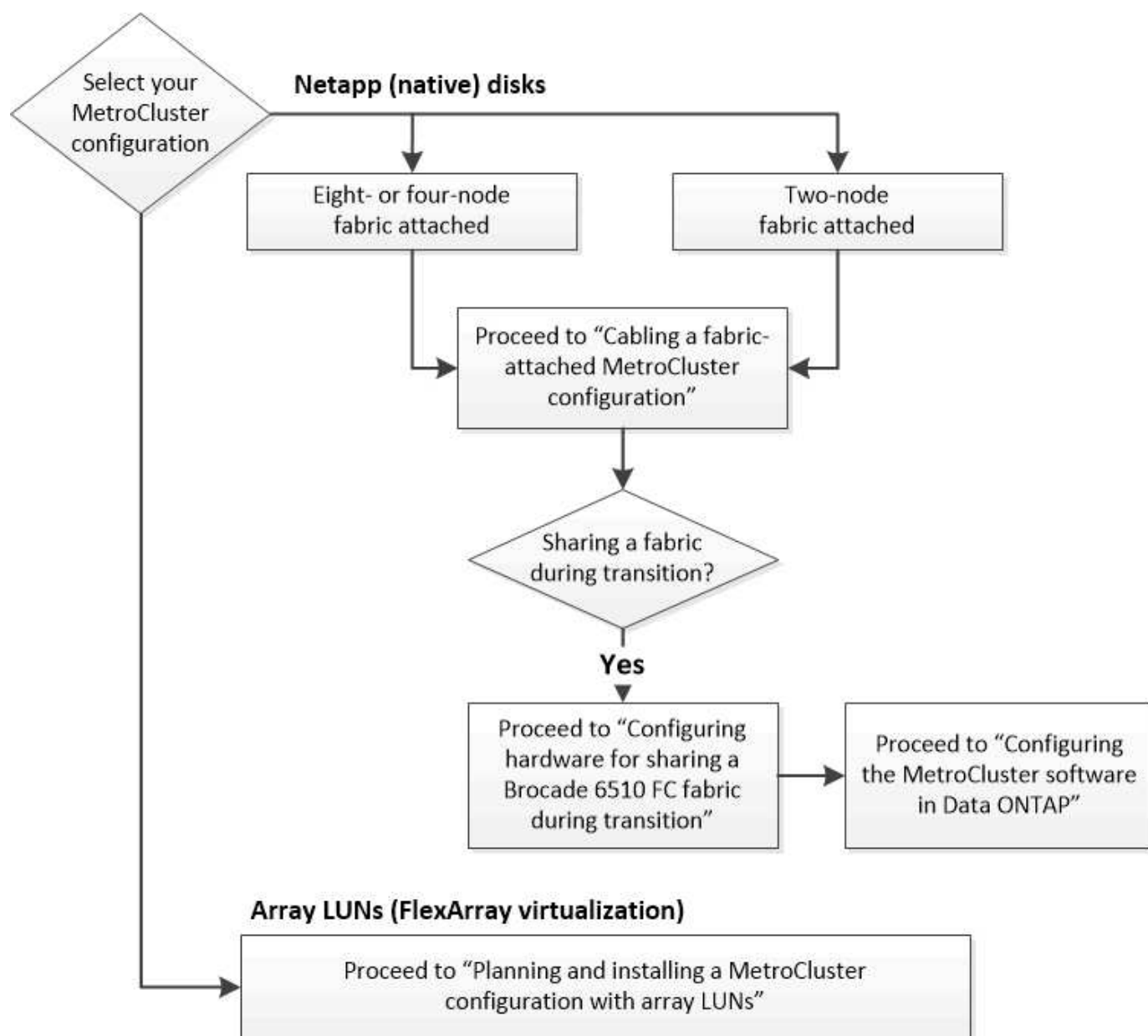
La seguente tabella mostra l'utilizzo della porta TCP/UDP in un firewall esterno posizionato tra due siti MetroCluster.

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

## Scelta della procedura di installazione corretta per la configurazione

È necessario scegliere la procedura di installazione corretta in base all'utilizzo di LUN FlexArray, al numero di nodi nella configurazione MetroCluster e alla condivisione di un fabric switch FC esistente utilizzato da un Fabric MetroCluster 7-Mode.

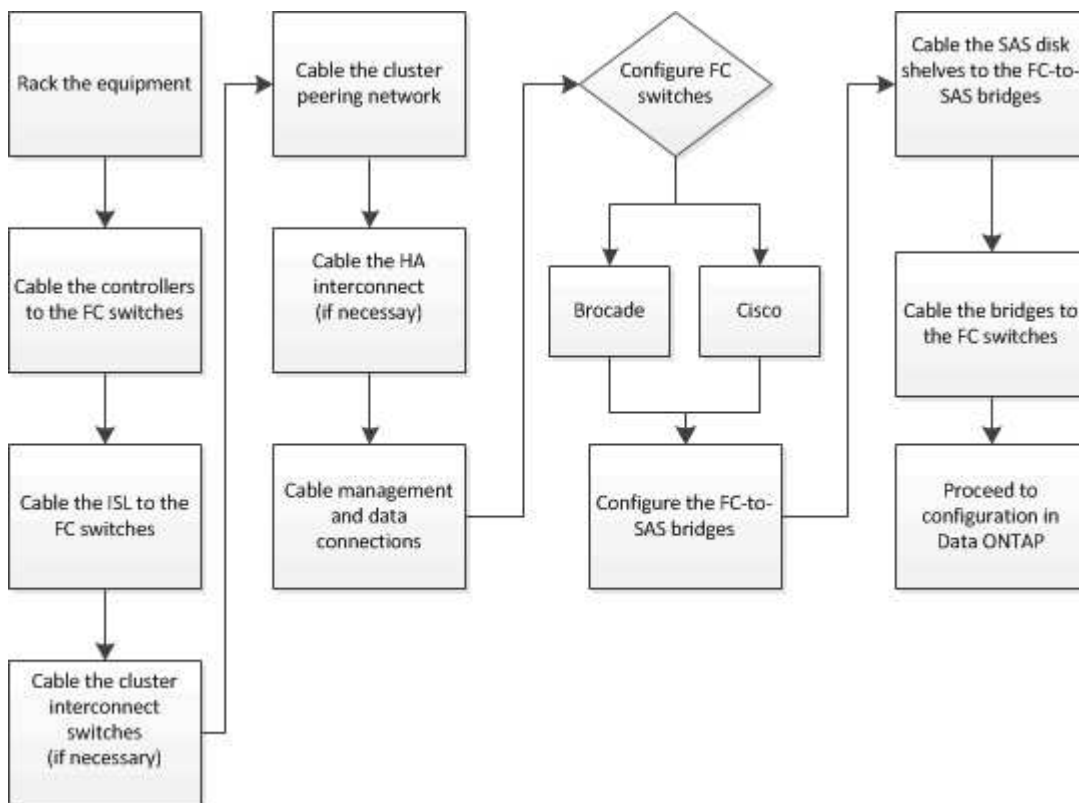


Per questo tipo di installazione...	Utilizzare queste procedure...
Configurazione fabric-attached con dischi NetApp (nativi)	<ol style="list-style-type: none"> <li>1. <a href="#">"Cablaggio di una configurazione MetroCluster collegata al fabric"</a></li> <li>2. <a href="#">"Configurazione del software MetroCluster in ONTAP"</a></li> </ol>
Configurazione fabric-attached durante la condivisione con un fabric switch FC esistente  Questa configurazione è supportata solo come configurazione temporanea con una configurazione Fabric MetroCluster 7-Mode che utilizza switch Brocade 6510.	<ol style="list-style-type: none"> <li>1. <a href="#">"Cablaggio di una configurazione MetroCluster collegata al fabric"</a></li> <li>2. <a href="#">"Configurazione dell'hardware MetroCluster per la condivisione di un fabric FC Brocade 6510 7-Mode durante la transizione"</a></li> <li>3. <a href="#">"Configurazione del software MetroCluster in ONTAP"</a></li> </ol>

## Collegare una configurazione MetroCluster collegata al fabric

### Cablaggio di una configurazione MetroCluster collegata al fabric

I componenti MetroCluster devono essere fisicamente installati, cablati e configurati in entrambi i siti geografici. I passaggi sono leggermente diversi per un sistema con shelf di dischi nativi rispetto a un sistema con LUN di array.



## Parti di una configurazione Fabric MetroCluster

### Parti di una configurazione Fabric MetroCluster

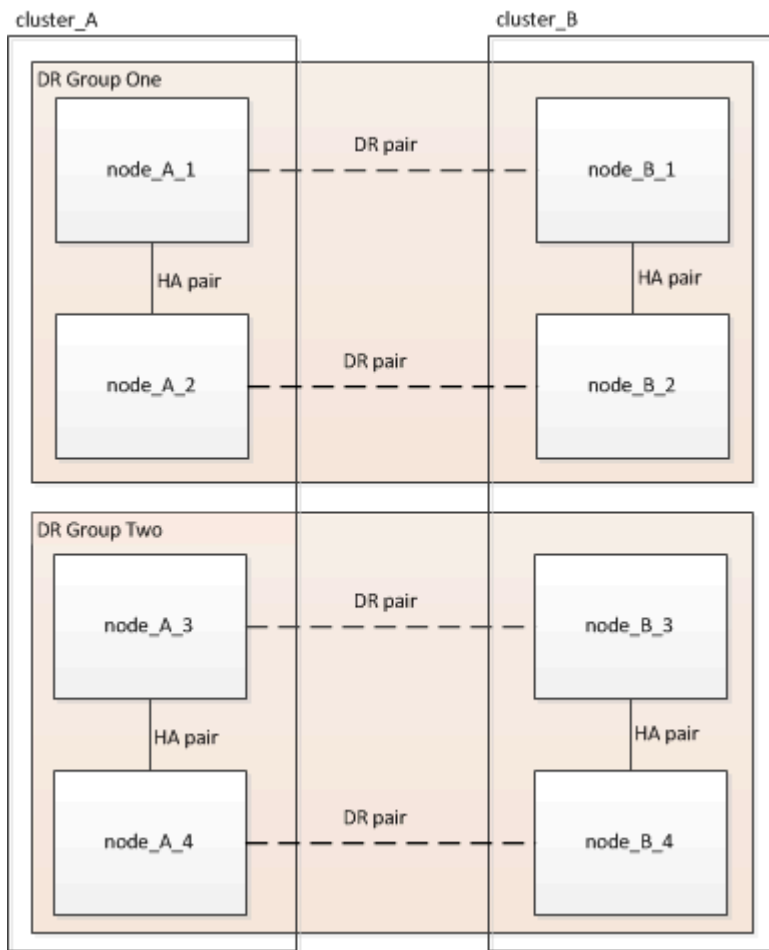
Durante la pianificazione della configurazione MetroCluster, è necessario comprendere i componenti hardware e il modo in cui si collegano.

#### Gruppi di disaster recovery (DR)

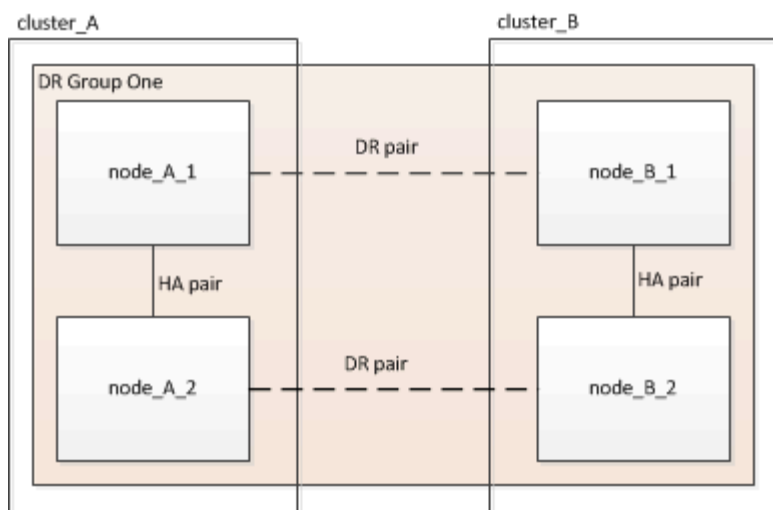
Una configurazione Fabric MetroCluster è costituita da uno o due gruppi DR, a seconda del numero di nodi nella configurazione MetroCluster. Ciascun gruppo di DR è costituito da quattro nodi.

- Una configurazione MetroCluster a otto nodi è costituita da due gruppi DR.
- Una configurazione MetroCluster a quattro nodi è costituita da un gruppo DR.

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



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



### Elementi hardware chiave

Una configurazione MetroCluster include i seguenti elementi hardware principali:

- Controller di storage

I controller storage non sono collegati direttamente allo storage, ma si collegano a due fabric switch FC ridondanti.

- Bridge FC-SAS

I bridge FC-SAS collegano gli stack di storage SAS agli switch FC, fornendo un bridging tra i due protocolli.

- Switch FC

Gli switch FC forniscono il backbone ISL a lungo raggio tra i due siti. Gli switch FC forniscono i due fabric di storage che consentono il mirroring dei dati nei pool di storage remoti.

- 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.

### Configurazione Fabric MetroCluster a otto nodi

Una configurazione a otto nodi è costituita da due cluster, uno per ciascun sito geograficamente separato. Cluster\_A si trova nel primo sito MetroCluster. Cluster\_B si trova nel secondo sito MetroCluster. Ogni sito dispone di uno stack di storage SAS. Sono supportati ulteriori stack di storage, ma ne viene mostrato solo uno per ciascun sito. Le coppie ha sono configurate come cluster senza switch, senza switch di interconnessione del cluster. Una configurazione commutata è supportata, ma non viene visualizzata.

Una configurazione a otto nodi include le seguenti connessioni:

- Connessioni FC da HBA e adattatori FC-VI di ciascun controller a ciascuno switch FC
- Una connessione FC da ciascun bridge FC-SAS a uno switch FC
- Connessioni SAS tra ogni shelf SAS e dalla parte superiore e inferiore di ogni stack a un bridge FC-SAS



- Un'interconnessione ha tra ciascun controller della coppia ha locale

Se i controller supportano una coppia ha a chassis singolo, l'interconnessione ha è interna, che si verifica attraverso la scheda madre, il che significa che non è necessaria un'interconnessione esterna.

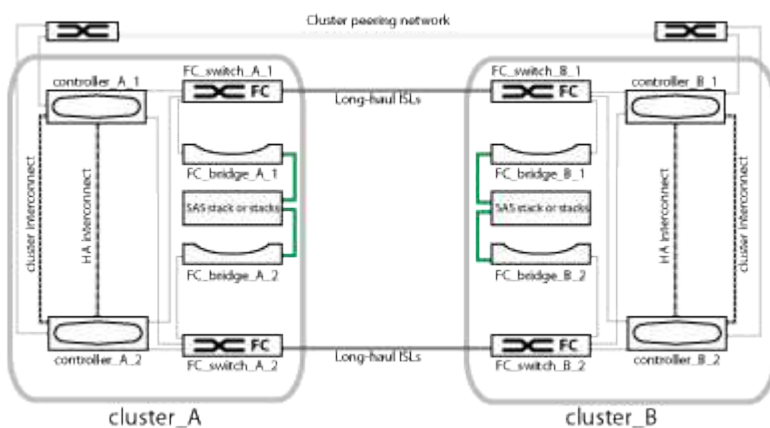
- Connessioni Ethernet dai controller alla rete fornita dal cliente utilizzata per il peering del cluster

La configurazione SVM viene replicata sulla rete di peering del cluster.

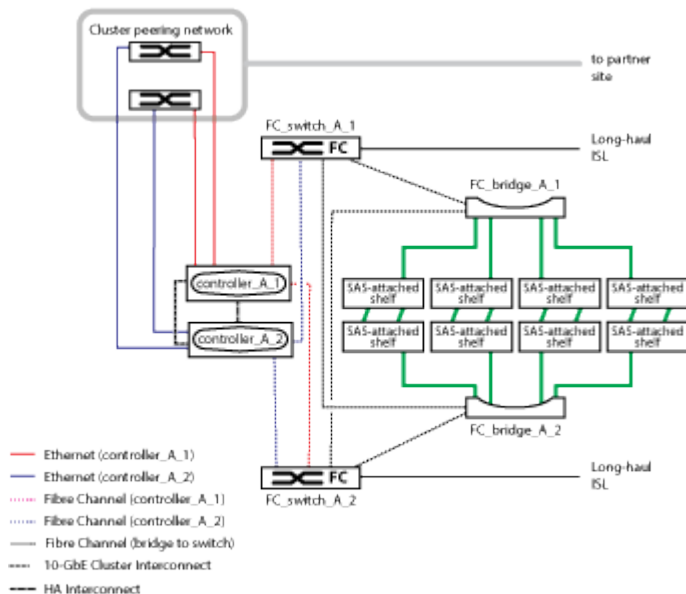
- Un'interconnessione del cluster tra ciascun controller del cluster locale

### Configurazione Fabric MetroCluster a quattro nodi

La figura seguente mostra una vista semplificata di una configurazione Fabric MetroCluster a quattro nodi. Per alcune connessioni, una singola linea rappresenta connessioni multiple e ridondanti tra i componenti. Le connessioni di rete per dati e gestione non vengono visualizzate.

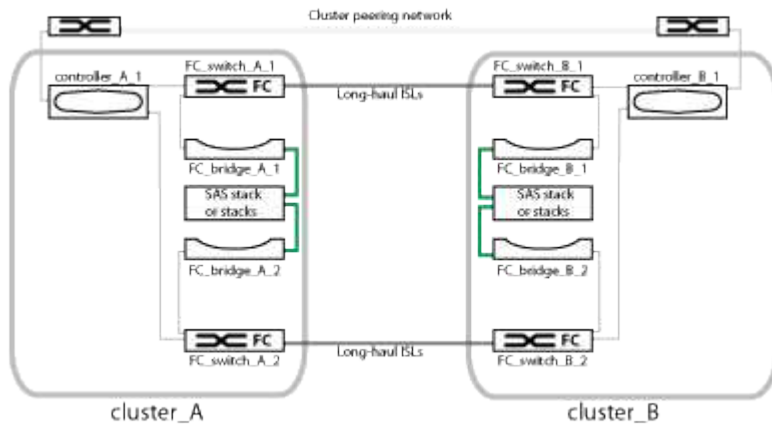


La seguente illustrazione mostra una vista più dettagliata della connettività in un singolo cluster MetroCluster (entrambi i cluster hanno la stessa configurazione):



## Configurazione Fabric MetroCluster a due nodi

La figura seguente mostra una vista semplificata di una configurazione MetroCluster fabric a due nodi. Per alcune connessioni, una singola linea rappresenta connessioni multiple e ridondanti tra i componenti. Le connessioni di rete per dati e gestione non vengono visualizzate.

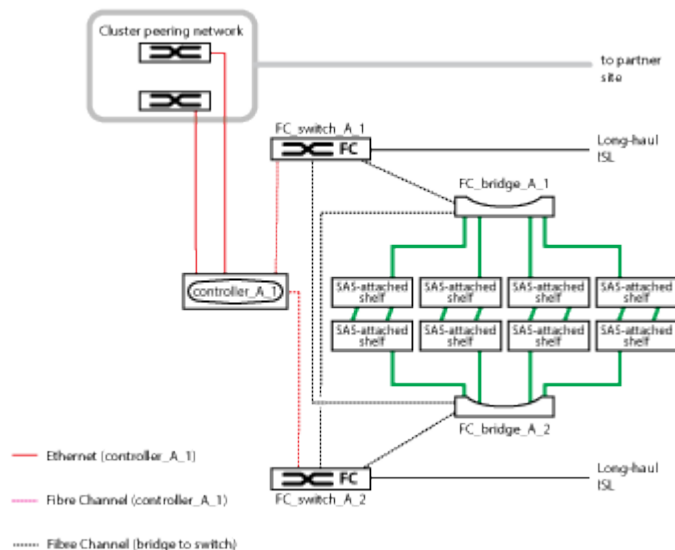


Una configurazione a due nodi è costituita da due cluster, uno per ogni sito separato geograficamente. Cluster\_A si trova nel primo sito MetroCluster. Cluster\_B si trova nel secondo sito MetroCluster. Ogni sito dispone di uno stack di storage SAS. Sono supportati ulteriori stack di storage, ma ne viene mostrato solo uno per ciascun sito.



In una configurazione a due nodi, i nodi non sono configurati come coppia ha.

La seguente illustrazione mostra una vista più dettagliata della connettività in un singolo cluster MetroCluster (entrambi i cluster hanno la stessa configurazione):



Una configurazione a due nodi include le seguenti connessioni:

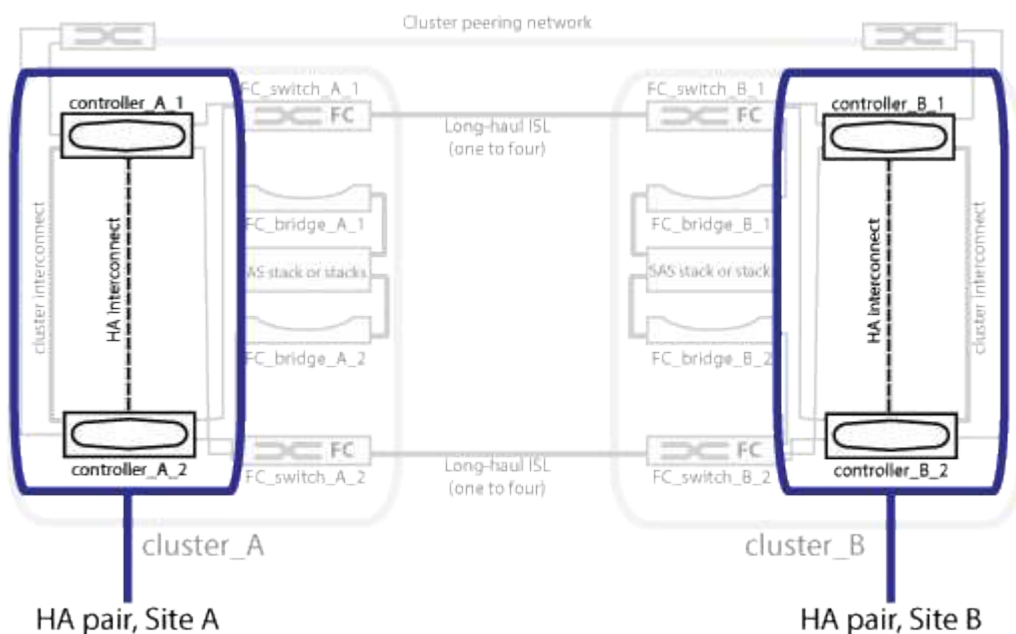
- Connessioni FC tra l'adattatore FC-VI su ciascun modulo controller
- Connessioni FC dagli HBA di ciascun modulo controller al bridge FC-SAS per ogni shelf stack SAS
- Connessioni SAS tra ogni shelf SAS e dalla parte superiore e inferiore di ogni stack a un bridge FC-SAS
- Connessioni Ethernet dai controller alla rete fornita dal cliente utilizzata per il peering del cluster

La configurazione SVM viene replicata sulla rete di peering del cluster.

### Immagine delle coppie ha locali in una configurazione MetroCluster

Nelle configurazioni MetroCluster a otto o quattro nodi, ogni sito è costituito da storage controller configurati come una o due coppie 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

["Immagine di bridge FC-SAS ridondanti"](#)

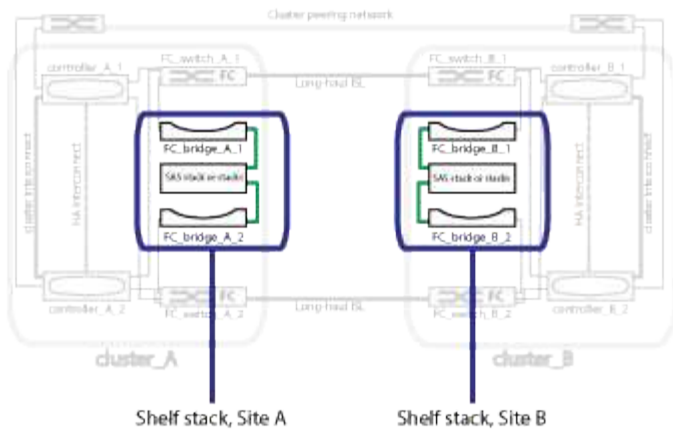
["Fabric switch FC ridondanti"](#)

["Immagine della rete di peering del cluster"](#)

["Concetti di ONTAP"](#)

### Immagine di bridge FC-SAS ridondanti

I bridge FC-SAS forniscono un bridging del protocollo tra i dischi SAS collegati e il fabric dello switch FC.



### Informazioni correlate

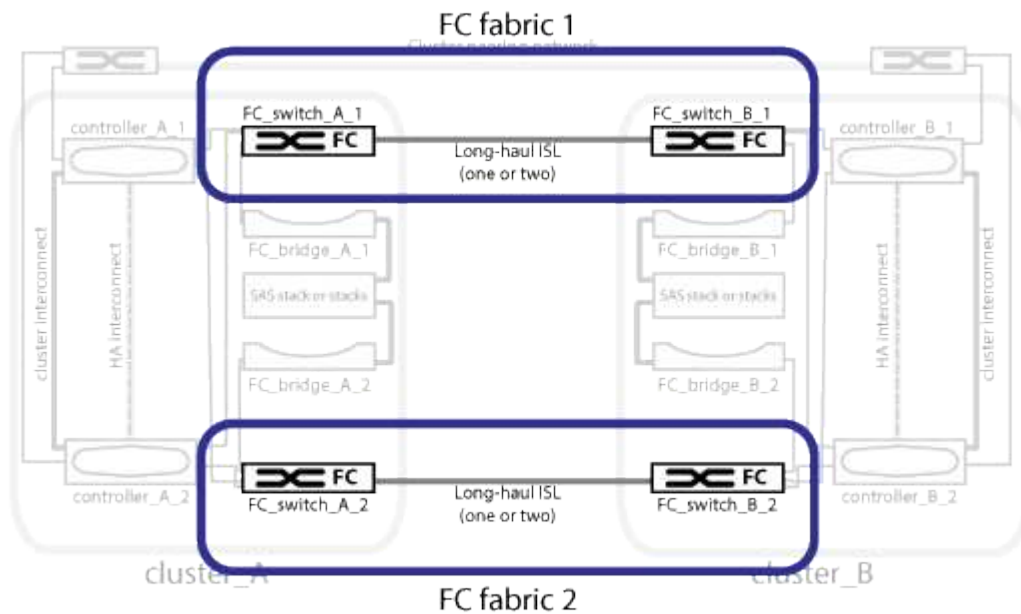
"Immagine delle coppie ha locali in una configurazione MetroCluster"

"Fabric switch FC ridondanti"

"Immagine della rete di peering del cluster"

### Fabric switch FC ridondanti

Ogni fabric di switch include i link inter-switch (ISL) che collegano i siti. I dati vengono replicati da un sito all'altro attraverso l'ISL. Per la ridondanza, ciascun fabric dello switch deve trovarsi su percorsi fisici diversi.



### Informazioni correlate

"Immagine delle coppie ha locali in una configurazione MetroCluster"

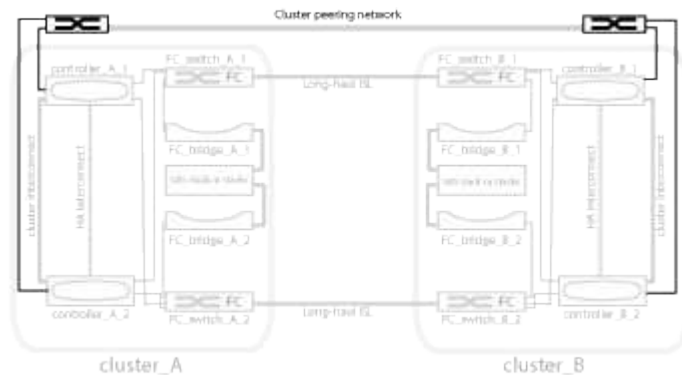
"Immagine di bridge FC-SAS ridondanti"

"Immagine della rete di peering del cluster"

## 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

["Immagine delle coppie ha locali in una configurazione MetroCluster"](#)

["Immagine di bridge FC-SAS ridondanti"](#)

["Fabric switch FC ridondanti"](#)

["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 MetroCluster FC richiesti e convenzioni di denominazione

Durante la pianificazione della configurazione MetroCluster FC, 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. Ad esempio, un sito viene indicato come Sito A e l'altro come Sito B.

## Software e hardware supportati

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

["NetApp Hardware Universe"](#)

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

configurati come sistemi AFF.



Gli SFP a onde lunghe non sono supportati negli switch di storage MetroCluster. Per una tabella degli SPF supportati, consultare il report tecnico di MetroCluster.

### **Ridondanza dell'hardware nella configurazione MetroCluster FC**

A causa della ridondanza hardware nella configurazione MetroCluster FC, 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.

#### **Requisito per due cluster ONTAP**

La configurazione MetroCluster FC fabric-attached richiede 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

#### **Requisito per quattro switch FC**

La configurazione Fabric-Attached MetroCluster FC richiede quattro switch FC (modelli Brocade o Cisco supportati).

I quattro switch formano due fabric storage switch che forniscono l'ISL tra ciascuno dei cluster nella configurazione MetroCluster FC.

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

#### **Requisito per due, quattro o otto moduli controller**

La configurazione Fabric-Attached MetroCluster FC richiede due, quattro o otto moduli controller.

In una configurazione MetroCluster a quattro o otto nodi, i moduli controller di ogni sito formano una o due coppie. Ogni modulo controller dispone di un partner DR nell'altro sito.

I moduli controller devono soddisfare i seguenti requisiti:

- La denominazione deve essere univoca all'interno della configurazione MetroCluster.
- Tutti i moduli controller nella configurazione MetroCluster devono eseguire la stessa versione di ONTAP.
- Tutti i moduli controller di un gruppo DR devono essere dello stesso modello.

Tuttavia, nelle configurazioni con due gruppi DR, ciascun gruppo DR può essere costituito da diversi modelli di moduli controller.

- Tutti i moduli controller di un gruppo DR devono utilizzare la stessa configurazione FC-VI.

Alcuni moduli controller supportano due opzioni per la connettività FC-VI:

- Porte FC-VI integrate
- Una scheda FC-VI nello slot 1 Non è supportata la combinazione di un modulo controller che utilizza porte FC-VI integrate e un'altra che utilizza una scheda FC-VI aggiuntiva. Ad esempio, se un nodo utilizza una configurazione FC-VI integrata, tutti gli altri nodi del gruppo DR devono utilizzare anche la configurazione FC-VI integrata.

Nomi di esempio:

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

### **Requisito per quattro switch di interconnessione cluster**

La configurazione Fabric-Attached MetroCluster FC richiede quattro switch di interconnessione cluster (se non si utilizzano cluster senza switch a due nodi)

Questi switch forniscono la comunicazione del cluster tra i moduli controller di ciascun cluster. Gli switch non sono necessari se i moduli controller di ciascun sito sono configurati come cluster senza switch a due nodi.

### **Requisiti per i bridge FC-SAS**

La configurazione MetroCluster FC con collegamento a fabric richiede una coppia di bridge FC-SAS per ciascun gruppo di stack di shelf SAS.



I bridge FibreBridge 6500N non sono supportati nelle configurazioni con ONTAP 9.8 e versioni successive.

- I bridge FibreBridge 7600N o 7500N supportano fino a quattro stack SAS.
- Ogni stack può utilizzare diversi modelli di IOM.

Una combinazione di moduli IOM12 e moduli IOM3 non è supportata nello stesso stack di storage. Una combinazione di moduli IOM12 e moduli IOM6 è supportata nello stesso stack di storage se il sistema esegue una versione supportata di ONTAP.

I moduli IOM supportati dipendono dalla versione di ONTAP in esecuzione.

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

I nomi suggeriti utilizzati come esempi in questa documentazione identificano il modulo controller e lo stack a cui il bridge si collega, come illustrato di seguito.

### **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.

La configurazione di MetroCluster richiede la configurazione minima in ogni sito:

- Ogni nodo dispone di almeno un pool locale e di un pool remoto nel sito.

Ad esempio, in una configurazione MetroCluster a quattro nodi con due nodi in ogni sito, sono necessari quattro pool in ogni 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.

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

La tua versione di ONTAP deve supportare la combinazione di shelf. Fare riferimento allo strumento matrice di interoperabilità (IMT) per verificare se la versione di ONTAP in uso supporta la combinazione di shelf.

["Interoperabilità NetApp"](#)

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

### Convenzioni di denominazione dei bridge

I bridge utilizzano il seguente esempio di denominazione:

bridge\_site\_stack grouplocation in pair

Questa parte del nome...	Identifica...	Valori possibili...
sito	Sito in cui risiede fisicamente la coppia di bridge.	A o B.



gruppo di stack	<p>Numero del gruppo di stack a cui si connette la coppia di bridge.</p> <p>I bridge FibreBridge 7600N o 7500N supportano fino a quattro stack nel gruppo di stack.</p> <p>Il gruppo di stack non può contenere più di 10 shelf di storage.</p>	1, 2, ecc.
posizione in coppia	Bridge all'interno della coppia di bridge. Una coppia di bridge si connette a uno specifico gruppo di stack.	a o b

Esempi di nomi di bridge per un gruppo di stack su ciascun sito:

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

## Fogli di lavoro per la configurazione di switch FC e bridge FC-SAS

Prima di iniziare la configurazione dei siti MetroCluster, è possibile utilizzare i seguenti fogli di lavoro per registrare le informazioni sul sito:

["Sito Di Un foglio di lavoro"](#)

["Foglio di lavoro del sito B."](#)

## Installare e cablare i componenti MetroCluster

### 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.

#### "Documentazione dei sistemi hardware ONTAP"

4. Installare gli switch FC 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.
- Gli shelf ID devono essere univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster (inclusi entrambi i siti).

6. Installare ciascun bridge FC-SAS:

- a. Fissare le staffe "L" sulla parte anteriore del bridge alla parte anteriore del rack (montaggio a filo) con le quattro viti.

Le aperture delle staffe "L" del ponte sono conformi allo standard ETA-310-X per rack da 19" (482.6 mm).

Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il modello di bridge contiene ulteriori informazioni e un'illustrazione dell'installazione.



Per un accesso adeguato allo spazio delle porte e una manutenzione FRU adeguata, è necessario lasciare uno spazio 1U sotto la coppia di bridge e coprire questo spazio con un pannello di chiusura senza utensili.

- b. Collegare ciascun bridge a una fonte di alimentazione che fornisca una messa a terra adeguata.

- c. Accendere ciascun bridge.



Per ottenere la massima resilienza, i bridge collegati allo stesso stack di shelf di dischi devono essere collegati a diverse fonti di alimentazione.

Il LED Bridge Ready potrebbe impiegare fino a 30 secondi per accendersi, a indicare che il bridge ha completato la sequenza di test automatico all'accensione.

### Collegamento delle porte FC-VI e HBA del nuovo modulo controller agli switch FC

Le porte FC-VI e gli HBA (host bus adapter) devono essere cablati agli switch FC del sito su ciascun modulo controller nella configurazione MetroCluster.

#### Fasi

1. Collegare le porte FC-VI e HBA utilizzando la tabella per la configurazione e il modello di switch in uso.
  - "Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"
  - "Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"
  - "Assegnazioni delle porte per switch FC quando si utilizzano sistemi AFF A900"
  - "Assegnazioni delle porte per i sistemi che utilizzano due porte initiator"

### Collegamento degli ISL tra siti MetroCluster

È necessario collegare gli switch FC in ogni sito attraverso i collegamenti interswitch in

fibra ottica (ISL) per formare i fabric switch che collegano i componenti MetroCluster.

### A proposito di questa attività

Questa operazione deve essere eseguita per entrambi i fabric switch.

### Fasi

1. Collegare gli switch FC di ogni sito a tutti gli ISL, utilizzando il cablaggio nella tabella corrispondente alla configurazione e al modello di switch in uso.
  - ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)
  - ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

### Informazioni correlate

["Considerazioni per gli ISL"](#)

### Assegnazioni delle porte per i sistemi che utilizzano due porte initiator

È possibile configurare i sistemi FAS8020, AFF8020, FAS8200 e AFF A300 utilizzando una singola porta iniziatore per ciascun fabric e due porte iniziatore per ciascun controller.

È possibile seguire il cablaggio per il bridge FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2). Invece di utilizzare quattro iniziatori, collegare solo due iniziatori e lasciare vuoti gli altri due collegati alla porta dello switch.

Se lo zoning viene eseguito manualmente, seguire lo zoning utilizzato per un bridge FibreBridge 7500N o 7600N utilizzando una porta FC (FC1 o FC2). In questo scenario, viene aggiunta una porta iniziatore anziché due a ciascun membro di zona per fabric.

È possibile modificare la suddivisione in zone o eseguire un aggiornamento da FibreBridge 6500N a FibreBridge 7500N utilizzando la procedura descritta in ["Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N"](#).

La seguente tabella mostra le assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive.

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)			
MetroCluster 1 o DR Group 1			
Componente	Porta	* Modelli di switch Brocade 6505, 6510, 6520, 7840, G620, G610 e DCX 8510-8*	
		Si collega allo switch FC...	Si collega alla porta dello switch...

controller_x_1	Porta FC-VI A.	1	0
	Porta FC-VI b	2	0
	Porta FC-VI c	1	1
	Porta FC-VI d	2	1
	Porta HBA a	1	2
	Porta HBA b	2	2
	Porta HBA c	-	-
	Porta HBA d	-	-
Stack 1	bridge_x_1a	1	8
bridge_x_1b	2	8	Stack y
bridge_x_ya	1	11	bridge_x_yb

La seguente tabella mostra le assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.0.

Configurazione MetroCluster a due nodi			
Componente	Porta	Brocade 6505, 6510 o DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
Porta FC-VI b	-	0	Porta HBA a
1	-	Porta HBA b	-
1	Porta HBA c	2	-

### Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0

Quando si cablano gli switch FC, verificare di utilizzare le assegnazioni delle porte specificate. Le assegnazioni delle porte sono diverse tra ONTAP 9.0 e le versioni successive di ONTAP.

È possibile riconfigurare le porte non utilizzate per il collegamento di porte initiator, porte FC-VI o ISL in modo da fungere da porte di storage. Tuttavia, se vengono utilizzati gli RCF supportati, la zoning deve essere modificata di conseguenza.

Se vengono utilizzati i file RCF supportati, le porte ISL potrebbero non essere collegate alle stesse porte qui mostrate e potrebbe essere necessario riconfigurarle manualmente.

### Linee guida generali per il cablaggio

Quando si utilizzano le tabelle di cablaggio, è necessario conoscere le seguenti linee guida:

- Gli switch Brocade e Cisco utilizzano diverse numerazioni delle porte:
  - Negli switch Brocade, la prima porta è numerata 0.
  - Sugli switch Cisco, la prima porta è numerata 1.
- Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.
- I sistemi storage AFF A300 e FAS8200 possono essere ordinati con una delle due opzioni per la connettività FC-VI:
  - Porte integrate 0e e 0f configurate in modalità FC-VI.
  - Porte 1a e 1b su una scheda FC-VI nello slot 1.

### Utilizzo della porta Brocade per le connessioni dei controller in una configurazione MetroCluster a otto nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La seguente tabella mostra l'utilizzo della porta del controller sugli switch Brocade:

Configurazione MetroCluster a otto nodi			
Componente	Porta	Brocade 6505, 6510 o DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
Porta FC-VI b	-	0	Porta HBA a
1	-	Porta HBA b	-
1	Porta HBA c	2	-
Porta HBA d	-	2	controller_x_2
Porta FC-VI A.	3	-	Porta FC-VI b
-	3	Porta HBA a	4
-	Porta HBA b	-	4
Porta HBA c	5	-	Porta HBA d
-	5	controller_x_3	Porta FC-VI A.

6		Porta FC-VI b	-
6	Porta HBA a	7	-
Porta HBA b	-	7	Porta HBA c
8	-	Porta HBA d	-
8	controller_x_4	Porta FC-VI A.	9
-	Porta FC-VI b	-	9
Porta HBA a	10	-	Porta HBA b
-	10	Porta HBA c	11
-	Porta HBA d	-	11

#### Utilizzo della porta Brocade per connessioni bridge FC-SAS in una configurazione MetroCluster a otto nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo delle porte bridge quando si utilizzano i bridge FibreBridge 7500N e 7600N:

Configurazione MetroCluster a otto nodi			
Ponte FibreBridge 7500N o 7600N	Porta	Brocade 6505, 6510 o DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
FC2	-	12	bridge_x_1b
FC1	13	-	FC2
-	13	bridge_x_2a	FC1
14	-	FC2	-
14	bridge_x_2b	FC1	15
-	FC2	-	15
bridge_x_3a	FC1	16	-
FC2	-	16	bridge_x_3b

FC1	17	-	FC2
-	17	bridge_x_4a	FC1
18	-	FC2	-
18	bridge_x_4b	FC1	19
-	FC2	-	19

#### Utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster a otto nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a otto nodi			
Porta ISL	Brocade 6505, 6510 o DCX 8510-8		
	FC_switch_x_1	FC_switch_x_2	
Porta ISL 1	20	20	
Porta ISL 2	21	21	
Porta ISL 3	22	22	
Porta ISL 4	23	23	

#### Utilizzo della porta Brocade per i controller in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

Configurazione MetroCluster a quattro nodi			
Componente	Porta	Brocade 6505, 6510 o DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
Porta FC-VI b	-	0	Porta HBA a
1	-	Porta HBA b	-
1	Porta HBA c	2	-
Porta HBA d	-	2	controller_x_2

Porta FC-VI A.	3	-	Porta FC-VI b
-	3	Porta HBA a	4
-	Porta HBA b	-	4
Porta HBA c	5	-	Porta HBA d

#### Utilizzo della porta Brocade per bridge in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La tabella seguente mostra l'utilizzo delle porte bridge fino alla porta 17 quando si utilizzano i bridge FibreBridge 7500N e 7600N. È possibile cablare altri bridge alle porte da 18 a 23.

Configurazione MetroCluster a quattro nodi					
Ponte FibreBridge 7500N o 7600N	Porta	Brocade 6510 o DCX 8510-8		Brocade 6505	
		FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	6	-	6	-
FC2	-	6	-	6	bridge_x_1b
FC1	7	-	7	-	FC2
-	7	-	7	bridge_x_2a	FC1
8	-	12	-	FC2	-
8	-	12	bridge_x_2b	FC1	9
-	13	-	FC2	-	9
-	13	bridge_x_3a	FC1	10	-
14	-	FC2	-	10	-
14	bridge_x_3b	FC1	11	-	15
-	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
FC2	-	12	-	16	bridge_x_4b



FC1	13	-	17	-	FC2
-	13	-	17		

#### Utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a quattro nodi				
Porta ISL	Brocade 6510, DCX 8510-8		Brocade 6505	
	FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	20	20	8	8
Porta ISL 2	21	21	9	9
Porta ISL 3	22	22	10	10
Porta ISL 4	23	23	11	11

#### Utilizzo della porta Brocade per i controller in una configurazione MetroCluster a due nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

Configurazione MetroCluster a due nodi			
Componente	Porta	Brocade 6505, 6510 o DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
Porta FC-VI b	-	0	Porta HBA a
1	-	Porta HBA b	-
1	Porta HBA c	2	-

#### Utilizzo della porta Brocade per bridge in una configurazione MetroCluster a due nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La tabella seguente mostra l'utilizzo delle porte bridge fino alla porta 17 quando si utilizzano i bridge FibreBridge 7500N e 7600N. È possibile cablare altri bridge alle porte da 18 a 23.

Configurazione MetroCluster a due nodi
--

Ponte FibreBridge 7500N o 7600N	Porta	Brocade 6510, DCX 8510-8		Brocade 6505	
		FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	6	-	6	-
FC2	-	6	-	6	bridge_x_1b
FC1	7	-	7	-	FC2
-	7	-	7	bridge_x_2a	FC1
8	-	12	-	FC2	-
8	-	12	bridge_x_2b	FC1	9
-	13	-	FC2	-	9
-	13	bridge_x_3a	FC1	10	-
14	-	FC2	-	10	-
14	bridge_x_3b	FC1	11	-	15
-	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
FC2	-	12	-	16	bridge_x_4b
FC1	13	-	17	-	FC2
-	13	-	17		

#### Utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster a due nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a due nodi				
Porta ISL	Brocade 6510, DCX 8510-8		Brocade 6505	
	FC_switch_x_1	FC_switch_x_2	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	20	20	8	8
Porta ISL 2	21	21	9	9

Porta ISL 3	22	22	10	10
Porta ISL 4	23	23	11	11

#### Utilizzo delle porte Cisco per controller in una configurazione MetroCluster a otto nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta del controller sugli switch Cisco:

Configurazione MetroCluster a otto nodi			
Componente	Porta	Cisco 9148 o 9148S	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta HBA a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta HBA d	-	3	controller_x_2
Porta FC-VI A.	4	-	Porta FC-VI b
-	4	Porta HBA a	5
-	Porta HBA b	-	5
Porta HBA c	6	-	Porta HBA d
-	6	controller_x_3	Porta FC-VI A.
7		Porta FC-VI b	-
7	Porta HBA a	8	-
Porta HBA b	-	8	Porta HBA c
9	-	Porta HBA d	-
9	controller_x_4	Porta FC-VI A.	10
-	Porta FC-VI b	-	10

Porta HBA a	11	-	Porta HBA b
-	11	Porta HBA c	13
-	Porta HBA d	-	13

#### Utilizzo della porta Cisco per bridge FC-SAS in una configurazione MetroCluster a otto nodi con ONTAP 9.0

La tabella seguente mostra l'utilizzo delle porte bridge fino alla porta 23 quando si utilizzano i bridge FibreBridge 7500N o 7600N. È possibile collegare altri bridge utilizzando le porte da 25 a 48.

Configurazione MetroCluster a otto nodi			
Ponte FibreBridge 7500N o 7600N	Porta	Cisco 9148 o 9148S	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	14	14
FC2	-	-	bridge_x_1b
FC1	15	15	FC2
-	-	bridge_x_2a	FC1
17	17	FC2	-
-	bridge_x_2b	FC1	18
18	FC2	-	-
bridge_x_3a	FC1	19	19
FC2	-	-	bridge_x_3b
FC1	21	21	FC2
-	-	bridge_x_4a	FC1
22	22	FC2	-
-	bridge_x_4b	FC1	23
23	FC2	-	-

## Utilizzo delle porte Cisco per gli ISL in una configurazione MetroCluster a otto nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a otto nodi		
Porta ISL	Cisco 9148 o 9148S	
	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	12	12
Porta ISL 2	16	16
Porta ISL 3	20	20
Porta ISL 4	24	24

## Utilizzo della porta Cisco per controller in una configurazione MetroCluster a quattro nodi

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La seguente tabella mostra l'utilizzo della porta del controller sugli switch Cisco:

Configurazione MetroCluster a quattro nodi			
Componente	Porta	Cisco 9148, 9148S o 9250i	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta HBA a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta HBA d	-	3	controller_x_2
Porta FC-VI A.	4	-	Porta FC-VI b
-	4	Porta HBA a	5
-	Porta HBA b	-	5
Porta HBA c	6	-	Porta HBA d

### Utilizzo della porta Cisco per bridge FC-SAS in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

La tabella seguente mostra l'utilizzo delle porte bridge fino alla porta 14 quando si utilizzano i bridge FibreBridge 7500N o 7600N. È possibile collegare ulteriori bridge alle porte da 15 a 32 seguendo lo stesso schema.

Configurazione MetroCluster a quattro nodi			
Ponte FibreBridge 7500N o 7600N	Porta	Cisco 9148, 9148S o 9250i	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
FC2	-	7	bridge_x_1b
FC1	8	-	FC2
-	8	bridge_x_2a	FC1
9	-	FC2	-
9	bridge_x_2b	FC1	10
-	FC2	-	10
bridge_x_3a	FC1	11	-
FC2	-	11	bridge_x_3b
FC1	12	-	FC2
-	12	bridge_x_4a	FC1
13	-	FC2	-
13	bridge_x_4b	FC1	14
-	FC2	-	14

### Utilizzo delle porte Cisco 9148 e 9148S per gli ISL in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a quattro nodi
--

Porta ISL	Cisco 9148 o 9148S	
	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	36	36
Porta ISL 2	40	40
Porta ISL 3	44	44
Porta ISL 4	48	48

#### Utilizzo della porta Cisco 9250i per gli ISL in una configurazione MetroCluster a quattro nodi con ONTAP 9.0

Lo switch Cisco 9250i utilizza le porte FCIP per ISL.

Le porte da 40 a 48 sono porte da 10 GbE e non vengono utilizzate nella configurazione MetroCluster.

#### Utilizzo della porta Cisco per i controller in una configurazione MetroCluster a due nodi

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La seguente tabella mostra l'utilizzo della porta del controller sugli switch Cisco:

Configurazione MetroCluster a due nodi			
Componente	Porta	Cisco 9148, 9148S o 9250i	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta HBA a
2	-	Porta HBA b	-
2	Porta HBA c	3	-

#### Utilizzo della porta Cisco per bridge FC-SAS in una configurazione MetroCluster a due nodi con ONTAP 9.0

La tabella seguente mostra l'utilizzo delle porte bridge fino alla porta 14 quando si utilizzano i bridge FibreBridge 7500N e 7600N. È possibile collegare ulteriori bridge alle porte da 15 a 32 seguendo lo stesso schema.

Configurazione MetroCluster a due nodi			
Ponte FibreBridge 7500N o 7600N	Porta	Cisco 9148, 9148S o 9250i	
		FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-

FC2	-	7	bridge_x_1b
FC1	8	-	FC2
-	8	bridge_x_2a	FC1
9	-	FC2	-
9	bridge_x_2b	FC1	10
-	FC2	-	10
bridge_x_3a	FC1	11	-
FC2	-	11	bridge_x_3b
FC1	12	-	FC2
-	12	bridge_x_4a	FC1
13	-	FC2	-
13	bridge_x_4b	FC1	14
-	FC2	-	14

#### Utilizzo delle porte Cisco 9148 o 9148S per gli ISL in una configurazione MetroCluster a due nodi con ONTAP 9.0

Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.

La seguente tabella mostra l'utilizzo della porta ISL:

Configurazione MetroCluster a due nodi		
Porta ISL	Cisco 9148 o 9148S	
	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	36	36
Porta ISL 2	40	40
Porta ISL 3	44	44
Porta ISL 4	48	48



## Utilizzo della porta Cisco 9250i per gli ISL in una configurazione MetroCluster a due nodi con ONTAP 9.0

Lo switch Cisco 9250i utilizza le porte FCIP per ISL.

Le porte da 40 a 48 sono porte da 10 GbE e non vengono utilizzate nella configurazione MetroCluster.

### Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.1 o versione successiva

Verificare di utilizzare le assegnazioni delle porte specificate quando si cablano gli switch FC utilizzando ONTAP 9.1 e versioni successive.

È possibile riconfigurare le porte non utilizzate per il collegamento di porte initiator, porte FC-VI o ISL in modo da fungere da porte di storage. Tuttavia, se vengono utilizzati gli RCF supportati, la zoning deve essere modificata di conseguenza.

Se si utilizzano gli RCF supportati, le porte ISL potrebbero non connettersi alle stesse porte mostrate e potrebbe essere necessario riconfigurarle manualmente.

Se gli switch sono stati configurati utilizzando le assegnazioni delle porte per ONTAP 9, è possibile continuare a utilizzare le assegnazioni precedenti. Tuttavia, le nuove configurazioni che eseguono ONTAP 9.1 o versioni successive devono utilizzare le assegnazioni delle porte indicate di seguito.

### Linee guida generali per il cablaggio

Quando si utilizzano le tabelle di cablaggio, è necessario conoscere le seguenti linee guida:

- Gli switch Brocade e Cisco utilizzano diverse numerazioni delle porte:
  - Negli switch Brocade, la prima porta è numerata 0.
  - Sugli switch Cisco, la prima porta è numerata 1.
- Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.
- I sistemi storage AFF A300 e FAS8200 possono essere ordinati con una delle due opzioni per la connettività FC-VI:
  - Porte integrate 0e e 0f configurate in modalità FC-VI.
  - Porte 1a e 1b su una scheda FC-VI nello slot 1.
- I sistemi storage AFF A700 e FAS9000 richiedono quattro porte FC-VI. Le seguenti tabelle mostrano il cablaggio degli switch FC con quattro porte FC-VI su ciascun controller, ad eccezione dello switch Cisco 9250i.

Per gli altri sistemi storage, utilizzare i cavi mostrati nelle tabelle ma ignorare i cavi delle porte FC-VI c e d.

È possibile lasciare vuote queste porte.

- I sistemi storage AFF A400 e FAS8300 utilizzano le porte 2a e 2b per la connettività FC-VI.
- Se si dispone di due configurazioni MetroCluster che condividono gli ISL, utilizzare le stesse assegnazioni delle porte di un cablaggio MetroCluster a otto nodi.

Il numero di ISL che si cablano può variare a seconda dei requisiti del sito.

Consultare la sezione relativa alle considerazioni sull'ISL.

## Utilizzo della porta Brocade per i controller in una configurazione MetroCluster con ONTAP 9.1 o versione successiva

Le seguenti tabelle mostrano l'utilizzo delle porte sugli switch Brocade. Le tabelle mostrano la configurazione massima supportata, con otto moduli controller in due gruppi DR. Per le configurazioni più piccole, ignorare le righe dei moduli controller aggiuntivi. Si noti che otto ISL sono supportati solo su Brocade 6510, Brocade DCX 8510-8, G620, G630, G620-1, Switch G630-1 e G720.



- L'utilizzo delle porte per gli switch Brocade 6505 e Brocade G610 in una configurazione MetroCluster a otto nodi non viene mostrato. A causa del numero limitato di porte, le assegnazioni delle porte devono essere effettuate sito per sito, a seconda del modello di modulo controller e del numero di ISL e coppie di bridge in uso.
- Lo switch Brocade DCX 8510-8 può utilizzare lo stesso layout delle porte dello switch 6510 **oppure** dello switch 7840.

### Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)

#### MetroCluster 1 o DR Group 1

Componente	Porta	Switch Brocade modelli 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 E DCX 8510-8		
		Si connette allo switch FC...	Si collega alla porta dello switch...	Si collega alla porta dello switch...
controller_x_1	Porta FC-VI A.	1	0	0
Porta FC-VI b	2	0	0	Porta FC-VI c
1	1	1	Porta FC-VI d	2
1	1	Porta HBA a	1	2
8	Porta HBA b	2	2	8
Porta HBA c	1	3	9	Porta HBA d
2	3	9	controller_x_2	Porta FC-VI A.
1	4	4	Porta FC-VI b	2
4	4	Porta FC-VI c	1	5
5	Porta FC-VI d	2	5	5
Porta HBA a	1	6	12	Porta HBA b
2	6	12	Porta HBA c	1

7	13	Porta HBA d	2	7
---	----	-------------	---	---

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)

MetroCluster 1 o DR Group 1

Componente	Porta	Switch Brocade modelli 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 E DCX 8510-8		
		Si connette allo switch FC...	Si collega alla porta dello switch...	Si collega alla porta dello switch...
Stack 1	bridge_x_1a	1	8	10
bridge_x_1b	2	8	10	Stack 2
bridge_x_2a	1	9	11	bridge_x_2b
2	9	11	Stack 3	bridge_x_3a
1	10	14	bridge_x_4b	2
10	14	Stack y	bridge_x_ya	1
11	15	bridge_x_yb	2	11

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)

MetroCluster 2 o DR Group 2

			Modello di switch Brocade				
Componente	Porta	Si connette a FC_switch ...	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720
controller_x_3	Porta FC-VI A.	1	24	48	12	18	18
Porta FC-VI b	2	24	48	12	18	18	Porta FC-VI c
1	25	49	13	19	19	Porta FC-VI d	2
25	49	13	19	19	Porta HBA a	1	26
50	14	24	26	Porta HBA b	2	26	50

14	24	26	Porta HBA c	1	27	51	15
25	27	Porta HBA d	2	27	51	15	25
27	controller_x_4	Porta FC-VI A.	1	28	52	16	22
22	Porta FC-VI b	2	28	52	16	22	22
Porta FC-VI c	1	29	53	17	23	23	Porta FC-VI d
2	29	53	17	23	23	Porta HBA a	1
30	54	18	28	30	Porta HBA b	2	30
54	18	28	30	Porta HBA c	1	31	55
19	29	31	Porta HBA d	2	32	55	19
29	31	Stack 1	bridge_x_51 a	1	32	56	20
26	32	bridge_x_51 b	2	32	56	20	26
32	Stack 2	bridge_x_52 a	1	33	57	21	27
33	bridge_x_52 b	2	33	57	21	27	33
Stack 3	bridge_x_53 a	1	34	58	22	30	34
bridge_x_54 b	2	34	58	22	30	34	Stack y
bridge_x_5a	1	35	59	23	31	35	bridge_x_5b

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)

MetroCluster 1 o DR Group 1

Componente		Porta	Switch Brocade modelli 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, E DCX 8510-8		Switch Brocade G720
			Si connette a FC_switch...	Si collega alla porta dello switch...	Si collega alla porta dello switch...
Stack 1	bridge_x_1a	FC1	1	8	10
FC2	2	8	10	bridge_x_1B	FC1
1	9	11	FC2	2	9
11	Stack 2	bridge_x_2a	FC1	1	10
14	FC2	2	10	14	bridge_x_2B
FC1	1	11	15	FC2	2
11	15	Stack 3	bridge_x_3a	FC1	1
12*	16	FC2	2	12*	16
bridge_x_3B	FC1	1	13*	17	FC2
2	13*	17	Stack y	bridge_x_ya	FC1
1	14*	20	FC2	2	14*
20	bridge_x_yb	FC1	1	15*	21

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)

#### MetroCluster 2 o DR Group 2

Componente		Porta	Modello di switch Brocade					
			Si connette a FC_switch ...	6510, DCX 8510-8	6520	7840, DCX 8510-8	G620, G620-1, G630, G630-1	G720
controller_x_3	Porta FC-VI A.	1	24	48	12	18	18	Porta FC-VI b
2	24	48	12	18	18	Porta FC-VI c	1	25

49	13	19	19	Porta FC- VI d	2	25	49	13
19	19	Porta HBA a	1	26	50	14	24	26
Porta HBA b	2	26	50	14	24	26	Porta HBA c	1
27	51	15	25	27	Porta HBA d	2	27	51
15	25	27	controller_ x_4	Porta FC- VI A.	1	28	52	16
22	22	Porta FC- VI b	2	28	52	16	22	22
Porta FC- VI c	1	29	53	17	23	23	Porta FC- VI d	2
29	53	17	23	23	Porta HBA a	1	30	54
18	28	30	Porta HBA b	2	30	54	18	28
30	Porta HBA c	1	31	55	19	29	31	Porta HBA d
2	31	55	19	29	31	Stack 1	bridge_x_ 51a	FC1
1	32	56	20	26	32	FC2	2	32
56	20	26	32	bridge_x_ 51b	FC1	1	33	57
21	27	33	FC2	2	33	57	21	27
33	Stack 2	bridge_x_ 52a	FC1	1	34	58	22	30
34	FC2	2	34	58	22	30	34	bridge_x_ 52b
FC1	1	35	59	23	31	35	FC2	2

35	59	23	31	35	Stack 3	bridge_x_53a	FC1	1
36	60	-	32	36	FC2	2	36	60
-	32	36	bridge_x_53b	FC1	1	37	61	-
33	37	FC2	2	37	61	-	33	37
Stack y	bridge_x_5ya	FC1	1	38	62	-	34	38
FC2	2	38	62	-	34	38	bridge_x_5yb	FC1
1	39	63	-	35	39	FC2	2	39

#### Utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster con ONTAP 9.1 o versione successiva

La seguente tabella mostra l'utilizzo della porta ISL per gli switch Brocade.



I sistemi AFF A700 o FAS9000 supportano fino a otto ISL per migliorare le performance. Gli switch Brocade 6510 e G620 supportano otto ISL.

Modello di switch	Porta ISL	Porta dello switch
Brocade 6520	Porta ISL 1	23
Porta ISL 2	47	Porta ISL 3
71	Porta ISL 4	95
Brocade 6505	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43

Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46
Porta ISL 8	47	Brocade 7810
Porta ISL 1	ge2 (10 Gbps)	Porta ISL 2
ge3 (10 Gbps)	Porta ISL 3	ge4 (10 Gbps)
Porta ISL 4	Ge5 (10 Gbps)	Porta ISL 5
Ge6 (10 Gbps)	Porta ISL 6	Ge7 (10 Gbps)
Brocade 7840  <b>Nota:</b> Lo switch Brocade 7840 supporta due porte VE da 40 Gbps o fino a quattro porte VE da 10 Gbps per switch per la creazione di ISL FCIP.	Porta ISL 1	ge0 (40 Gbps) o ge2 (10 Gbps)
Porta ISL 2	ge1 (40 Gbps) o ge3 (10 Gbps)	Porta ISL 3
Ge10 (10 Gbps)	Porta ISL 4	Ge11 (10 Gbps)
Brocade G610	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
BROCADE G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46

#### Utilizzo della porta Cisco per i controller in una configurazione MetroCluster con ONTAP 9.4 o versione successiva

Le tabelle mostrano le configurazioni massime supportate, con otto moduli controller in due gruppi DR. Per le



configurazioni più piccole, ignorare le righe dei moduli controller aggiuntivi.



Per Cisco 9132T, vedere [Utilizzo delle porte Cisco 9132T in una configurazione MetroCluster che esegue ONTAP 9,4 o versione successiva.](#)

Cisco 9396S			
Componente	Porta	Interruttore 1	Interruttore 2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta FC-VI c
2	-	Porta FC-VI d	-
2	Porta HBA a	3	-
Porta HBA b	-	3	Porta HBA c
4	-	Porta HBA d	-
4	controller_x_2	Porta FC-VI A.	5
-	Porta FC-VI b	-	5
Porta FC-VI c	6	-	Porta FC-VI d
-	6	Porta HBA a	7
-	Porta HBA b	-	7
Porta HBA c	8		Porta HBA d
-	8	controller_x_3	Porta FC-VI A.
49		Porta FC-VI b	-
49	Porta FC-VI c	50	-
Porta FC-VI d	-	50	Porta HBA a
51	-	Porta HBA b	-
51	Porta HBA c	52	
Porta HBA d	-	52	controller_x_4

Porta FC-VI A.	53	-	Porta FC-VI b
-	53	Porta FC-VI c	54
-	Porta FC-VI d	-	54
Porta HBA a	55	-	Porta HBA b
-	55	Porta HBA c	56
-	Porta HBA d	-	56

Cisco 9148S			
Componente	Porta	Interruttore 1	Interruttore 2
controller_x_1	Porta FC-VI A.	1	
Porta FC-VI b	-	1	Porta FC-VI c
2	-	Porta FC-VI d	-
2	Porta HBA a	3	-
Porta HBA b	-	3	Porta HBA c
4	-	Porta HBA d	-
4	controller_x_2	Porta FC-VI A.	5
-	Porta FC-VI b	-	5
Porta FC-VI c	6	-	Porta FC-VI d
-	6	Porta HBA a	7
-	Porta HBA b	-	7
Porta HBA c	8	-	Porta HBA d
-	8	controller_x_3	Porta FC-VI A.
25		Porta FC-VI b	-
25	Porta FC-VI c	26	-

Porta FC-VI d	-	26	Porta HBA a
27	-	Porta HBA b	-
27	Porta HBA c	28	-
Porta HBA d	-	28	controller_x_4
Porta FC-VI A.	29	-	Porta FC-VI b
-	29	Porta FC-VI c	30
-	Porta FC-VI d	-	30
Porta HBA a	31	-	Porta HBA b
-	31	Porta HBA c	32
-	Porta HBA d	-	32



La seguente tabella mostra i sistemi con due porte FC-VI. I sistemi AFF A700 e FAS9000 dispongono di quattro porte FC-VI (a, b, c e d). Se si utilizza un sistema AFF A700 o FAS9000, le assegnazioni delle porte si spostano di una posizione. Ad esempio, le porte FC-VI c e d vanno alla porta dello switch 2 e alle porte HBA a e b vanno alla porta dello switch 3.

Cisco 9250i Nota: Lo switch Cisco 9250i non è supportato per le configurazioni MetroCluster a otto nodi.

Componente	Porta	Interruttore 1	Interruttore 2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta HBA a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta HBA d	-	3	controller_x_2
Porta FC-VI A.	4	-	Porta FC-VI b
-	4	Porta HBA a	5
-	Porta HBA b	-	5

Porta HBA c	6	-	Porta HBA d
-	6	controller_x_3	Porta FC-VI A.
7	-	Porta FC-VI b	-
7	Porta HBA a	8	-
Porta HBA b	-	8	Porta HBA c
9	-	Porta HBA d	-
9	controller_x_4	Porta FC-VI A.	10
-	Porta FC-VI b	-	10
Porta HBA a	11	-	Porta HBA b
-	11	Porta HBA c	13
-	Porta HBA d	-	13

**Utilizzo della porta Cisco per bridge FC-SAS in una configurazione MetroCluster con ONTAP 9.1 o versione successiva**

Cisco 9396S			
FibreBridge 7500N o 7600N utilizzando due porte FC	Porta	Interruttore 1	Interruttore 2
bridge_x_1a	FC1	9	-
FC2	-	9	bridge_x_1b
FC1	10	-	FC2
-	10	bridge_x_2a	FC1
11	-	FC2	-
11	bridge_x_2b	FC1	12
-	FC2	-	12
bridge_x_3a	FC1	13	-

FC2	-	13	bridge_x_3b
FC1	14	-	FC2
-	14	bridge_x_4a	FC1
15	-	FC2	-
15	bridge_x_4b	FC1	16
-	FC2	-	16

È possibile collegare altri bridge utilizzando le porte da 17 a 40 e da 57 a 88 seguendo lo stesso schema.

Cisco 9148S			
FibreBridge 7500N o 7600N utilizzando due porte FC	Porta	Interruttore 1	Interruttore 2
bridge_x_1a	FC1	9	-
FC2	-	9	bridge_x_1b
FC1	10	-	FC2
-	10	bridge_x_2a	FC1
11	-	FC2	-
11	bridge_x_2b	FC1	12
-	FC2	-	12
bridge_x_3a	FC1	13	-
FC2	-	13	bridge_x_3b
FC1	14	-	FC2
-	14	bridge_x_4a	FC1
15	-	FC2	-
15	bridge_x_4b	FC1	16

-	FC2	-	16
---	-----	---	----

È possibile collegare ulteriori bridge per un secondo gruppo DR o una seconda configurazione MetroCluster utilizzando le porte da 33 a 40 seguendo lo stesso schema.

Cisco 9250i			
FibreBridge 7500N o 7600N utilizzando due porte FC	Porta	Interruttore 1	Interruttore 2
bridge_x_1a	FC1	14	-
FC2	-	14	bridge_x_1b
FC1	15	-	FC2
-	15	bridge_x_2a	FC1
17	-	FC2	-
17	bridge_x_2b	FC1	18
-	FC2	-	18
bridge_x_3a	FC1	19	-
FC2	-	19	bridge_x_3b
FC1	21	-	FC2
-	21	bridge_x_4a	FC1
22	-	FC2	-
22	bridge_x_4b	FC1	23
-	FC2	-	23

È possibile collegare ulteriori bridge per un secondo gruppo DR o una seconda configurazione MetroCluster utilizzando le porte da 25 a 48 seguendo lo stesso schema.

Le tabelle seguenti mostrano l'utilizzo delle porte bridge quando si utilizzano bridge FibreBridge 7500N o 7600N che utilizzano solo una porta FC (FC1 o FC2). Per i bridge FibreBridge 7500N o 7600N che utilizzano una porta FC, è possibile collegare via cavo FC1 o FC2 alla porta indicata come FC1. È possibile collegare altri bridge utilizzando le porte 25-48.

Bridge 7500N o 7600N FibreBridge mediante una porta FC			
FibreBridge 7500N o 7600N utilizzando una porta FC	Porta	Cisco 9396S	
		Interruttore 1	Interruttore 2
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

È possibile collegare altri bridge utilizzando le porte da 17 a 40 e da 57 a 88 seguendo lo stesso schema.

Bridge 7500N o 7600N FibreBridge mediante una porta FC			
Ponte	Porta	Cisco 9148S	
		Interruttore 1	Interruttore 2
bridge_x_1a	FC1	9	-

bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

È possibile collegare ulteriori bridge per un secondo gruppo DR o una seconda configurazione MetroCluster utilizzando le porte da 25 a 48 seguendo lo stesso schema.

Cisco 9250i			
FibreBridge 7500N o 7600N utilizzando una porta FC	Porta	Interruttore 1	Interruttore 2
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15



bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23

È possibile collegare altri bridge utilizzando le porte da 25 a 48 seguendo lo stesso schema.

#### Utilizzo delle porte Cisco per gli ISL in una configurazione a otto nodi in una configurazione MetroCluster con ONTAP 9.1 o versione successiva

La seguente tabella mostra l'utilizzo della porta ISL. L'utilizzo della porta ISL è lo stesso su tutti gli switch della configurazione.



Per Cisco 9132T, vedere [Utilizzo della porta ISL per Cisco 9132T in una configurazione MetroCluster che esegue ONTAP 9,1 o versione successiva](#).

Modello di switch	Porta ISL	Porta dello switch
Cisco 9396S	ISL 1	44
ISL 2	48	ISL 3
92	ISL 4	96
Cisco 9250i con licenza a 24 porte	ISL 1	12
ISL 2	16	ISL 3

20	ISL 4	24
Cisco 9148S	ISL 1	20
ISL 2	24	ISL 3
44	ISL 4	48

#### Utilizzo delle porte Cisco 9132T in configurazioni MetroCluster a quattro e otto nodi che eseguono ONTAP 9,4 e versioni successive

La tabella seguente mostra l'utilizzo della porta su uno switch Cisco 9132T. La tabella mostra le configurazioni massime supportate con quattro e otto moduli controller in due gruppi DR.



Per le configurazioni a otto nodi, è necessario eseguire lo zoning manualmente, perché gli RCF non sono forniti.

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)						
MetroCluster 1 o DR Group 1						
				Quattro nodi		Otto nodi
Componente		Porta	Si connette a FC_switch...	9132T (1 LEM)	9132T (2 LEM)	9132T (2 LEM)
controller_x_1	Porta FC-VI A.	1	LEM1-1	LEM1-1	LEM1-1	Porta FC-VI b
2	LEM1-1	LEM1-1	LEM1-1	Porta FC-VI c	1	LEM1-2
LEM1-2	LEM1-2	Porta FC-VI d	2	LEM1-2	LEM1-2	LEM1-2
Porta HBA a	1	LEM1-5	LEM1-5	LEM1-3	Porta HBA b	2
LEM1-5	LEM1-5	LEM1-3	Porta HBA c	1	LEM1-6	LEM1-6
LEM1-4	Porta HBA d	2	LEM1-6	LEM1-6	LEM1-4	controller_x_2
Porta FC-VI A.	1	LEM1-7	LEM1-7	LEM1-5	Porta FC-VI b	2
LEM1-7	LEM1-7	LEM1-5	Porta FC-VI c	1	LEM1-8	LEM1-8
LEM1-6	Porta FC-VI d	2	LEM1-8	LEM1-8	LEM1-6	Porta HBA a
1	LEM1-11	LEM1-11	LEM1-7	Porta HBA b	2	LEM1-11

LEM1-11	LEM1-7	Porta HBA c	1	LEM1-12	LEM1-12	LEM1-8
---------	--------	-------------	---	---------	---------	--------



- Nelle configurazioni a quattro nodi, è possibile collegare bridge aggiuntivi alle porte da LEM2-5 a LEM2-8 in switch 9132T con 2x LEMS.
- Nelle configurazioni a otto nodi, è possibile collegare bridge aggiuntivi alle porte da LEM2-13 a LEM2-16 in switch 9132T con 2x LEMS.
- Solo uno (1) stack di bridge è supportato utilizzando gli switch 9132T con 1 modulo LEM.

**Utilizzo delle porte Cisco 9132T per gli ISL in configurazioni a quattro e otto nodi in una configurazione MetroCluster che esegue ONTAP 9,1 o versione successiva**

La tabella seguente mostra l'utilizzo della porta ISL per uno switch Cisco 9132T.

MetroCluster 1 o DR Group 1			
Porta	Quattro nodi		Otto nodi
	9132T (1 LEM)	9132T (2 LEM)	9132T (2 LEM)
ISL1	LEM1-15	LEM2-9	LEM1-13
ISL2	LEM1-16	LEM2-10	LEM1-14
ISL3		LEM2-11	LEM1-15
ISL4		LEM2-12	LEM1-16
ISL5		LEM2-13	
ISL6		LEM2-14	
ISL7		LEM2-15	
ISL8		LEM2-16	

### Assegnazioni delle porte per switch FC quando si utilizzano sistemi AFF A900 o FAS9500

Quando si utilizzano ONTAP 9.10.1 e versioni successive, verificare di utilizzare le assegnazioni delle porte specificate quando si cablano gli switch FC.

È possibile riconfigurare le porte non utilizzate per il collegamento di porte initiator, porte FC-VI o ISL in modo da fungere da porte di storage. Tuttavia, se vengono utilizzati gli RCF supportati, la zoning deve essere modificata di conseguenza.

Se si utilizzano gli RCF supportati, le porte ISL potrebbero non connettersi alle stesse porte mostrate e potrebbe essere necessario riconfigurarle manualmente.

Se gli switch sono stati configurati utilizzando le assegnazioni delle porte per ONTAP 9, è possibile continuare a utilizzare le assegnazioni precedenti. Tuttavia, le nuove configurazioni che eseguono ONTAP 9.1 o versioni successive devono utilizzare le assegnazioni delle porte indicate di seguito.

### Linee guida generali per il cablaggio

Quando si utilizzano le tabelle di cablaggio, è necessario conoscere le seguenti linee guida:

- I sistemi storage AFF A900 o FAS9500 richiedono otto porte FC-VI. Se si utilizza un AFF A900 o FAS9500, è necessario utilizzare la configurazione a otto porte. Se la configurazione include gli altri modelli di sistemi di storage, utilizzare i cavi mostrati nelle tabelle ma ignorare i cavi delle porte FC-VI non necessarie.
- Se si dispone di due configurazioni MetroCluster che condividono gli ISL, utilizzare le stesse assegnazioni delle porte di un cablaggio MetroCluster a otto nodi.
- Il numero di ISL che si cablano può variare a seconda dei requisiti del sito.
- Consultare la sezione relativa alle considerazioni sull'ISL.

### "Considerazioni per gli ISL"

#### Utilizzo della porta Brocade per i controller AFF A900 o FAS9500 in una configurazione MetroCluster con ONTAP 9.10.1 o versione successiva

Le seguenti tabelle mostrano l'utilizzo delle porte sugli switch Brocade. Le tabelle mostrano la configurazione massima supportata, con otto moduli controller in quattro gruppi DR. I sistemi AFF A900 e FAS9500 dispongono di otto porte FC-VI (a, b, c e d per FC-VI-1 e FC-VI-2)

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)							
MetroCluster 1 o DR Group 1							
Componente	Porta	Modello di switch Brocade					
		Si connette a FC_switch ...	6510	6505, G610	G620, G620-1	G630, G630-1	G720

controller_x_1	Porta FC-VI-1 a	1	0	0	0	0	0
	Porta FC-VI-1 b	2	0	0	0	0	0
	Porta FC-VI-1 c	1	1	1	1	1	1
	Porta FC-VI-1 d	2	1	1	1	1	1
	Porta FC-VI-2 a	1	20	16	16	16	2
	Porta FC-VI-2 b	2	20	16	16	16	2
	Porta FC-VI-2 c	1	21	17	17	17	3
	Porta FC-VI-2 d	2	21	17	17	17	3
	Porta HBA a	1	2	2	2	2	8
	Porta HBA b	2	2	2	2	2	8
	Porta HBA c	1	3	3	3	3	9
	Porta HBA d	2	3	3	3	3	9

controller_x_2		Porta FC-VI-1 a	1	4	4	4	4	4
		Porta FC-VI-1 b	2	4	4	4	4	4
		Porta FC-VI-1 c	1	5	5	5	5	5
		Porta FC-VI-1 d	2	5	5	5	5	5
		Porta FC-VI-2 a	1	22	18	20	20	6
		Porta FC-VI-2 b	2	22	18	20	20	6
		Porta FC-VI-2 c	1	23	19	21	21	7
		Porta FC-VI-2 d	2	23	19	21	21	7
		Porta HBA a	1	6	6	6	6	12
		Porta HBA b	2	6	6	6	6	12
		Porta HBA c	1	7	7	7	7	13
		Porta HBA d	2	7	7	7	7	13
Stack 1	bridge_x_1 a	FC1	1	8	8	8	8	10
		FC2	2	8	8	8	8	10
	bridge_x_1 b	FC1	1	9	9	9	9	11
		FC2	2	9	9	9	9	11
Stack 2	bridge_x_2 a	FC1	1	10	10	10	10	14
		FC2	2	10	10	10	10	14
	bridge_x_2 b	FC1	1	11	11	11	11	15
		FC2	2	11	11	11	11	15
Stack 3	bridge_x_3 a	FC1	1	12	12	12	12	16
		FC2	2	12	12	12	12	16
	bridge_x_3 b	FC1	1	13	13	13	13	17
		FC2	2	13	13	13	13	17

Stack y	bridge_x_y a	FC1	1	14	14	14	14	20
		FC2	2	14	14	14	14	20
	bridge_x_y b	FC1	1	15	15	15	15	21
		FC2	2	15	15	15	15	21

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)

MetroCluster 2 o DR Group 2

Componente	Porta	Modello di switch Brocade					
		Si connette a FC_switch ...	6510	6505, G610	G620, G620-1	G630, G630-1	G720
controller_x_3	Porta FC- VI-1 a	1	24	-	18	18	18
	Porta FC- VI-1 b	2	24	-	18	18	18
	Porta FC- VI-1 c	1	25	-	19	19	19
	Porta FC- VI-1 d	2	25	-	19	19	19
	Porta FC- VI-2 a	1	36	-	36	36	24
	Porta FC- VI-2 b	2	36	-	36	36	24
	Porta FC- VI-2 c	1	37	-	37	37	25
	Porta FC- VI-2 d	2	37	-	37	37	25
	Porta HBA a	1	26	-	24	24	26
	Porta HBA b	2	26	-	24	24	26
	Porta HBA c	1	27	-	25	25	27
	Porta HBA d	2	27	-	25	25	27

controller_x_4		Porta FC-VI-1 a	1	28	-	22	22	22
		Porta FC-VI-1 b	2	28	-	22	22	22
		Porta FC-VI-1 c	1	29	-	23	23	23
		Porta FC-VI-1 d	2	29	-	23	23	23
		Porta FC-VI-2 a	1	38	-	38	38	28
		Porta FC-VI-2 b	2	38	-	38	38	28
		Porta FC-VI-2 c	1	39	-	39	39	29
		Porta FC-VI-2 d	2	39	-	39	39	29
		Porta HBA a	1	30	-	28	28	30
		Porta HBA b	2	30	-	28	28	30
		Porta HBA c	1	31	-	29	29	31
		Porta HBA d	2	31	-	29	29	31
Stack 1	bridge_x_5 1a	FC1	1	32	-	26	26	32
		FC2	2	32	-	26	26	32
	bridge_x_5 1b	FC1	1	33	-	27	27	33
		FC2	2	33	-	27	27	33
Stack 2	bridge_x_5 2a	FC1	1	34	-	30	30	34
		FC2	2	34	-	30	30	34
	bridge_x_5 2b	FC1	1	35	-	31	31	35
		FC2	2	35	-	31	31	35
Stack 3	bridge_x_5 3a	FC1	1	-	-	32	32	36
		FC2	2	-	-	32	32	36
	bridge_x_5 3b	FC1	1	-	-	33	33	37
		FC2	2	-	-	33	33	37



Stack y	bridge_x_5 ya	FC1	1	-	-	34	34	38
		FC2	2	-	-	34	34	38
	bridge_x_5 yb	FC1	1	-	-	35	35	39
		FC2	2	-	-	35	35	39

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)

MetroCluster 3 o DR Gruppo 3

Componente	Porta	Modello di switch Brocade	
		Si connette a FC_switch...	G630, G630-1
controller_x_5	Porta FC-VI-1 a	1	48
	Porta FC-VI-1 b	2	48
	Porta FC-VI-1 c	1	49
	Porta FC-VI-1 d	2	49
	Porta FC-VI-2 a	1	64
	Porta FC-VI-2 b	2	64
	Porta FC-VI-2 c	1	65
	Porta FC-VI-2 d	2	65
	Porta HBA a	1	50
	Porta HBA b	2	50
	Porta HBA c	1	51
	Porta HBA d	2	51
controller_x_6	Porta FC-VI-1 a	1	52
	Porta FC-VI-1 b	2	52
	Porta FC-VI-1 c	1	53
	Porta FC-VI-1 d	2	53
	Porta FC-VI-2 a	1	68
	Porta FC-VI-2 b	2	68
	Porta FC-VI-2 c	1	69
	Porta FC-VI-2 d	2	69
	Porta HBA a	1	54
	Porta HBA b	2	54
	Porta HBA c	1	55
	Porta HBA d	2	55

Stack 1	bridge_x_1a	FC1	1	56
		FC2	2	56
	bridge_x_1b	FC1	1	57
		FC2	2	57
Stack 2	bridge_x_2a	FC1	1	58
		FC2	2	58
	bridge_x_2b	FC1	1	59
		FC2	2	59
Stack 3	bridge_x_3a	FC1	1	60
		FC2	2	60
	bridge_x_3b	FC1	1	61
		FC2	2	61
Stack y	bridge_x_ya	FC1	1	62
		FC2	2	62
	bridge_x_yb	FC1	1	63
		FC2	2	63

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)

MetroCluster 4 o DR Group 4

Componente	Porta	Modello di switch Brocade	
		Si connette a FC_switch...	G630, G630-1
controller_x_7	Porta FC-VI-1 a	1	66
	Porta FC-VI-1 b	2	66
	Porta FC-VI-1 c	1	67
	Porta FC-VI-1 d	2	67
	Porta FC-VI-2 a	1	84
	Porta FC-VI-2 b	2	84
	Porta FC-VI-2 c	1	85
	Porta FC-VI-2 d	2	85
	Porta HBA a	1	72
	Porta HBA b	2	72
	Porta HBA c	1	73
	Porta HBA d	2	73

controller_x_8		Porta FC-VI-1 a	1	70
		Porta FC-VI-1 b	2	70
		Porta FC-VI-1 c	1	71
		Porta FC-VI-1 d	2	71
		Porta FC-VI-2 a	1	86
		Porta FC-VI-2 b	2	86
		Porta FC-VI-2 c	1	87
		Porta FC-VI-2 d	2	87
		Porta HBA a	1	76
		Porta HBA b	2	76
		Porta HBA c	1	77
		Porta HBA d	2	77
Stack 1	bridge_x_51a	FC1	1	74
		FC2	2	74
	bridge_x_51b	FC1	1	75
		FC2	2	75
Stack 2	bridge_x_52a	FC1	1	78
		FC2	2	78
	bridge_x_52b	FC1	1	79
		FC2	2	79
Stack 3	bridge_x_53a	FC1	1	80
		FC2	2	80
	bridge_x_53b	FC1	1	81
		FC2	2	81
Stack y	bridge_x_5ya	FC1	1	82
		FC2	2	82
	bridge_x_5yb	FC1	1	83
		FC2	2	83

**AFF A900 o FAS9500 - utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster con ONTAP 9.10.1 o versione successiva**

La seguente tabella mostra l'utilizzo delle porte ISL per gli switch Brocade in un sistema AFF A900 o FAS9500.



I sistemi AFF A900 e FAS9500 supportano otto ISL. Sono supportati otto ISL su Brocade 6510, G620, G620-1, G630, G630-1, E G720.

Modello di switch	Porta ISL	Porta dello switch
6510, G620, G620-1, G630, G630-1, G720	ISL1	40
ISL2	41	ISL3
42	ISL4	43
ISL5	44	ISL6
45	ISL7	46
ISL8	47	6505, G610
ISL1	20	
ISL2	21	
ISL3	22	

Utilizzo della porta Cisco per controller AFF A900 o FAS9500 in una configurazione MetroCluster con ONTAP 9.10.1 o versione successiva

Le tabelle mostrano le configurazioni massime supportate, con otto moduli controller AFF A900 o FAS9500 in un gruppo di DR.



- La seguente tabella mostra i sistemi con otto porte FC-VI. AFF A900 e FAS9500 dispongono di otto porte FC-VI (a, b, c e d per FC-VI-1 e FC-VI-2).
- MetroCluster 2 o DR 2 non è supportato dagli switch 9132T.

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)				
MetroCluster 1 o DR Group 1				
Componente	Porta	Modello di switch Cisco		
		Si connette a FC_switch...	9132T (1 LEM)	9132T (2 LEM)

controller_x_1		Porta FC-VI-1 a	1	LEM1-1	LEM1-1
		Porta FC-VI-1 b	2	LEM1-1	LEM1-1
		Porta FC-VI-1 c	1	LEM1-2	LEM1-2
		Porta FC-VI-1 d	2	LEM1-2	LEM1-2
		Porta FC-VI-2 a	1	LEM1-3	LEM1-3
		Porta FC-VI-2 b	2	LEM1-3	LEM1-3
		Porta FC-VI-2 c	1	LEM1-4	LEM1-4
		Porta FC-VI-2 d	2	LEM1-4	LEM1-4
		Porta HBA a	1	LEM1-5	LEM1-5
		Porta HBA b	2	LEM1-5	LEM1-5
		Porta HBA c	1	LEM1-6	LEM1-6
		Porta HBA d	2	LEM1-6	LEM1-6
controller_x_2		Porta FC-VI-1 a	1	LEM1-7	LEM1-7
		Porta FC-VI-1 b	2	LEM1-7	LEM1-7
		Porta FC-VI-1 c	1	LEM1-8	LEM1-8
		Porta FC-VI-1 d	2	LEM1-8	LEM1-8
		Porta FC-VI-2 a	1	LEM1-9	LEM1-9
		Porta FC-VI-2 b	2	LEM1-9	LEM1-9
		Porta FC-VI-2 c	1	LEM1-10	LEM1-10
		Porta FC-VI-2 d	2	LEM1-10	LEM1-10
		Porta HBA a	1	LEM1-11	LEM1-11
		Porta HBA b	2	LEM1-11	LEM1-11
		Porta HBA c	1	LEM1-12	LEM1-12
		Porta HBA d	2	LEM1-12	LEM1-12
Stack 1	bridge_x_1a	FC1	1	LEM1-13	LEM1-13
		FC2	2	LEM1-13	LEM1-13
	bridge_x_1b	FC1	1	LEM1-14	LEM1-14
		FC2	2	LEM1-14	LEM1-14
Stack 2	bridge_x_2a	FC1	1	-	LEM1-15
		FC2	2	-	LEM1-15
	bridge_x_2b	FC1	1	-	LEM1-16
		FC2	2	-	LEM1-16

Stack 3	bridge_x_3a	FC1	1	-	LEM2-1
		FC2	2	-	LEM2-1
	bridge_x_3b	FC1	1	-	LEM2-2
		FC2	2	-	LEM2-2
Stack y	bridge_x_ya	FC1	1	-	LEM2-3
		FC2	2	-	LEM2-3
	bridge_x_yb	FC1	1	-	LEM2-4
		FC2	2	-	LEM2-4



- È possibile collegare ponti aggiuntivi alle porte da LEM2-5 a LEM2-8 in switch 9132T con 2x moduli LEM.
- Solo uno (1) stack di bridge è supportato utilizzando gli switch 9132T con 1 modulo LEM.

**AFF A900 o FAS9500 - utilizzo della porta Cisco per gli ISL in una configurazione a otto nodi in una configurazione MetroCluster con ONTAP 9.10.1 o versione successiva**

La seguente tabella mostra l'utilizzo della porta ISL. L'utilizzo della porta ISL è lo stesso su tutti gli switch della configurazione.

Modello di switch	Porta ISL	Porta dello switch
Cisco 9132T con 1 LEM	ISL1	LEM1-15
	ISL2	LEM1-16
Cisco 9132T con 2 LEM	ISL1	LEM2-9
	ISL2	LEM2-10
	ISL3	LEM2-11
	ISL4	LEM2-12
	ISL5	LEM2-13
	ISL6	LEM2-14
	ISL7	LEM2-15
	ISL8	LEM2-16

### Cablaggio dell'interconnessione del cluster in configurazioni a otto o quattro nodi

Nelle configurazioni MetroCluster a otto o quattro nodi, è necessario collegare l'interconnessione del cluster tra i moduli controller locali di ciascun sito.

#### A proposito di questa attività

Questa attività non è richiesta nelle configurazioni MetroCluster a due nodi.

Questa attività deve essere eseguita in entrambi i siti MetroCluster.

#### Fase

1. Collegare l'interconnessione del cluster da un modulo controller all'altro o, se si utilizzano switch di interconnessione del cluster, da ciascun modulo controller agli switch.

#### Informazioni correlate

["Documentazione dei sistemi hardware ONTAP"](#)

["Gestione di rete e LIF"](#)

#### Cablaggio delle connessioni di peering del cluster

È necessario collegare le porte del modulo controller utilizzate per il peering del cluster in modo che siano connessi al cluster sul sito del partner.

#### A proposito di questa attività

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.

#### Fase

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.

#### Informazioni correlate

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

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 e decidere se utilizzare porte condivise o dedicate per tali relazioni.

["Peering dei cluster"](#)

#### Cablaggio dell'interconnessione ha

Se si dispone di una configurazione MetroCluster a otto o quattro nodi e i controller storage all'interno delle coppie ha si trovano in uno chassis separato, è necessario collegare l'interconnessione ha tra i controller.

#### A proposito di questa attività

- Questa attività non si applica alle configurazioni MetroCluster a due nodi.
- Questa attività deve essere eseguita in entrambi i siti MetroCluster.
- L'interconnessione ha deve essere cablata solo se i controller storage all'interno della coppia ha si trovano in uno chassis separato.

Alcuni modelli di storage controller supportano due controller in un unico chassis, nel qual caso utilizzano un'interconnessione ha interna.

## Fasi

1. Collegare l'interconnessione ha se il partner ha del controller di storage si trova in uno chassis separato.

["Documentazione dei sistemi hardware ONTAP"](#)

2. Se il sito MetroCluster include due coppie ha, ripetere i passaggi precedenti sulla seconda coppia ha.
3. Ripetere questa operazione sul sito del partner MetroCluster.

## Cablaggio della gestione e delle connessioni dati

È necessario collegare le porte di gestione e dati di ciascun controller di storage alle reti del sito.

### A proposito di questa attività

Questa attività deve essere ripetuta per ogni nuovo controller in entrambi i siti MetroCluster.

È possibile collegare le porte di gestione del controller e dello switch del cluster agli switch esistenti nella rete o a nuovi switch di rete dedicati, come gli switch di gestione del cluster NetApp CN1601.

## Fase

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

["Documentazione dei sistemi hardware ONTAP"](#)

## Configurare gli switch FC

### Panoramica della configurazione degli switch FC

È possibile configurare gli switch Cisco e Brocade FC utilizzando i file RCF oppure, se necessario, configurare manualmente gli switch.

Se...	Utilizzare la procedura...
Disporre di un RCF che soddisfi i requisiti dell'utente	<ul style="list-style-type: none"><li>• <a href="#">"Configurare gli switch Brocade FC con i file RCF"</a></li><li>• <a href="#">"Configurare gli switch FC Cisco con i file RCF"</a></li></ul>
Non disporre di un RCF o di un RCF che non soddisfi i requisiti dell'utente	<ul style="list-style-type: none"><li>• <a href="#">"Configurare manualmente gli switch Brocade FC"</a></li><li>• <a href="#">"Configurare manualmente gli switch Cisco FC"</a></li></ul>

### Configurare gli switch Brocade FC con i file RCF

#### Ripristino delle impostazioni predefinite dello switch Brocade FC

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

### A proposito di questa attività

È necessario ripetere questi passaggi su ciascuno switch FC nella configurazione MetroCluster Fabric.



## Fasi

1. Accedere allo switch come amministratore.
2. Disattivare la funzione Brocade Virtual Fabrics (VF):

```
fosconfig options
```

```
FC_switch_A_1:admin> fosconfig --disable vf
WARNING: This is a disruptive operation that requires a reboot to take
effect.
Would you like to continue [Y/N]: y
```

3. Scollegare i cavi ISL dalle porte dello switch.
4. Disattivare lo switch:

```
switchcfgpersistentdisable
```

```
FC_switch_A_1:admin> switchcfgpersistentdisable
```

5. Disattivare la configurazione:

```
cfgDisable
```

```
FC_switch_A_1:admin> cfgDisable
You are about to disable zoning configuration. This action will disable
any previous zoning configuration enabled.
Do you want to disable zoning configuration? (yes, y, no, n): [no] y
Updating flash ...
Effective configuration is empty. "No Access" default zone mode is ON.
```

6. Cancellare la configurazione:

```
cfgClear
```

```
FC_switch_A_1:admin> cfgClear
The Clear All action will clear all Aliases, Zones, FA Zones
and configurations in the Defined configuration.
Run cfgSave to commit the transaction or cfgTransAbort to
cancel the transaction.
Do you really want to clear all configurations? (yes, y, no, n): [no] y
```

7. Salvare la configurazione:

```
cfgSave
```

```
FC_switch_A_1:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only? (yes, y, no,
n): [no] y
Updating flash ...
```

## 8. Impostare la configurazione predefinita:

`configDefault`

```
FC_switch_A_1:admin> configDefault
WARNING: This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

## 9. Impostare la configurazione della porta sul valore predefinito per tutte le porte:

`portcfgdefault port-number`

```
FC_switch_A_1:admin> portcfgdefault <port number>
```

È necessario completare questo passaggio per ciascuna porta.

## 10. Verificare che lo switch stia utilizzando il metodo dinamico POD (Port on Demand).



Per le versioni Brocade Fabric OS precedenti alla 8.0, eseguire i seguenti comandi come admin e per le versioni 8.0 e successive come root.

a. Eseguire il comando License:

**Per Fabric OS 8.2.x e versioni precedenti**

Eseguire il comando `licenseport --show`.

**Per Fabric OS 9.0 e versioni successive**

Eseguire il comando `license --show -port`.

```
FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

b. Attivare l'utente root se è disattivato da Brocade.

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

c. Eseguire il comando License:

**Per Fabric OS 8.2.x e versioni precedenti**

Eseguire il comando `licenseport --show`.

**Per Fabric OS 9.0 e versioni successive**

Eseguire il comando `license --show -port`.

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Se si utilizza Fabric OS 8.2.x e versioni precedenti, è necessario modificare il metodo di licenza in dinamico:

```
licenseport --method dynamic
```

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```



In Fabric OS 9.0 e versioni successive, il metodo di licenza è dinamico per impostazione predefinita. Il metodo di licenza statico non è supportato.

#### 11. Riavviare lo switch:

fastBoot

```
FC_switch_A_1:admin> fastboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
```

#### 12. Verificare che le impostazioni predefinite siano state implementate:

switchShow

#### 13. Verificare che l'indirizzo IP sia impostato correttamente:

ipAddrShow

Se necessario, è possibile impostare l'indirizzo IP con il seguente comando:

ipAddrSet

#### Download del file RCF dello switch FC Brocade

È necessario scaricare il file di configurazione di riferimento (RCF) su ogni switch nella configurazione MetroCluster Fabric.

#### A proposito di questa attività

Per utilizzare questi file RCF, il sistema deve eseguire ONTAP 9.1 o versione successiva ed è necessario utilizzare il layout delle porte per ONTAP 9.1 o versione successiva.

Se si prevede di utilizzare solo una delle porte FC sui bridge FibreBridge, configurare manualmente gli switch Fibre Channel back-end seguendo le istruzioni riportate nella sezione, ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#).

#### Fasi

1. Fare riferimento alla tabella dei file RCF nella pagina di download di Brocade RCF e identificare il file RCF corretto per ogni switch nella configurazione.

I file RCF devono essere applicati agli switch corretti.

2. Scaricare i file RCF per gli switch da ["Download di MetroCluster RCF"](#) pagina.

I file devono essere collocati in una posizione in cui possono essere trasferiti allo switch. È disponibile un file separato per ciascuno dei quattro switch che compongono il fabric a due switch.

3. Ripetere questi passaggi su ogni switch nella configurazione.

## Installazione del file RCF dello switch FC Brocade

Quando si configura uno switch FC Brocade, è possibile installare i file di configurazione dello switch che forniscono le impostazioni complete per determinate configurazioni.

### A proposito di questa attività

- Ripetere questa procedura su ciascuno switch FC Brocade nella configurazione MetroCluster Fabric.
- Se si utilizza una configurazione xWDM, potrebbero essere necessarie impostazioni aggiuntive sugli ISL. Per ulteriori informazioni, consultare la documentazione del fornitore di xWDM.

### Fasi

1. Avviare il processo di download e configurazione:

```
configDownload
```

Rispondere alle richieste come mostrato nell'esempio seguente.

```
FC_switch_A_1:admin> configDownload
Protocol (scp, ftp, sftp, local) [ftp]:
Server Name or IP Address [host]: <user input>
User Name [user]:<user input>
Path/Filename [<home dir>/config.txt]:path to configuration file
Section (all|chassis|switch [all]): all
.
.
.
Do you want to continue [y/n]: y
Password: <user input>
```

Una volta immessa la password, lo switch scarica ed esegue il file di configurazione.

2. Verificare che il file di configurazione abbia impostato il dominio dello switch:

```
switchShow
```

A ogni switch viene assegnato un numero di dominio diverso a seconda del file di configurazione utilizzato dallo switch.

```
FC_switch_A_1:admin> switchShow
switchName: FC_switch_A_1
switchType: 109.1
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 5
```

3. Verificare che allo switch sia stato assegnato il valore di dominio corretto, come indicato nella seguente

tabella.

Fabric	Switch	Dominio dello switch
1	A_1	5
B_1	7	2
A_2	6	B_2

#### 4. Modificare la velocità della porta:

`portcfgspeed`

```
FC_switch_A_1:admin> portcfgspeed port number port speed
```

Per impostazione predefinita, tutte le porte sono configurate per funzionare a 16 Gbps. È possibile modificare la velocità della porta per i seguenti motivi:

- La velocità delle porte dello switch di interconnessione deve essere modificata quando si utilizza un adattatore FC-VI a 8 Gbps e la velocità della porta dello switch deve essere impostata su 8 Gbps.
- La velocità delle porte ISL deve essere modificata quando l'ISL non è in grado di funzionare a 16 Gbps.

#### 5. Calcolare la distanza ISL.

A causa del comportamento di FC-VI, è necessario impostare la distanza su 1.5 volte la distanza reale con un minimo di 10 (LE). La distanza per l'ISL viene calcolata come segue, arrotondata al chilometro completo successivo:  $1.5 \times \text{distanza reale} = \text{distanza}$ .

Se la distanza è di 3 km,  $1.5 \times 3 \text{ km} = 4.5$ . È inferiore a 10; pertanto, è necessario impostare l'ISL sul livello DI distanza LE.

La distanza è di 20 km, quindi  $1.5 \times 20 \text{ km} = 30$ . È necessario impostare l'ISL sul livello di distanza LS.

#### 6. Impostare la distanza per ciascuna porta ISL:

`portcfglongdistance port level vc_link_init -distance distance_value`

Un valore `vc_link_init` pari a 1 utilizza la parola fillword "ARB" per impostazione predefinita. Un valore pari a 0 utilizza la parola fillword "IDLE". Il valore richiesto potrebbe variare a seconda del collegamento utilizzato. In questo esempio, l'impostazione predefinita è impostata e la distanza si presume sia di 20 km. Quindi, l'impostazione è "30" con un valore `vc_link_init` "1" e la porta ISL è "21".

Esempio: LS

```
FC_switch_A_1:admin> portcfglongdistance 21 LS 1 -distance 30
```

Esempio: LE

```
FC_switch_A_1:admin> portcfglongdistance 21 LE 1
```

7. Abilitare costantemente lo switch:

```
switchcfgpersistentenable
```

L'esempio mostra come abilitare in modo permanente lo switch FC\_A\_1.

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

8. Verificare che l'indirizzo IP sia impostato correttamente:

```
ipAddrshow
```

```
FC_switch_A_1:admin> ipAddrshow
```

È possibile impostare l'indirizzo IP, se necessario:

```
ipAddrSet
```

9. Impostare il fuso orario dal prompt dello switch:

```
tstimezone --interactive
```

Rispondere alle richieste secondo necessità.

```
FC_switch_A_1:admin> tstimezone --interactive
```

10. Riavviare lo switch:

```
reboot
```

L'esempio mostra come riavviare lo switch FC\_A\_1.

```
FC_switch_A_1:admin> reboot
```

11. Verificare l'impostazione della distanza:

```
portbuffershow
```

Un'impostazione della distanza DI LE viene visualizzata come 10 km

```

FC_Switch_A_1:admin> portbuffershow
User Port Lx    Max/Resv Buffer Needed  Link      Remaining
Port Type Mode Buffers  Usage  Buffers Distance Buffers
-----
...
21    E    -      8      67      67      30 km
22    E    -      8      67      67      30 km
...
23    -    8      0      -      -      466

```

12. Ricollegare i cavi ISL alle porte degli switch in cui sono stati rimossi.

I cavi ISL sono stati scollegati quando sono state ripristinate le impostazioni predefinite.

["Ripristino delle impostazioni predefinite dello switch Brocade FC"](#)

13. Convalidare la configurazione.

a. Verificare che gli switch formino un unico fabric:

```
switchshow
```

L'esempio seguente mostra l'output per una configurazione che utilizza gli ISL sulle porte 20 e 21.

```

FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:      5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:      OFF
switchBeacon: OFF

Index Port Address Media Speed State  Proto
=====
...
20    20  010C00   id    16G  Online FC   LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream) (trunk master)
21    21  010D00   id    16G  Online FC   LE E-Port  (Trunk port,
master is Port 20)
...

```

b. Confermare la configurazione dei fabric:



fabricshow

```
FC_switch_A_1:admin> fabricshow
Switch ID      Worldwide Name      Enet IP Addr FC IP Addr Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55 0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65 0.0.0.0
>"FC_switch_B_1"
```

c. Verificare che gli ISL funzionino:

islshow

```
FC_switch_A_1:admin> islshow
```

d. Verificare che lo zoning sia replicato correttamente:

cfgshow+ zoneshow

Entrambi gli output devono mostrare le stesse informazioni di configurazione e le stesse informazioni di zoning per entrambi gli switch.

e. Se viene utilizzato il trunking, confermare quanto segue:

trunkshow

```
FC_switch_A_1:admin> trunkshow
```

## Configurare gli switch FC Cisco con i file RCF

### Ripristino delle impostazioni predefinite dello switch FC Cisco

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

#### A proposito di questa attività

È necessario ripetere questi passaggi su ciascuno switch FC nella configurazione MetroCluster Fabric.



Le uscite mostrate si riferiscono agli switch IP Cisco; tuttavia, questi passaggi sono applicabili anche agli switch FC Cisco.

#### 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], dovresti rispondere **yes** per procedere.

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

- Password amministratore
- Nome dello switch
- Configurazione della gestione fuori banda
- Gateway predefinito
- Servizio SSH (Remote Support Agent).

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 quando si accede allo 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.
```

- e. Inserire le informazioni di base nel successivo set di prompt, inclusi nome dello switch, indirizzo di gestione e gateway, quindi immettere **rsa** Per la chiave SSH come mostrato nell'esempio:

```

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 MetroCluster Fabric.

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

### 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

Questi passaggi devono essere ripetuti su ciascuno switch FC nella configurazione MetroCluster Fabric.

È necessario utilizzare la versione del software dello switch supportata.

["NetApp Hardware Universe"](#)



Le uscite mostrate si riferiscono agli switch IP Cisco; tuttavia, questi passaggi sono applicabili anche agli switch FC Cisco.

### Fasi

1. Scaricare il file software NX-OS supportato.

["Pagina di download di 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 `nxos.7.0.3.I4.6.bin` Il file 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
```

L'esempio seguente mostra la presenza dei file 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 system bootflash:nxos.version-number.bin kickstart
bootflash:nxos.version-kickstart-number.bin
```

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

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

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

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

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

Extracting "system" version from image bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS
...
```

Lo switch si riavvia automaticamente dopo l'installazione del software dello switch.

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 sugli altri tre switch FC nella configurazione MetroCluster Fabric.

#### Download e installazione dei file Cisco FC RCF

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

#### Prima di iniziare

Questa operazione richiede un software per il trasferimento dei file, ad esempio FTP, Trivial file Transfer Protocol (TFTP), SFTP o Secure Copy Protocol (SCP), per copiare i file sugli switch.

### A proposito di questa attività

Questi passaggi devono essere ripetuti su ciascuno switch FC Cisco nella configurazione MetroCluster Fabric.

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 MetroCluster Fabric. È necessario utilizzare i file RCF corretti per il modello di switch in uso.

Switch	File RCF
Switch_FC_A_1	NX3232_v1.80_Switch-A1.txt
Switch_FC_A_2	NX3232_v1.80_Switch-A2.txt
Switch_FC_B_1	NX3232_v1.80_Switch-B1.txt
Switch_FC_B_2	NX3232_v1.80_Switch-B2.txt



Le uscite mostrate si riferiscono agli switch IP Cisco; tuttavia, questi passaggi sono applicabili anche agli switch FC Cisco.

### Fasi

1. Scaricare i file Cisco FC RCF da "[Pagina di download di MetroCluster RCF](#)".
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 NX3232\_v1.80\_Switch-A1.txt Il file RCF viene copiato dal server SFTP all'indirizzo 10.10.99.99 al bootflash 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_v1.8T-
X1_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 in ogni switch bootflash directory:

```
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. 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
```

5. 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
```

6. Ricaricare lo switch:

```
reload
```

```
IP_switch_A_1# reload
```

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

## Configurazione manuale degli switch Brocade FC

È necessario configurare ciascuno dei fabric dello switch Brocade nella configurazione MetroCluster.

### Prima di iniziare

- È necessario disporre di una workstation PC o UNIX con accesso Telnet o Secure Shell (SSH) agli switch FC.
- È necessario utilizzare quattro switch Brocade supportati dello stesso modello con la stessa versione e licenza del sistema operativo Brocade Fabric (FOS).

### "Tool di matrice di interoperabilità NetApp"

In IMT, è possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

- I quattro switch Brocade supportati devono essere collegati a due fabric di due switch ciascuno, con ciascun fabric che si estende su entrambi i siti.
- Ciascun controller di storage deve disporre di quattro porte di iniziatore per la connessione ai fabric dello switch. È necessario collegare due porte initiator da ciascun controller di storage a ciascun fabric.



È possibile configurare i sistemi FAS8020, AFF8020, FAS8200 e AFF A300 con due porte di iniziatori per controller (una singola porta di iniziatore per ciascun fabric) se vengono soddisfatti tutti i seguenti criteri:

- Sono disponibili meno di quattro porte FC Initiator per collegare lo storage su disco e non è possibile configurare porte aggiuntive come iniziatori FC.
- Tutti gli slot sono in uso e non è possibile aggiungere alcuna scheda FC Initiator.

### A proposito di questa attività

- È necessario attivare il trunking ISL (Inter-Switch link) quando è supportato dai collegamenti.

## "Considerazioni sull'utilizzo di apparecchiature TDM/WDM con configurazioni MetroCluster collegate al fabric"

- Se si utilizza una configurazione xWDM, potrebbero essere necessarie impostazioni aggiuntive sugli ISL. Per ulteriori informazioni, consultare la documentazione del fornitore di xWDM.
- Tutti gli ISL devono avere la stessa lunghezza e la stessa velocità in un unico fabric.

Nei diversi tessuti è possibile utilizzare lunghezze diverse. La stessa velocità deve essere utilizzata in tutti i fabric.

- Metro-e e TDM (SONET/SDH) non sono supportati e non sono supportati frame o segnali nativi non FC.

Metro-e indica che il frame o la segnalazione Ethernet si verifica in modo nativo su una distanza metropolitana o tramite TDM (Time-Division Multiplexing), MPLS (MultiProtocol Label Switching) o WDM (Wavelength-Division Multiplexing).

- Gli interni TDMS, FCR (routing FC nativo) o FCIP non sono supportati per il fabric dello switch FC MetroCluster.
- Alcuni switch del fabric dello switch FC MetroCluster supportano crittografia o compressione e talvolta entrambi.

## "Tool di matrice di interoperabilità NetApp (IMT)"

In IMT, è possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

- La funzione Brocade Virtual Fabric (VF) non è supportata.
- Lo zoning FC basato sulla porta del dominio è supportato, ma lo zoning basato sul nome mondiale (WWN) non è supportato.

### Analisi dei requisiti di licenza Brocade

Sono necessarie alcune licenze per gli switch in una configurazione MetroCluster. È necessario installare queste licenze su tutti e quattro gli switch.

### A proposito di questa attività

La configurazione di MetroCluster prevede i seguenti requisiti di licenza Brocade:

- Licenza trunking per sistemi che utilizzano più di un ISL, come consigliato.
- Licenza fabric estesa (per distanze ISL superiori a 6 km)
- Licenza Enterprise per siti con più di un ISL e una distanza ISL superiore a 6 km

La licenza Enterprise include Brocade Network Advisor e tutte le licenze, ad eccezione delle licenze per porte aggiuntive.

### Fase

1. Verificare che le licenze siano installate:

**Per Fabric OS 8.2.x e versioni precedenti**

Eseguire il comando `licenseshow`.

**Per Fabric OS 9.0 e versioni successive**

Eseguire il comando `license --show`.

Se non si dispone di queste licenze, contattare il rappresentante commerciale prima di procedere.

**Impostazione dei valori predefiniti dello switch Brocade FC**

Per garantire una corretta configurazione, è necessario impostare lo switch sui valori predefiniti. È inoltre necessario assegnare a ciascun switch un nome univoco.

**A proposito di questa attività**

Negli esempi di questa procedura, il fabric è costituito da BrocadeSwitchA e BrocadeSwitchB.

**Fasi**

1. Stabilire una connessione alla console e accedere a entrambi gli switch in un unico fabric.
2. Disattivare lo switch in modo persistente:

```
switchcfgpersistentdisable
```

In questo modo, lo switch rimane disattivato dopo un riavvio o un avvio rapido. Se questo comando non è disponibile, utilizzare `switchdisable` comando.

L'esempio seguente mostra il comando su BrocadeSwitchA:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

L'esempio seguente mostra il comando su BrocadeSwitchB:

```
BrocadeSwitchB:admin> switchcfgpersistentdisable
```

3. Impostare il nome dello switch:

```
switchname switch_name
```

Gli switch devono avere un nome univoco. Dopo aver impostato il nome, il prompt cambia di conseguenza.

L'esempio seguente mostra il comando su BrocadeSwitchA:

```
BrocadeSwitchA:admin> switchname "FC_switch_A_1"  
FC_switch_A_1:admin>
```

L'esempio seguente mostra il comando su BrocadeSwitchB:

```
BrocadeSwitchB:admin> switchname "FC_Switch_B_1"  
FC_switch_B_1:admin>
```

#### 4. Impostare tutte le porte sui valori predefiniti:

```
portcfgdefault
```

Questa operazione deve essere eseguita per tutte le porte dello switch.

L'esempio seguente mostra i comandi su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> portcfgdefault 0  
FC_switch_A_1:admin> portcfgdefault 1  
...  
FC_switch_A_1:admin> portcfgdefault 39
```

L'esempio seguente mostra i comandi su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> portcfgdefault 0  
FC_switch_B_1:admin> portcfgdefault 1  
...  
FC_switch_B_1:admin> portcfgdefault 39
```

#### 5. Cancellare le informazioni di zoning:

```
cfgdisable
```

```
cfgclear
```

```
cfgsave
```

L'esempio seguente mostra i comandi su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> cfgdisable  
FC_switch_A_1:admin> cfgclear  
FC_switch_A_1:admin> cfgsave
```

L'esempio seguente mostra i comandi su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> cfgdisable  
FC_switch_B_1:admin> cfgclear  
FC_switch_B_1:admin> cfgsave
```

6. Impostare le impostazioni generali dello switch sui valori predefiniti:

```
configdefault
```

L'esempio seguente mostra il comando su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> configdefault
```

L'esempio seguente mostra il comando su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> configdefault
```

7. Impostare tutte le porte sulla modalità non trunking:

```
switchcfgtrunk 0
```

L'esempio seguente mostra il comando su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> switchcfgtrunk 0
```

L'esempio seguente mostra il comando su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> switchcfgtrunk 0
```

8. Sugli switch Brocade 6510, disattivare la funzione Brocade Virtual Fabrics (VF):

```
fosconfig options
```

L'esempio seguente mostra il comando su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> fosconfig --disable vf
```

L'esempio seguente mostra il comando su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> fosconfig --disable vf
```

9. Cancellare la configurazione del dominio amministrativo (ad):

L'esempio seguente mostra i comandi su FC\_switch\_A\_1:



```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

L'esempio seguente mostra i comandi su FC\_switch\_B\_1:

```
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
```

#### 10. Riavviare lo switch:

```
reboot
```

L'esempio seguente mostra il comando su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> reboot
```

L'esempio seguente mostra il comando su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> reboot
```

### Configurazione delle impostazioni di base dello switch

È necessario configurare le impostazioni globali di base, incluso l'ID di dominio, per gli switch Brocade.

#### A proposito di questa attività

Questa attività contiene i passaggi che devono essere eseguiti su ogni switch in entrambi i siti MetroCluster.

In questa procedura, impostare l'ID di dominio univoco per ogni switch, come illustrato nell'esempio seguente. Nell'esempio, gli ID di dominio 5 e 7 formano Fabric\_1 e gli ID di dominio 6 e 8 formano Fabric\_2.

- FC\_switch\_A\_1 è assegnato all'ID di dominio 5
- FC\_switch\_A\_2 è assegnato all'ID di dominio 6
- FC\_switch\_B\_1 è assegnato all'ID di dominio 7
- FC\_switch\_B\_2 è assegnato all'ID di dominio 8

#### Fasi

1. Accedere alla modalità di configurazione:

```
configure
```

2. Seguire le istruzioni:

- a. Impostare l'ID di dominio dello switch.

- b. Premere **Invio** in risposta alle richieste fino a visualizzare "RDP polling Cycle" (ciclo di polling RDP), quindi impostare il valore su 0 per disattivare il polling.
- c. Premere **Invio** fino a quando non si torna al prompt di switch.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = 5
.
.

RSCN Transmission Mode [yes, y, no, no: [no] y

End-device RSCN Transmission Mode
(0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric
RSCN): (0..2) [1]
Domain RSCN To End-device for switch IP address or name change
(0 = disabled, 1 = enabled): (0..1) [0] 1

.
.

RDP Polling Cycle(hours) [0 = Disable Polling]: (0..24) [1] 0
```

3. Se si utilizzano due o più ISL per fabric, è possibile configurare la distribuzione in-order (IOD) dei frame o la distribuzione out-of-order (OOOD) dei frame.



Si consigliano le impostazioni IOD standard. Configurare OOD solo se necessario.

["Considerazioni sull'utilizzo di apparecchiature TDM/WDM con configurazioni MetroCluster collegate al fabric"](#)

- a. Per configurare l'IOD dei frame, è necessario eseguire le seguenti operazioni su ciascun fabric dello switch:

- i. Attiva IOD:

```
iodset
```

- ii. Impostare il criterio APT (Advanced Performance Tuning) su 1:

```
aptpolicy 1
```

- iii. Disattiva Dynamic Load Sharing (DLS):

```
dlsreset
```

- iv. Verificare le impostazioni IOD utilizzando `iodshow`, `aptpolicy`, e `dlsshow` comandi.

Ad esempio, eseguire i seguenti comandi su FC\_switch\_A\_1:

```

FC_switch_A_1:admin> iodshow
IOD is set

FC_switch_A_1:admin> aptpolicy
Current Policy: 1 0(ap)

3 0(ap) : Default Policy
1: Port Based Routing Policy
3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
command aptpolicy completed

FC_switch_A_1:admin> dlsshow
DLS is not set

```

- i. Ripetere questa procedura sul secondo fabric dello switch.
- b. Per configurare l'OOD dei frame, è necessario eseguire le seguenti operazioni su ciascun fabric dello switch:

- i. Attiva OOOD:

```
iodreset
```

- ii. Impostare il criterio APT (Advanced Performance Tuning) su 3:

```
aptpolicy 3
```

- iii. Disattiva Dynamic Load Sharing (DLS):

```
dlsreset
```

- iv. Verificare le impostazioni OOOD:

```
iodshow
```

```
aptpolicy
```

```
dlsshow
```

Ad esempio, eseguire i seguenti comandi su FC\_switch\_A\_1:

```

FC_switch_A_1:admin> iodshow
IOD is not set

FC_switch_A_1:admin> aptpolicy
Current Policy: 3 0(ap)
3 0(ap) : Default Policy
1: Port Based Routing Policy
3: Exchange Based Routing Policy
0: AP Shared Link Policy
1: AP Dedicated Link Policy
command aptpolicy completed

FC_switch_A_1:admin> dlsshow
DLS is set by default with current routing policy

```

- i. Ripetere questa procedura sul secondo fabric dello switch.



Quando si configura ONTAP sui moduli controller, OOD deve essere configurato esplicitamente su ciascun modulo controller nella configurazione MetroCluster.

#### "Configurazione della consegna in-order o out-of-order dei frame sul software ONTAP"

4. Verificare che lo switch stia utilizzando il metodo di licenza della porta dinamica.
  - a. Eseguire il comando License:

##### **Per Fabric OS 8.2.x e versioni precedenti**

Eseguire il comando `licenseport --show`.

##### **Per Fabric OS 9.0 e versioni successive**

Eseguire il comando `license --show -port`.

```

FC_switch_A_1:admin> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use

```



Le versioni Brocade FabricOS precedenti alla 8.0 eseguono i seguenti comandi come `admin` e le versioni 8.0 e successive come `root`.

- b. Abilitare l'utente `root`.

Se l'utente `root` è già disattivato da Brocade, attivare l'utente `root` come illustrato nell'esempio

seguito:

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

c. Eseguire il comando License:

```
license --show -port
```

```
FC_switch_A_1:root> license --show -port
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Se si utilizza Fabric OS 8.2.x e versioni precedenti, è necessario modificare il metodo di licenza in dinamico:

```
licenseport --method dynamic
```

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

+



In Fabric OS 9.0 e versioni successive, il metodo di licenza è dinamico per impostazione predefinita. Il metodo di licenza statico non è supportato.

5. Abilitare il trap per T11-FC-ZONE-SERVER-MIB per fornire un monitoraggio corretto dello stato degli switch in ONTAP:

a. Abilitare il server DI ZONA T11-FC-MIB:

```
snmpconfig --set mibCapability -mib_name T11-FC-ZONE-SERVER-MIB -bitmask
0x3f
```

b. Attivare il trap T11-FC-ZONE-SERVER-MIB:

```
snmpconfig --enable mibcapability -mib_name SW-MIB -trap_name
swZoneConfigChangeTrap
```

c. Ripetere i passaggi precedenti sul secondo fabric dello switch.

6. **Opzionale:** Se si imposta la stringa di comunità su un valore diverso da "pubblico", è necessario configurare i monitor dello stato di salute ONTAP utilizzando la stringa di comunità specificata:

a. Modificare la stringa di comunità esistente:

```
snmpconfig --set snmpv1
```

- b. Premere **Invio** fino a visualizzare il testo "Community (ro): [Public]".
- c. Immettere la stringa di comunità desiderata.

Su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]      in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_A_1:admin>
```

Su FC\_switch\_B\_1:

```

FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]      in this example it is set to
"mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_B_1:admin>

```

#### 7. Riavviare lo switch:

reboot

Su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> reboot
```

Su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> reboot
```

#### 8. Abilitare costantemente lo switch:

switchcfgpersistenable

Su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> switchcfgpersistenable
```

Su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> switchcfgpersistenable
```

## Configurazione delle impostazioni di base dello switch su uno switch Brocade DCX 8510-8

È necessario configurare le impostazioni globali di base, incluso l'ID di dominio, per gli switch Brocade.

### A proposito di questa attività

È necessario eseguire le operazioni su ogni switch in entrambi i siti MetroCluster. In questa procedura, impostare l'ID di dominio per ogni switch come illustrato negli esempi seguenti:

- FC\_switch\_A\_1 è assegnato all'ID di dominio 5
- FC\_switch\_A\_2 è assegnato all'ID di dominio 6
- FC\_switch\_B\_1 è assegnato all'ID di dominio 7
- FC\_switch\_B\_2 è assegnato all'ID di dominio 8

Nell'esempio precedente, gli ID di dominio 5 e 7 formano Fabric\_1 e gli ID di dominio 6 e 8 formano Fabric\_2.



È inoltre possibile utilizzare questa procedura per configurare gli switch quando si utilizza un solo switch DCX 8510-8 per sito.

Utilizzando questa procedura, è necessario creare due switch logici su ciascuno switch Brocade DCX 8510-8. I due switch logici creati su entrambi gli switch Brocade DCX8510-8 formeranno due fabric logici, come illustrato negli esempi seguenti:

- FABRIC LOGICO 1: Switch 1/Blade1 e Switch 2 Blade 1
- FABRIC LOGICO 2: Switch 1/Blade2 e Switch 2 Blade 2

### Fasi

1. Accedere alla modalità di comando:

```
configure
```

2. Seguire le istruzioni:

- a. Impostare l'ID di dominio dello switch.
- b. Continuare a selezionare **Enter** fino a visualizzare "RDP polling Cycle" (ciclo di polling RDP), quindi impostare il valore su 0 per disattivare il polling.
- c. Selezionare **Invio** fino a quando non si torna al prompt dello switch.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = `5

RDP Polling Cycle(hours) [0 = Disable Polling]: (0..24) [1] 0
`
```

3. Ripetere questi passaggi su tutti gli switch in Fabric\_1 e Fabric\_2.
4. Configurare i fabric virtuali.



a. Abilitare i fabric virtuali sullo switch:

```
fosconfig --enablevf
```

b. Configurare il sistema in modo che utilizzi la stessa configurazione di base su tutti gli switch logici:

```
configurechassis
```

L'esempio seguente mostra l'output per `configurechassis` comando:

```
System (yes, y, no, n): [no] n
cfgload attributes (yes, y, no, n): [no] n
Custom attributes (yes, y, no, n): [no] y
Config Index (0 to ignore): (0..1000) [3]:
```

5. Creare e configurare lo switch logico:

```
scfg --create fabricID
```

6. Aggiungere tutte le porte da un blade al fabric virtuale:

```
lscfg --config fabricID -slot slot -port lowest-port - highest-port
```



I blade che formano un fabric logico (ad esempio Switch 1 Blade 1 e Switch 3 Blade 1) devono avere lo stesso ID fabric.

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

## Informazioni correlate

["Requisiti per l'utilizzo di uno switch Brocade DCX 8510-8"](#)

## Configurazione di e-port su switch FC Brocade mediante porte FC

Per gli switch Brocade su cui i collegamenti Inter-Switch (ISL) sono configurati utilizzando le porte FC, è necessario configurare le porte dello switch su ciascun fabric dello switch che collega l'ISL. Queste porte ISL sono note anche come e-port.

## Prima di iniziare

- Tutti gli ISL in un fabric di switch FC devono essere configurati con la stessa velocità e distanza.
- La combinazione di porta switch e SFP (Small form-factor pluggable) deve supportare la velocità.
- La distanza ISL supportata dipende dal modello di switch FC.

## "Tool di matrice di interoperabilità NetApp"

In IMT, è possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster.

Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

- Il collegamento ISL deve avere un valore lambda dedicato e il collegamento deve essere supportato da Brocade per la distanza, il tipo di switch e il sistema operativo Fabric (FOS).

### A proposito di questa attività

Non utilizzare l'impostazione L0 per l'emissione di `portCfgLongDistance` comando. Utilizzare invece l'impostazione LE o LS per configurare la distanza sugli switch Brocade con un livello minimo di distanza LE.

Non utilizzare l'impostazione LD per l'emissione di `portCfgLongDistance` Comando quando si lavora con apparecchiature xWDM/TDM. Utilizzare invece l'impostazione LE o LS per configurare la distanza sugli switch Brocade.

È necessario eseguire questa attività per ogni fabric di switch FC.

Le seguenti tabelle mostrano le porte ISL per i diversi switch e il diverso numero di ISL in una configurazione che esegue ONTAP 9.1 o 9.2. Gli esempi illustrati in questa sezione si riferiscono a uno switch Brocade 6505. È necessario modificare gli esempi per utilizzare le porte applicabili al proprio tipo di switch.

Se nella configurazione è in esecuzione ONTAP 9.0 o versione precedente, consultare ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#).

È necessario utilizzare il numero richiesto di ISL per la configurazione.

Modello di switch	Porta ISL	Porta dello switch
Brocade 6520	Porta ISL 1	23
	Porta ISL 2	47
	Porta ISL 3	71
	Porta ISL 4	95
Brocade 6505	Porta ISL 1	20
	Porta ISL 2	21
	Porta ISL 3	22
	Porta ISL 4	23

Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
	Porta ISL 2	41
	Porta ISL 3	42
	Porta ISL 4	43
	Porta ISL 5	44
	Porta ISL 6	45
	Porta ISL 7	46
	Porta ISL 8	47
Brocade 7810	Porta ISL 1	ge2 (10 Gbps)
	Porta ISL 2	ge3 (10 Gbps)
	Porta ISL 3	ge4 (10 Gbps)
	Porta ISL 4	Ge5 (10 Gbps)
	Porta ISL 5	Ge6 (10 Gbps)
	Porta ISL 6	Ge7 (10 Gbps)
Brocade 7840 <b>Nota:</b> lo switch Brocade 7840 supporta due porte VE da 40 Gbps o fino a quattro porte VE da 10 Gbps per switch per la creazione di ISL FCIP.	Porta ISL 1	ge0 (40 Gbps) o ge2 (10 Gbps)
	Porta ISL 2	ge1 (40 Gbps) o ge3 (10 Gbps)
	Porta ISL 3	Ge10 (10 Gbps)
	Porta ISL 4	Ge11 (10 Gbps)
Brocade G610	Porta ISL 1	20
	Porta ISL 2	21
	Porta ISL 3	22
	Porta ISL 4	23

BROCADE G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
	Porta ISL 2	41
	Porta ISL 3	42
	Porta ISL 4	43
	Porta ISL 5	44
	Porta ISL 6	45
	Porta ISL 7	46

## Fasi

1. Configura la velocità della porta:

```
portcfgspeed port-numberspeed
```

È necessario utilizzare la massima velocità comune supportata dai componenti del percorso.

Nell'esempio seguente, sono disponibili due ISL per ogni fabric:

```
FC_switch_A_1:admin> portcfgspeed 20 16
FC_switch_A_1:admin> portcfgspeed 21 16

FC_switch_B_1:admin> portcfgspeed 20 16
FC_switch_B_1:admin> portcfgspeed 21 16
```

2. Configurare la modalità trunking per ogni ISL:

```
portcfgtrunkport port-number
```

- Se si configurano gli ISL per il trunking (IOD), impostare portcfgtrunking port-numberport-number su 1 come mostrato nell'esempio seguente:

```
FC_switch_A_1:admin> portcfgtrunkport 20 1
FC_switch_A_1:admin> portcfgtrunkport 21 1
FC_switch_B_1:admin> portcfgtrunkport 20 1
FC_switch_B_1:admin> portcfgtrunkport 21 1
```

- Se non si desidera configurare l'ISL per il trunking (OOD), impostare portcfgtrunkport-number su 0 come mostrato nell'esempio seguente:

```

FC_switch_A_1:admin> portcfgtrunkport 20 0
FC_switch_A_1:admin> portcfgtrunkport 21 0
FC_switch_B_1:admin> portcfgtrunkport 20 0
FC_switch_B_1:admin> portcfgtrunkport 21 0

```

### 3. Abilitare il traffico QoS per ciascuna porta ISL:

```
portcfgqos --enable port-number
```

Nell'esempio seguente, sono disponibili due ISL per fabric dello switch:

```

FC_switch_A_1:admin> portcfgqos --enable 20
FC_switch_A_1:admin> portcfgqos --enable 21

FC_switch_B_1:admin> portcfgqos --enable 20
FC_switch_B_1:admin> portcfgqos --enable 21

```

### 4. Verificare le impostazioni:

```
portCfgShow command
```

Nell'esempio seguente viene illustrato l'output di una configurazione che utilizza due ISL collegati alla porta 20 e alla porta 21. L'impostazione della porta trunk deve essere ON per IOD e OFF per OOD:

Ports of Slot	0	12	13	14	15	16	17	18	19	20	21	22	23	24
Speed	AN	AN	AN	AN	AN	AN	AN	8G	AN	AN	AN	16G	16G	
Fill Word	0	0	0	0	0	0	0	3	0	0	0	3	3	3
AL_PA Offset 13	..	..	..	..	..	..	..	..	..	..	..	..	..	..
Trunk Port	..	..	..	..	..	..	..	..	..	ON	ON	..	..	..
Long Distance	..	..	..	..	..	..	..	..	..	..	..	..	..	..
VC Link Init	..	..	..	..	..	..	..	..	..	..	..	..	..	..
Locked L_Port	..	..	..	..	..	..	..	..	..	..	..	..	..	..
Locked G_Port	..	..	..	..	..	..	..	..	..	..	..	..	..	..
Disabled E_Port	..	..	..	..	..	..	..	..	..	..	..	..	..	..

```

.. .. ..
Locked E_Port      .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
ISL R_RDY Mode     .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
RSCN Suppressed    .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
Persistent Disable.. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
LOS TOV enable     .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
NPIV capability    ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON
ON  ON  ON  ON
NPIV PP Limit      126 126 126 126 126 126 126 126 126 126 126 126
126 126 126 126
QOS E_Port         AE  AE  AE  AE  AE  AE  AE  AE  AE  AE  AE  AE  AE
AE  AE  AE  AE
Mirror Port        .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
Rate Limit         .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
Credit Recovery    ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON  ON
ON  ON  ON  ON
Fport Buffers      .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
Port Auto Disable  .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..
CSCTL mode         .. .. .. .. .. .. .. .. .. .. .. ..
.. .. .. ..

Fault Delay        0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0

```

## 5. Calcolare la distanza ISL.

A causa del comportamento di FC-VI, la distanza deve essere impostata su 1.5 volte la distanza reale con una distanza minima di 10 km (utilizzando il livello DI distanza LE).

La distanza per l'ISL viene calcolata come segue, arrotondata al chilometro completo successivo:

$$1.5 \times \text{real\_distance} = \text{distanza}$$

Se la distanza è di 3 km, allora  $1.5 \times 3 \text{ km} = 4.5 \text{ km}$  Si tratta di una distanza inferiore a 10 km, pertanto l'ISL deve essere impostato sul livello DI distanza LE.

Se la distanza è di 20 km, allora  $1.5 \times 20 \text{ km} = 30 \text{ km}$  L'ISL deve essere impostato su 30 km e deve utilizzare il livello di distanza LS.

## 6. Impostare la distanza su ciascuna porta ISL:

```
portcfglongdistance portdistance-level vc_link_init distance
```

R `vc_link_init` valore di 1 Utilizza la parola di riempimento ARB (impostazione predefinita). Un valore di 0 Utilizza i DATI INATTIVI. Il valore richiesto potrebbe dipendere dal collegamento utilizzato. I comandi devono essere ripetuti per ogni porta ISL.

Per una distanza ISL di 3 km, come indicato nell'esempio della fase precedente, l'impostazione predefinita è 4.5 km `vc_link_init` valore di 1. Poiché un'impostazione di 4.5 km è inferiore a 10 km, la porta deve essere impostata sul livello DI distanza LE:

```
FC_switch_A_1:admin> portcfglongdistance 20 LE 1

FC_switch_B_1:admin> portcfglongdistance 20 LE 1
```

Per una distanza ISL di 20 km, come indicato nell'esempio della fase precedente, l'impostazione è 30 km con il valore predefinito `vc_link_init` di 1:

```
FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30

FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30
```

#### 7. Verificare l'impostazione della distanza:

```
portbuffershow
```

Un livello di distanza di LE appare come 10 km

L'esempio seguente mostra l'output per una configurazione che utilizza gli ISL sulla porta 20 e sulla porta 21:

```
FC_switch_A_1:admin> portbuffershow
```

User Port	Port Type	Lx Mode	Max/Resv Buffers	Buffer Usage	Needed Buffers	Link Distance	Remaining Buffers
----	----	----	-----	-----	-----	-----	-----
...							
20	E	-	8	67	67	30km	
21	E	-	8	67	67	30km	
...							
23		-	8	0	-	-	466

#### 8. Verificare che entrambi gli switch formino un unico fabric:

```
switchshow
```

L'esempio seguente mostra l'output per una configurazione che utilizza gli ISL sulla porta 20 e sulla porta 21:

```

FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:      5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:      OFF
switchBeacon: OFF

Index Port Address Media Speed State  Proto
=====
...
20   20  010C00   id    16G  Online FC   LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream) (trunk master)
21   21  010D00   id    16G  Online FC   LE E-Port  (Trunk port, master
is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:      7
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:      OFF
switchBeacon: OFF

Index Port Address Media Speed State  Proto
=====
...
20   20  030C00   id    16G  Online FC   LE E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream) (Trunk master)
21   21  030D00   id    16G  Online FC   LE E-Port  (Trunk port, master
is Port 20)
...

```

## 9. Confermare la configurazione dei fabric:

```

fabricshow

```



```

FC_switch_A_1:admin> fabricshow
  Switch ID      Worldwide Name      Enet IP Addr FC IP Addr Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"

```

```

FC_switch_B_1:admin> fabricshow
  Switch ID      Worldwide Name      Enet IP Addr FC IP Addr      Name
-----
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"

3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"

```

## 10. Conferma del trunking degli ISL:

trunkshow

- Se si configurano gli ISL per il trunking (IOD), l'output dovrebbe essere simile a quanto segue:

```

FC_switch_A_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
FC_switch_B_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16

```

- Se non si configurano gli ISL per il trunking (OOD), l'output dovrebbe essere simile a quanto segue:

```

FC_switch_A_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER
FC_switch_B_1:admin> trunkshow
1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER

```

## 11. Ripetere [Fase 1](#) attraverso [Fase 10](#) Per il secondo fabric switch FC.

### Informazioni correlate

["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)

## Configurazione delle porte VE a 10 Gbps sugli switch Brocade FC 7840

Quando si utilizzano le porte VE a 10 Gbps (che utilizzano FCIP) per gli ISL, è necessario creare interfacce IP su ciascuna porta e configurare i tunnel e i circuiti FCIP in ciascun tunnel.

### A proposito di questa attività

Questa procedura deve essere eseguita su ciascun fabric switch nella configurazione MetroCluster.

Gli esempi di questa procedura presuppongono che i due switch Brocade 7840 abbiano i seguenti indirizzi IP:

- FC\_switch\_A\_1 è locale.
- FC\_switch\_B\_1 è remoto.

### Fasi

1. Creare indirizzi di interfaccia IP (ipif) per le porte da 10 Gbps su entrambi gli switch del fabric:

```
portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_IP_address
netmask netmask_number vlan 2 mtu auto
```

Il seguente comando crea gli indirizzi ipif sulle porte ge2.dp0 e ge3.dp0 di FC\_switch\_A\_1:

```
portcfg ipif ge2.dp0 create 10.10.20.71 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif ge3.dp0 create 10.10.21.71 netmask 255.255.0.0 vlan 2 mtu
auto
```

Il seguente comando crea gli indirizzi ipif sulle porte ge2.dp0 e ge3.dp0 di FC\_switch\_B\_1:

```
portcfg ipif ge2.dp0 create 10.10.20.72 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif ge3.dp0 create 10.10.21.72 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. Verificare che gli indirizzi ipif siano stati creati correttamente su entrambi gli switch:

```
portshow ipif all
```

Il seguente comando mostra gli indirizzi ipif sullo switch FC\_switch\_A\_1:

```
FC_switch_A_1:root> portshow ipif all
```

Port	IP Address	/ Pfx	MTU	VLAN	Flags
-----					
ge2.dp0	10.10.20.71	/ 24	AUTO	2	U R M I
ge3.dp0	10.10.21.71	/ 20	AUTO	2	U R M I
-----					
-----					
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running					
I=InUse					
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport					

Il seguente comando mostra gli indirizzi ipif sullo switch FC\_switch\_B\_1:

```
FC_switch_B_1:root> portshow ipif all
```

Port	IP Address	/ Pfx	MTU	VLAN	Flags
-----					
ge2.dp0	10.10.20.72	/ 24	AUTO	2	U R M I
ge3.dp0	10.10.21.72	/ 20	AUTO	2	U R M I
-----					
-----					
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running					
I=InUse					
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport					

3. Creare il primo dei due tunnel FCIP utilizzando le porte su dp0:

```
portcfg fciptunnel
```

Questo comando crea un tunnel con un singolo circuito.

Il seguente comando crea il tunnel sullo switch FC\_switch\_A\_1:

```
portcfg fciptunnel 24 create -S 10.10.20.71 -D 10.10.20.72 -b 10000000  
-B 10000000
```

Il seguente comando crea il tunnel sullo switch FC\_switch\_B\_1:

```
portcfg fciptunnel 24 create -S 10.10.20.72 -D 10.10.20.71 -b 10000000  
-B 10000000
```

4. Verificare che i tunnel FCIP siano stati creati correttamente:

```
portshow fcip tunnel all
```

L'esempio seguente mostra che i tunnel sono stati creati e i circuiti sono attivi:

```
FC_switch_B_1:root>

  Tunnel Circuit  OpStatus  Flags      Uptime  TxMBps  RxMBps  ConnCnt
CommRt Met/G
-----
-----
  24    -          Up      -----    2d8m    0.05    0.41    3        -
-
-----
-----
  Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                  a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                  I=IP-Ext
```

5. Creare un circuito aggiuntivo per dp0.

Il seguente comando crea un circuito sull'interruttore FC\_switch\_A\_1 per dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72 --min
-comm-rate 5000000 --max-comm-rate 5000000
```

Il seguente comando crea un circuito sull'interruttore FC\_switch\_B\_1 per dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71 --min
-comm-rate 5000000 --max-comm-rate 5000000
```

6. Verificare che tutti i circuiti siano stati creati correttamente:

```
portshow fcipcircuit all
```

Il seguente comando indica i circuiti e il loro stato:

```
FC_switch_A_1:root> portshow fcipcircuit all
```

Tunnel	Circuit	OpStatus	Flags	Uptime	TxMBps	RxMBps	ConnCnt
CommRt	Met/G						
-----							
24	0 ge2	Up	---va---4	2d12m	0.02	0.03	3
10000/10000 0/-							
24	1 ge3	Up	---va---4	2d12m	0.02	0.04	3
10000/10000 0/-							
-----							
-----							
Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4							
6=IPv6							
ARL a=Auto r=Reset s=StepDown t=TimedStepDown S=SLA							

### Configurazione di porte VE a 40 Gbps su switch FC Brocade 7810 e 7840

Quando si utilizzano le due porte 40 GbE VE (che utilizzano FCIP) per gli ISL, è necessario creare interfacce IP su ciascuna porta e configurare i tunnel e i circuiti FCIP in ciascun tunnel.

#### A proposito di questa attività

Questa procedura deve essere eseguita su ciascun fabric switch nella configurazione MetroCluster.

Gli esempi di questa procedura utilizzano due switch:

- FC\_switch\_A\_1 è locale.
- FC\_switch\_B\_1 è remoto.

#### Fasi

1. Creare indirizzi di interfaccia IP (ipif) per le porte da 40 Gbps su entrambi gli switch del fabric:

```
portcfg ipif FC_switch_namefirst_port_name create FC_switch_IP_address netmask  
netmask_number vlan 2 mtu auto
```

Il seguente comando crea gli indirizzi ipif sulle porte ge0.dp0 e ge1.dp0 di FC\_switch\_A\_1:

```
portcfg ipif ge0.dp0 create 10.10.82.10 netmask 255.255.0.0 vlan 2 mtu  
auto  
portcfg ipif ge1.dp0 create 10.10.82.11 netmask 255.255.0.0 vlan 2 mtu  
auto
```

Il seguente comando crea gli indirizzi ipif sulle porte ge0.dp0 e ge1.dp0 di FC\_switch\_B\_1:

```
portcfg ipif ge0.dp0 create 10.10.83.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif ge1.dp0 create 10.10.83.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. Verificare che gli indirizzi ipif siano stati creati correttamente su entrambi gli switch:

```
portshow ipif all
```

L'esempio seguente mostra le interfacce IP su FC\_switch\_A\_1:

Port	IP Address	/ Pfx	MTU	VLAN	Flags
ge0.dp0	10.10.82.10	/ 16	AUTO	2	U R M
ge1.dp0	10.10.82.11	/ 16	AUTO	2	U R M

Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running  
I=InUse  
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport

L'esempio seguente mostra le interfacce IP su FC\_switch\_B\_1:

Port	IP Address	/ Pfx	MTU	VLAN	Flags
ge0.dp0	10.10.83.10	/ 16	AUTO	2	U R M
ge1.dp0	10.10.83.11	/ 16	AUTO	2	U R M

Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running  
I=InUse  
N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport

3. Creare il tunnel FCIP su entrambi gli switch:

```
portcfg fciptunnel
```

Il seguente comando crea il tunnel su FC\_switch\_A\_1:

```
portcfg fciptunnel 24 create -S 10.10.82.10 -D 10.10.83.10 -b 10000000  
-B 10000000
```

Il seguente comando crea il tunnel su FC\_switch\_B\_1:

```
portcfg fciptunnel 24 create -S 10.10.83.10 -D 10.10.82.10 -b 10000000  
-B 10000000
```

#### 4. Verificare che il tunnel FCIP sia stato creato correttamente:

```
portshow fciptunnel all
```

L'esempio seguente mostra che il tunnel è stato creato e i circuiti sono attivi:

```
FC_switch_A_1:root>  
  
Tunnel Circuit OpStatus  Flags      Uptime  TxMBps  RxMBps ConnCnt  
CommRt Met/G  
-----  
-----  
24      -      Up      -----      2d8m    0.05    0.41    3      -  
-  
-----  
-----  
Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON  
r=ReservedBW  
                a=FastDeflate d=Deflate D=AggrDeflate P=Protocol  
                I=IP-Ext
```

#### 5. Creare un circuito aggiuntivo su ciascun interruttore:

```
portcfg fcipcircuit 24 create 1 -S source-IP-address -D destination-IP-address  
--min-comm-rate 10000000 --max-comm-rate 10000000
```

Il seguente comando crea un circuito sull'interruttore FC\_switch\_A\_1 per dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.82.11 -D 10.10.83.11 --min  
-comm-rate 10000000 --max-comm-rate 10000000
```

Il seguente comando crea un circuito sullo switch FC\_switch\_B\_1 per dp1:

```
portcfg fcipcircuit 24 create 1 -S 10.10.83.11 -D 10.10.82.11 --min
-comm-rate 10000000 --max-comm-rate 10000000
```

6. Verificare che tutti i circuiti siano stati creati correttamente:

```
portshow fcipcircuit all
```

L'esempio seguente elenca i circuiti e mostra che il relativo OpStatus è attivo:

```
FC_switch_A_1:root> portshow fcipcircuit all

Tunnel Circuit  OpStatus  Flags      Uptime    TxMBps    RxMBps    ConnCnt
CommRt Met/G
-----
-----
 24      0 ge0      Up        ---va---4   2d12m     0.02      0.03      3
10000/10000 0/-
 24      1 ge1      Up        ---va---4   2d12m     0.02      0.04      3
10000/10000 0/-
-----
-----
Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                    ARL a=Auto r=Reset s=StepDown t=TimedStepDown S=SLA
```

### Configurazione delle porte non-e sullo switch Brocade

È necessario configurare le porte non-e sullo switch FC. In una configurazione MetroCluster, si tratta delle porte che collegano lo switch agli iniziatori HBA, alle interconnessioni FC-VI e ai bridge FC-SAS. Questi passaggi devono essere eseguiti per ciascuna porta.

#### A proposito di questa attività

Nell'esempio seguente, le porte collegano un bridge FC-SAS:

- Porta 6 su FC\_FC\_switch\_A\_1 nel sito\_A.
- Porta 6 su FC\_FC\_switch\_B\_1 nel sito\_B.

#### Fasi

1. Configurare la velocità della porta per ciascuna porta non-e:

```
portcfgspeed portspeed
```

Si consiglia di utilizzare la velocità comune più elevata, che è la velocità massima supportata da tutti i componenti del percorso dati: Il modulo SFP, la porta dello switch su cui è installato il modulo SFP e il dispositivo collegato (HBA, bridge e così via).

Ad esempio, i componenti potrebbero avere le seguenti velocità supportate:



- Il modulo SFP è in grado di supportare 4, 8 o 16 GB.
- La porta dello switch supporta 4, 8 o 16 GB.
- La velocità massima dell'HBA collegato è di 16 GB. In questo caso, la velocità comune più elevata è di 16 GB, pertanto la porta deve essere configurata per una velocità di 16 GB.

```
FC_switch_A_1:admin> portcfgspeed 6 16
```

```
FC_switch_B_1:admin> portcfgspeed 6 16
```

## 2. Verificare le impostazioni:

```
portcfgshow
```

```
FC_switch_A_1:admin> portcfgshow
```

```
FC_switch_B_1:admin> portcfgshow
```

Nell'output di esempio, la porta 6 ha le seguenti impostazioni; la velocità è impostata su 16G:

Ports of Slot 0	0	1	2	3	4	5	6	7	8
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----									
Speed	16G	16G	16G	16G	16G	16G	16G	16G	16G
AL_PA Offset 13	..	..	..	..	..	..	..	..	..
Trunk Port	..	..	..	..	..	..	..	..	..
Long Distance	..	..	..	..	..	..	..	..	..
VC Link Init	..	..	..	..	..	..	..	..	..
Locked L_Port	-	-	-	-	-	-	-	-	-
Locked G_Port	..	..	..	..	..	..	..	..	..
Disabled E_Port	..	..	..	..	..	..	..	..	..
Locked E_Port	..	..	..	..	..	..	..	..	..
ISL R_RDY Mode	..	..	..	..	..	..	..	..	..
RSCN Suppressed	..	..	..	..	..	..	..	..	..
Persistent Disable	..	..	..	..	..	..	..	..	..
LOS TOV enable	..	..	..	..	..	..	..	..	..
NPIV capability	ON	ON	ON	ON	ON	ON	ON	ON	ON
NPIV PP Limit	126	126	126	126	126	126	126	126	126
QOS Port	AE	AE	AE	AE	AE	AE	AE	AE	ON
EX Port	..	..	..	..	..	..	..	..	..
Mirror Port	..	..	..	..	..	..	..	..	..
Rate Limit	..	..	..	..	..	..	..	..	..
Credit Recovery	ON	ON	ON	ON	ON	ON	ON	ON	ON
Fport Buffers	..	..	..	..	..	..	..	..	..
Eport Credits	..	..	..	..	..	..	..	..	..
Port Auto Disable	..	..	..	..	..	..	..	..	..
CSCTL mode	..	..	..	..	..	..	..	..	..
D-Port mode	..	..	..	..	..	..	..	..	..
D-Port over DWDM	..	..	..	..	..	..	..	..	..
FEC	ON	ON	ON	ON	ON	ON	ON	ON	ON
Fault Delay	0	0	0	0	0	0	0	0	0
Non-DFE	..	..	..	..	..	..	..	..	..

### Configurazione della compressione sulle porte ISL su uno switch Brocade G620

Se si utilizzano switch Brocade G620 e si attiva la compressione sugli ISL, è necessario configurarla su ogni e-port sugli switch.

#### A proposito di questa attività

Questa attività deve essere eseguita sulle porte ISL di entrambi gli switch che utilizzano l'ISL.

#### Fasi

1. Disattivare la porta su cui si desidera configurare la compressione:

```
portdisable port-id
```

2. Abilitare la compressione sulla porta:

```
portCfgCompress --enable port-id
```

3. Abilitare la porta per attivare la configurazione con compressione:

```
portenable port-id
```

4. Verificare che l'impostazione sia stata modificata:

```
portcfgshow port-id
```

Nell'esempio seguente viene attivata la compressione sulla porta 0.

```
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

È possibile utilizzare il comando `islshow` per verificare che `e_port` sia online con crittografia o compressione configurata e attiva.

```
FC_switch_A_1:admin> islshow
1: 0-> 0 10:00:c4:f5:7c:8b:29:86    5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

È possibile utilizzare il comando `portEncCompShow` per visualizzare le porte attive. In questo esempio è possibile vedere che crittografia e compressione sono configurate e attive sulla porta 0.

```
FC_switch_A_1:admin> portenccompshow
```

User	Encryption		Compression		Speed	Config
Port	Configured	Active	Configured	Active		
----	-----	-----	-----	-----	-----	
0	Yes	Yes	Yes	Yes		16G

### Configurazione dello zoning sugli switch Brocade FC

È necessario assegnare le porte dello switch per separare le zone per separare il traffico del controller e dello storage.

## Zoning per porte FC-VI

Per ciascun gruppo di DR in MetroCluster, è necessario configurare due zone per le connessioni FC-VI che consentono il traffico controller-controller. Queste zone contengono le porte dello switch FC che si collegano alle porte FC-VI del modulo controller. Queste zone sono zone di qualità del servizio (QoS).

Il nome di una zona QoS inizia con il prefisso QOSHid\_, seguito da una stringa definita dall'utente per differenziarla da una zona normale. Queste zone QoS sono le stesse indipendentemente dal modello di bridge FibreBridge utilizzato.

Ciascuna zona contiene tutte le porte FC-VI, una per ogni cavo FC-VI di ciascun controller. Queste zone sono configurate per la priorità alta.

Le seguenti tabelle mostrano le zone FC-VI per due gruppi DR.

### DR group 1: Zona QOSH1 FC-VI per porta FC-VI a / c

Switch FC	Sito	Dominio dello switch	porta 6505 / 6510	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	0	0	0	Porta controller_A_1 FC-VI a
Switch_FC_A_1	R	5	1	1	1	Porta controller_A_1 FC-VI c
Switch_FC_A_1	R	5	4	4	4	Porta controller_A_2 FC-VI a
Switch_FC_A_1	R	5	5	5	5	Porta controller_A_2 FC-VI c
Switch_FC_B_1	B	7	0	0	0	Porta controller_B_1 FC-VI a
Switch_FC_B_1	B	7	1	1	1	Porta controller_B_1 FC-VI c
Switch_FC_B_1	B	7	4	4	4	Porta controller_B_2 FC-VI a
Switch_FC_B_1	B	7	5	5	5	Porta controller_B_2 FC-VI c

Zona nel fabric_1	Porte dei membri
QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5

### DR group 1: Zona QOSH1 FC-VI per porta FC-VI b / d

Switch FC	Sito	Dominio dello switch	porta 6505 / 6510	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	0	0	0	Porta controller_A_1 FC-VI b
			1	1	1	Porta controller_A_1 FC-VI d
			4	4	4	Porta controller_A_2 FC-VI b
			5	5	5	Porta controller_A_2 FC-VI d
Switch_FC_B_2	B	8	0	0	0	Porta controller_B_1 FC-VI b
			1	1	1	Porta controller_B_1 FC-VI d
			4	4	4	Porta controller_B_2 FC-VI b
			5	5	5	Porta controller_B_2 FC-VI d

Zona nel fabric_1	Porte dei membri
QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5

#### DR group 2: Zona QOSH2 FC-VI per porta FC-VI a / c

Switch FC	Sito	Dominio dello switch	Porta dello switch			Si connette a...
			6510	6520	G620	
Switch_FC_A_1	R	5	24	48	18	Porta controller_A_3 FC-VI a
			25	49	19	Porta controller_A_3 FC-VI c
			28	52	22	Porta controller_A_4 FC-VI a

Switch FC	Sito	Dominio dello switch	Porta dello switch			Si connette a...
			29	53	23	Porta controller_A_4 FC-VI c
Switch_FC_B_1	B	7	24	48	18	Porta controller_B_3 FC-VI a
			25	49	19	Porta controller_B_3 FC-VI c
			28	52	22	Porta controller_B_4 FC-VI a
			29	53	23	Porta controller_B_4 FC-VI c

Zona nel fabric_1	Porte dei membri
QOSH2_MC2_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
QOSH2_MC2_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

#### DR group 2: Zona QOSH2 FC-VI per porta FC-VI b / d

Switch FC	Sito	Dominio dello switch	porta 6510	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	24	48	18	Porta controller_A_3 FC-VI b
Switch_FC_A_2	R	6	25	49	19	Porta controller_A_3 FC-VI d
Switch_FC_A_2	R	6	28	52	22	Porta controller_A_4 FC-VI b
Switch_FC_A_2	R	6	29	53	23	Porta controller_A_4 FC-VI d
Switch_FC_B_2	B	8	24	48	18	Porta controller_B_3 FC-VI b
Switch_FC_B_2	B	8	25	49	19	Porta controller_B_3 FC-VI d

Switch FC	Sito	Dominio dello switch	porta 6510	porta 6520	Porta G620	Si connette a...
Switch_FC_B_2	B	8	28	52	22	Porta controller_B_4 FC-VI b
Switch_FC_B_2	B	8	29	53	23	Porta controller_B_4 FC-VI d

Zona nel fabric_2	Porte dei membri
QOSH2_MC2_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
QOSH2_MC2_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

La seguente tabella fornisce un riepilogo delle zone FC-VI:

Fabric	Nome della zona	Porte dei membri
FC_switch_A_1 e FC_switch_B_1	QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
	QOSH2_MC1_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
	QOSH2_MC1_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53
FC_switch_A_2 e FC_switch_B_2	QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
	QOSH2_MC1_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
	QOSH2_MC1_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

### Zoning per i bridge 7500N o 7600N di FibreBridge attraverso una porta FC

Se si utilizzano bridge FibreBridge 7500N o 7600N che utilizzano solo una delle due porte FC, è necessario creare zone di archiviazione per le porte bridge. Prima di configurare le zone, è necessario conoscere le zone e le porte associate.

Gli esempi mostrano lo zoning solo per il gruppo DR 1. Se la configurazione include un secondo gruppo DR, configurare lo zoning per il secondo gruppo DR nello stesso modo, utilizzando le porte corrispondenti dei controller e dei bridge.

#### Zone richieste

È necessario configurare una zona per ciascuna delle porte FC del bridge FC-SAS che consente il traffico tra gli iniziatori di ciascun modulo controller e il bridge FC-SAS.

Ciascuna zona di storage contiene nove porte:

- Otto porte HBA Initiator (due connessioni per ciascun controller)
- Una porta per il collegamento a una porta FC bridge FC-SAS

Le zone di storage utilizzano lo zoning standard.

Gli esempi mostrano due coppie di bridge che collegano due gruppi di stack in ciascun sito. Poiché ogni bridge utilizza una porta FC, vi sono un totale di quattro zone di storage per fabric (otto in totale).

## Naming del bridge

I bridge utilizzano il seguente esempio di denominazione: bridge\_Site\_stack grouplocation in coppia

Questa parte del nome...	Identifica...	Valori possibili...
sito	Sito in cui risiede fisicamente la coppia di bridge.	A o B.
gruppo di stack	Numero del gruppo di stack a cui si connette la coppia di bridge.  I bridge FibreBridge 7600N o 7500N supportano fino a quattro stack nel gruppo di stack.  Il gruppo di stack non può contenere più di 10 shelf di storage.	1, 2, ecc.
posizione in coppia	Bridge all'interno della coppia di bridge. Una coppia di bridge si connette a uno specifico gruppo di stack.	a o b

Esempi di nomi di bridge per un gruppo di stack su ciascun sito:

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

**Gruppo DR 1 - Stack 1 presso il sito\_A.**

**DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1:**



Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	5	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	7	Porta controller_A_2 0c
Switch_FC_A_1	R	5	8	bridge_A_1a FC1
Switch_FC_B_1	B	7	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	6	Porta controller_B_2 0a
Switch_FC_B_1	B	7	7	Porta controller_B_2 0c

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_BOT\_FC1:

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	6	2	Porta controller_A_1 0b
Switch_FC_A_1	R	6	3	Porta controller_A_1 0d
Switch_FC_A_1	R	6	6	Porta controller_A_2 0b
Switch_FC_A_1	R	6	7	Porta controller_A_2 0d
Switch_FC_A_1	R	6	8	bridge_A_1b FC1
Switch_FC_B_1	B	8	2	Porta controller_B_1 0b

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_B_1	B	8	3	Porta controller_B_1 0d
Switch_FC_B_1	B	8	6	Porta controller_B_2 0b
Switch_FC_B_1	B	8	7	Porta controller_B_2 0d

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8

### Gruppo DR 1 - Stack 2 presso il sito\_A.

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	5	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	7	Porta controller_A_2 0c
Switch_FC_A_1	R	5	9	bridge_A_2a FC1
Switch_FC_B_1	B	7	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	6	Porta controller_B_2 0a
Switch_FC_B_1	B	7	7	Porta controller_B_2 0c

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_BOT\_FC1:

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	6	2	Porta controller_A_1 0b
Switch_FC_A_1	R	6	3	Porta controller_A_1 0d
Switch_FC_A_1	R	6	6	Porta controller_A_2 0b
Switch_FC_A_1	R	6	7	Porta controller_A_2 0d
Switch_FC_A_1	R	6	9	bridge_A_2b FC1
Switch_FC_B_1	B	8	2	Porta controller_B_1 0b
Switch_FC_B_1	B	8	3	Porta controller_B_1 0d
Switch_FC_B_1	B	8	6	Porta controller_B_2 0b
Switch_FC_B_1	B	8	7	Porta controller_B_2 0d

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9

#### Gruppo DR 1 - Stack 1 presso il sito\_B.

#### MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	5	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	7	Porta controller_A_2 0c
Switch_FC_B_1	B	7	2	Porta controller_B_1 0a

Switch FC	Sito	Dominio dello switch	Switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_B_1	B	7	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	6	Porta controller_B_2 0a
Switch_FC_B_1	B	7	7	Porta controller_B_2 0c
Switch_FC_B_1	B	7	8	bridge_B_1a FC1

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_BOT\_FC1:

Switch FC	Sito	Dominio dello switch	Switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	6	2	Porta controller_A_1 0b
Switch_FC_A_1	R	6	3	Porta controller_A_1 0d
Switch_FC_A_1	R	6	6	Porta controller_A_2 0b
Switch_FC_A_1	R	6	7	Porta controller_A_2 0d
Switch_FC_B_1	B	8	2	Porta controller_B_1 0b
Switch_FC_B_1	B	8	3	Porta controller_B_1 0d
Switch_FC_B_1	B	8	6	Porta controller_B_2 0b
Switch_FC_B_1	B	8	7	Porta controller_B_2 0d
Switch_FC_B_1	B	8	8	bridge_B_1b FC1

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8

#### Gruppo DR 1 - Stack 2 presso il sito\_B.

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	5	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	7	Porta controller_A_2 0c
Switch_FC_B_1	B	7	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	6	Porta controller_B_2 0a
Switch_FC_B_1	B	7	7	Porta controller_B_2 0c
Switch_FC_B_1	B	7	9	bridge_b_2a FC1

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_BOT\_FC1:

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_A_1	R	6	2	Porta controller_A_1 0b
Switch_FC_A_1	R	6	3	Porta controller_A_1 0d
Switch_FC_A_1	R	6	6	Porta controller_A_2 0b
Switch_FC_A_1	R	6	7	Porta controller_A_2 0d
Switch_FC_B_1	B	8	2	Porta controller_B_1 0b
Switch_FC_B_1	B	8	3	Porta controller_B_1 0d

Switch FC	Sito	Dominio dello switch	Porta switch Brocade 6505, 6510, 6520, G620 o G610	Si connette a...
Switch_FC_B_1	B	8	6	Porta controller_B_2 0b
Switch_FC_B_1	B	8	7	Porta controller_B_2 0d
Switch_FC_B_1	B	8	9	bridge_B_1b FC1

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

### Riepilogo delle zone di storage

Fabric	Nome della zona	Porte dei membri
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

### Zoning per i bridge FibreBridge 7500N che utilizzano entrambe le porte FC

Se si utilizzano bridge FibreBridge 7500N con entrambe le porte FC, è necessario creare zone di storage per le porte bridge. Prima di configurare le zone, è necessario conoscere le zone e le porte associate.

#### Zone richieste

È necessario configurare una zona per ciascuna delle porte FC del bridge FC-SAS che consente il traffico tra gli iniziatori di ciascun modulo controller e il bridge FC-SAS.

Ciascuna zona di storage contiene cinque porte:

- Quattro porte HBA Initiator (una connessione per ciascun controller)
- Una porta per il collegamento a una porta FC bridge FC-SAS

Le zone di storage utilizzano lo zoning standard.

Gli esempi mostrano due coppie di bridge che collegano due gruppi di stack in ciascun sito. Poiché ciascun bridge utilizza una porta FC, sono disponibili otto zone di storage per fabric (sedici in totale).

## Naming del bridge

I bridge utilizzano il seguente esempio di denominazione: bridge\_Site\_stack grouplocation in coppia

Questa parte del nome...	Identifica...	Valori possibili...
sito	Sito in cui risiede fisicamente la coppia di bridge.	A o B.
gruppo di stack	Numero del gruppo di stack a cui si connette la coppia di bridge.  I bridge FibreBridge 7600N o 7500N supportano fino a quattro stack nel gruppo di stack.  Il gruppo di stack non può contenere più di 10 shelf di storage.	1, 2, ecc.
posizione in coppia	Bridge all'interno della coppia di bridge. Una coppia di bridge si connette a un gruppo di stack specifico.	a o b

Esempi di nomi di bridge per un gruppo di stack su ciascun sito:

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

## Gruppo DR 1 - Stack 1 presso il sito\_A.

### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610/ G620	porta 6520	Si connette a...
-----------	------	----------------------	--------------------------------	------------	------------------

Switch_FC_A_1	R	5	2	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	6	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	8	8	bridge_A_1a FC1
Switch_FC_B_1	B	7	2	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	6	6	Porta controller_B_2 0a

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	3	3	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	7	7	7	Porta controller_A_2 0c
Switch_FC_A_1	R	5	9	9	9	bridge_A_1b FC1
Switch_FC_B_1	B	7	3	3	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	7	7	7	Porta controller_B_2 0c

Zona nel fabric_2	Porte dei membri
-------------------	------------------



MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
---	---------------------

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_BOT\_FC1:

Switch FC	Sito	Dominio dello switch	6505 / 6510 / G610	6520	G620	Si connette a...
Switch_FC_A_2	R	6	2	2	2	Porta controller_A_1 0b
Switch_FC_A_2	R	6	6	6	6	Porta controller_A_2 0b
Switch_FC_A_2	R	6	8	8	8	bridge_A_1a FC2
Switch_FC_B_2	B	8	2	2	2	Porta controller_B_1 0b
Switch_FC_B_2	B	8	6	6	6	Porta controller_B_2 0b

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_1\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	6505 / 6510 / G610	6520	G620	Si connette a...
Switch_FC_A_2	R	6	3	3	3	Porta controller_A_1 0d
Switch_FC_A_2	R	6	7	7	7	Porta controller_A_2 0d
Switch_FC_A_2	R	6	9	9	9	bridge_A_1b FC2

Switch_FC_B_2	B	8	3	3	3	Porta controller_B_1 0d
Switch_FC_B_2	B	8	7	7	7	Porta controller_B_2 0d

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9

### Gruppo DR 1 - Stack 2 presso il sito\_A.

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	2	2	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	6	6	6	Porta controller_A_2 0a
Switch_FC_A_1	R	5	10	10	10	bridge_A_2a FC1
Switch_FC_B_1	B	7	2	2	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	6	6	6	Porta controller_B_2 0a

Zona in fabric_1 hh	Porte dei membri
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_2\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
-----------	------	----------------------	--------------------------	------------	------------	------------------

Switch_FC_A_1	R	5	3	3	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	7	7	7	Porta controller_A_2 0c
Switch_FC_A_1	R	5	11	11	11	bridge_A_2b FC1
Switch_FC_B_1	B	7	3	3	3	Porta controller_B_1 0c
Switch_FC_B_1	B	7	7	7	7	Porta controller_B_2 0c

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_2\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	2	0	0	Porta controller_A_1 0b
Switch_FC_A_2	R	6	6	4	4	Porta controller_A_2 0b
Switch_FC_A_2	R	6	10	10	10	bridge_A_2a FC2
Switch_FC_B_2	B	8	2	2	2	Porta controller_B_1 0b
Switch_FC_B_2	B	8	6	6	6	Porta controller_B_2 0b

Zona nel fabric_1	Porte dei membri
-------------------	------------------

MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10
---	----------------------

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_A\_STK\_GRP\_2\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	3	3	3	Porta controller_A_1 0d
Switch_FC_A_2	R	6	7	7	7	Porta controller_A_2 0d
Switch_FC_A_2	R	6	11	11	11	bridge_A_2b FC2
Switch_FC_B_2	B	8	3	3	3	Porta controller_B_1 0d
Switch_FC_B_2	B	8	7	7	7	Porta controller_B_2 0d

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11

#### Gruppo DR 1 - Stack 1 presso il sito\_B.

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	2	2	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	6	6	6	Porta controller_A_2 0a
Switch_FC_B_1	B	7	2	2	8	Porta controller_B_1 0a

Switch_FC_B_1	B	7	6	6	2	Porta controller_B_2 0a
Switch_FC_B_1	B	7	8	8	6	bridge_B_1a FC1

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_1\_TOP\_FC1:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	3	3	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	7	7	7	Porta controller_A_2 0c
Switch_FC_B_1	B	7	3	3	9	Porta controller_B_1 0c
Switch_FC_B_1	B	7	7	7	3	Porta controller_B_2 0c
Switch_FC_B_1	B	7	9	9	7	bridge_B_1b FC1

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_1\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	2	2	2	Porta controller_A_1 0b

Switch_FC_A_2	R	6	6	6	6	Porta controller_A_2 0b
Switch_FC_B_2	B	8	2	2	2	Porta controller_B_1 0b
Switch_FC_B_2	B	8	6	6	6	Porta controller_B_2 0b
Switch_FC_B_2	B	8	8	8	8	bridge_B_1a FC2

<b>Zona nel fabric_1</b>	<b>Porte dei membri</b>
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_1\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	3	3	3	Porta controller_A_1 0d
Switch_FC_A_2	R	6	7	7	7	Porta controller_A_2 0d
Switch_FC_B_2	B	8	3	3	3	Porta controller_B_1 0d
Switch_FC_B_2	B	8	7	7	7	Porta controller_B_2 0d
Switch_FC_B_2	B	8	9	9	9	bridge_A_1b FC2

<b>Zona nel fabric_2</b>	<b>Porte dei membri</b>
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

**Gruppo DR 1 - Stack 2 presso il sito\_B.**

**DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1:**

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	2	2	2	Porta controller_A_1 0a
Switch_FC_A_1	R	5	6	6	6	Porta controller_A_2 0a
Switch_FC_B_1	B	7	2	2	2	Porta controller_B_1 0a
Switch_FC_B_1	B	7	6	6	6	Porta controller_B_2 0a
Switch_FC_B_1	B	7	10	10	10	bridge_B_2a FC1

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10

**DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_2\_TOP\_FC1:**

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_1	R	5	3	3	3	Porta controller_A_1 0c
Switch_FC_A_1	R	5	7	7	7	Porta controller_A_2 0c
Switch_FC_B_1	B	7	3	3	3	Porta controller_B_1 0c

Switch_FC_B_1	B	7	7	7	7	Porta controller_B_2 0c
Switch_FC_B_1	B	7	11	11	11	bridge_B_2b FC1

Zona in fabric_2 hh	Porte dei membri
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

#### DRGROUP 1: MC1\_INIT\_GRP\_1\_SITE\_B\_STK\_GRP\_2\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	2	2	2	Porta controller_A_1 0b
Switch_FC_A_2	R	6	6	6	6	Porta controller_A_2 0b
Switch_FC_B_2	B	8	2	2	2	Porta controller_B_1 0b
Switch_FC_B_2	B	8	6	6	6	Porta controller_B_2 0b
Switch_FC_B_2	B	8	10	10	10	bridge_B_2a FC2

Zona nel fabric_1	Porte dei membri
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10

#### DRGROUP 1: MC1\_INIT\_GRP\_2\_SITE\_B\_STK\_GRP\_2\_BOT\_FC2:

Switch FC	Sito	Dominio dello switch	Porta 6505 / 6510 / G610	porta 6520	Porta G620	Si connette a...
Switch_FC_A_2	R	6	3	3	3	Porta controller_A_1 0d



Switch_FC_A_2	R	6	7	7	7	Porta controller_A_2 0d
Switch_FC_B_2	B	8	3	3	3	Porta controller_B_1 0d
Switch_FC_B_2	B	8	7	7	7	Porta controller_B_2 0d
Switch_FC_B_2	B	8	11	11	11	bridge_B_2b FC2

Zona nel fabric_2	Porte dei membri
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

### Riepilogo delle zone di storage

Fabric	Nome della zona	Porte dei membri
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10
FC_switch_A_1 e FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10
FC_switch_A_2 e FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

## Configurazione dello zoning sugli switch Brocade FC

È necessario assegnare le porte dello switch per separare le zone per separare il traffico di storage e controller, con zone per le porte FC-VI e zone per le porte di storage.

### A proposito di questa attività

La seguente procedura utilizza lo zoning standard per la configurazione MetroCluster.

["Zoning per porte FC-VI"](#)

["Zoning per i bridge 7500N o 7600N di FibreBridge attraverso una porta FC"](#)

["Zoning per i bridge FibreBridge 7500N che utilizzano entrambe le porte FC"](#)

### Fasi

1. Creare le zone FC-VI su ogni switch:

```
zonecreate "QOSH1_FCVI_1", member;member ...
```

In questo esempio viene creata una zona QOS FCVI contenente le porte 5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5:

```
Switch_A_1:admin> zonecreate "QOSH1_FCVI_1",  
"5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
```

## 2. Configurare le zone di storage su ogni switch.

È possibile configurare lo zoning per il fabric da uno switch nel fabric. Nell'esempio seguente, lo zoning viene configurato su Switch\_A\_1.

- a. Creare la zona di storage per ciascun dominio dello switch nel fabric dello switch:

```
zonecreate name, member;member ...
```

In questo esempio viene creata una zona di storage per un FibreBridge 7500N che utilizza entrambe le porte FC. Le zone contengono le porte 5,2;5,6;7,2;7,6;5,16:

```
Switch_A_1:admin> zonecreate  
"MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
```

- b. Creare la configurazione nel primo fabric switch:

```
cfgcreate config_name, zone;zone...
```

In questo esempio viene creata una configurazione con il nome CFG\_1 e le due zone QOSH1\_MC1\_FAB\_1\_FCVI e MC1\_INIT\_GRP\_1\_SITE\_A\_STK\_GRP\_1\_TOP\_FC1

```
Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;  
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
```

- c. Aggiungere zone alla configurazione, se necessario:

```
cfgadd config_namezone;zone...
```

- d. Abilitare la configurazione:

```
cfgenable config_name
```

```
Switch_A_1:admin> cfgenable "CFG_1"
```

- e. Salvare la configurazione:

```
cfgsave
```

```
Switch_A_1:admin> cfgsave
```

- f. Convalidare la configurazione dello zoning:

```
zone --validate
```

```

Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
-----
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone

```

### Impostazione della crittografia ISL sugli switch Brocade 6510 o G620

Sugli switch Brocade 6510 o G620, è possibile utilizzare la funzione di crittografia Brocade sulle connessioni ISL. Se si desidera utilizzare la funzione di crittografia, è necessario eseguire ulteriori procedure di configurazione su ogni switch nella configurazione MetroCluster.

#### Prima di iniziare

- È necessario disporre di switch Brocade 6510 o G620.



Il supporto per la crittografia ISL sugli switch Brocade G620 è supportato solo su ONTAP 9.4 e versioni successive.

- È necessario aver selezionato due switch dallo stesso fabric.
- Per verificare i limiti di larghezza di banda e di porta, è necessario consultare la documentazione Brocade relativa alla versione dello switch e del sistema operativo fabric in uso.

### A proposito di questa attività

I passaggi devono essere eseguiti su entrambi gli switch dello stesso fabric.

### Disattivazione del fabric virtuale

Per impostare la crittografia ISL, è necessario disattivare il fabric virtuale su tutti e quattro gli switch utilizzati in una configurazione MetroCluster.

#### Fasi

1. Disattivare il fabric virtuale immettendo il seguente comando nella console dello switch:

```
fosconfig --disable vf
```

2. Riavviare lo switch.

### Impostazione del payload

Dopo aver disattivato il fabric virtuale, è necessario impostare il payload o le dimensioni del campo dati su entrambi gli switch del fabric.

### A proposito di questa attività

La dimensione del campo dati non deve superare 2048.

#### Fasi

1. Disattivare lo switch:

```
switchdisable
```

2. Configurare e impostare il payload:

```
configure
```

3. Impostare i seguenti parametri dello switch:

- a. Impostare il parametro Fabric come segue: `y`
- b. Impostare gli altri parametri, ad esempio dominio, PID persistente basato su WWN e così via.
- c. Impostare le dimensioni del campo dati: `2048`

### Impostazione del criterio di autenticazione

È necessario impostare il criterio di autenticazione e i parametri associati.

### A proposito di questa attività

I comandi devono essere eseguiti dalla console dello switch.

#### Fasi

1. Impostare il segreto di autenticazione:

- a. Avviare il processo di configurazione:

```
secAuthSecret --set
```

Questo comando avvia una serie di prompt a cui si risponde nei seguenti passaggi:

- a. Fornire il nome globale (WWN) dell'altro switch nel fabric per il parametro "Enter peer WWN, Domain, or switch name".
- b. Fornire il peer secret per il parametro "Enter peer secret".
- c. Fornire il segreto locale per il parametro "Enter local secret".
- d. Invio `Y` Per il parametro "are you done".

Di seguito viene riportato un esempio di impostazione del segreto di autenticazione:

```
brcd> secAuthSecret --set
```

This command is used to set up secret keys for the DH-CHAP authentication.

The minimum length of a secret key is 8 characters and maximum 40 characters. Setting up secret keys does not initiate DH-CHAP authentication. If switch is configured to do DH-CHAP, it is performed whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > `<cr>`

Enter peer WWN, Domain, or switch name (Leave blank when done):

10:00:00:05:33:76:2e:99

Enter peer secret: `<hidden>`

Re-enter peer secret: `<hidden>`

Enter local secret: `<hidden>`

Re-enter local secret: `<hidden>`

Enter peer WWN, Domain, or switch name (Leave blank when done):

Are you done? (yes, y, no, n): `[no] yes`

Saving data to key store... Done.

## 2. Impostare il gruppo di autenticazione su 4:

```
authUtil --set -g 4
```

## 3. Impostare il tipo di autenticazione su "dhchap":

```
authUtil --set -a dhchap
```

Il sistema visualizza il seguente output:

```
Authentication is set to dhchap.
```

4. Impostare il criterio di autenticazione sullo switch su ON:

```
authUtil --policy -sw on
```

Il sistema visualizza il seguente output:

```
Warning: Activating the authentication policy requires either DH-CHAP
secrets or PKI certificates depending on the protocol selected.
Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE (yes, y, no, n): [no] yes
Auth Policy is set to ON
```

## Abilitazione della crittografia ISL sugli switch Brocade

Dopo aver impostato il criterio di autenticazione e il segreto di autenticazione, è necessario attivare la crittografia ISL sulle porte per rendere effettiva la crittografia.

### A proposito di questa attività

- Questi passaggi devono essere eseguiti su un fabric switch alla volta.
- I comandi devono essere eseguiti sulla console dello switch.

### Fasi

1. Abilitare la crittografia su tutte le porte ISL:

```
portCfgEncrypt --enable port_number
```

Nell'esempio seguente, la crittografia è attivata sulle porte 8 e 12:

```
portCfgEncrypt --enable 8
```

```
portCfgEncrypt --enable 12
```

2. Abilitare lo switch:

```
switchenable
```

3. Verificare che l'ISL sia attivo e funzionante:

```
islshow
```

4. Verificare che la crittografia sia attivata:

```
portenccompshow
```

L'esempio seguente mostra che la crittografia è attivata sulle porte 8 e 12:

User Port	Encryption configured	Active
----	-----	-----
8	yes	yes
9	No	No
10	No	No
11	No	No
12	yes	yes

### Cosa fare in seguito

Eseguire tutte le operazioni sugli switch dell'altro fabric in una configurazione MetroCluster.

### Configurazione manuale degli switch Cisco FC

Ogni switch Cisco nella configurazione MetroCluster deve essere configurato in modo appropriato per le connessioni ISL e storage.

#### Prima di iniziare

I seguenti requisiti si applicano agli switch FC Cisco:

- È necessario utilizzare quattro switch Cisco supportati dello stesso modello con la stessa versione e licenza NX-OS.
- La configurazione MetroCluster richiede quattro switch.

I quattro switch devono essere collegati in due fabric di due switch ciascuno, con ciascun fabric che si estende su entrambi i siti.

- Lo switch deve supportare la connettività al modello ATTO FibreBridge.
- Non è possibile utilizzare la crittografia o la compressione nello storage fabric FC di Cisco. Non è supportato nella configurazione MetroCluster.

In "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)", È possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

#### A proposito di questa attività

I seguenti requisiti si applicano alle connessioni ISL (Inter-Switch link):

- Tutti gli ISL devono avere la stessa lunghezza e la stessa velocità in un unico fabric.

È possibile utilizzare diverse lunghezze di ISL nei diversi fabric. La stessa velocità deve essere utilizzata in tutti i fabric.

Per le connessioni di storage si applica il seguente requisito:

- Ciascun controller di storage deve disporre di quattro porte di iniziatore per la connessione ai fabric dello



switch.

È necessario collegare due porte initiator da ciascun controller di storage a ciascun fabric.



È possibile configurare i sistemi FAS8020, AFF8020, FAS8200 e AFF A300 con due porte di iniziatori per controller (una singola porta di iniziatore per ciascun fabric) se vengono soddisfatti tutti i seguenti criteri:

- Sono disponibili meno di quattro porte FC Initiator per collegare lo storage su disco e non è possibile configurare porte aggiuntive come iniziatori FC.
- Tutti gli slot sono in uso e non è possibile aggiungere alcuna scheda FC Initiator.

## Informazioni correlate

["Tool di matrice di interoperabilità NetApp"](#)

### Requisiti di licenza per switch Cisco

Alcune licenze basate sulle funzioni potrebbero essere necessarie per gli switch Cisco in una configurazione Fabric-Attached MetroCluster. Queste licenze consentono di utilizzare funzionalità come QoS o crediti in modalità a lunga distanza sugli switch. È necessario installare le licenze basate sulle funzionalità richieste su tutti e quattro gli switch in una configurazione MetroCluster.

In una configurazione MetroCluster potrebbero essere necessarie le seguenti licenze basate sulle funzionalità:

- ENTERPRISE\_PKG

Questa licenza consente di utilizzare la funzione QoS sugli switch Cisco.

- PORT\_ACTIVATION\_PKG

È possibile utilizzare questa licenza per gli switch Cisco 9148. Questa licenza consente di attivare o disattivare le porte sugli switch, purché siano attive solo 16 porte alla volta. Per impostazione predefinita, negli switch Cisco MDS 9148 sono attivate 16 porte.

- FM\_SERVER\_PKG

Questa licenza consente di gestire i fabric simultaneamente e gli switch attraverso un browser Web.

La licenza FM\_SERVER\_PKG consente inoltre di utilizzare funzionalità di gestione delle performance, come le soglie delle performance e il monitoraggio delle soglie. Per ulteriori informazioni su questa licenza, vedere Cisco Fabric Manager Server Package.

È possibile verificare che le licenze siano installate utilizzando il comando `show License usage` (Mostra utilizzo licenza). Se non si dispone di queste licenze, contattare il rappresentante commerciale prima di procedere con l'installazione.



Gli switch Cisco MDS 9250i dispongono di due porte fisse per servizi di storage IP da 1/10 GbE. Non sono richieste licenze aggiuntive per queste porte. Il pacchetto applicativo Cisco SAN Extension over IP è una licenza standard su questi switch che abilita funzionalità come FCIP e compressione.

## Impostazione dello switch FC Cisco sui valori predefiniti

Per garantire la corretta configurazione, è necessario impostare lo switch sui valori predefiniti. In questo modo, lo switch si avvia da una configurazione pulita.

### A proposito di questa attività

Questa attività deve essere eseguita su tutti gli switch nella configurazione MetroCluster.

#### Fasi

1. Stabilire una connessione alla console e accedere a entrambi gli switch nello stesso fabric.
2. Ripristinare le impostazioni predefinite dello switch:

```
write erase
```

È possibile rispondere a “y” quando richiesto per confermare il comando. In questo modo, tutte le licenze e le informazioni di configurazione sullo switch vengono cancellati.

3. Riavviare lo switch:

```
reload
```

È possibile rispondere a “y” quando richiesto per confermare il comando.

4. Ripetere il `write erase` e `reload` comandi sull'altro switch.

Dopo l'emissione di `reload` lo switch si riavvia e visualizza le domande di configurazione. A questo punto, passare alla sezione successiva.

### Esempio

L'esempio seguente mostra il processo su un fabric costituito da FC\_switch\_A\_1 e FC\_switch\_B\_1.

```
FC_Switch_A_1# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n)  [n] y
FC_Switch_A_1# reload
This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n)  [n] y
FC_Switch_B_1# reload
This command will reboot the system. (y/n)?  [n] y
```

## Configurare le impostazioni di base dello switch FC Cisco e la stringa di comunità

Specificare le impostazioni di base con `setup` o dopo l'emissione di `reload` comando.

#### Fasi

1. Se lo switch non visualizza le domande di configurazione, configurare le impostazioni di base dello switch:

setup

2. Accettare le risposte predefinite alle domande di configurazione fino a quando non viene richiesta la stringa della community SNMP.
3. Impostare la stringa di community su "public" (in minuscolo) per consentire l'accesso dai monitor dello stato di salute ONTAP.

È possibile impostare la stringa di comunità su un valore diverso da "public", ma è necessario configurare i monitor dello stato di salute ONTAP utilizzando la stringa di comunità specificata.

L'esempio seguente mostra i comandi su FC\_switch\_A\_1:

```
FC_switch_A_1# setup
  Configure read-only SNMP community string (yes/no) [n]: y
  SNMP community string : public
  Note: Please set the SNMP community string to "Public" or another
value of your choosing.
  Configure default switchport interface state (shut/noshut) [shut]:
noshut
  Configure default switchport port mode F (yes/no) [n]: n
  Configure default zone policy (permit/deny) [deny]: deny
  Enable full zoneset distribution? (yes/no) [n]: yes
```

L'esempio seguente mostra i comandi su FC\_switch\_B\_1:

```
FC_switch_B_1# setup
  Configure read-only SNMP community string (yes/no) [n]: y
  SNMP community string : public
  Note: Please set the SNMP community string to "Public" or another
value of your choosing.
  Configure default switchport interface state (shut/noshut) [shut]:
noshut
  Configure default switchport port mode F (yes/no) [n]: n
  Configure default zone policy (permit/deny) [deny]: deny
  Enable full zoneset distribution? (yes/no) [n]: yes
```

### Acquisizione di licenze per le porte

Non è necessario utilizzare le licenze dello switch Cisco su un intervallo continuo di porte; è invece possibile acquistare licenze per porte specifiche utilizzate e rimuovere le licenze dalle porte inutilizzate.

### Prima di iniziare

Verificare il numero di porte concesse in licenza nella configurazione dello switch e, se necessario, spostare le licenze da una porta all'altra in base alle necessità.

### Fasi

1. Visualizzare l'utilizzo della licenza per un fabric di switch:

```
show port-resources module 1
```

Determinare quali porte richiedono licenze. Se alcune di queste porte non sono dotate di licenza, determinare se si dispone di porte con licenza extra e prendere in considerazione la possibilità di rimuovere le licenze da esse.

2. Accedere alla modalità di configurazione:

```
config t
```

3. Rimuovere la licenza dalla porta selezionata:

a. Selezionare la porta da non concedere in licenza:

```
interface interface-name
```

b. Rimuovere la licenza dalla porta:

```
no port-license acquire
```

c. Uscire dall'interfaccia di configurazione della porta:

```
exit
```

4. Acquisire la licenza per la porta selezionata:

a. Selezionare la porta da non concedere in licenza:

```
interface interface-name
```

b. Rendere la porta idonea all'acquisizione di una licenza:

```
port-license
```

c. Acquisire la licenza sulla porta:

```
port-license acquire
```

d. Uscire dall'interfaccia di configurazione della porta:

```
exit
```

5. Ripetere l'operazione per le porte aggiuntive.

6. Uscire dalla modalità di configurazione:

```
exit
```

## Rimozione e acquisizione di una licenza su una porta

Questo esempio mostra che una licenza viene rimossa dalla porta fc1/2, la porta fc1/1 viene resa idonea all'acquisizione di una licenza e la licenza acquisita sulla porta fc1/1:

```
Switch_A_1# conf t
Switch_A_1(config)# interface fc1/2
Switch_A_1(config)# shut
Switch_A_1(config-if)# no port-license acquire
Switch_A_1(config-if)# exit
Switch_A_1(config)# interface fc1/1
Switch_A_1(config-if)# port-license
Switch_A_1(config-if)# port-license acquire
Switch_A_1(config-if)# no shut
Switch_A_1(config-if)# end
Switch_A_1# copy running-config startup-config
```

```
Switch_B_1# conf t
Switch_B_1(config)# interface fc1/2
Switch_B_1(config)# shut
Switch_B_1(config-if)# no port-license acquire
Switch_B_1(config-if)# exit
Switch_B_1(config)# interface fc1/1
Switch_B_1(config-if)# port-license
Switch_B_1(config-if)# port-license acquire
Switch_B_1(config-if)# no shut
Switch_B_1(config-if)# end
Switch_B_1# copy running-config startup-config
```

L'esempio seguente mostra l'utilizzo della licenza della porta verificato:

```
Switch_A_1# show port-resources module 1
Switch_B_1# show port-resources module 1
```

### Abilitazione delle porte in uno switch Cisco MDS 9148 o 9148S

Negli switch Cisco MDS 9148 o 9148S, è necessario attivare manualmente le porte richieste in una configurazione MetroCluster.

#### A proposito di questa attività

- È possibile attivare manualmente 16 porte in uno switch Cisco MDS 9148 o 9148S.
- Gli switch Cisco consentono di applicare la licenza POD su porte casuali, invece di applicarla in sequenza.
- Gli switch Cisco richiedono l'utilizzo di una porta per ciascun gruppo di porte, a meno che non siano necessarie più di 12 porte.

#### Fasi

1. Visualizzare i gruppi di porte disponibili in uno switch Cisco:

```
show port-resources module blade_number
```

2. Concedere in licenza e acquisire la porta richiesta in un gruppo di porte:

```
config t

interface port_number

shut

port-license acquire

no shut
```

Ad esempio, la seguente sequenza di comandi concede in licenza e acquisisce la porta fc 1/45:

```
switch# config t
switch(config)#
switch(config)# interface fc 1/45
switch(config-if)#
switch(config-if)# shut
switch(config-if)# port-license acquire
switch(config-if)# no shut
switch(config-if)# end
```

3. Salvare la configurazione:

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

### Configurazione delle porte F su uno switch FC Cisco

È necessario configurare le porte F sullo switch FC.

#### A proposito di questa attività

In una configurazione MetroCluster, le porte F sono le porte che collegano lo switch agli iniziatori HBA, alle interconnessioni FC-VI e ai bridge FC-SAS.

Ciascuna porta deve essere configurata singolarmente.

Fare riferimento alle seguenti sezioni per identificare le porte F (switch-to-node) per la configurazione:

- ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)
- ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

Questa attività deve essere eseguita su ogni switch nella configurazione MetroCluster.

#### Fasi

1. Accedere alla modalità di configurazione:

```
config t
```

2. Accedere alla modalità di configurazione dell'interfaccia per la porta:

```
interface port-ID
```

3. Chiudere la porta:

```
shutdown
```

4. Impostare le porte sulla modalità F:

```
switchport mode F
```

5. Impostare le porte su una velocità fissa:

```
switchport speed speed-value
```

*speed-value* è uno dei due 8000 oppure 16000

6. Impostare la modalità rate della porta dello switch su Dedicated (dedicata):

```
switchport rate-mode dedicated
```

7. Riavviare la porta:

```
no shutdown
```

8. Uscire dalla modalità di configurazione:

```
end
```

### Esempio

L'esempio seguente mostra i comandi sui due switch:

```
Switch_A_1# config t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

## Assegnazione di crediti buffer-to-buffer a F-Ports nello stesso gruppo di porte dell'ISL

È necessario assegnare i crediti buffer-to-buffer alle porte F se si trovano nello stesso gruppo di porte dell'ISL. Se le porte non dispongono dei crediti buffer-to-buffer richiesti, l'ISL potrebbe non funzionare.

### A proposito di questa attività

Questa attività non è necessaria se le porte F non si trovano nello stesso gruppo di porte della porta ISL.

Se le porte F si trovano in un gruppo di porte che contiene l'ISL, questa attività deve essere eseguita su ogni switch FC nella configurazione MetroCluster.

### Fasi

1. Accedere alla modalità di configurazione:

```
config t
```

2. Impostare la modalità di configurazione dell'interfaccia per la porta:

```
interface port-ID
```

3. Disattivare la porta:

```
shut
```

4. Se la porta non è già in modalità F, impostarla su F mode:

```
switchport mode F
```

5. Impostare il credito buffer-to-buffer delle porte non-e su 1:

```
switchport fcrxbbcredit 1
```

6. Riattivare la porta:

```
no shut
```

7. Uscire dalla modalità di configurazione:

```
exit
```

8. Copiare la configurazione aggiornata nella configurazione di avvio:

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

9. Verificare il credito buffer-to-buffer assegnato a una porta:

```
show port-resources module 1
```

10. Uscire dalla modalità di configurazione:

```
exit
```

11. Ripetere questa procedura sull'altro switch del fabric.

12. Verificare le impostazioni:



```
show port-resource module 1
```

### Esempio

In questo esempio, la porta fc1/40 è l'ISL. Le porte fc1/37, fc1/38 e fc1/39 si trovano nello stesso gruppo di porte e devono essere configurate.

I seguenti comandi mostrano l'intervallo di porte configurato per fc1/37 fino a fc1/39:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

I seguenti comandi e l'output di sistema mostrano che le impostazioni sono applicate correttamente:

```

FC_switch_A_1# show port-resource module 1
...
Port-Group 11
  Available dedicated buffers are 93

-----
Interfaces in the Port-Group      B2B Credit  Bandwidth  Rate Mode
                                Buffers        (Gbps)
-----
fc1/37                          32          8.0    dedicated
fc1/38                          1           8.0    dedicated
fc1/39                          1           8.0    dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
  Available dedicated buffers are 93

-----
Interfaces in the Port-Group      B2B Credit  Bandwidth  Rate Mode
                                Buffers        (Gbps)
-----
fc1/37                          32          8.0    dedicated
fc1/38                          1           8.0    dedicated
fc1/39                          1           8.0    dedicated
...

```

### Creazione e configurazione di reti VSAN su switch FC Cisco

È necessario creare un VSAN per le porte FC-VI e un VSAN per le porte di storage su ogni switch FC nella configurazione MetroCluster.

#### A proposito di questa attività

Le reti VSAN devono avere un numero e un nome univoci. Se si utilizzano due ISL con distribuzione dei frame in ordine, è necessario eseguire una configurazione aggiuntiva.

Gli esempi di questa attività utilizzano le seguenti convenzioni di denominazione:

Fabric dello switch	Nome VSAN	Numero ID
1	FCVI_1_10	10
STOR_1_20	20	2

FCVI_2_30	30	STOR_2_20
-----------	----	-----------

Questa attività deve essere eseguita su ogni fabric di switch FC.

## Fasi

### 1. Configurare il VSAN FC-VI:

- Accedere alla modalità di configurazione, se non è già stata eseguita questa operazione:

```
config t
```

- Modificare il database VSAN:

```
vsan database
```

- Impostare l'ID VSAN:

```
vsan vsan-ID
```

- Impostare il nome VSAN:

```
vsan vsan-ID name vsan_name
```

### 2. Aggiunta di porte a FC-VI VSAN:

- Aggiungere le interfacce per ciascuna porta nel VSAN:

```
vsan vsan-ID interface interface_name
```

Per FC-VI VSAN, vengono aggiunte le porte che collegano le porte FC-VI locali.

- Uscire dalla modalità di configurazione:

```
end
```

- Copiare running-config in startup-config:

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

Nell'esempio seguente, le porte sono fc1/1 e fc1/13:

```

FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config

```

### 3. Verificare l'appartenenza alla porta di VSAN:

```
show vsan member
```

```

FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member

```

### 4. Configurare il VSAN per garantire la consegna in ordine dei frame o la consegna fuori ordine dei frame:



Si consigliano le impostazioni IOD standard. Configurare OOD solo se necessario.

"Considerazioni sull'utilizzo di apparecchiature TDM/WDM con configurazioni MetroCluster collegate al fabric"

- Per configurare l'erogazione dei frame in ordine, è necessario eseguire le seguenti operazioni:

- i. Accedere alla modalità di configurazione:

```
conf t
```

- ii. Consentire la garanzia degli scambi per VSAN:

```
in-order-guarantee vsan vsan-ID
```



Per le SAN FC-VI (FCVI\_1\_10 e FCVI\_2\_30), è necessario abilitare la garanzia in-order di frame e scambi solo su VSAN 10.

- iii. Abilitare il bilanciamento del carico per VSAN:

```
vsan vsan-ID loadbalancing src-dst-id
```

- iv. Uscire dalla modalità di configurazione:

```
end
```

v. Copiare running-config in startup-config:

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

I comandi per configurare l'erogazione in ordine dei frame su FC\_switch\_A\_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

I comandi per configurare l'erogazione in ordine dei frame su FC\_switch\_B\_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

◦ Per configurare la consegna fuori ordine dei frame, è necessario eseguire le seguenti operazioni:

i. Accedere alla modalità di configurazione:

```
conf t
```

ii. Disattivare la garanzia di scambio in-order per VSAN:

```
no in-order-guarantee vsan vsan-ID
```

iii. Abilitare il bilanciamento del carico per VSAN:

```
vsan vsan-ID loadbalancing src-dst-id
```

iv. Uscire dalla modalità di configurazione:

```
end
```

v. Copiare running-config in startup-config:

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

I comandi per configurare l'erogazione fuori ordine dei frame su FC\_switch\_A\_1:

```

FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

```

I comandi per configurare l'erogazione fuori ordine dei frame su FC\_switch\_B\_1:

```

FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config

```

+



Quando si configura ONTAP sui moduli controller, OOD deve essere configurato esplicitamente su ciascun modulo controller nella configurazione MetroCluster.

### "Configurazione della consegna in-order o out-of-order dei frame sul software ONTAP"

#### 5. Impostare i criteri QoS per FC-VI VSAN:

##### a. Accedere alla modalità di configurazione:

```
conf t
```

##### b. Abilitare la QoS e creare una mappa di classi immettendo i seguenti comandi in sequenza:

```
qos enable
```

```
qos class-map class_name match-any
```

##### c. Aggiungere alla mappa dei criteri la mappa delle classi creata in un passaggio precedente:

```
class class_name
```

##### d. Impostare la priorità:

```
priority high
```

##### e. Aggiungere il VSAN alla mappa dei criteri creata in precedenza in questa procedura:

```
qos service policy policy_name vsan vsan-id
```

##### f. Copiare la configurazione aggiornata nella configurazione di avvio:

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

I comandi per impostare i criteri QoS su FC\_switch\_A\_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

I comandi per impostare i criteri QoS su FC\_switch\_B\_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

## 6. Configurare lo storage VSAN:

### a. Impostare l'ID VSAN:

```
vsan vsan-ID
```

### b. Impostare il nome VSAN:

```
vsan vsan-ID name vsan_name
```

I comandi per configurare lo storage VSAN su FC\_switch\_A\_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

I comandi per configurare lo storage VSAN su FC\_switch\_B\_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

## 7. Aggiungere porte al VSAN dello storage.

Per lo storage VSAN, è necessario aggiungere tutte le porte che collegano HBA o bridge FC-SAS. In questo esempio fc1/5, fc1/9, fc1/17, fc1/21. vengono aggiunti fc1/25, fc1/29, fc1/33 e fc1/37.

I comandi per aggiungere porte al VSAN dello storage su FC\_switch\_A\_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

I comandi per aggiungere porte al VSAN dello storage su FC\_switch\_B\_1:



```

FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config

```

### Configurazione di e-port

È necessario configurare le porte dello switch che collegano l'ISL (queste sono le e-Port).

#### A proposito di questa attività

La procedura da seguire dipende dallo switch in uso:

- [Configurazione delle e-port sullo switch FC Cisco](#)
- [Configurazione delle porte FCIP per un singolo ISL sugli switch FC Cisco 9250i](#)
- [Configurazione delle porte FCIP per un ISL doppio sugli switch FC Cisco 9250i](#)

### Configurazione delle e-port sullo switch FC Cisco

È necessario configurare le porte dello switch FC che collegano il collegamento tra switch (ISL).

#### A proposito di questa attività

Si tratta delle e-port e la configurazione deve essere eseguita per ciascuna porta. A tale scopo, è necessario calcolare il numero corretto di crediti buffer-to-buffer (BBC).

Tutti gli ISL nel fabric devono essere configurati con le stesse impostazioni di velocità e distanza.

Questa attività deve essere eseguita su ciascuna porta ISL.

#### Fasi

1. Utilizzare la seguente tabella per determinare i BBC richiesti regolati per chilometro in base alle possibili velocità delle porte.

Per determinare il numero corretto di BBC, moltiplicare i BBC regolati richiesti (determinati dalla tabella seguente) per la distanza in chilometri tra gli interruttori. Per tenere conto del comportamento del framing FC-VI, è necessario un fattore di regolazione pari a 1.5.

Velocità in Gbps	BBC richiesti per chilometro	BBC regolati richiesti (BBC per km x 1.5)
1	0.5	0.75

2	1	1.5
4	2	3
8	4	6
16	8	12

Ad esempio, per calcolare il numero richiesto di crediti per una distanza di 30 km su un collegamento a 4 Gbps, effettuare i seguenti calcoli:

- Speed in Gbps è 4
- Adjusted BBCs required è 3
- Distance in kilometers between switches è di 30 km
- $3 \times 30 = 90$

a. Accedere alla modalità di configurazione:

```
config t
```

b. Specificare la porta che si sta configurando:

```
interface port-name
```

c. Chiudere la porta:

```
shutdown
```

d. Impostare la modalità rate della porta su "dedicata":

```
switchport rate-mode dedicated
```

e. Impostare la velocità della porta:

```
switchport speed speed-value
```

f. Impostare i crediti buffer-to-buffer per la porta:

```
switchport fcrxbbcredit number_of_buffers
```

g. Impostare la porta in modalità e:

```
switchport mode E
```

h. Attivare la modalità trunk per la porta:

```
switchport trunk mode on
```

i. Aggiungere le VSAN (Virtual Storage Area Network) ISL al trunk:

```
switchport trunk allowed vsan 10
```

```
switchport trunk allowed vsan add 20
```

- j. Aggiungere la porta al canale della porta 1:

```
channel-group 1
```

- k. Ripetere i passaggi precedenti per la porta ISL corrispondente sullo switch partner nel fabric.

L'esempio seguente mostra la porta fc1/41 configurata per una distanza di 30 km e 8 Gbps:

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

- l. Immettere il seguente comando su entrambi gli switch per riavviare le porte:

```
no shutdown
```

- m. Ripetere i passaggi precedenti per le altre porte ISL del fabric.

- n. Aggiungere il VSAN nativo all'interfaccia port-channel su entrambi gli switch nello stesso fabric:

```
interface port-channel number
```

```
switchport trunk allowed vsan add native_san_id
```

- o. Verificare la configurazione del port-channel:

```
show interface port-channel number
```

Il canale della porta deve avere i seguenti attributi:

- Il port-channel è "trunking".
- Admin port mode (modalità porta amministratore) è e, trunk mode (modalità trunk) è ON.
- Speed (velocità): Mostra il valore cumulativo di tutte le velocità di collegamento ISL.

Ad esempio, due porte ISL che operano a 4 Gbps dovrebbero mostrare una velocità di 8 Gbps.

- Trunk vsans (admin allowed and active) Mostra tutti i VSAN consentiti.
- Trunk vsans (up) Mostra tutti i VSAN consentiti.
- L'elenco dei membri mostra tutte le porte ISL aggiunte al port-channel.
- Il numero VSAN della porta deve essere lo stesso del VSAN che contiene gli ISL (in genere vsan nativo 1).

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
  Hardware is Fibre Channel
  Port WWN is 24:01:54:7f:ee:e2:8d:a0
  Admin port mode is E, trunk mode is on
  snmp link state traps are enabled
  Port mode is TE
  Port vsan is 1
  Speed is 8 Gbps
  Trunk vsans (admin allowed and active) (1,10,20)
  Trunk vsans (up) (1,10,20)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) ()
  5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
  5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
  535724861 frames input,1069616011292 bytes
    0 discards,0 errors
    0 invalid CRC/FCS,0 unknown class
    0 too long,0 too short
  572290295 frames output,1144869385204 bytes
    0 discards,0 errors
  5 input OLS,11 LRR,2 NOS,0 loop inits
  14 output OLS,5 LRR, 0 NOS, 0 loop inits
Member[1] : fc1/36
Member[2] : fc1/40
Interface last changed at Thu Oct 16 11:48:00 2014
```

a. Configurazione dell'interfaccia di uscita su entrambi gli switch:

end

- b. Copiare la configurazione aggiornata nella configurazione di avvio su entrambi i fabric:

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

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

- a. Ripetere i passaggi precedenti sul secondo fabric dello switch.

### Informazioni correlate

Quando si utilizzano ONTAP 9.1 e versioni successive, verificare di utilizzare le assegnazioni delle porte specificate quando si cablano gli switch FC. Fare riferimento a ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)

### Configurazione delle porte FCIP per un singolo ISL sugli switch FC Cisco 9250i

È necessario configurare le porte dello switch FCIP che collegano l'ISL (e-ports) creando profili e interfacce FCIP, quindi assegnandoli all'interfaccia GbE IPStorage1/1.

#### A proposito di questa attività

Questa attività è valida solo per le configurazioni che utilizzano un singolo ISL per fabric di switch, utilizzando l'interfaccia IPStorage1/1 su ogni switch.

Questa attività deve essere eseguita su ogni switch FC.

Su ogni switch vengono creati due profili FCIP:

- Fabric 1
  - FC\_switch\_A\_1 è configurato con i profili FCIP 11 e 111.
  - FC\_switch\_B\_1 è configurato con i profili FCIP 12 e 121.
- Fabric 2
  - FC\_switch\_A\_2 è configurato con i profili FCIP 13 e 131.
  - FC\_switch\_B\_2 è configurato con i profili FCIP 14 e 141.

### Fasi

1. Accedere alla modalità di configurazione:

```
config t
```

2. Attiva FCIP:

```
feature fcip
```

3. Configurare l'interfaccia GbE IPStorage1/1:

- a. Accedere alla modalità di configurazione:

```
conf t
```

- b. Specificare l'interfaccia IPStorage1/1:

```
interface IPStorage1/1
```

- c. Specificare l'indirizzo IP e la subnet mask:

```
interface ip-address subnet-mask
```

- d. Specificare la dimensione MTU di 2500:

```
switchport mtu 2500
```

- e. Abilitare la porta:

```
no shutdown
```

- f. Uscire dalla modalità di configurazione:

```
exit
```

L'esempio seguente mostra la configurazione di una porta IPStorage1/1:

```
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```

#### 4. Configurare il profilo FCIP per il traffico FC-VI:

- a. Configurare un profilo FCIP e accedere alla modalità di configurazione del profilo FCIP:

```
fcip profile FCIP-profile-name
```

Il nome del profilo dipende dallo switch che si sta configurando.

- b. Assegnare l'indirizzo IP dell'interfaccia IPStorage1/1 al profilo FCIP:

```
ip address ip-address
```

- c. Assegnare il profilo FCIP alla porta TCP 3227:

```
port 3227
```

- d. Per impostare le impostazioni TCP:

```

tcp keepalive-timeout 1

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable ``no tcp cwm

```

L'esempio seguente mostra la configurazione del profilo FCIP:

```

conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

```

## 5. Configurare il profilo FCIP per il traffico di storage:

- a. Configurare un profilo FCIP con il nome 111 e accedere alla modalità di configurazione del profilo FCIP:

```
fcip profile 111
```

- b. Assegnare l'indirizzo IP dell'interfaccia IPStorage1/1 al profilo FCIP:

```
ip address ip-address
```

- c. Assegnare il profilo FCIP alla porta TCP 3229:

```
port 3229
```

- d. Per impostare le impostazioni TCP:

```
tcp keepalive-timeout 1
```

```

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable ``no tcp cwm

```

L'esempio seguente mostra la configurazione del profilo FCIP:

```

conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

```

## 6. Creare la prima di due interfacce FCIP:

```
interface fcip 1
```

Questa interfaccia viene utilizzata per il traffico FC-IV.

### a. Selezionare il profilo 11 creato in precedenza:

```
use-profile 11
```

### b. Impostare l'indirizzo IP e la porta della porta IPStorage1/1 sullo switch partner:

```
peer-info ipaddr partner-switch-port-ip port 3227
```

### c. Selezionare la connessione TCP 2:

```
tcp-connection 2
```

### d. Disattiva compressione:



```
no ip-compression
```

e. Abilitare l'interfaccia:

```
no shutdown
```

f. Configurare la connessione TCP di controllo su 48 e la connessione dati su 26 per contrassegnare tutti i pacchetti sul valore DSCP (differenziate Services code point):

```
qos control 48 data 26
```

g. Uscire dalla modalità di configurazione dell'interfaccia:

```
exit
```

L'esempio seguente mostra la configurazione dell'interfaccia FCIP:

```
interface fcip 1
  use-profile 11
  # the port # listed in this command is the port that the remote switch
  is listening on
  peer-info ipaddr 192.168.32.334    port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. Creare la seconda di due interfacce FCIP:

```
interface fcip 2
```

Questa interfaccia viene utilizzata per il traffico di storage.

a. Selezionare il profilo 111 creato in precedenza:

```
use-profile 111
```

b. Impostare l'indirizzo IP e la porta della porta IPStorage1/1 sullo switch partner:

```
peer-info ipaddr partner-switch-port-ip port 3229
```

c. Selezionare la connessione TCP 2:

```
tcp-connection 5
```

d. Disattiva compressione:

```
no ip-compression
```

e. Abilitare l'interfaccia:

```
no shutdown
```

f. Configurare la connessione TCP di controllo su 48 e la connessione dati su 26 per contrassegnare tutti i pacchetti sul valore DSCP (differenziate Services code point):

```
qos control 48 data 26
```

g. Uscire dalla modalità di configurazione dell'interfaccia:

```
exit
```

L'esempio seguente mostra la configurazione dell'interfaccia FCIP:

```
interface fcip 2
  use-profile 11
  # the port # listed in this command is the port that the remote switch
  is listening on
  peer-info ipaddr 192.168.32.33e port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. Configurare le impostazioni switchport sull'interfaccia fcip 1:

a. Accedere alla modalità di configurazione:

```
config t
```

b. Specificare la porta che si sta configurando:

```
interface fcip 1
```

c. Chiudere la porta:

```
shutdown
```

d. Impostare la porta in modalità e:

```
switchport mode E
```

e. Attivare la modalità trunk per la porta:

```
switchport trunk mode on
```

f. Impostare il vsan di linea consentito su 10:

```
switchport trunk allowed vsan 10
```

g. Impostare la velocità della porta:

```
switchport speed speed-value
```

9. Configurare le impostazioni switchport sull'interfaccia fcip 2:

a. Accedere alla modalità di configurazione:

```
config t
```

b. Specificare la porta che si sta configurando:

```
interface fcip 2
```

c. Chiudere la porta:

```
shutdown
```

d. Impostare la porta in modalità e:

```
switchport mode E
```

e. Attivare la modalità trunk per la porta:

```
switchport trunk mode on
```

f. Impostare il vsan di linea consentito su 20:

```
switchport trunk allowed vsan 20
```

g. Impostare la velocità della porta:

```
switchport speed speed-value
```

10. Ripetere i passaggi precedenti sul secondo interruttore.

Le uniche differenze sono gli indirizzi IP appropriati e i nomi dei profili FCIP univoci.

- Durante la configurazione del primo fabric switch, FC\_switch\_B\_1 viene configurato con i profili FCIP 12 e 121.
- Durante la configurazione del primo fabric switch, FC\_switch\_A\_2 viene configurato con i profili FCIP 13 e 131 e FC\_switch\_B\_2 viene configurato con i profili FCIP 14 e 141.

11. Riavviare le porte su entrambi gli switch:

```
no shutdown
```

12. Uscire dalla configurazione dell'interfaccia su entrambi gli switch:

```
end
```

13. Copiare la configurazione aggiornata nella configurazione di avvio su entrambi gli switch:

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

```

FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config

```

14. Ripetere i passaggi precedenti sul secondo fabric dello switch.

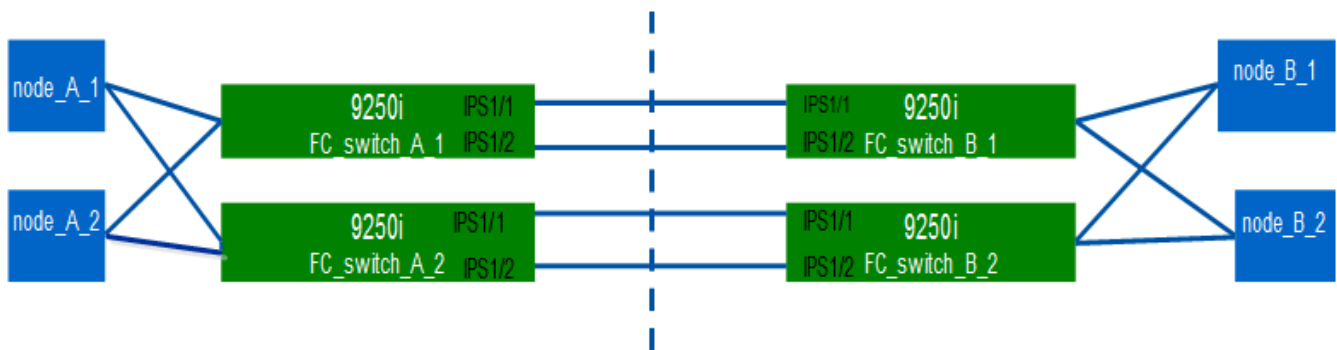
### Configurazione delle porte FCIP per un ISL doppio sugli switch FC Cisco 9250i

È necessario configurare le porte dello switch FCIP che collegano le ISL (e-ports) creando profili e interfacce FCIP, quindi assegnandoli alle interfacce GbE IPStorage1/1 e IPStorage1/2.

#### A proposito di questa attività

Questa attività è valida solo per le configurazioni che utilizzano un ISL doppio per fabric switch, utilizzando le interfacce IPStorage1/1 e IPStorage1/2 GbE su ogni switch.

Questa attività deve essere eseguita su ogni switch FC.



L'attività e gli esempi utilizzano le seguenti tabelle di configurazione del profilo:

- [\[fabric1\\_table\]](#)
- [\[fabric2\\_table\]](#)

#### Tabella di configurazione del profilo fabric 1

Fabric dello switch	Interfaccia IPStorage	Indirizzo IP	Tipo di porta	Interfaccia FCIP	Profilo FCIP	Porta	IP/porta peer	ID VSAN
Switch_FC_A_1	IPStorage 1/1	1. a.a.	FC-VI	fcip 1	15	3220	c.c. c.c. c/3230	10
Storage	fcip 2	20	3221	c.c. c.c. c/3231	20	IPStorage 1/2	b.b.b.b	FC-VI
fcip 3	25	3222	d.d.g. d/3232	10	Storage	fcip 4	30	3223

d.d.g. d/3233	20	Switch_FC _B_1	IPStorage 1/1	1. c.c.c.	FC-VI	fcip 1	15	3230
a.a.a.a/32 20	10	Storage	fcip 2	20	3231	a.a.a.a/32 21	20	IPStorage 1/2
d.d.d.d	FC-VI	fcip 3	25	3232	b.b.b.b.b.b /3222	10	Storage	fcip 4

### Tabella di configurazione del profilo fabric 2

Fabric dello switch	Interfaccia IPStorage	Indirizzo IP	Tipo di porta	Interfaccia FCIP	Profilo FCIP	Porta	IP/porta peer	ID VSAN
Switch_FC _A_2	IPStorage 1/1	e.e.e.	FC-VI	fcip 1	15	3220	g.g. g.g.g./g/32 30	10
Storage	fcip 2	20	3221	g.g. g.g.g./g/32 31	20	IPStorage 1/2	f.f.f.f	FC-VI
fcip 3	25	3222	h.h.h. h./3232	10	Storage	fcip 4	30	3223
h.h.h. h./3233	20	Switch_FC _B_2	IPStorage 1/1	g.g.g.g	FC-VI	fcip 1	15	3230
e.e.e.e/32 20	10	Storage	fcip 2	20	3231	e.e.e.e/32 21	20	IPStorage 1/2
h.h.h.h	FC-VI	fcip 3	25	3232	f.f.f.f/3222	10	Storage	fcip 4

### Fasi

1. Accedere alla modalità di configurazione:

```
config t
```

2. Attiva FCIP:

```
feature fcip
```

3. Su ogni switch, configurare le due interfacce IPStorage ("IPStorage1/1" e "IPStorage1/2"):

- a. accedere alla modalità di configurazione:

```
conf t
```

- b. Specificare l'interfaccia IPStorage da creare:

```
interface ipstorage
```

Il *ipstorage* Il valore del parametro è "IPStorage1/1" o "IPStorage1/2".

- c. Specificare l'indirizzo IP e la subnet mask dell'interfaccia IPStorage precedentemente specificata:

```
interface ip-address subnet-mask
```



Su ogni switch, le interfacce IPStorage "IPStorage1/1" e "IPStorage1/2" devono avere indirizzi IP diversi.

- a. Specificare la dimensione MTU come 2500:

```
switchport mtu 2500
```

- b. Abilitare la porta:

```
no shutdown
```

- c. Esci dalla modalità di configurazione:

```
exit
```

- d. Ripetere [substep "a"](#) attraverso [substep "f"](#) Per configurare l'interfaccia GbE IPStorage1/2 con un indirizzo IP diverso.

4. Configurare i profili FCIP per il traffico FC-VI e storage con i nomi dei profili indicati nella tabella di configurazione del profilo:

- a. Accedere alla modalità di configurazione:

```
conf t
```

- b. Configurare i profili FCIP con i seguenti nomi di profilo:

```
fcip profile FCIP-profile-name
```

Nell'elenco riportato di seguito sono riportati i valori per *FCIP-profile-name* parametro:

- 15 per FC-VI su IPStorage1/1
- 20 per lo storage su IPStorage1/1
- 25 per FC-VI su IPStorage1/2
- 30 per lo storage su IPStorage1/2

- c. Assegnare le porte del profilo FCIP in base alla tabella di configurazione del profilo:

```
port port_number
```

- d. Per impostare le impostazioni TCP:

```
tcp keepalive-timeout 1
```

```

tcp max-retransmissions 3

max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3

tcp min-retransmit-time 200

tcp keepalive-timeout 1

tcp pmtu-enable reset-timeout 3600

tcp sack-enable

no tcp cwm

```

## 5. Creare interfacce FCIP:

```
interface fcip FCIP_interface
```

Il *FCIP\_interface* il valore del parametro è "1", "2", "3" o "4", come mostrato nella tabella di configurazione del profilo.

### a. Mappare le interfacce con i profili creati in precedenza:

```
use-profile profile
```

### b. Impostare l'indirizzo IP peer e il numero di porta del profilo peer:

```
peer-info peer IPstorage ipaddr port peer_profile_port_number
```

### c. Selezionare le connessioni TCP:

```
tcp-connection connection-#
```

Il *connection-#* Il valore del parametro è "2" per i profili FC-VI e "5" per i profili di storage.

### a. Disattiva compressione:

```
no ip-compression
```

### b. Abilitare l'interfaccia:

```
no shutdown
```

### c. Configurare la connessione TCP di controllo su "48" e la connessione dati su "26" per contrassegnare tutti i pacchetti con valore DSCP (differenziate Services code point):

```
qos control 48 data 26
```

### d. Uscire dalla modalità di configurazione:

```
exit
```

6. Configurare le impostazioni switchport su ciascuna interfaccia FCIP:

- a. Accedere alla modalità di configurazione:

```
config t
```

- b. Specificare la porta che si sta configurando:

```
interface fcip 1
```

- c. Chiudere la porta:

```
shutdown
```

- d. Impostare la porta in modalità e:

```
switchport mode E
```

- e. Attivare la modalità trunk per la porta:

```
switchport trunk mode on
```

- f. Specificare la linea consentita su un VSAN specifico:

```
switchport trunk allowed vsan vsan_id
```

Il valore del parametro *vsan\_id* è “VSAN 10” per i profili FC-VI e “VSAN 20” per i profili di storage.

- a. Impostare la velocità della porta:

```
switchport speed speed-value
```

- b. Uscire dalla modalità di configurazione:

```
exit
```

7. Copiare la configurazione aggiornata nella configurazione di avvio su entrambi gli switch:

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

I seguenti esempi mostrano la configurazione delle porte FCIP per un ISL doppio negli switch FC\_switch\_A\_1 e FC\_switch\_B\_1 del fabric 1.

**Per FC\_switch\_A\_1:**

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings
```



```

feature fcip

conf t
interface IPStorage1/1
# IP address: a.a.a.a
# Mask: y.y.y.y
ip address <a.a.a.a y.y.y.y>
switchport mtu 2500
no shutdown
exit
conf t
fcip profile 15
ip address <a.a.a.a>
port 3220
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pm tu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
fcip profile 20
ip address <a.a.a.a>
port 3221
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200
tcp keepalive-timeout 1
tcp pm tu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
interface IPStorage1/2
# IP address: b.b.b.b
# Mask: y.y.y.y
ip address <b.b.b.b y.y.y.y>
switchport mtu 2500
no shutdown
exit

```

```

conf t
fcip profile 25
    ip address <b.b.b.b>
    port 3222
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
    tcp min-retransmit-time 200
    tcp keepalive-timeout 1
    tcp pmtu-enable reset-timeout 3600
    tcp sack-enable
    no tcp cwm

conf t
fcip profile 30
    ip address <b.b.b.b>
    port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
    tcp min-retransmit-time 200
    tcp keepalive-timeout 1
    tcp pmtu-enable reset-timeout 3600
    tcp sack-enable
    no tcp cwm
interface fcip 1
    use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
    peer-info ipaddr <c.c.c.c> port 3230
    tcp-connection 2
    no ip-compression
    no shutdown
    qos control 48 data 26
exit

interface fcip 2
    use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
    peer-info ipaddr <c.c.c.c> port 3231
    tcp-connection 5
    no ip-compression

```

```

no shutdown
qos control 48 data 26
exit

interface fcip 3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr < d.d.d.d > port 3232
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip 4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
  peer-info ipaddr < d.d.d.d > port 3233
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip 1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip 2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip 3

```

```

shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip 4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

```

### Per FC\_switch\_B\_1:

```

FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature fcip

conf t
interface IPStorage1/1
# IP address: c.c.c.c
# Mask: y.y.y.y
ip address <c.c.c.c y.y.y.y>
switchport mtu 2500
no shutdown
exit

conf t
fcip profile 15
ip address <c.c.c.c>
port 3230
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
tcp min-retransmit-time 200

```

```

tcp keepalive-timeout 1
tcp pmtu-enable reset-timeout 3600
tcp sack-enable
no tcp cwm

conf t
fcip profile 20
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
# IP address: d.d.d.d
# Mask: y.y.y.y
  ip address <b.b.b.b y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233

```

```

tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
    tcp min-retransmit-time 200
    tcp keepalive-timeout 1
    tcp pmtu-enable reset-timeout 3600
    tcp sack-enable
    no tcp cwm

interface fcip 1
    use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
    peer-info ipaddr <a.a.a.a> port 3220
    tcp-connection 2
    no ip-compression
    no shutdown
    qos control 48 data 26
exit

interface fcip 2
    use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
    peer-info ipaddr <a.a.a.a> port 3221
    tcp-connection 5
    no ip-compression
    no shutdown
    qos control 48 data 26
exit

interface fcip 3
    use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
    peer-info ipaddr < b.b.b.b > port 3222
    tcp-connection 2
    no ip-compression
    no shutdown
    qos control 48 data 26
exit

interface fcip 4
    use-profile 30
# the port # listed in this command is the port that the remote switch is

```

```
listening on
peer-info ipaddr < b.b.b.b > port 3223
tcp-connection 5
no ip-compression
no shutdown
qos control 48 data 26
exit
```

```
conf t
interface fcip 1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip 2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

```
conf t
interface fcip 3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit
```

```
conf t
interface fcip 4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

## Configurazione dello zoning su uno switch FC Cisco

È necessario assegnare le porte dello switch a zone separate per isolare il traffico di storage (HBA) e controller (FC-VI).

### A proposito di questa attività

Questi passaggi devono essere eseguiti su entrambi i fabric switch FC.

La seguente procedura utilizza la suddivisione in zone descritta nella sezione suddivisione in zone per un FibreBridge 7500N in una configurazione MetroCluster a quattro nodi. Fare riferimento a ["Zoning per porte FC-VI"](#).

### Fasi

1. Cancellare le zone e il set di zone esistenti, se presenti.

a. Determinare quali zone e gruppi di zone sono attivi:

```
show zoneset active
```

```
FC_switch_A_1# show zoneset active
```

```
FC_switch_B_1# show zoneset active
```

b. Disattivare i set di zone attive identificati nel passaggio precedente:

```
no zoneset activate name zoneset_name vsan vsan_id
```

Nell'esempio seguente vengono mostrati due gruppi di zone disabilitati:

- ZoneSet\_A su FC\_switch\_A\_1 in VSAN 10
- ZoneSet\_B su FC\_switch\_B\_1 in VSAN 20

```
FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10
```

```
FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
```

c. Una volta disattivati tutti i set di zone, cancellare il database delle zone:

```
clear zone database zone-name
```

```
FC_switch_A_1# clear zone database 10
```

```
FC_switch_A_1# copy running-config startup-config
```

```
FC_switch_B_1# clear zone database 20
```

```
FC_switch_B_1# copy running-config startup-config
```

2. Ottenere il nome mondiale dello switch (WWN):



```
show wwn switch
```

### 3. Configurare le impostazioni di base della zona:

#### a. Impostare il criterio di zoning predefinito su "Permit":

```
no system default zone default-zone permit
```

#### b. Abilitare la distribuzione completa delle zone:

```
system default zone distribute full
```

#### c. Impostare il criterio di zoning predefinito per ogni VSAN:

```
no zone default-zone permit vsanid
```

#### d. Impostare la distribuzione di zona completa predefinita per ogni VSAN:

```
zoneset distribute full vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

### 4. Creare zone di storage e aggiungervi le porte di storage.



Eseguire questa procedura su un solo switch in ogni fabric.

Lo zoning dipende dal modello di bridge FC-SAS in uso. Per ulteriori informazioni, consulta la sezione relativa al tuo modello bridge. Gli esempi mostrano le porte dello switch Brocade, quindi regola le porte di conseguenza.

- "Zoning per i bridge 7500N o 7600N di FibreBridge attraverso una porta FC"
- "Zoning per i bridge FibreBridge 7500N che utilizzano entrambe le porte FC"

Ciascuna zona di storage contiene le porte HBA Initiator di tutti i controller e una singola porta che collega un bridge FC-SAS.

a. Creare le zone di storage:

```
zone name STOR-zone-name vsan vsanid
```

b. Aggiungere porte di storage alla zona:

```
member portswitch WWN
```

c. Attivare il set di zone:

```
zoneset activate name STOR-zone-name-setname vsan vsan-id
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. Creare un set di zone di storage e aggiungere le zone di storage al nuovo set.



Eseguire questa procedura su un solo switch nel fabric.

a. Creare il set di zone di storage:

```
zoneset name STOR-zone-set-name vsan vsan-id
```

b. Aggiunta di zone di storage al set di zone:

```
member STOR-zone-name
```

c. Attivare il set di zone:

```
zoneset activate name STOR-zone-set-name vsan vsanid
```

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan 20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Creare zone FCVI e aggiungervi le porte FCVI.

Ogni zona FCVI contiene le porte FCVI di tutti i controller di un gruppo DR.



Eseguire questa procedura su un solo switch nel fabric.

Lo zoning dipende dal modello di bridge FC-SAS in uso. Per ulteriori informazioni, consulta la sezione relativa al tuo modello bridge. Gli esempi mostrano le porte dello switch Brocade, quindi regola le porte di conseguenza.

- ["Zoning per i bridge 7500N o 7600N di FibreBridge attraverso una porta FC"](#)
- ["Zoning per i bridge FibreBridge 7500N che utilizzano entrambe le porte FC"](#)

Ciascuna zona di storage contiene le porte HBA Initiator di tutti i controller e una singola porta che collega un bridge FC-SAS.

a. Creare le zone FCVI:

```
zone name FCVI-zone-name vsan vsanid
```

b. Aggiungere le porte FCVI alla zona:

```
member FCVI-zone-name
```

c. Attivare il set di zone:

```
zoneset activate name FCVI-zone-name-set-name vsan vsanid
```

```

FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config

```

## 7. Creare un set di zone FCVI e aggiungervi le zone FCVI:



Eeguire questa procedura su un solo switch nel fabric.

### a. Creare il set di zone FCVI:

```
zoneset name FCVI_zone_set_name vsan vsan-id
```

### b. Aggiungere zone FCVI al gruppo di zone:

```
member FCVI_zonename
```

### c. Attivare il set di zone:

```
zoneset activate name FCVI_zone_set_name vsan vsan-id
```

```

FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config

```

## 8. Verificare lo zoning:

```
show zone
```

## 9. Ripetere i passaggi precedenti sul secondo fabric switch FC.

### **Assicurarsi che la configurazione dello switch FC sia salvata**

Assicurarsi che la configurazione dello switch FC sia salvata nella configurazione di avvio su tutti gli switch.

#### **Fase**

Eseguire il seguente comando su entrambi i fabric switch FC:

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

```
FC_switch_A_1# copy running-config startup-config
```

```
FC_switch_B_1# copy running-config startup-config
```

### **Installazione di bridge FC-SAS e shelf di dischi SAS**

Quando si aggiunge nuovo storage alla configurazione, si installano e cablano i bridge RTO FibreBridge e gli shelf di dischi SAS.

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

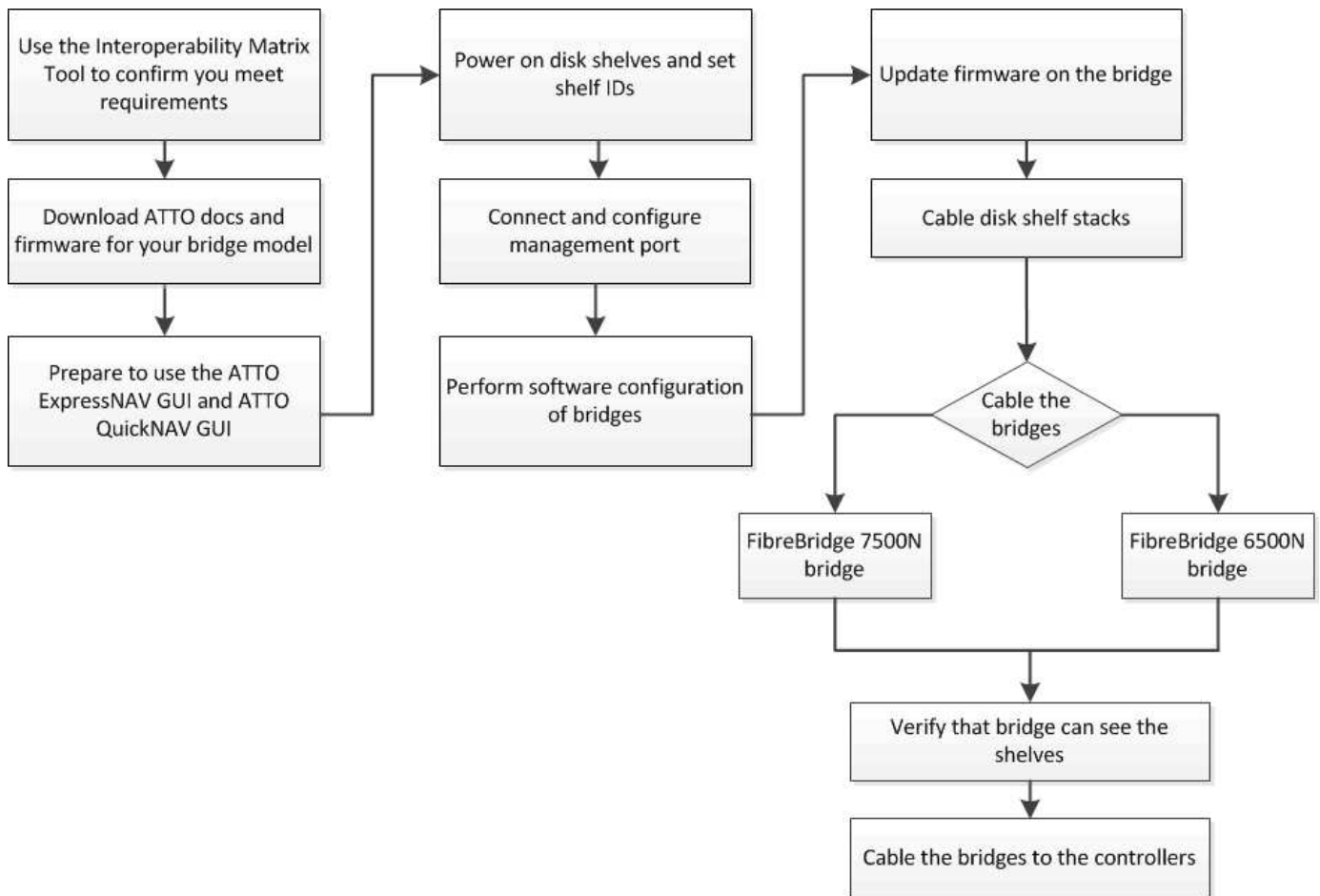
Per i sistemi ricevuti in fabbrica, i bridge FC-SAS sono preconfigurati e non richiedono alcuna configurazione aggiuntiva.

Questa procedura si basa sul presupposto che si stiano utilizzando le interfacce di gestione del bridge consigliate: L'interfaccia grafica di ATTO ExpressNAV e l'utility di barra di navigazione atto.

L'interfaccia grafica di ATTO ExpressNAV consente di configurare e gestire un bridge e di aggiornare il firmware del bridge. Utilizzare l'utility barra di navigazione atto per configurare la porta di gestione Ethernet del bridge 1.

Se necessario, è possibile utilizzare altre interfacce di gestione, ad esempio una porta seriale o Telnet, per configurare e gestire un bridge e per configurare la porta di gestione Ethernet 1 e FTP per aggiornare il firmware del bridge.

Questa procedura utilizza il seguente flusso di lavoro:



## Gestione in-band dei bridge FC-SAS

A partire dai bridge ONTAP 9.5 con FibreBridge 7500N o 7600N, la *gestione in-band* dei bridge è supportata come alternativa alla gestione IP dei bridge. A partire da ONTAP 9.8, la gestione fuori banda è obsoleta.



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

Quando si utilizza la gestione in-band, i bridge possono essere gestiti e monitorati dall'interfaccia CLI ONTAP tramite la connessione FC al bridge. Non è richiesto l'accesso fisico al bridge tramite le porte Ethernet del bridge, riducendo la vulnerabilità di sicurezza del bridge.

La disponibilità della gestione in-band dei bridge dipende dalla versione di ONTAP:

- A partire da ONTAP 9.8, i bridge vengono gestiti tramite connessioni in-band per impostazione predefinita e la gestione out-of-band dei bridge tramite SNMP è obsoleta.
- ONTAP da 9.5 a 9.7: È supportata la gestione in-band o fuori banda.
- Prima di ONTAP 9.5, è supportata solo la gestione SNMP out-of-band.

I comandi di Bridge CLI possono essere emessi dall'interfaccia ONTAP `storage bridge run-cli -name bridge_name -command bridge_command_name` All'interfaccia ONTAP.



Si consiglia di utilizzare la gestione in-band con accesso IP disattivato per migliorare la sicurezza limitando la connettività fisica del bridge.

## Preparazione per l'installazione

Quando si prepara l'installazione dei bridge come parte del nuovo sistema MetroCluster, è necessario assicurarsi che il sistema soddisfi determinati requisiti, tra cui il rispetto dei requisiti di configurazione e configurazione dei bridge. Altri requisiti includono il download dei documenti necessari, l'utility barra di navigazione atto e il firmware bridge.

### Prima di iniziare

- Il sistema deve essere già installato in un rack se non è stato spedito in un cabinet di sistema.
- La configurazione deve utilizzare modelli hardware e versioni software supportati.

In "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)", È possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

- Ogni switch FC deve disporre di una porta FC per il collegamento di un bridge.
- È necessario aver acquisito dimestichezza con la gestione dei cavi SAS e con le considerazioni e le Best practice per l'installazione e il cablaggio degli shelf di dischi.

La *Guida all'installazione e al servizio* per il modello di shelf di dischi descrive le considerazioni e le Best practice.

- Per utilizzare l'interfaccia grafica di ATTO ExpressNAV, il computer utilizzato per configurare i bridge deve disporre di un browser Web supportato da atto.

Le *note di rilascio dei prodotti atto* dispongono di un elenco aggiornato dei browser Web supportati. È possibile accedere a questo documento dal sito Web di atto come descritto nella seguente procedura.

### Fasi

1. Scarica la *Guida all'installazione e al servizio* per il tuo modello di shelf di dischi:
2. Accedere al sito Web atto utilizzando il collegamento fornito per il modello FibreBridge e scaricare il manuale e l'utility barra di navigazione.



Il *Manuale d'installazione e di funzionamento di FibreBridge atto* per il tuo modello bridge contiene ulteriori informazioni sulle interfacce di gestione.

Puoi accedere a questo e ad altri contenuti sul sito web di atto utilizzando il link fornito nella pagina ATTO Fibrebridge Description.

3. Raccogliere l'hardware e le informazioni necessarie per utilizzare le interfacce di gestione del bridge consigliate, l'interfaccia grafica di ATTO ExpressNAV e l'utility di navigazione atto:
  - a. Determinare un nome utente e una password non predefiniti (per l'accesso ai bridge).

Modificare il nome utente e la password predefiniti.

- b. Per la configurazione della gestione IP dei bridge, è necessario il cavo Ethernet schermato fornito con i bridge (che collega la porta di gestione Ethernet del bridge 1 alla rete).

- c. Se si configura per la gestione IP dei bridge, è necessario disporre di un indirizzo IP, di una subnet mask e di informazioni sul gateway per la porta di gestione Ethernet 1 su ciascun bridge.
- d. Disattivare i client VPN sul computer in uso per la configurazione.

I client VPN attivi causano un errore nella ricerca di bridge nella barra di navigazione.

## Installazione del bridge FC-SAS e degli shelf SAS

Dopo aver effettuato la verifica che il sistema soddisfi tutti i requisiti di “preparazione dell’installazione”, è possibile installare il nuovo sistema.

### A proposito di questa attività

- La configurazione del disco e dello shelf in entrambi i siti deve essere identica.

Se si utilizza un aggregato non mirrorato, la configurazione di disco e shelf in ogni sito potrebbe essere diversa.



Tutti i dischi del gruppo di disaster recovery devono utilizzare lo stesso tipo di connessione ed essere visibili a tutti i nodi del gruppo di disaster recovery, indipendentemente dai dischi utilizzati per l’aggregato mirrorato o non mirrorato.

- I requisiti di connettività di sistema per le distanze massime per shelf di dischi, switch FC e dispositivi a nastro di backup che utilizzano cavi in fibra ottica multimodale da 50 micron si applicano anche ai bridge FibreBridge.

["NetApp Hardware Universe"](#)

- Una combinazione di moduli IOM12 e moduli IOM3 non è supportata nello stesso stack di storage. Una combinazione di moduli IOM12 e moduli IOM6 è supportata nello stesso stack di storage se il sistema esegue una versione supportata di ONTAP.



L’ACP in-band è supportato senza cavi aggiuntivi nei seguenti shelf e bridge FibreBridge 7500N o 7600N:

- IOM12 (DS460C) dietro un bridge 7500N o 7600N con ONTAP 9.2 e versioni successive
- IOM12 (DS212C e DS224C) con un bridge 7500N o 7600N con ONTAP 9.1 e versioni successive



Gli shelf SAS nelle configurazioni MetroCluster non supportano il cablaggio ACP.

### Abilitazione dell’accesso alla porta IP sul bridge FibreBridge 7600N, se necessario

Se si utilizza una versione di ONTAP precedente alla 9.5 o si intende utilizzare un accesso out-of-band al bridge FibreBridge 7600N utilizzando telnet o altri protocolli e servizi di porta IP (FTP, ExpressNAV, ICMP o barra di navigazione), è possibile attivare i servizi di accesso tramite la porta della console.

### A proposito di questa attività

A differenza dei bridge atto FibreBridge 7500N, il bridge FibreBridge 7600N viene fornito con tutti i protocolli e i servizi delle porte IP disattivati.

A partire da ONTAP 9.5, è supportata la *gestione in-band* dei bridge. Ciò significa che i bridge possono essere configurati e monitorati dall’interfaccia CLI ONTAP tramite la connessione FC al bridge. Non è richiesto



l'accesso fisico al bridge tramite le porte Ethernet del bridge e non sono necessarie le interfacce utente del bridge.

A partire da ONTAP 9.8, la *gestione in-band* dei bridge è supportata per impostazione predefinita e la gestione SNMP out-of-band è obsoleta.

Questa attività è necessaria se si utilizza **non** la gestione in-band per gestire i bridge. In questo caso, è necessario configurare il bridge tramite la porta di gestione Ethernet.

### Fasi

1. Accedere all'interfaccia della console del bridge collegando un cavo seriale alla porta seriale del bridge FibreBridge 7600N.
2. Utilizzando la console, attivare i servizi di accesso, quindi salvare la configurazione:

```
set closeport none
```

```
saveconfiguration
```

Il `set closeport none` il comando attiva tutti i servizi di accesso sul bridge.

3. Disattivare un servizio, se lo si desidera, emettendo `set closeport` e ripetere il comando secondo necessità fino a quando tutti i servizi desiderati non vengono disattivati:

```
set closeport service
```

Il `set closeport` il comando disattiva un singolo servizio alla volta.

Il parametro `service` è possibile specificare una delle seguenti opzioni:

- navigazione veloce
- ftp
- icmp
- barra di navigazione
- snmp
- telnet

È possibile verificare se un protocollo specifico è attivato o disattivato utilizzando `get closeport` comando.

4. Se si attiva SNMP, è necessario immettere anche il seguente comando:

```
set SNMP enabled
```

SNMP è l'unico protocollo che richiede un comando di abilitazione separato.

5. Salvare la configurazione:

```
saveconfiguration
```

## Configurazione dei bridge FC-SAS

Prima di collegare il modello di bridge FC-SAS, è necessario configurare le impostazioni nel software FibreBridge.

### Prima di iniziare

Devi decidere se utilizzare la gestione in-band dei bridge.



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

### A proposito di questa attività

Se si utilizza la gestione in-band del bridge piuttosto che la gestione IP, è possibile saltare i passaggi per la configurazione della porta Ethernet e delle impostazioni IP, come indicato nei relativi passaggi.

### Fasi

1. Configurare la porta della console seriale su ATTO FibreBridge impostando la velocità della porta su 115000 baud:

```
get serialportbaudrate
SerialPortBaudRate = 115200

Ready.

set serialportbaudrate 115200

Ready. *
saveconfiguration
Restart is necessary....
Do you wish to restart (y/n) ? y
```

2. Se si esegue la configurazione per la gestione in banda, collegare un cavo dalla porta seriale RS-232 di FibreBridge alla porta seriale (COM) di un personal computer.

La connessione seriale viene utilizzata per la configurazione iniziale, quindi la gestione in-band tramite ONTAP e le porte FC possono essere utilizzate per monitorare e gestire il bridge.

3. Se si esegue la configurazione per la gestione IP, collegare la porta Ethernet 1 di gestione di ciascun bridge alla rete utilizzando un cavo Ethernet.

Nei sistemi che eseguono ONTAP 9.5 o versioni successive, è possibile utilizzare la gestione in-band per accedere al bridge tramite le porte FC anziché la porta Ethernet. A partire da ONTAP 9.8, è supportata solo la gestione in-band e la gestione SNMP è obsoleta.

La porta di gestione Ethernet 1 consente di scaricare rapidamente il firmware del bridge (utilizzando le interfacce di gestione ATTO ExpressNAV o FTP) e di recuperare i file principali ed estrarre i log.

4. Se si esegue la configurazione per la gestione IP, configurare la porta di gestione Ethernet 1 per ciascun bridge seguendo la procedura descritta nella sezione 2.0 del *ATTO FibreBridge Installation and Operation*

*Manual* per il modello di bridge in uso.

Nei sistemi che eseguono ONTAP 9.5 o versioni successive, è possibile utilizzare la gestione in-band per accedere al bridge tramite le porte FC anziché la porta Ethernet. A partire da ONTAP 9.8, è supportata solo la gestione in-band e la gestione SNMP è obsoleta.

Quando si esegue la barra di navigazione per configurare una porta di gestione Ethernet, viene configurata solo la porta di gestione Ethernet collegata tramite il cavo Ethernet. Ad esempio, se si desidera configurare anche la porta di gestione Ethernet 2, è necessario collegare il cavo Ethernet alla porta 2 ed eseguire la barra di navigazione.

## 5. Configurare il bridge.

Annotare il nome utente e la password designati.



Non configurare la sincronizzazione dell'ora su ATTO FibreBridge 7600N o 7500N. La sincronizzazione temporale per ATTO FibreBridge 7600N o 7500N viene impostata sul tempo del cluster dopo il rilevamento del bridge da parte di ONTAP. Viene inoltre sincronizzato periodicamente una volta al giorno. Il fuso orario utilizzato è GMT e non è modificabile.

### a. Se si esegue la configurazione per la gestione IP, configurare le impostazioni IP del bridge.

Nei sistemi che eseguono ONTAP 9.5 o versioni successive, è possibile utilizzare la gestione in-band per accedere al bridge tramite le porte FC anziché la porta Ethernet. A partire da ONTAP 9.8, è supportata solo la gestione in-band e la gestione SNMP è obsoleta.

Per impostare l'indirizzo IP senza l'utilità barra di navigazione, è necessario disporre di una connessione seriale a FibreBridge.

Se si utilizza l'interfaccia CLI, è necessario eseguire i seguenti comandi:

```
set ipaddress mp1 ip-address  
  
set ipsubnetmask mp1 subnet-mask  
  
set ipgateway mp1 x.x.x.x  
  
set ipdhcp mp1 disabled  
  
set ethernetspeed mp1 1000
```

### b. Configurare il nome del bridge.

I bridge devono avere un nome univoco all'interno della configurazione MetroCluster.

Esempi di nomi di bridge per un gruppo di stack su ciascun sito:

- bridge\_A\_1a
- bridge\_A\_1b
- bridge\_B\_1a
- bridge\_B\_1b

Se si utilizza la CLI, è necessario eseguire il seguente comando:

```
set bridgename bridge_name
```

- c. Se si esegue ONTAP 9.4 o versioni precedenti, attivare SNMP sul bridge:

```
set SNMP enabled
```

Nei sistemi che eseguono ONTAP 9.5 o versioni successive, è possibile utilizzare la gestione in-band per accedere al bridge tramite le porte FC anziché la porta Ethernet. A partire da ONTAP 9.8, è supportata solo la gestione in-band e la gestione SNMP è obsoleta.

## 6. Configurare le porte FC del bridge.

- a. Configurare la velocità/velocità dei dati delle porte FC del bridge.

La velocità di trasferimento dati FC supportata dipende dal modello di bridge in uso.

- Il bridge FibreBridge 7600N supporta fino a 32, 16 o 8 Gbps.
- Il bridge FibreBridge 7500N supporta fino a 16, 8 o 4 Gbps.



La velocità FCDataRate selezionata è limitata alla velocità massima supportata sia dal bridge che dalla porta FC del modulo controller a cui si connette la porta bridge. Le distanze di cablaggio non devono superare i limiti degli SFP e di altri hardware.

Se si utilizza la CLI, è necessario eseguire il seguente comando:

```
set FCDataRate port-number port-speed
```

- b. Se si sta configurando un bridge FibreBridge 7500N, configurare la modalità di connessione utilizzata dalla porta su "ptp".



L'impostazione FCConnMode non è richiesta quando si configura un bridge FibreBridge 7600N.

Se si utilizza la CLI, è necessario eseguire il seguente comando:

```
set FCConnMode port-number ptp
```

- c. Se si sta configurando un bridge FibreBridge 7600N o 7500N, è necessario configurare o disattivare la porta FC2.

- Se si utilizza la seconda porta, è necessario ripetere i passaggi precedenti per la porta FC2.
- Se non si utilizza la seconda porta, è necessario disattivarla:

```
FCPortDisable port-number
```

L'esempio seguente mostra la disattivazione della porta FC 2:

```
FCPortDisable 2
```

```
Fibre Channel Port 2 has been disabled.
```

- a. Se si sta configurando un bridge FibreBridge 7600N o 7500N, disattivare le porte SAS inutilizzate:

```
SASPortDisable sas-port
```



Le porte SAS Da A a D sono attivate per impostazione predefinita. È necessario disattivare le porte SAS non utilizzate.

Se si utilizza solo la porta SAS A, è necessario disattivare le porte SAS B, C e D. Nell'esempio seguente viene illustrata la disattivazione della porta SAS B. Analogamente, è necessario disattivare le porte SAS C e D:

```
SASPortDisable b
```

```
SAS Port B has been disabled.
```

7. Accesso sicuro al bridge e salvataggio della configurazione del bridge. Scegliere un'opzione tra quelle riportate di seguito, a seconda della versione di ONTAP in esecuzione nel sistema.

Versione di ONTAP	Fasi
<b>ONTAP 9.5 o versione successiva</b>	<p>a. Visualizzare lo stato dei bridge:</p> <pre>storage bridge show</pre> <p>L'output mostra quale bridge non è protetto.</p> <p>b. Fissare il bridge:</p> <pre>securebridge</pre>

**ONTAP 9.4 o versione precedente**

a. Visualizzare lo stato dei bridge:

```
storage bridge show
```

L'output mostra quale bridge non è protetto.

b. Controllare lo stato delle porte del bridge non protetto:

```
info
```

L'output mostra lo stato delle porte Ethernet MP1 e MP2.

c. Se la porta Ethernet MP1 è abilitata, eseguire:

```
set EthernetPort mp1 disabled
```

Se è attivata anche la porta Ethernet MP2, ripetere il passaggio precedente per la porta MP2.

d. Salvare la configurazione del bridge.

È necessario eseguire i seguenti comandi:

```
SaveConfiguration
```

```
FirmwareRestart
```

Viene richiesto di riavviare il bridge.

8. Dopo aver completato la configurazione MetroCluster, utilizzare `flashimages` Comando per verificare la versione del firmware FibreBridge in uso e, se i bridge non utilizzano la versione più recente supportata, aggiornare il firmware su tutti i bridge nella configurazione.

["Gestire i componenti di MetroCluster"](#)

**Informazioni correlate**

["Gestione in-band dei bridge FC-SAS"](#)

**Collegamento degli shelf di dischi ai bridge**

Per il cablaggio degli shelf di dischi, è necessario utilizzare i bridge FC-SAS corretti.

**Scelte**

- [Collegamento di un bridge FibreBridge 7600N o 7500N con shelf di dischi mediante moduli IOM12](#)
- [Collegamento di un bridge FibreBridge 7600N o 7500N con shelf di dischi utilizzando moduli IOM6 o IOM3](#)

**Collegamento di un bridge FibreBridge 7600N o 7500N con shelf di dischi mediante moduli IOM12**

Dopo aver configurato il bridge, è possibile iniziare a cablare il nuovo sistema.

**A proposito di questa attività**

Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore).

## Fasi

### 1. Collegamento a margherita degli shelf di dischi in ogni stack:

- a. A partire dal primo shelf logico nello stack, collegare la porta IOM A 3 alla porta IOM A 1 dello shelf successivo fino a collegare ciascun IOM A dello stack.
- b. Ripetere il passaggio precedente per IOM B.
- c. Ripetere i passaggi precedenti per ogni stack.

La *Guida all'installazione e al servizio* per il modello di shelf di dischi fornisce informazioni dettagliate sugli shelf di dischi con concatenamento a margherita.

### 2. Accendere gli shelf di dischi, quindi impostare gli ID dello shelf.

- È necessario spegnere e riaccendere ogni shelf di dischi.
- Gli shelf ID devono essere univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster (inclusi entrambi i siti).

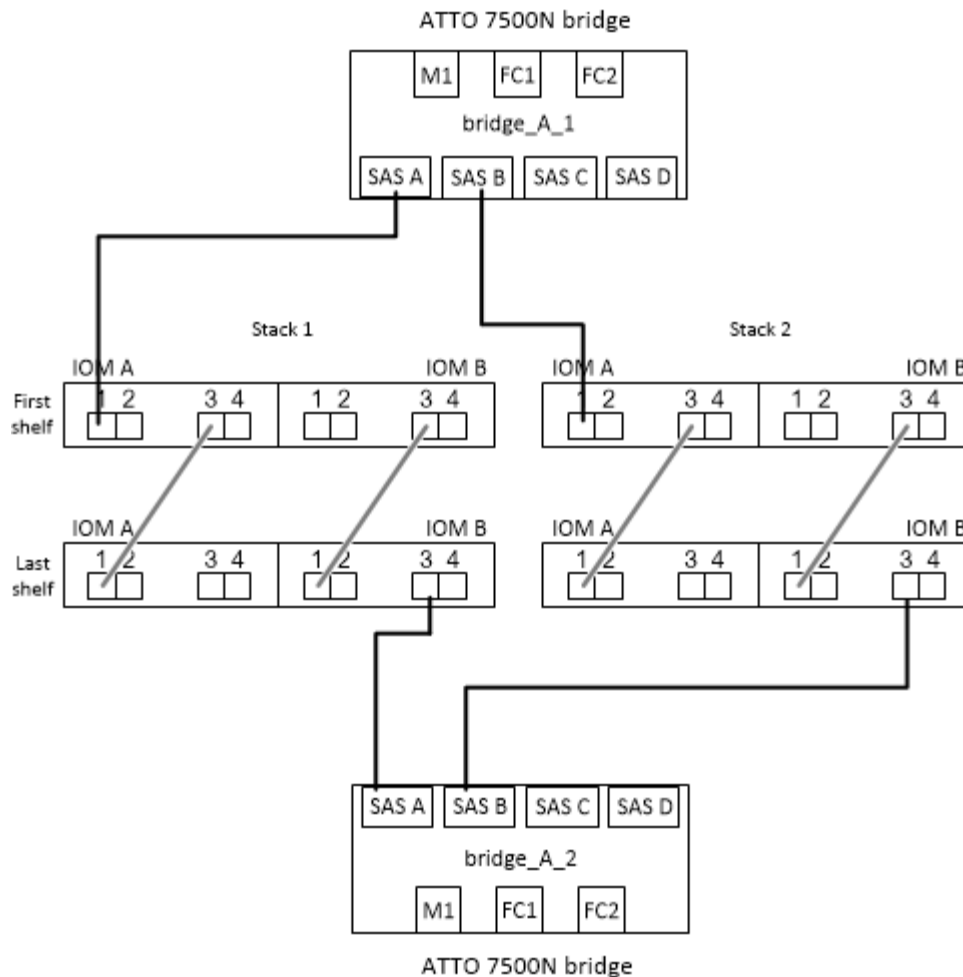
### 3. Collegare gli shelf di dischi ai bridge FibreBridge.

- a. Per il primo stack di shelf di dischi, collegare il cavo IOM A del primo shelf alla porta SAS A su FibreBridge A e il cavo IOM B dell'ultimo shelf alla porta SAS A su FibreBridge B.
- b. Per ulteriori stack di shelf, ripetere il passaggio precedente utilizzando la successiva porta SAS disponibile sui bridge FibreBridge, utilizzando la porta B per il secondo stack, la porta C per il terzo stack e la porta D per il quarto stack.
- c. Durante il cablaggio, collegare gli stack basati sui moduli IOM12 e IOM3/IOM6 allo stesso bridge, purché siano collegati a porte SAS separate.



Ogni stack può utilizzare diversi modelli di IOM, ma tutti gli shelf di dischi all'interno di uno stack devono utilizzare lo stesso modello.

La figura seguente mostra gli shelf di dischi collegati a una coppia di bridge FibreBridge 7600N o 7500N:



## Collegamento di un bridge FibreBridge 7600N o 7500N con shelf utilizzando moduli IOM6 o IOM3

Dopo aver configurato il bridge, è possibile iniziare a cablare il nuovo sistema. Il bridge FibreBridge 7600N o 7500N utilizza connettori mini-SAS e supporta shelf che utilizzano moduli IOM6 o IOM3.

### A proposito di questa attività

I moduli IOM3 non sono supportati con i bridge FibreBridge 7600N.

Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore).

### Fasi

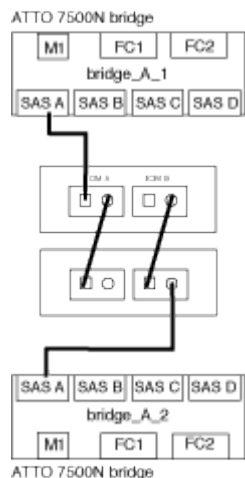
1. Concatenare a margherita gli shelf in ogni stack.
  - a. Per il primo stack di shelf, collegare IOM A una porta quadrata del primo shelf alla porta SAS A su FibreBridge A.
  - b. Per il primo stack di shelf, collegare la porta IOM B circolare dell'ultimo shelf alla porta SAS A su FibreBridge B.

La *Guida all'installazione e al servizio* per il modello di shelf fornisce informazioni dettagliate sugli shelf con concatenamento a margherita.

["Guida all'installazione e al servizio degli shelf di dischi SAS per DS4243, DS2246, DS4486 e DS4246"](#)

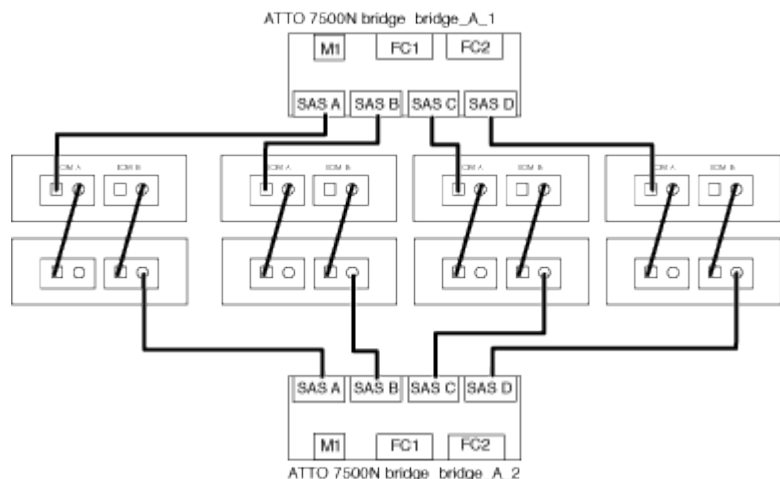


La figura seguente mostra un set di bridge collegati a una pila di shelf:



- Per ulteriori stack di shelf, ripetere i passaggi precedenti utilizzando la successiva porta SAS disponibile sui bridge FibreBridge, utilizzando la porta B per un secondo stack, la porta C per un terzo stack e la porta D per un quarto stack.

La figura seguente mostra quattro stack collegati a una coppia di bridge FibreBridge 7600N o 7500N.



### Verifica della connettività del bridge e cablaggio delle porte FC del bridge

Verificare che ciascun bridge sia in grado di rilevare tutte le unità disco, quindi collegare ciascun bridge agli switch FC locali.

### Fasi

- verificare che ciascun bridge sia in grado di rilevare tutti i dischi e gli shelf di dischi a cui è collegato:

Se si utilizza...	Quindi...
-------------------	-----------

GUI ExpressNAV	<p>a. In un browser Web supportato, inserire l'indirizzo IP di un bridge nella casella del browser.</p> <p>Viene visualizzato il sito Web di ATTO FibreBridge del bridge per il quale è stato immesso l'indirizzo IP, che dispone di un collegamento.</p> <p>b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge.</p> <p>Viene visualizzata la pagina di stato di ATTO FibreBridge del bridge con un menu a sinistra.</p> <p>c. Fare clic su <b>Avanzate</b>.</p> <p>d. Visualizzare i dispositivi collegati utilizzando il comando <code>sastargets</code>, quindi fare clic su <b>Submit</b> (Invia).</p>
Connessione alla porta seriale	<p>Visualizzare i dispositivi connessi:</p> <p><code>sastargets</code></p>

L'output mostra i dispositivi (dischi e shelf di dischi) a cui è collegato il bridge. Le linee di output sono numerate in sequenza in modo da poter contare rapidamente i dispositivi. Ad esempio, il seguente output mostra che sono collegati 10 dischi:

```

Tgt  VendorID  ProductID          Type          SerialNumber
0  NETAPP    X410_S15K6288A15  DISK          3QP1CLE300009940UHJV
1  NETAPP    X410_S15K6288A15  DISK          3QP1ELF600009940V1BV
2  NETAPP    X410_S15K6288A15  DISK          3QP1G3EW00009940U2M0
3  NETAPP    X410_S15K6288A15  DISK          3QP1EWMP00009940U1X5
4  NETAPP    X410_S15K6288A15  DISK          3QP1FZLE00009940G8YU
5  NETAPP    X410_S15K6288A15  DISK          3QP1FZLF00009940TZKZ
6  NETAPP    X410_S15K6288A15  DISK          3QP1CEB400009939MGXL
7  NETAPP    X410_S15K6288A15  DISK          3QP1G7A900009939FNNTT
8  NETAPP    X410_S15K6288A15  DISK          3QP1FY0T00009940G8PA
9  NETAPP    X410_S15K6288A15  DISK          3QP1FXW600009940VERQ

```



Se all'inizio dell'output viene visualizzato il testo "response troncato", è possibile utilizzare Telnet per connettersi al bridge e immettere lo stesso comando per visualizzare tutto l'output.

- Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi nello stack a cui dovrebbe essere collegato.

Se l'output è...	Quindi...
Esatto	Ripetere <a href="#">Fase 1</a> per ogni bridge rimanente.

Non corretto	<p>a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo il cablaggio.</p> <p><a href="#">Collegamento degli shelf di dischi ai bridge</a></p> <p>b. Ripetere <a href="#">Fase 1</a>.</p>
--------------	--

3. Collegare ciascun bridge agli switch FC locali, utilizzando i cavi riportati nella tabella per il modello di configurazione e di switch e il modello di bridge FC-SAS:



La seconda connessione alla porta FC sul bridge FibreBridge 7500N non deve essere cablata fino al completamento della zoning.

Vedere le assegnazioni delle porte per la versione di ONTAP in uso.

4. Ripetere la fase precedente sui bridge presso il sito del partner.

### Informazioni correlate

["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)

Quando si utilizzano ONTAP 9.1 e versioni successive, verificare di utilizzare le assegnazioni delle porte specificate quando si cablano gli switch FC.

["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

Quando si cablano gli switch FC, verificare di utilizzare le assegnazioni delle porte specificate. Le assegnazioni delle porte sono diverse tra ONTAP 9.0 e la versione successiva di ONTAP.

### Protezione o annullamento della protezione del bridge FibreBridge

Per disattivare facilmente i protocolli Ethernet potenzialmente non sicuri su un bridge, a partire da ONTAP 9.5 è possibile proteggere il bridge. In questo modo vengono disattivate le porte Ethernet del bridge. È anche possibile riabilitare l'accesso Ethernet.

#### A proposito di questa attività

- La protezione del bridge disattiva il protocollo telnet e altri protocolli e servizi delle porte IP (FTP, ExpressNAV, ICMP o barra di navigazione) sul bridge.
- Questa procedura utilizza la gestione out-of-band utilizzando il prompt ONTAP, disponibile a partire da ONTAP 9.5.

Se non si utilizza la gestione fuori banda, è possibile eseguire i comandi dalla CLI del bridge.

- Il `unsecurebridge` Il comando può essere utilizzato per riattivare le porte Ethernet.
- In ONTAP 9.7 e versioni precedenti, con l'esecuzione di `securebridge` Il comando sul FibreBridge atto potrebbe non aggiornare correttamente lo stato del bridge sul cluster partner. In tal caso, eseguire `securebridge` dal cluster partner.



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

## Fasi

1. Dal prompt ONTAP del cluster contenente il bridge, proteggere o non proteggere il bridge.

- Il seguente comando protegge Bridge\_A\_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
```

- Il seguente comando sprotette Bridge\_A\_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
```

2. Dal prompt ONTAP del cluster contenente il bridge, salvare la configurazione del bridge:

```
storage bridge run-cli -bridge bridge-name -command saveconfiguration
```

Il seguente comando protegge Bridge\_A\_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command  
saveconfiguration
```

3. Dal prompt ONTAP del cluster che contiene il bridge, riavviare il firmware del bridge:

```
storage bridge run-cli -bridge bridge-name -command firmwarerestart
```

Il seguente comando protegge Bridge\_A\_1:

```
cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
```

## Configurare l'hardware per la condivisione di un fabric FC Brocade 6510 durante la transizione

### Configurazione dell'hardware per la condivisione di un fabric FC Brocade 6510 durante la transizione

Se la configurazione 7-Mode Fabric MetroCluster utilizza switch Brocade 6510, è possibile condividere i fabric switch esistenti con la nuova configurazione Clustered MetroCluster. Fabric switch condivisi significa che la nuova configurazione MetroCluster non richiede un nuovo fabric switch separato. Questa configurazione temporanea è supportata solo con lo switch Brocade 6510 a scopo di transizione.

#### Prima di iniziare

- 7-Mode Fabric MetroCluster deve utilizzare switch Brocade 6510.

Se la configurazione MetroCluster non utilizza attualmente switch Brocade 6510, è necessario aggiornare gli switch a Brocade 6510 prima di utilizzare questa procedura.

- La configurazione 7-Mode Fabric MetroCluster deve utilizzare solo shelf di storage SAS.

Se la configurazione esistente include shelf di storage FC (come DS14mk4 FC), la condivisione fabric dello switch FC non è supportata.

- Gli SFP sulle porte dello switch utilizzati dalla nuova configurazione Clustered MetroCluster devono supportare velocità a 16 Gbps.

Il fabric MetroCluster 7-Mode esistente può rimanere connesso alle porte utilizzando SFP a 8 Gbps o 16 Gbps.

- Su ciascuno dei quattro switch Brocade 6510, le porte da 24 a 45 devono essere disponibili per collegare le porte dei nuovi componenti MetroCluster.
- Verificare che i collegamenti Inter-Switch (ISL) esistenti si trovino sulle porte 46 e 47.
- Gli switch Brocade 6510 devono eseguire una versione del firmware FOS supportata sia nella configurazione 7-Mode Fabric MetroCluster che in quella Clustered ONTAP MetroCluster.

### Al termine

Dopo aver condiviso il fabric e aver completato la configurazione MetroCluster, è possibile trasferire i dati dalla configurazione 7-Mode Fabric MetroCluster.

Dopo aver effettuato la transizione dei dati, è possibile rimuovere il cablaggio 7-Mode Fabric MetroCluster e, se necessario, spostare il cablaggio Clustered ONTAP MetroCluster sulle porte con numero inferiore precedentemente utilizzate per il cablaggio 7-Mode MetroCluster. Le porte sono illustrate nella sezione "analisi delle assegnazioni delle porte degli switch FC per un MetroCluster a quattro nodi". È necessario regolare lo zoning per le porte ridisposte.

["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)

### Informazioni correlate

["Transizione basata sulla copia"](#)

## Analisi dei requisiti di licenza Brocade

Sono necessarie alcune licenze per gli switch in una configurazione MetroCluster. È necessario installare queste licenze su tutti e quattro gli switch.

La configurazione di MetroCluster prevede i seguenti requisiti di licenza Brocade:

- Licenza trunking per sistemi che utilizzano più di un ISL, come consigliato.
- Licenza fabric estesa (per distanze ISL superiori a 6 km)
- Licenza Enterprise per siti con più di un ISL e una distanza ISL superiore a 6 km

La licenza Enterprise include Brocade Network Advisor e tutte le licenze, ad eccezione delle licenze per porte aggiuntive.

È possibile verificare che le licenze siano installate utilizzando il comando "licenza".

#### Per Fabric OS 8.2.x e versioni precedenti

Eseguire il comando `licenseshow`.

#### Per Fabric OS 9.0 e versioni successive

Eseguire il comando `license --show`.

Se non si dispone di queste licenze, contattare il rappresentante commerciale prima di procedere.

## 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.

#### "Documentazione dei sistemi hardware ONTAP"

4. Installare gli switch FC 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.
  - Gli shelf ID devono essere univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster (inclusi entrambi i siti).
6. Installare ciascun bridge FC-SAS:

- a. Fissare le staffe "L" sulla parte anteriore del bridge alla parte anteriore del rack (montaggio a filo) con le quattro viti.

Le aperture delle staffe "L" del ponte sono conformi allo standard ETA-310-X per rack da 19" (482.6 mm).

Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il modello di bridge contiene ulteriori informazioni e un'illustrazione dell'installazione.



Per un accesso adeguato allo spazio delle porte e una manutenzione FRU adeguata, è necessario lasciare uno spazio 1U sotto la coppia di bridge e coprire questo spazio con un pannello di chiusura senza utensili.

- b. Collegare ciascun bridge a una fonte di alimentazione che fornisca una messa a terra adeguata.
- c. Accendere ciascun bridge.



Per ottenere la massima resilienza, i bridge collegati allo stesso stack di shelf di dischi devono essere collegati a diverse fonti di alimentazione.

Il LED Bridge Ready potrebbe impiegare fino a 30 secondi per accendersi, a indicare che il bridge ha completato la sequenza di test automatico all'accensione.

## Collegamento dei nuovi controller MetroCluster ai fabric FC esistenti

Su ciascun controller nella configurazione Clustered ONTAP MetroCluster, l'adattatore FC-VI e gli HBA devono essere cablati a porte specifiche sugli switch FC esistenti.

### Fasi

1. Collegare le porte FC-VI e HBA in base alla seguente tabella:

Sito A		Sito B	
Collegare il sito A un componente e una porta...	Porta FC_switch_A_1...	Collegare il componente e la porta del sito B...	Porta FC_switch_B_1...
Controller_A_1 porta FC-VI 1	32	Controller_B_1 porta FC-VI 1	32
Controller_A_1 porta HBA 1	33	Controller_B_1 porta HBA 1	33
Controller_A_1 porta HBA 2	34	Controller_B_1 porta HBA 2	34
Controller_A_2 porta FC-VI 1	35	Controller_B_2 porta FC-VI 1	35
Controller_A_2 HBA 1	36	Controller_B_2 HBA 1	36
Controller_A_2 HBA 2	37	Controller_B_2 HBA 2	37

2. Collegare ciascun bridge FC-SAS nel primo fabric switch agli switch FC.

Il numero di bridge varia in base al numero di stack di storage SAS.

Sito A		Sito B	
Collegare questo sito A un ponte...	Porta FC_switch_A_1...	Collegare il bridge del sito B...	Porta FC_switch_B_1...
bridge_A_1_38	38	bridge_B_1_38	38
bridge_A_1_39	39	bridge_B_1_39	39

3. Collegare ciascun bridge nel secondo fabric switch agli switch FC.

Il numero di bridge varia in base al numero di stack di storage SAS.

Sito A		Sito B	
Collegare questo sito A un ponte...	Porta FC_switch_A_2...	Collegare il bridge del sito B...	Porta FC_switch_B_2...

bridge_A_2_38	38	bridge_B_2_38	38
bridge_A_2_39	39	bridge_B_2_39	39

## Configurare la condivisione di fabric switch tra la configurazione 7-Mode e Clustered MetroCluster

### Disattivazione di uno dei fabric dello switch

È necessario disattivare uno dei fabric dello switch per modificarne la configurazione. Una volta completata la configurazione e riattivata la struttura dello switch, ripetere la procedura sull'altro fabric.

#### Prima di iniziare

È necessario eseguire l'utility `fmc_DC` sulla configurazione Fabric MetroCluster 7-Mode esistente e risolvere eventuali problemi prima di iniziare il processo di configurazione.

#### A proposito di questa attività

Per garantire il funzionamento continuo della configurazione MetroCluster, non è necessario disattivare il secondo fabric mentre il primo fabric è disattivato.

#### Fasi

1. Disattivare ciascuno switch nel fabric:

```
switchCfgPersistentDisable
```

Se questo comando non è disponibile, utilizzare `switchDisable` comando.

- L'esempio seguente mostra il comando emesso su `FC_switch_A_1`:

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

- L'esempio seguente mostra il comando emesso su `FC_switch_B_1`:

```
FC_switch_B_1:admin> switchCfgPersistentDisable
```

2. Assicurarsi che la configurazione 7-Mode MetroCluster funzioni correttamente utilizzando il fabric ridondante:

- a. Verificare che il failover del controller sia integro:

```
cf status
```

```
node_A> cf status
Controller Failover enabled, node_A is up.
VIA Interconnect is up (link 0 down, link 1 up).
```



b. Verificare che i dischi siano visibili:

```
storage show disk -p
```

```
node_A> storage show disk -p
```

PRIMARY	PORT	SECONDARY	PORT	SHELF	BAY
Brocade-6510-2K0GG:5.126L27	B			1	0
Brocade-6510-2K0GG:5.126L28	B			1	1
Brocade-6510-2K0GG:5.126L29	B			1	2
Brocade-6510-2K0GG:5.126L30	B			1	3
Brocade-6510-2K0GG:5.126L31	B			1	4
.					
.					
.					

c. Verificare che gli aggregati siano integri:

```
aggr status
```

```
node_A> aggr status
```

Aggr State	Status	Options
aggr0 online	raid_dp, aggr mirrored 64-bit	root, nosnap=on

## Eliminazione dello zoning ti e configurazione delle impostazioni IOD

È necessario eliminare lo zoning ti esistente e riconfigurare le impostazioni IOD (in-order-delivery) sul fabric dello switch.

### Fasi

1. Identificare le zone ti configurate sul fabric:

```
zone --show
```

L'esempio seguente mostra la zona FCVI\_ti\_FAB\_2.

```
Brocade-6510:admin> zone --show
```

```
Defined TI zone configuration:
```

```
TI Zone Name:    FCVI_TI_FAB_2
```

```
Port List:       1,0; 1,3; 2,0; 2,3
```

```
configured Status: Activated / Failover-Disabled
```

```
Enabled Status: Activated / Failover-Disabled
```

2. Eliminare le zone ti:

```
zone --delete zone-name
```

L'esempio seguente mostra l'eliminazione della zona FCVI\_ti\_FAB\_2.

```
Brocade-6510:admin> zone --delete FCVI_TI_FAB_2
```

3. Verificare che le zone siano state eliminate:

```
zone --show
```

L'output dovrebbe essere simile a quanto segue:

```
Brocade-6510:admin> zone --show

Defined TI zone configuration:
no TI zone configuration defined
```

4. Salvare la configurazione:

```
cfgsave
```

5. Abilitare la consegna in-order:

```
iodset
```

6. Selezionare Advanced Performance Tuning (APT) policy 1, quindi Port Based Routing Policy (criterio di routing basato su porta):

```
aptpolicy 1
```

7. Disattiva Dynamic Load Sharing (DLS):

```
dlsreset
```

8. Verificare le impostazioni IOD:

```
iodshow
```

```
aptpolicy
```

```
dlsshow
```

L'output dovrebbe essere simile a quanto segue:

```
Brocade-6510:admin> iodshow

IOD is set

Brocade-6510:admin> aptpolicy
Current Policy: 1

3 : Default Policy
1: Port Based Routing Policy
2: Device Based Routing Policy (FICON support only)
3: Exchange Based Routing Policy
Brocade-6510:admin> dlsshow

DLS is not set
```

### Garantire che gli ISL si trovino nello stesso gruppo di porte e configurare lo zoning

Assicurarsi che i collegamenti interswitch (ISL) si trovino nello stesso gruppo di porte e configurare lo zoning per le configurazioni MetroCluster in modo che condividano correttamente i fabric switch.

#### Fasi

1. Se gli ISL non si trovano nello stesso gruppo di porte, spostare una delle porte ISL nello stesso gruppo di porte dell'altra.

È possibile utilizzare qualsiasi porta disponibile, ad eccezione di 32 fino a 45, utilizzata dalla nuova configurazione MetroCluster. Le porte ISL consigliate sono 46 e 47.

2. Seguire la procedura descritta in ["Configurazione dello zoning sugli switch Brocade FC"](#) Sezione per attivare il trunking e la zona QoS.

I numeri delle porte durante la condivisione dei fabric sono diversi da quelli mostrati nella sezione. Durante la condivisione, utilizzare le porte 46 e 47 per le porte ISL. Se sono state spostate le porte ISL, è necessario utilizzare la procedura descritta in ["Configurazione delle e-port \(porte ISL\) su uno switch FC Brocade"](#) per configurare le porte.

3. [\[\[fase 3\\_zone\]\]](#) seguire i passaggi descritti nella ["Configurazione delle porte non-e sullo switch Brocade"](#) Sezione per configurare le porte non-E.
4. Non eliminare le zone o i set di zone già presenti negli switch back-end (per 7-Mode Fabric MetroCluster) ad eccezione delle zone di isolamento del traffico (ti) in [Fase 3](#).
5. Seguire la procedura descritta in ["Configurazione delle e-port \(porte ISL\) su uno switch FC Brocade"](#) Sezione per aggiungere le zone richieste dal nuovo MetroCluster ai set di zone esistenti.

L'esempio seguente mostra i comandi e l'output di sistema per la creazione delle zone:

```

Brocade-6510-2K0GG:admin> zonecreate "QOSH2_FCVI_1", "2,32; 2,35; 1,32;
1,35"

Brocade-6510-2K0GG:admin> zonecreate "STOR_A_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 1,47"

Brocade-6510-2K0GG:admin> zonecreate "STOR_B_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 2,47"

Brocade-6510-2K0GG:admin> cfgadd config_1_FAB2, "QOSH2_FCVI_1;
STOR_A_2_47; STOR_B_2_47"

Brocade-6510-2K0GG:admin> cfgenable "config_1_FAB2"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'config_1_FAB2' configuration (yes, y, no, n):
[no] yes

Brocade-6510-2K0GG:admin> cfsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only? (yes, y, no,
n): [no] yes
Nothing changed: nothing to save, returning ...
Brocade-6510-2K0GG:admin>

```

## Riabilitare il fabric dello switch e verificarne il funzionamento

È necessario attivare il fabric dello switch FC e assicurarsi che gli switch e i dispositivi funzionino correttamente.

### Fasi

1. Abilitare gli switch:

```
switchCfgPersistentEnable
```

Se questo comando non è disponibile, lo switch deve trovarsi nello stato abilitato dopo `fastBoot` viene emesso il comando.

- L'esempio seguente mostra il comando emesso su `FC_switch_A_1`:

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

- L'esempio seguente mostra il comando emesso su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> switchCfgPersistentEnable
```

2. Verificare che gli switch siano in linea e che tutti i dispositivi siano collegati correttamente:

```
switchShow
```

L'esempio seguente mostra il comando emesso su FC\_switch\_A\_1:

```
FC_switch_A_1:admin> switchShow
```

L'esempio seguente mostra il comando emesso su FC\_switch\_B\_1:

```
FC_switch_B_1:admin> switchShow
```

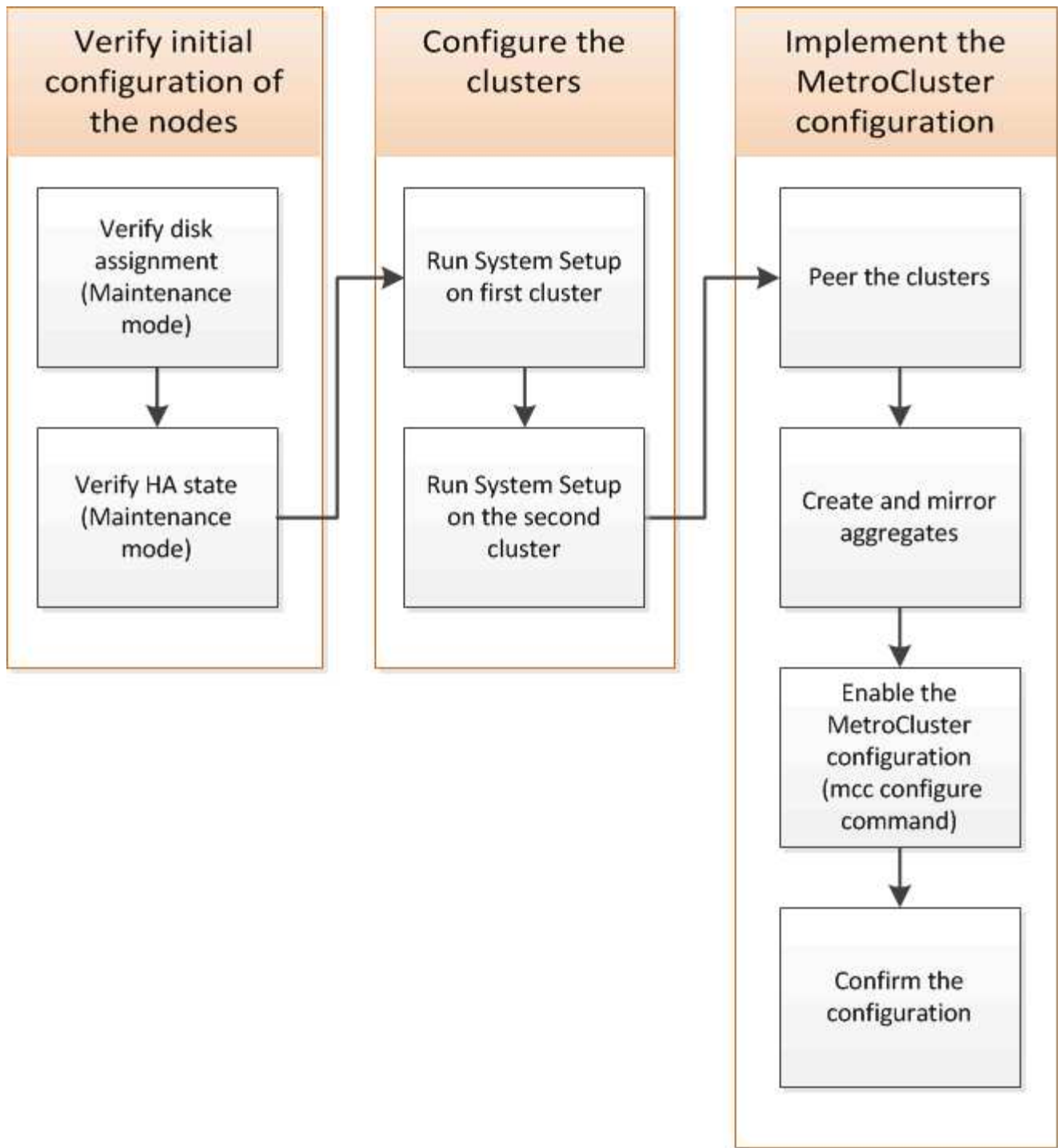
3. Eseguire l'utility `fmc_DC` per assicurarsi che 7-Mode Fabric MetroCluster funzioni correttamente.

È possibile ignorare gli errori relativi allo zoning e al trunking dell'isolamento del traffico (ti).

4. Ripetere le operazioni per il secondo fabric dello switch.

## 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. I passaggi per i sistemi con shelf di dischi nativi sono leggermente diversi da quelli per i sistemi con LUN di array.



## Raccolta delle informazioni richieste

Prima di iniziare il processo di configurazione, è necessario raccogliere gli indirizzi IP richiesti per i moduli controller.

### Foglio di lavoro con le informazioni sulla rete IP per il sito A.

Prima di configurare il sistema, è necessario ottenere gli indirizzi IP e altre informazioni di rete per il primo sito MetroCluster (sito A) dall'amministratore di rete.

### Informazioni sullo switch del sito A (cluster con switch)

Quando si collega il sistema, è necessario disporre di un nome host e di un indirizzo IP di gestione per ogni switch del cluster. Queste informazioni non sono necessarie se si utilizza un cluster senza switch a due nodi o se si dispone di una configurazione MetroCluster a due nodi (un nodo per ogni sito).

Switch del cluster	Nome host	Indirizzo IP	Maschera di rete	Gateway predefinito
Interconnessione 1				
Interconnessione 2				
Gestione 1				
Gestione 2				

### Informazioni sulla creazione del cluster del sito A.

Quando si crea il cluster per la prima volta, sono necessarie le seguenti informazioni:

Tipo di informazione	I tuoi valori
Nome del cluster Esempio utilizzato in questa guida: Site_A.	
Dominio DNS	
Server dei nomi DNS	
Posizione	
Password dell'amministratore	

### Informazioni sul nodo del sito A.

Per ciascun nodo del cluster, sono necessari un indirizzo IP di gestione, una maschera di rete e un gateway predefinito.

Nodo	Porta	Indirizzo IP	Maschera di rete	Gateway predefinito
Nodo 1 Esempio utilizzato in questa guida: Controller_A_1				

<p>Nodo 2</p> <p>Non richiesto se si utilizza una configurazione MetroCluster a due nodi (un nodo per ogni sito).</p> <p>Esempio utilizzato in questa guida: Controller_A_2</p>				
---	--	--	--	--

#### Porta e LIF del sito A per il peering del cluster

Per ciascun nodo del cluster, sono necessari gli indirizzi IP di due LIF intercluster, tra cui una maschera di rete e un gateway predefinito. Le LIF dell'intercluster vengono utilizzate per eseguire il peer dei cluster.

Nodo	Porta	Indirizzo IP della LIF dell'intercluster	Maschera di rete	Gateway predefinito
Nodo 1 IC LIF 1				
Nodo 1 IC LIF 2				
<p>Nodo 2 IC LIF 1</p> <p>Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).</p>				
<p>Nodo 2 IC LIF 2</p> <p>Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).</p>				

#### Informazioni sul server di riferimento orario del sito A.

È necessario sincronizzare l'ora, che richiede uno o più server di riferimento orario NTP.

Nodo	Nome host	Indirizzo IP	Maschera di rete	Gateway predefinito
Server NTP 1				
Server NTP 2				



### Sito A informazioni AutoSupport

È necessario configurare AutoSupport su ciascun nodo, che richiede le seguenti informazioni:

Tipo di informazione		I tuoi valori
Da indirizzo e-mail		Mail host
Indirizzi IP o nomi		Protocollo di trasporto
HTTP, HTTPS O SMTP		Server proxy
	Indirizzi e-mail o liste di distribuzione del destinatario	Messaggi completi
	Messaggi concisi	

### Sito A informazioni SP

È necessario abilitare l'accesso al Service Processor (SP) di ciascun nodo per la risoluzione dei problemi e la manutenzione, che richiede le seguenti informazioni di rete per ciascun nodo:

Nodo	Indirizzo IP	Maschera di rete	Gateway predefinito
Nodo 1			
Nodo 2			
Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).			

### Foglio di lavoro con le informazioni della rete IP per il sito B

Prima di configurare il sistema, è necessario ottenere gli indirizzi IP e altre informazioni di rete per il secondo sito MetroCluster (sito B) dall'amministratore di rete.

#### Informazioni sullo switch del sito B (cluster con switch)

Quando si collega il sistema, è necessario disporre di un nome host e di un indirizzo IP di gestione per ogni switch del cluster. Queste informazioni non sono necessarie se si utilizza un cluster senza switch a due nodi o si dispone di una configurazione MetroCluster a due nodi (un nodo per ogni sito).

Switch del cluster	Nome host	Indirizzo IP	Maschera di rete	Gateway predefinito
Interconnessione 1				
Interconnessione 2				

Gestione 1				
Gestione 2				

#### Informazioni sulla creazione del cluster del sito B.

Quando si crea il cluster per la prima volta, sono necessarie le seguenti informazioni:

Tipo di informazione	I tuoi valori
Nome del cluster	
Esempio utilizzato in questa guida: Site_B.	
Dominio DNS	
Server dei nomi DNS	
Posizione	
Password dell'amministratore	

#### Informazioni sul nodo del sito B.

Per ciascun nodo del cluster, sono necessari un indirizzo IP di gestione, una maschera di rete e un gateway predefinito.

Nodo	Porta	Indirizzo IP	Maschera di rete	Gateway predefinito
Nodo 1				
Esempio utilizzato in questa guida: Controller_B_1				
Nodo 2				
Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).				
Esempio utilizzato in questa guida: Controller_B_2				

### LIF e porte del sito B per il peering dei cluster

Per ciascun nodo del cluster, sono necessari gli indirizzi IP di due LIF intercluster, tra cui una maschera di rete e un gateway predefinito. Le LIF dell'intercluster vengono utilizzate per eseguire il peer dei cluster.

Nodo	Porta	Indirizzo IP della LIF dell'intercluster	Maschera di rete	Gateway predefinito
Nodo 1 IC LIF 1				
Nodo 1 IC LIF 2				
Nodo 2 IC LIF 1  Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).				
Nodo 2 IC LIF 2  Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).				

### Informazioni sul server di riferimento orario del sito B.

È necessario sincronizzare l'ora, che richiede uno o più server di riferimento orario NTP.

Nodo	Nome host	Indirizzo IP	Maschera di rete	Gateway predefinito
Server NTP 1				
Server NTP 2				

### Sito B nbsp;informazioni AutoSupport

È necessario configurare AutoSupport su ciascun nodo, che richiede le seguenti informazioni:

Tipo di informazione		I tuoi valori
Da indirizzo e-mail		
Mail host	Indirizzi IP o nomi	
Protocollo di trasporto	HTTP, HTTPS O SMTP	

Server proxy		Indirizzi e-mail o liste di distribuzione del destinatario
Messaggi completi		Messaggi concisi
	Partner	

#### Sito B informazioni SP

È necessario abilitare l'accesso al Service Processor (SP) di ciascun nodo per la risoluzione dei problemi e la manutenzione, che richiede le seguenti informazioni di rete per ciascun nodo:

Nodo	Indirizzo IP	Maschera di rete	Gateway predefinito
Nodo 1 (controller_B_1)			
Nodo 2 (controller_B_2)			
Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito).			

## 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	
Configurare i nodi nel cluster come coppie ha	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
---	-----------------	--------------

## Ripristino delle impostazioni predefinite del sistema e configurazione del tipo di HBA su un modulo controller

### A proposito di questa attività

Per garantire una corretta installazione di MetroCluster, ripristinare le impostazioni predefinite dei moduli controller.

### Importante

Questa attività è necessaria solo per le configurazioni stretch che utilizzano bridge FC-SAS.

### Fasi

1. Al prompt DEL CARICATORE, riportare le variabili ambientali alle impostazioni predefinite:

```
set-defaults
```

2. Avviare il nodo in modalità manutenzione, quindi configurare le impostazioni per gli HBA nel sistema:

- a. Avviare in modalità di manutenzione:

```
boot_ontap maint
```

- b. Verificare le impostazioni correnti delle porte:

```
ucadmin show
```

- c. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata...	Utilizzare questo comando...
FC CNA	<pre>ucadmin modify -m fc -t initiator adapter_name</pre>
Ethernet CNA	<pre>ucadmin modify -mode cna adapter_name</pre>
Destinazione FC	<pre>fcadmin config -t target adapter_name</pre>
Iniziatore FC	<pre>fcadmin config -t initiator adapter_name</pre>

3. Uscire dalla modalità di manutenzione:

```
halt
```

Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

4. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

```
boot_ontap maint
```

5. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA...	Utilizzare questo comando...
CNA	<code>ucadmin show</code>
FC	<code>fcadmin show</code>

6. Uscire dalla modalità di manutenzione:

```
halt
```

Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

7. Avviare il nodo dal menu di boot:

```
boot_ontap menu
```

Dopo aver eseguito il comando, attendere che venga visualizzato il menu di avvio.

8. Cancellare la configurazione del nodo digitando “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.

## Configurazione delle porte FC-VI su una scheda X1132A-R6 quad-port su sistemi FAS8020

Se si utilizza la scheda a quattro porte X1132A-R6 su un sistema FAS8020, è possibile accedere alla modalità di manutenzione per configurare le porte 1a e 1b per l'utilizzo di FC-VI e Initiator. Questa operazione non è necessaria sui sistemi MetroCluster ricevuti dalla fabbrica, in cui le porte sono impostate in modo appropriato per la configurazione.

### A proposito di questa attività

Questa attività deve essere eseguita in modalità manutenzione.



La conversione di una porta FC in una porta FC-VI con il comando `ucadmin` è supportata solo sui sistemi FAS8020 e AFF 8020. La conversione delle porte FC in porte FCVI non è supportata su altre piattaforme.

### Fasi

#### 1. Disattivare le porte:

```
storage disable adapter 1a
```

```
storage disable adapter 1b
```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

#### 2. Verificare che le porte siano disattivate:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
-----	-----	-----	-----	-----	-----
...					
1a	fc	initiator	-	-	offline
1b	fc	initiator	-	-	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

### 3. Impostare le porte a e b sulla modalità FC-VI:

```
ucadmin modify -adapter 1a -type fcvi
```

Il comando imposta la modalità su entrambe le porte della coppia di porte, 1a e 1b (anche se solo 1a è specificata nel comando).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

### 4. Confermare che la modifica è in sospeso:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
-----	-----	-----	-----	-----	-----
...					
1a	fc	initiator	-	fcvi	offline
1b	fc	initiator	-	fcvi	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

### 5. Spegner il controller, quindi riavviarlo in modalità di manutenzione.

### 6. Confermare la modifica della configurazione:

```
ucadmin show local
```



```

Node           Adapter  Mode   Type           Mode   Type           Status
-----
...
controller_B_1
      1a         fc     fcvi           -       -           online
controller_B_1
      1b         fc     fcvi           -       -           online
controller_B_1
      1c         fc     initiator      -       -           online
controller_B_1
      1d         fc     initiator      -       -           online
6 entries were displayed.

```

## Verifica dell'assegnazione dei dischi in modalità Maintenance in una configurazione a otto o quattro nodi

Prima di avviare completamente il sistema su ONTAP, è possibile eseguire l'avvio in modalità manutenzione e verificare l'assegnazione dei dischi sui nodi. I dischi devono essere assegnati per creare una configurazione Active-Active completamente simmetrica, in cui ciascun pool ha un numero uguale di dischi assegnati.

### A proposito di questa attività

I nuovi sistemi MetroCluster hanno completato l'assegnazione dei dischi prima della spedizione.

La tabella seguente mostra esempi di assegnazioni di pool per una configurazione MetroCluster. I dischi vengono assegnati ai pool in base allo shelf.

### Shelf di dischi nel sito A

Shelf di dischi (nome_shelf_campione)...	Appartiene a...	E viene assegnato al nodo...
Shelf di dischi 1 (shelf_A_1_1)	Nodo A 1	Pool 0
Shelf di dischi 2 (shelf_A_1_3)		
Shelf di dischi 3 (shelf_B_1_1)	Nodo B 1	Pool 1
Shelf di dischi 4 (shelf_B_1_3)		
Shelf di dischi 5 (shelf_A_2_1)	Nodo A 2	Pool 0
Shelf di dischi 6 (shelf_A_2_3)		
Shelf di dischi 7 (shelf_B_2_1)	Nodo B 2	Pool 1
Shelf di dischi 8 (shelf_B_2_3)		
Shelf di dischi 1 (shelf_A_3_1)	Nodo A 3	Pool 0
Shelf di dischi 2 (shelf_A_3_3)		

Shelf di dischi 3 (shelf_B_3_1)	Nodo B 3	Pool 1
Shelf di dischi 4 (shelf_B_3_3)		
Shelf di dischi 5 (shelf_A_4_1)	Nodo A 4	Pool 0
Shelf di dischi 6 (shelf_A_4_3)		
Shelf di dischi 7 (shelf_B_4_1)	Nodo B 4	Pool 1
Shelf di dischi 8 (shelf_B_4_3)		

### Shelf di dischi nel sito B

Shelf di dischi (nome_shelf_campione)...	Appartiene a...	E viene assegnato al nodo...
Shelf di dischi 9 (shelf_B_1_2)	Nodo B 1	Pool 0
Shelf di dischi 10 (shelf_B_1_4)	Shelf di dischi 11 (shelf_A_1_2)	Nodo A 1
Pool 1	Shelf di dischi 12 (shelf_A_1_4)	Shelf di dischi 13 (shelf_B_2_2)
Nodo B 2	Pool 0	Shelf di dischi 14 (shelf_B_2_4)
Shelf di dischi 15 (shelf_A_2_2)	Nodo A 2	Pool 1
Shelf di dischi 16 (shelf_A_2_4)	Shelf di dischi 1 (shelf_B_3_2)	Nodo A 3
Pool 0	Shelf di dischi 2 (shelf_B_3_4)	Shelf di dischi 3 (shelf_A_3_2)
Nodo B 3	Pool 1	Shelf di dischi 4 (shelf_A_3_4)
Shelf di dischi 5 (shelf_B_4_2)	Nodo A 4	Pool 0
Shelf di dischi 6 (shelf_B_4_4)	Shelf di dischi 7 (shelf_A_4_2)	Nodo B 4

### Fasi

1. Confermare le assegnazioni degli shelf:

```
disk show -v
```

2. Se necessario, assegnare esplicitamente i dischi sugli shelf di dischi collegati al pool appropriato:

```
disk assign
```

L'utilizzo dei caratteri jolly nel comando consente di assegnare tutti i dischi su uno shelf di dischi con un unico comando. È possibile identificare gli ID e gli alloggiamenti degli shelf di dischi per ciascun disco con `storage show disk -x` comando.

## Assegnazione della proprietà del disco in sistemi non AFF

Se i dischi non sono stati assegnati correttamente ai nodi MetroCluster o se si utilizzano shelf di dischi DS460C nella configurazione, è necessario assegnare i dischi a ciascuno dei nodi nella configurazione MetroCluster in base allo shelf-by-shelf. Verrà creata una configurazione in cui ciascun nodo ha lo stesso numero di dischi nei pool di dischi locali e remoti.

### Prima di iniziare

I controller dello storage devono essere in modalità Maintenance (manutenzione).

### A proposito di questa attività

Se la configurazione non include shelf di dischi DS460C, questa attività non è necessaria se i dischi sono stati assegnati correttamente al momento della ricezione dalla fabbrica.



Il pool 0 contiene sempre i dischi che si trovano nello stesso sito del sistema di storage che li possiede.

Il pool 1 contiene sempre i dischi remoti del sistema di storage proprietario.

Se la configurazione include shelf di dischi DS460C, è necessario assegnare manualmente i dischi utilizzando le seguenti linee guida per ciascun cassetto da 12 dischi:

Assegnare questi dischi nel cassetto...	A questo nodo e pool...
0 - 2	Pool del nodo locale 0
3 - 5	Pool del nodo partner HA 0
6 - 8	Partner DR del pool del nodo locale 1
9 - 11	Partner DR del pool del partner ha 1

Questo schema di assegnazione dei dischi garantisce che un aggregato venga influenzato in modo minimo nel caso in cui un cassetto venga scollegato.

### Fasi

1. In caso contrario, avviare ciascun sistema in modalità di manutenzione.
2. Assegnare gli shelf di dischi ai nodi situati nel primo sito (sito A):

Gli shelf di dischi nello stesso sito del nodo vengono assegnati al pool 0 e gli shelf di dischi situati nel sito del partner vengono assegnati al pool 1.

È necessario assegnare un numero uguale di shelf a ciascun pool.

- a. Sul primo nodo, assegnare sistematicamente gli shelf di dischi locali al pool 0 e gli shelf di dischi remoti al pool 1:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

Se lo storage controller Controller Controller Controller\_A\_1 dispone di quattro shelf, eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

- b. Ripetere la procedura per il secondo nodo nel sito locale, assegnando sistematicamente gli shelf di dischi locali al pool 0 e gli shelf di dischi remoti al pool 1:

```
disk assign -shelf local-switch-name:shelf-name.port -p pool
```

Se lo storage controller Controller Controller Controller\_A\_2 dispone di quattro shelf, eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

### 3. Assegnare gli shelf di dischi ai nodi situati nel secondo sito (sito B):

Gli shelf di dischi nello stesso sito del nodo vengono assegnati al pool 0 e gli shelf di dischi situati nel sito del partner vengono assegnati al pool 1.

È necessario assegnare un numero uguale di shelf a ciascun pool.

- a. Sul primo nodo del sito remoto, assegnare sistematicamente i propri shelf di dischi locali al pool 0 e i relativi shelf di dischi remoti al pool 1:

```
disk assign -shelf local-switch-namesshelf-name -p pool
```

Se lo storage controller Controller Controller Controller\_B\_1 dispone di quattro shelf, eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

- b. Ripetere la procedura per il secondo nodo del sito remoto, assegnando sistematicamente i propri shelf di dischi locali al pool 0 e i relativi shelf di dischi remoti al pool 1:

```
disk assign -shelf shelf-name -p pool
```

Se lo storage controller Controller Controller Controller\_B\_2 dispone di quattro shelf, eseguire i

seguenti comandi:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confermare le assegnazioni degli shelf:

```
storage show shelf
```

5. Uscire dalla modalità di manutenzione:

```
halt
```

6. Visualizzare il menu di avvio:

```
boot_ontap menu
```

7. Su ciascun nodo, selezionare l'opzione **4** per inizializzare tutti i dischi.

### Assegnazione della proprietà del disco nei sistemi AFF

Se si utilizzano sistemi AFF in una configurazione con aggregati mirrorati e i nodi non hanno i dischi (SSD) assegnati correttamente, è necessario assegnare metà dei dischi su ogni shelf a un nodo locale e l'altra metà dei dischi al nodo partner ha. È necessario creare una configurazione in cui ciascun nodo abbia lo stesso numero di dischi nei pool di dischi locali e remoti.

#### Prima di iniziare

I controller dello storage devono essere in modalità Maintenance (manutenzione).

#### A proposito di questa attività

Ciò non si applica alle configurazioni che hanno aggregati senza mirror, una configurazione attiva/passiva o che hanno un numero di dischi diverso nei pool locali e remoti.

Questa attività non è necessaria se i dischi sono stati assegnati correttamente al momento della ricezione dalla fabbrica.



Il pool 0 contiene sempre i dischi che si trovano nello stesso sito del sistema di storage che li possiede.

Il pool 1 contiene sempre i dischi remoti del sistema di storage proprietario.

#### Fasi

1. In caso contrario, avviare ciascun sistema in modalità di manutenzione.
2. Assegnare i dischi ai nodi situati nel primo sito (sito A):

È necessario assegnare un numero uguale di dischi a ciascun pool.

- a. Sul primo nodo, assegnare sistematicamente metà dei dischi su ogni shelf al pool 0 e l'altra metà al pool 0 del partner ha:

```
disk assign -disk disk-name -p pool -n number-of-disks
```

Se lo storage controller Controller Controller\_A\_1 ha quattro shelf, ciascuno con 8 SSD, devi eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

- b. Ripetere la procedura per il secondo nodo del sito locale, assegnando sistematicamente metà dei dischi su ogni shelf al pool 1 e l'altra metà al pool 1 del partner ha:

```
disk assign -disk disk-name -p pool
```

Se lo storage controller Controller Controller\_A\_1 ha quattro shelf, ciascuno con 8 SSD, devi eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

### 3. Assegnare i dischi ai nodi situati nel secondo sito (sito B):

È necessario assegnare un numero uguale di dischi a ciascun pool.

- a. Sul primo nodo del sito remoto, assegnare sistematicamente metà dei dischi su ogni shelf al pool 0 e l'altra metà al pool del partner ha 0:

```
disk assign -disk disk-name -p pool
```

Se lo storage controller Controller Controller\_B\_1 ha quattro shelf, ciascuno con 8 SSD, devi eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

- b. Ripetere la procedura per il secondo nodo del sito remoto, assegnando sistematicamente metà dei

dischi su ogni shelf al pool 1 e l'altra metà al pool 1 del partner ha:

```
disk assign -disk disk-name -p pool
```

Se lo storage controller Controller Controller Controller\_B\_2 dispone di quattro shelf, ciascuno con 8 SSD, devi eseguire i seguenti comandi:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

#### 4. Confermare le assegnazioni dei dischi:

```
storage show disk
```

#### 5. Uscire dalla modalità di manutenzione:

```
halt
```

#### 6. Visualizzare il menu di avvio:

```
boot_ontap menu
```

#### 7. Su ciascun nodo, selezionare l'opzione **4** per inizializzare tutti i dischi.

## Verifica dell'assegnazione dei dischi in modalità manutenzione in una configurazione a due nodi

Prima di avviare completamente il sistema su ONTAP, è possibile avviare il sistema in modalità manutenzione e verificare l'assegnazione dei dischi sui nodi. I dischi devono essere assegnati in modo da creare una configurazione completamente simmetrica con entrambi i siti che possiedono i propri shelf di dischi e i dati di servizio, in cui a ciascun nodo e a ciascun pool è assegnato un numero uguale di dischi mirrorati.

### Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

### A proposito di questa attività

I nuovi sistemi MetroCluster hanno completato l'assegnazione dei dischi prima della spedizione.

La tabella seguente mostra esempi di assegnazioni di pool per una configurazione MetroCluster. I dischi vengono assegnati ai pool in base allo shelf.

Shelf di dischi (nome di esempio)...	Sul sito...	Appartiene a...	E viene assegnato al nodo...
--------------------------------------	-------------	-----------------	------------------------------

Shelf di dischi 1 (shelf_A_1_1)	Sito A	Nodo A 1	Pool 0
Shelf di dischi 2 (shelf_A_1_3)			
Shelf di dischi 3 (shelf_B_1_1)		Nodo B 1	Pool 1
Shelf di dischi 4 (shelf_B_1_3)			
Shelf di dischi 9 (shelf_B_1_2)	Sito B	Nodo B 1	Pool 0
Shelf di dischi 10 (shelf_B_1_4)			
Shelf di dischi 11 (shelf_A_1_2)		Nodo A 1	Pool 1
Shelf di dischi 12 (shelf_A_1_4)			

Se la configurazione include shelf di dischi DS460C, è necessario assegnare manualmente i dischi utilizzando le seguenti linee guida per ciascun cassetto da 12 dischi:

Assegnare questi dischi nel cassetto...	A questo nodo e pool...
1 - 6	Pool del nodo locale 0
7 - 12	Pool del partner DR 1

Questo schema di assegnazione dei dischi riduce al minimo l'effetto su un aggregato se un cassetto passa offline.

## Fasi

1. Se il sistema è stato ricevuto dalla fabbrica, confermare le assegnazioni degli shelf:

```
disk show -v
```

2. Se necessario, è possibile assegnare esplicitamente i dischi sugli shelf di dischi collegati al pool appropriato utilizzando il comando `disk assign`.

Gli shelf di dischi nello stesso sito del nodo vengono assegnati al pool 0 e gli shelf di dischi situati nel sito del partner vengono assegnati al pool 1. È necessario assegnare un numero uguale di shelf a ciascun pool.

- a. In caso contrario, avviare ciascun sistema in modalità di manutenzione.
- b. Sul nodo del sito A, assegnare sistematicamente gli shelf di dischi locali al pool 0 e gli shelf di dischi remoti al pool 1:

```
disk assign -shelf disk_shelf_name -p pool
```

Se lo storage controller `node_A_1` dispone di quattro shelf, eseguire i seguenti comandi:



```
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0

*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
```

- c. Sul nodo del sito remoto (sito B), assegnare sistematicamente i propri shelf di dischi locali al pool 0 e i relativi shelf di dischi remoti al pool 1:

```
disk assign -shelf disk_shelf_name -p pool
```

Se lo storage controller node\_B\_1 dispone di quattro shelf, eseguire i seguenti comandi:

```
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0

*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
```

- a. Mostrare gli ID e gli alloggiamenti degli shelf di dischi per ciascun disco:

```
disk show -v
```

## Verifica e configurazione dello stato ha dei componenti in modalità manutenzione

Quando si configura un sistema storage in una configurazione MetroCluster, è necessario assicurarsi che lo stato di alta disponibilità (ha) del modulo controller e dei componenti dello chassis sia mcc o mcc-2n in modo che questi componenti si avviino correttamente.

### Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

### A proposito di questa attività

Questa attività non è richiesta sui sistemi ricevuti dalla fabbrica.

### Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

```
ha-config show
```

Lo stato ha corretto dipende dalla configurazione di MetroCluster.

Numero di controller nella configurazione MetroCluster	Lo stato HA per tutti i componenti deve essere...
Configurazione MetroCluster FC a otto o quattro nodi	mcc

Configurazione MetroCluster FC a due nodi	mcc-2n
Configurazione IP MetroCluster	mccip

2. Se lo stato di sistema visualizzato del controller non è corretto, impostare lo stato ha per il modulo controller:

Numero di controller nella configurazione MetroCluster	Comando
Configurazione MetroCluster FC a otto o quattro nodi	ha-config modify controller mcc
Configurazione MetroCluster FC a due nodi	ha-config modify controller mcc-2n
Configurazione IP MetroCluster	ha-config modify controller mccip

3. Se lo stato di sistema visualizzato dello chassis non è corretto, impostare lo stato ha per lo chassis:

Numero di controller nella configurazione MetroCluster	Comando
Configurazione MetroCluster FC a otto o quattro nodi	ha-config modify chassis mcc
Configurazione MetroCluster FC a due nodi	ha-config modifica telaio mcc-2n
Configurazione IP MetroCluster	ha-config modify chassis mccip

4. Avviare il nodo su ONTAP:

```
boot_ontap
```

5. Ripetere questi passaggi su ciascun nodo della configurazione MetroCluster.

## Configurazione di ONTAP

È necessario impostare ONTAP su ciascun modulo controller.

Se è necessario eseguire il netboot dei nuovi controller, vedere ["Avvio in rete dei nuovi moduli controller"](#) Nella Guida all'aggiornamento, alla transizione e all'espansione di MetroCluster.

### Scelte

- [Impostazione di ONTAP in una configurazione MetroCluster a due nodi](#)
- [Impostazione di ONTAP in una configurazione MetroCluster a otto o quattro nodi](#)

## Impostazione di ONTAP in una configurazione MetroCluster a due nodi

In una configurazione MetroCluster a due nodi, su ciascun cluster è necessario avviare il nodo, uscire dalla procedura guidata di installazione del cluster e utilizzare il comando di installazione del cluster per configurare il nodo in un cluster a nodo singolo.

### Prima di iniziare

Non è necessario aver configurato il Service Processor.

### A proposito di questa attività

Questa attività è destinata alle configurazioni MetroCluster a due nodi che utilizzano lo storage NetApp nativo.

I nuovi sistemi MetroCluster sono preconfigurati; non è necessario eseguire questa procedura. Tuttavia, è necessario configurare AutoSupport.

Questa attività deve essere eseguita su entrambi i cluster nella configurazione MetroCluster.

Per ulteriori informazioni generali sulla configurazione di ONTAP, vedere ["Configurare ONTAP"](#).

### Fasi

1. Accendere il primo nodo.



Ripetere questo passaggio sul nodo del sito di disaster recovery (DR).

Il nodo si avvia, quindi viene avviata la procedura guidata di configurazione del cluster sulla console, che informa che AutoSupport verrà attivato automaticamente.

```
::> 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
```

```
Enter the node management interface port [e0M]:
```

```
Enter the node management interface IP address [10.101.01.01]:
```

```
Enter the node management interface netmask [101.010.101.0]:
```

```
Enter the node management interface default gateway [10.101.01.0]:
```

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

## 2. Creare un nuovo cluster:

```
create
```

## 3. Scegliere se utilizzare il nodo come cluster a nodo singolo.

```
Do you intend for this node to be used as a single node cluster? {yes,  
no} [yes]:
```

## 4. Accettare le impostazioni predefinite del sistema yes Premendo Invio, oppure immettere i propri valori

digitando `no`, Quindi premere Invio.

5. Seguire le istruzioni per completare la procedura guidata **Cluster Setup**, premere Invio per accettare i valori predefiniti o digitare i propri valori, quindi premere Invio.

I valori predefiniti vengono determinati automaticamente in base alla piattaforma e alla configurazione di rete.

6. Dopo aver completato la procedura guidata **Cluster Setup** e aver chiuso, verificare che il cluster sia attivo e che il primo nodo funzioni correttamente: `

```
cluster show
```

L'esempio seguente mostra un cluster in cui il primo nodo (cluster1-01) è integro e idoneo a partecipare:

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
cluster1-01                       true    true
```

Se è necessario modificare una delle impostazioni immesse per l'SVM amministrativa o il nodo SVM, è possibile accedere alla procedura guidata di installazione del cluster utilizzando il comando di installazione del cluster.

## Impostazione di ONTAP in una configurazione MetroCluster a otto o quattro nodi

Dopo aver avviato ciascun nodo, viene richiesto di eseguire il programma di installazione del sistema per 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.

### A proposito di questa attività

Questa attività è destinata alle configurazioni MetroCluster a otto o quattro nodi che utilizzano lo storage NetApp nativo.

I nuovi sistemi MetroCluster sono preconfigurati; non è necessario eseguire questa procedura. Tuttavia, è necessario configurare lo strumento AutoSupport.

Questa attività deve essere eseguita su entrambi i cluster nella configurazione MetroCluster.

Questa procedura utilizza lo strumento di configurazione del sistema. Se lo si desidera, è possibile utilizzare la configurazione guidata del cluster CLI.

### Fasi

1. Se non lo si è già fatto, accendere ciascun nodo e lasciarlo avviare completamente.

Se il sistema è in modalità manutenzione, eseguire il comando `halt` per uscire dalla modalità manutenzione, quindi eseguire il seguente comando dal prompt DEL CARICATORE:

```
boot_ontap
```

L'output dovrebbe essere simile a quanto segue:

```
Welcome to node setup

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 setup wizard.
                Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.
.
.
.
```

2. Attivare lo strumento AutoSupport seguendo le istruzioni fornite dal sistema.
3. Rispondere alle richieste per configurare l'interfaccia di gestione dei nodi.

I prompt sono simili ai seguenti:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Verificare che i nodi siano configurati in modalità ad alta disponibilità:

```
storage failover show -fields mode
```

In caso contrario, eseguire il seguente comando su ciascun nodo e riavviare il nodo:

```
storage failover modify -mode ha -node localhost
```

Questo comando configura la modalità di disponibilità elevata ma non attiva il failover dello storage. Il failover dello storage viene attivato automaticamente quando la configurazione MetroCluster viene eseguita successivamente nel processo di configurazione.

5. Verificare che siano configurate quattro porte come interconnessioni cluster:

```
network port show
```

L'esempio seguente mostra l'output per cluster\_A:

```
cluster_A::> network port show
```

(Mbps)					Speed	
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	
-----						
node_A_1						
	**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
	e0g	Default	Default	up	1500	auto/1000
node_A_2						
	**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
	e0g	Default	Default	up	1500	auto/1000
14 entries were displayed.						

6. Se si crea un cluster senza switch a due nodi (un cluster senza switch di interconnessione del cluster), attivare la modalità di rete senza switch del cluster:

- a. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

Puoi rispondere `y` quando viene richiesto di passare alla modalità avanzata. Viene visualizzato il prompt della modalità avanzata (\*).

- a. Abilitare la modalità cluster senza switch:

```
network options switchless-cluster modify -enabled true
```

- b. Tornare al livello di privilegio admin:

```
set -privilege admin
```

7. Avviare il programma di installazione del sistema seguendo le istruzioni fornite dalle informazioni visualizzate sulla console del sistema dopo l'avvio iniziale.

8. Utilizzare lo strumento di configurazione del sistema per configurare ciascun nodo e creare il cluster, ma non per creare aggregati.



È possibile creare aggregati mirrorati nelle attività successive.

### Al termine

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.

### 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.

### Configurazione delle LIF tra 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.

### Scelte

- [Configurazione di LIF intercluster su porte dedicate](#)
- [Configurazione delle LIF tra cluster su porte dati condivise](#)

### 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 riportato di seguito vengono assegnate le porte "e0e" e "e0f" al gruppo di failover Intercluster01 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.

**ONTAP 9.6 e versioni successive**

```
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
```

**ONTAP 9.5 e versioni precedenti**

```
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
```

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:

**ONTAP 9.6 e versioni successive**

Eseguire il comando: `network interface show -service-policy default-intercluster`

**ONTAP 9.5 e versioni precedenti**

Eseguire il comando: `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
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:

#### ONTAP 9.6 e versioni successive

Eseguire il comando: `network interface show -service-policy default-intercluster -failover`

#### ONTAP 9.5 e versioni precedenti

Eseguire il comando: `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 SVM "e0e" effettueranno il failover sulla porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster -failover
```

	Logical	Home	Failover	Failover
Vserver	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"](#)

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, banda WAN disponibile, intervallo di replica, tasso di modifica e numero di porte.

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 nel cluster01:

```
cluster01::> network port show
```

(Mbps)					Speed	
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:

**ONTAP 9.6 e versioni successive**

Eseguire il comando: `network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask`

**ONTAP 9.5 e versioni precedenti**

Eseguire il comando: `network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask`

Per la sintassi completa dei comandi, vedere la pagina `man`. Nell'esempio seguente vengono creati i LIF di 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:

**ONTAP 9.6 e versioni successive**

Eseguire il comando: `network interface show -service-policy default-intercluster`

**ONTAP 9.5 e versioni precedenti**

Eseguire il comando: `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
Home				Port
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01
true				e0c
	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02
true				e0c

#### 4. Verificare che le LIF dell'intercluster siano ridondanti:

##### ONTAP 9.6 e versioni successive

Eseguire il comando: `network interface show -service-policy default-intercluster -failover`

##### ONTAP 9.5 e versioni precedenti

Eseguire il comando: `network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che i LIF dell'intercluster "cluster01\_icl01" e "cluster01\_icl02" sulla porta "e0c" effettueranno il failover sulla porta "e0d".

```
cluster01::> network interface show -service-policy default-intercluster -failover
```

	Logical	Home	Failover	Failover
Vserver	Interface	Node:Port	Policy	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 necessario creare la relazione peer del cluster tra i cluster MetroCluster.

### A proposito di questa attività

È possibile utilizzare `cluster peer create` per creare una relazione peer tra un cluster locale e remoto. Una volta creata la relazione peer, è possibile eseguire `cluster peer create` sul cluster remoto per autenticarlo nel cluster locale.

### Prima di iniziare

- 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 -ipspace ipspace
```

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 di una relazione peer del cluster (ONTAP 9.2 e versioni precedenti)

È possibile utilizzare `cluster peer create` per avviare una richiesta di relazione di peering tra un cluster locale e remoto. Una volta richiesta la relazione peer dal cluster locale, è possibile eseguire `cluster peer create` sul cluster remoto per accettare la relazione.

#### Prima di iniziare

- È necessario aver creato le LIF di intercluster su ogni nodo dei cluster in fase di peering.
- Gli amministratori del cluster devono aver concordato la passphrase utilizzata da ciascun cluster per autenticarsi con l'altro.

#### Fasi

1. Nel cluster di destinazione per la protezione dei dati, creare una relazione peer con il cluster di origine per la protezione dei dati:

```
cluster peer create -peer-addr peer_LIF_IPs -ipspace ipspace
```

Se non si utilizza un IPspace personalizzato, è possibile ignorare l'opzione `-ipspace`. Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio riportato di seguito viene creata una relazione peer del cluster con il cluster remoto agli indirizzi IP LIF dell'intercluster "192.168.2.201" e "192.168.2.202":

```
cluster02::> cluster peer create -peer-addr 192.168.2.201,192.168.2.202
Enter the passphrase:
Please enter the passphrase again:
```

Inserire la passphrase per la relazione peer quando richiesto.

2. Nel cluster di origine per la protezione dei dati, 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 "192.140.112.203" e "192.140.112.204" dell'intercluster:

```
cluster01::> cluster peer create -peer-addr 192.168.2.203,192.168.2.204
Please confirm the passphrase:
Please confirm the passphrase again:
```

Inserire la passphrase per la relazione peer quando richiesto.

3. Verificare che la relazione peer del cluster sia stata creata:

```
cluster peer show -instance
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. Verificare la connettività e lo stato dei nodi nella relazione peer:

```
cluster peer health show`
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> cluster peer health show
```

Node	cluster-Name	Node-Name	RDB-Health	Cluster-Health	Avail...
	Ping-Status				
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

## 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 con la CLI"](#)

## Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

- 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 assicurarsi di selezionare il tipo di disco corretto.
- 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. Vedere ["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 utilizzando il comando `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 di unità o LUN di array 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 `force-small-aggregate` Opzione 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 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, consultare `storage aggregate create` pagina man.

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
```

## 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.

### Prima di iniziare

- 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 FC, gli aggregati senza mirror saranno online solo dopo uno switchover se i dischi remoti nell'aggregato sono accessibili. In caso di errore degli ISL, il nodo locale potrebbe non essere in grado di accedere ai dati dei dischi remoti senza mirror. Il guasto di un aggregato può causare il riavvio del nodo locale.

- 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.



Gli aggregati senza mirror devono essere locali rispetto al nodo che li possiede.

- 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. Visualizzare un elenco delle parti di ricambio disponibili:

```
storage disk show -spare -owner node_name
```

#### 2. 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, 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 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
```

### 3. Verificare il gruppo RAID e i dischi del nuovo aggregato:

```
storage aggregate show-status -aggregate aggregate-name
```

## Informazioni correlate

["Gestione di dischi e Tier \(aggregato\)"](#)

## Implementazione della configurazione MetroCluster

È necessario eseguire `metrocluster configure` Comando per avviare la protezione dei dati in una configurazione MetroCluster.

### Prima di iniziare

- Su ciascun cluster devono essere presenti almeno due aggregati di dati mirrorati non root.

È possibile eseguire il mirroring o il mirroring di aggregati di dati aggiuntivi.

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 "mcc".

### A proposito di questa attività

Si emette il `metrocluster configure` Per abilitare la configurazione MetroCluster, eseguire una sola volta il comando su uno dei nodi. 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. Configura MetroCluster nel seguente formato:

Se la configurazione di MetroCluster dispone di...	Quindi...
Aggregati di dati multipli	<p>Dal prompt di qualsiasi nodo, configurare MetroCluster:</p> <pre>metrocluster configure node-name</pre>
Un singolo aggregato di dati mirrorato	<p>a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:</p> <pre>set -privilege advanced</pre> <p>Devi rispondere con <code>y</code> quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (*).</p> <p>b. Configurare MetroCluster con <code>-allow-with -one-aggregate true</code> parametro:</p> <pre>metrocluster configure -allow-with -one-aggregate true node-name</pre> <p>c. Tornare al livello di privilegio admin:</p> <pre>set -privilege admin</pre>





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
```

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

b. Verificare la configurazione dal sito B:

```
metrocluster show
```

```
cluster_B::> metrocluster show
```

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

## Configurazione della consegna in-order o out-of-order dei frame sul software ONTAP

È necessario configurare la consegna in-order (IOD) o la consegna out-of-order (OOD) dei frame in base alla configurazione dello switch Fibre Channel (FC).

### A proposito di questa attività

Se lo switch FC è configurato per IOD, il software ONTAP deve essere configurato per IOD. Analogamente, se lo switch FC è configurato per OOD, è necessario configurare ONTAP per OOD.



Riavviare il controller per modificare la configurazione.

### Fase

1. Configurare ONTAP per il funzionamento di IOD o OOD di frame.
  - Per impostazione predefinita, l'IOD dei frame è attivato in ONTAP. Per verificare i dettagli della configurazione:
    - i. Accedere alla modalità avanzata:

```
set advanced
```

ii. Verificare le impostazioni:

```
metrocluster interconnect adapter show
```

```
mcc4-b12_siteB:~*~> metrocluster interconnect adapter show
```

Node	Adapter Name	Adapter Type	Link Status	Is OOD Enabled?	IP Address	Port Number
mcc4-b1 6a	fcvi_device_0	FC-VI	Up	false	17.0.1.2	
mcc4-b1 6b	fcvi_device_1	FC-VI	Up	false	18.0.0.2	
mcc4-b1 ib2a	mlx4_0	IB	Down	false	192.0.5.193	
mcc4-b1 ib2b	mlx4_0	IB	Up	false	192.0.5.194	
mcc4-b2 6a	fcvi_device_0	FC-VI	Up	false	17.0.2.2	
mcc4-b2 6b	fcvi_device_1	FC-VI	Up	false	18.0.1.2	
mcc4-b2 ib2a	mlx4_0	IB	Down	false	192.0.2.9	
mcc4-b2 ib2b	mlx4_0	IB	Up	false	192.0.2.10	

8 entries were displayed.

- Per configurare l'OOD dei frame, è necessario eseguire le seguenti operazioni su ciascun nodo:

i. Accedere alla modalità avanzata:

```
set advanced
```

ii. Verificare le impostazioni di configurazione di MetroCluster:

```
metrocluster interconnect adapter show
```

```

mcc4-b12_siteB::*> metrocluster interconnect adapter show

```

Node	Adapter Name	Type	Link Status	Is OOD Enabled?	IP Address
Port Number					
mcc4-b1 6a	fcvi_device_0	FC-VI	Up	false	17.0.1.2
mcc4-b1 6b	fcvi_device_1	FC-VI	Up	false	18.0.0.2
mcc4-b1 ib2a	mlx4_0	IB	Down	false	192.0.5.193
mcc4-b1 ib2b	mlx4_0	IB	Up	false	192.0.5.194
mcc4-b2 6a	fcvi_device_0	FC-VI	Up	false	17.0.2.2
mcc4-b2 6b	fcvi_device_1	FC-VI	Up	false	18.0.1.2
mcc4-b2 ib2a	mlx4_0	IB	Down	false	192.0.2.9
mcc4-b2 ib2b	mlx4_0	IB	Up	false	192.0.2.10

8 entries were displayed.

iii. Abilitare OOOD sul nodo “mcc4-b1” e sul nodo “mcc4-b2”:

```

metrocluster interconnect adapter modify -node node_name -is-ood-enabled true

```

```

mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true

```

i. Riavviare il controller eseguendo un takeover ad alta disponibilità (ha) in entrambe le direzioni.

ii. Verificare le impostazioni:

```

metrocluster interconnect adapter show

```

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
```

Node	Adapter Name	Adapter Type	Link Status	Is OOD Enabled?	IP Address	Port
mcc4-b1	fcvi_device_0	FC-VI	Up	true	17.0.1.2	6a
mcc4-b1	fcvi_device_1	FC-VI	Up	true	18.0.0.2	6b
mcc4-b1	mlx4_0	IB	Down	false	192.0.5.193	ib2a
mcc4-b1	mlx4_0	IB	Up	false	192.0.5.194	ib2b
mcc4-b2	fcvi_device_0	FC-VI	Up	true	17.0.2.2	6a
mcc4-b2	fcvi_device_1	FC-VI	Up	true	18.0.1.2	6b
mcc4-b2	mlx4_0	IB	Down	false	192.0.2.9	ib2a
mcc4-b2	mlx4_0	IB	Up	false	192.0.2.10	ib2b

8 entries were displayed.

## Configurazione di SNMPv3 in una configurazione MetroCluster

### Prima di iniziare

I protocolli di autenticazione e privacy sugli switch e sul sistema ONTAP devono essere identici.

### A proposito di questa attività

ONTAP attualmente supporta la crittografia AES-128.

### Fasi

1. Creare un utente SNMP per ogni switch dal prompt del controller:

```
security login create
```

```
Controller_A_1:> security login create -user-or-group-name snmpv3user  
-application snmp -authentication-method usm -role none -remote-switch  
-ipaddress 10.10.10.10
```

2. Rispondere alle seguenti richieste in base alle esigenze della propria sede:

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

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

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

```
Enter the authentication protocol password again:
```

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

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

```
Enter privacy protocol password again:
```



Lo stesso nome utente può essere aggiunto a diversi switch con indirizzi IP diversi.

### 3. Creare un utente SNMP per gli altri switch.

Nell'esempio seguente viene illustrato come creare un nome utente per uno switch con l'indirizzo IP 10.10.10.11.

```
Controller_A_1::> security login create -user-or-group-name snmpv3user  
-application snmp -authentication-method usm -role none -remote-switch  
-ipaddress 10.  
10.10.11
```

### 4. Verificare che vi sia una voce di accesso per ogni switch:

```
security login show
```

```

Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

-----
-----

node_A_1 SVM 1 snmpv3user      snmp      usm
10.10.10.10

node_A_1 SVM 2 snmpv3user      snmp      usm
10.10.10.11

node_A_1 SVM 3 snmpv3user      snmp      usm
10.10.10.12

node_A_1 SVM 4 snmpv3user      snmp      usm
10.10.10.13

4 entries were displayed.

```

##### 5. Configurare SNMPv3 sugli switch dal prompt dello switch:

```
snmpconfig --set snmpv3
```

Se si richiede l'accesso RO, dopo "User (ro):" specificare "snmpv3user" come mostrato nell'esempio:

```

Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user database
will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]: (2..2) [3]

```

L'esempio mostra come configurare un utente di sola lettura. Se necessario, è possibile regolare gli utenti RW.

È inoltre necessario impostare le password degli account inutilizzati per proteggerli e utilizzare la migliore crittografia disponibile nella versione di ONTAP.

6. Configurare la crittografia e le password per gli altri utenti dello switch in base alle esigenze del sito.

## Configurazione dei componenti di MetroCluster per il monitoraggio dello stato di salute

Prima di monitorare i componenti in una configurazione MetroCluster, è necessario eseguire alcune procedure di configurazione speciali.

### A proposito di questa attività

Queste attività si applicano solo ai sistemi con bridge FC-SAS.

A partire da Fabric OS 9.0.1, SNMPv2 non è supportato per il monitoraggio dello stato degli switch Brocade, è necessario utilizzare SNMPv3. Se si utilizza SNMPv3, è necessario configurare SNMPv3 in ONTAP prima di passare alla sezione seguente. Per ulteriori informazioni, vedere [Configurazione di SNMPv3 in una configurazione MetroCluster](#).



- Per evitare interferenze da altre fonti, è necessario posizionare bridge e LIF di gestione dei nodi in una rete dedicata.
- Se si utilizza una rete dedicata per il monitoraggio dello stato di salute, ciascun nodo deve disporre di una LIF di gestione dei nodi in tale rete dedicata.

## Configurazione degli switch MetroCluster FC per il monitoraggio dello stato di salute

In una configurazione Fabric-Attached MetroCluster, è necessario eseguire alcune procedure di configurazione aggiuntive per monitorare gli switch FC.



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

### Fasi

1. Aggiungere uno switch con un indirizzo IP a ciascun nodo MetroCluster:

Il comando eseguito dipende dall'utilizzo di SNMPv2 o SNMPv3.

#### Aggiungere uno switch utilizzando SNMPv3:

```
storage switch add -address <ip_address> -snmp-version SNMPv3 -snmp  
-community-or-username <SNMP_user_configured_on_the_switch>
```

#### Aggiungere uno switch utilizzando SNMPv2:

```
storage switch add -address ipaddress
```

Questo comando deve essere ripetuto su tutti e quattro gli switch nella configurazione MetroCluster.



Gli switch FC Brocade 7840 e tutti gli avvisi sono supportati nel monitoraggio dello stato di salute, ad eccezione di `NoISLPresent_Alert`.

L'esempio seguente mostra il comando per aggiungere uno switch con indirizzo IP 10.10.10.10:



```
controller_A_1::> storage switch add -address 10.10.10.10
```

## 2. Verificare che tutti gli switch siano configurati correttamente:

```
storage switch show
```

Potrebbero essere necessari fino a 15 minuti per riflettere tutti i dati a causa dell'intervallo di polling di 15 minuti.

L'esempio seguente mostra il comando fornito per verificare che gli switch FC MetroCluster siano configurati:

```
controller_A_1::> storage switch show
Fabric          Switch Name      Vendor  Model          Switch WWN
Status
-----
-----
1000000533a9e7a6 brcd6505-fcs40   Brocade Brocade6505    1000000533a9e7a6
OK
1000000533a9e7a6 brcd6505-fcs42   Brocade Brocade6505    1000000533d3660a
OK
1000000533ed94d1 brcd6510-fcs44   Brocade Brocade6510    1000000533eda031
OK
1000000533ed94d1 brcd6510-fcs45   Brocade Brocade6510    1000000533ed94d1
OK
4 entries were displayed.

controller_A_1::>
```

Se viene visualizzato il nome internazionale (WWN) dello switch, il monitor dello stato di salute ONTAP può contattare e monitorare lo switch FC.

### Informazioni correlate

["Amministrazione del sistema"](#)

### Configurazione di bridge FC-SAS per il monitoraggio dello stato di salute

Nei sistemi con versioni di ONTAP precedenti alla 9.8, è necessario eseguire alcune procedure di configurazione speciali per monitorare i bridge FC-SAS nella configurazione di MetroCluster.

### A proposito di questa attività

- Gli strumenti di monitoraggio SNMP di terze parti non sono supportati per i bridge FibreBridge.
- A partire da ONTAP 9.8, i bridge FC-SAS vengono monitorati per impostazione predefinita tramite connessioni in-band e non è necessaria alcuna configurazione aggiuntiva.



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

## Fasi

1. Dal prompt del cluster ONTAP, aggiungere il bridge al monitoraggio dello stato di salute:

a. Aggiungere il bridge utilizzando il comando per la versione di ONTAP in uso:

Versione di ONTAP	Comando
9.5 e versioni successive	<code>storage bridge add -address 0.0.0.0 -managed-by in-band -name <i>bridge-name</i></code>
9.4 e versioni precedenti	<code>storage bridge add -address <i>bridge-ip-address</i> -name <i>bridge-name</i></code>

b. Verificare che il bridge sia stato aggiunto e configurato correttamente:

```
storage bridge show
```

A causa dell'intervallo di polling, potrebbero essere necessari 15 minuti per riflettere tutti i dati. Il monitor dello stato di ONTAP può contattare e monitorare il bridge se il valore nella colonna "Stato" è "ok" e vengono visualizzate altre informazioni, ad esempio il nome internazionale (WWN).

L'esempio seguente mostra che i bridge FC-SAS sono configurati:

```
controller_A_1::> storage bridge show
```

Bridge Model	Symbolic Name	Bridge WWN	Is Monitored	Monitor Status	Vendor
ATTO_10.10.20.10	atto01		true	ok	Atto
FibreBridge 7500N		20000010867038c0			
ATTO_10.10.20.11	atto02		true	ok	Atto
FibreBridge 7500N		20000010867033c0			
ATTO_10.10.20.12	atto03		true	ok	Atto
FibreBridge 7500N		20000010867030c0			
ATTO_10.10.20.13	atto04		true	ok	Atto
FibreBridge 7500N		2000001086703b80			

```
4 entries were displayed
```

```
controller_A_1::>
```

## Verifica della configurazione MetroCluster

È possibile verificare che i componenti e le relazioni nella configurazione di MetroCluster funzionino correttamente.

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.

### A proposito di questa attività

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` quindi non mostrerà 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. Visualizza risultati più dettagliati dei più recenti `metrocluster check run` comando:

```
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 Result	Aggregate	Check
-----	-----	-----
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

```

controller_A_2      controller_A_2_aggr0
ok                  mirroring-status
                   disk-pool-allocation
ok                  ownership-state
ok
                   controller_A_2_aggr1
ok                  mirroring-status
                   disk-pool-allocation
ok                  ownership-state
ok
                   controller_A_2_aggr2
ok                  mirroring-status
                   disk-pool-allocation
ok                  ownership-state
ok
18 entries were displayed.

```

Nell'esempio riportato di seguito viene illustrato il `metrocluster check cluster show` Output di comando 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"](#)

## Verifica degli errori di configurazione di MetroCluster con Config Advisor

È possibile accedere al sito di supporto NetApp e scaricare lo strumento Config Advisor per verificare la presenza di errori di configurazione comuni.

### A proposito di questa attività

Config Advisor è uno strumento per la convalida della configurazione e il controllo dello stato di salute. È possibile implementarlo sia in siti sicuri che in siti non sicuri per la raccolta di dati e l'analisi del sistema.



Il supporto per Config Advisor è limitato e disponibile solo online.

### Fasi

1. Accedere alla pagina di download di Config Advisor e scaricare lo strumento.

["Download NetApp: Config Advisor"](#)

2. Eseguire Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

## Verifica del funzionamento locale di ha

Se si dispone di una configurazione MetroCluster a quattro nodi, verificare il funzionamento delle coppie ha locali nella configurazione MetroCluster. Questo non è necessario per le configurazioni a due nodi.

### A proposito di questa attività

Le configurazioni MetroCluster a due nodi non sono costituite da coppie ha locali e questa attività non è applicabile.

Gli esempi di questa attività utilizzano le convenzioni di denominazione standard:

- Cluster\_A.
  - Controller\_A\_1
  - Controller\_A\_2
- Cluster\_B
  - Controller\_B\_1
  - Controller\_B\_2

### Fasi

1. Su cluster\_A, eseguire un failover e un giveback in entrambe le direzioni.
  - a. Verificare che il failover dello storage sia attivato:

```
storage failover show
```

L'output dovrebbe indicare che è possibile effettuare il takeover per entrambi i nodi:

```
cluster_A::> storage failover show
```

Node	Partner	Takeover Possible	State Description
controller_A_1	controller_A_2	true	Connected to controller_A_2
controller_A_2	controller_A_1	true	Connected to controller_A_1

2 entries were displayed.

- b. Prendere il controllo controller\_A\_2 da controller\_A\_1:

```
storage failover takeover controller_A_2
```

È possibile utilizzare `storage failover show-takeover` comando per monitorare l'avanzamento dell'operazione di takeover.

- c. Verificare che il rilevamento sia stato completato:

```
storage failover show
```

L'output dovrebbe indicare che controller\_A\_1 è in stato di Takeover, il che significa che ha assunto il controllo del partner ha:

```
cluster_A::> storage failover show
```

Node	Partner	Takeover Possible	State Description
controller_A_1	controller_A_2	false	In takeover
controller_A_2	controller_A_1	-	Unknown

2 entries were displayed.

- d. Restituire controller\_A\_2:

```
storage failover giveback controller_A_2
```

È possibile utilizzare `storage failover show-giveback` comando per monitorare l'avanzamento dell'operazione di giveback.

- e. Verificare che il failover dello storage sia tornato allo stato normale:

```
storage failover show
```

L'output dovrebbe indicare che è possibile effettuare il takeover per entrambi i nodi:

```
cluster_A::> storage failover show
```

Node	Partner	Takeover Possible	State Description
controller_A_1	controller_A_2	true	Connected to controller_A_2
controller_A_2	controller_A_1	true	Connected to controller_A_1

2 entries were displayed.

- a. Ripetere i passaggi precedenti, questa volta prendendo il controllo di controller\_A\_1 da controller\_A\_2.
2. Ripetere i passaggi precedenti su cluster\_B.

### Informazioni correlate

["Configurazione ad alta disponibilità"](#)

## Verifica dello switchover, della riparazione e dello switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

### Fase

1. Utilizzare le procedure per lo switchover negoziato, la riparazione e lo switchback indicate in ["Ripristino in caso di disastro"](#).

## 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*.

## 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 a ["Configurare le LIF IP virtuali"](#).





## Limitazioni di 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. In ONTAP 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.

Una volta configurato, l'esistenza di v0a (v0b e così via) convalida continuamente la connettività, garantendo che una migrazione LIF o un failover abbiano esito positivo (a differenza di L2, dove una configurazione interrotta 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 redistribuzione 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).

# 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.

**Fasi**

- 1. Verificare che la riparazione sia completata:

```
metrocluster node show
```

L'esempio seguente mostra il completamento corretto del comando:

```
cluster_A::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
-----
-----
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
```

- 2. 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  -
```

3. Avviare i nodi dal sito di emergenza.
4. Controllare lo stato del ripristino dello switchback:

```
metrocluster node show
```

```
cluster_A:> metrocluster node show
DR
Group Cluster Node      Configuration  DR
State          Mirroring Mode
-----
1      cluster_A
      node_A_1      configured    enabled      heal roots
completed
      cluster_B
      node_B_2      configured    enabled      waiting for
switchback                                     recovery

2 entries were displayed.
```

## 5. Eseguire lo switchback:

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful. Verify switchback
```

## 6. Confermare lo stato dei nodi:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR
Group Cluster Node          Configuration  DR
State          Mirroring Mode
-----
1      cluster_A
      node_A_1      configured    enabled     normal
      cluster_B
      node_B_2      configured    enabled     normal

2 entries were displayed.
```

## 7. Confermare lo stato:

```
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: -
```

## Perdita di un singolo bridge FC-SAS

È possibile verificare il guasto di un singolo bridge FC-SAS per assicurarsi che non vi sia un singolo punto di errore.

### A proposito di questa attività

Questo test dovrebbe richiedere circa 15 minuti.

Questa procedura ha i seguenti risultati attesi:

- Gli errori devono essere generati quando il bridge viene spento.
- Non devono verificarsi failover o perdita di servizio.
- È disponibile un solo percorso dal modulo controller alle unità dietro il bridge.



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

## Fasi

1. Spegnerne gli alimentatori del bridge.
2. Verificare che il monitoraggio del bridge indichi un errore:

```
storage bridge show
```

```
cluster_A::> storage bridge show
```

Monitor	Bridge	Symbolic Name	Vendor	Model	Bridge WWN	Is Monitored
ATTO_10.65.57.145	bridge_A_1	Atto	FibreBridge	6500N	200000108662d46c	true

```
error
```

3. Verificare che le unità dietro il bridge siano disponibili con un singolo percorso:

```
storage disk error show
```



```
cluster_A::> storage disk error show
Disk          Error Type          Error Text
-----
-----
1.0.0          onedomain          1.0.0 (5000cca057729118): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.1          onedomain          1.0.1 (5000cca057727364): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
1.0.2          onedomain          1.0.2 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
...
1.0.23         onedomain          1.0.23 (5000cca05772e9d4): All paths
to this array LUN are connected to the same fault domain. This is a
single point of failure.
```

## 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. Spegnerle 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 in seguito a un guasto del fabric dello switch

È possibile disattivare uno switch fabric per mostrare che la disponibilità dei dati non è influenzata dalla perdita.

### A proposito di questa attività

Questo test dovrebbe richiedere circa 15 minuti.

Il risultato previsto di questa procedura è che la disattivazione di un fabric comporta il passaggio di tutto il traffico di interconnessione del cluster e del disco all'altro fabric.

Negli esempi mostrati, il fabric dello switch 1 è disattivato. Questo fabric è costituito da due switch, uno per ciascun sito MetroCluster:

- FC\_switch\_A\_1 sul cluster\_A.

- FC\_switch\_B\_1 sul cluster\_B.

## Fasi

### 1. Disattivare la connettività a uno dei due fabric switch nella configurazione MetroCluster:

#### a. Disattivare il primo switch nel fabric:

```
switchdisable
```

```
FC_switch_A_1::> switchdisable
```

#### b. Disattivare il secondo switch nel fabric:

```
switchdisable
```

```
FC_switch_B_1::> switchdisable
```

### 2. Monitorare il risultato sulla console dei moduli controller.

È possibile utilizzare i seguenti comandi per controllare i nodi del cluster e assicurarsi che tutti i dati siano ancora disponibili. L'output del comando mostra i percorsi mancanti ai dischi. Questo è previsto.

- show di vserver
- visualizzazione dell'interfaccia di rete
- spettacolo aggr
- nodo di sistema runnodename-command storage show disk -p
- viene visualizzato un errore del disco di storage

### 3. Riabilitare la connettività a uno dei due fabric switch nella configurazione MetroCluster:

#### a. Riabilitare il primo switch nel fabric:

```
switchenable
```

```
FC_switch_A_1::> switchenable
```

#### b. Riabilitare il secondo switch nel fabric:

```
switchenable
```

```
FC_switch_B_1::> switchenable
```

### 4. Attendere almeno 10 minuti, quindi ripetere la procedura descritta sopra sull'altro fabric dello switch.

## 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
```

```
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 shelf 31 viene 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)

                                     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.

```

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 deve avere uno stato RAID "ddegradato" e i dischi sul plex interessato devono 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 "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 "normal", 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

È possibile rimuovere la configurazione MetroCluster da tutti i nodi della configurazione MetroCluster o da tutti i nodi di un gruppo di disaster recovery (DR). 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.](#)"

## Pianificare e installare una configurazione MetroCluster con LUN array

### Pianificazione di una configurazione MetroCluster con LUN array

La creazione di un piano dettagliato per la configurazione MetroCluster consente di comprendere i requisiti specifici per una configurazione MetroCluster che utilizza LUN sugli array di storage. L'installazione di una configurazione MetroCluster comporta la connessione e la configurazione di una serie di dispositivi, operazione che potrebbe essere eseguita da persone diverse. Pertanto, il piano consente anche di comunicare con altre persone coinvolte nell'installazione.

### Configurazione MetroCluster supportata con LUN array

È possibile impostare una configurazione MetroCluster con LUN array. Sono supportate le configurazioni stretch e fabric-attached. I sistemi AFF non sono supportati con i LUN degli array.

Le funzioni supportate nelle configurazioni MetroCluster variano in base ai tipi di configurazione. La seguente tabella elenca le funzionalità supportate dai diversi tipi di configurazioni MetroCluster con LUN array:

Funzione	Configurazioni fabric-attached			Configurazioni di estensione
	Otto nodi	Quattro nodi	A due nodi	A due nodi
Numero di controller	Otto	Quattro	Due	Due
Utilizza un fabric storage switch FC	Sì	Sì	Sì	Sì
Utilizza bridge FC-SAS	Sì	Sì	Sì	Sì
Supporta ha locale	Sì	Sì	No	No
Supporta lo switchover automatico	Sì	Sì	Sì	Sì

#### Informazioni correlate

["Differenze tra le configurazioni ONTAP MetroCluster"](#)

## Requisiti per una configurazione MetroCluster con LUN array

I sistemi ONTAP, gli storage array e gli switch FC utilizzati nelle configurazioni MetroCluster devono soddisfare i requisiti di tali tipi di configurazioni. Inoltre, è necessario considerare i requisiti SyncMirror per le configurazioni MetroCluster con LUN array.

### Requisiti per i sistemi ONTAP

- I sistemi ONTAP devono essere identificati come supportati per le configurazioni MetroCluster.

In "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)", È possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.



È necessario fare riferimento ai dettagli degli avvisi associati a qualsiasi configurazione selezionata nella matrice di interoperabilità.

- Tutti i sistemi ONTAP in una configurazione MetroCluster devono essere dello stesso modello.
- Gli adattatori FC-VI devono essere installati negli slot appropriati per ciascun sistema ONTAP, a seconda del modello.

["NetApp Hardware Universe"](#)

### Requisiti per gli array di storage

- Gli array di storage devono essere identificati come supportati per le configurazioni MetroCluster.

["Tool di matrice di interoperabilità NetApp"](#)

- Gli array di storage nella configurazione MetroCluster devono essere simmetrici:
  - I due array storage devono essere della stessa famiglia di vendor supportati e avere la stessa versione del firmware installata.

["Implementazione della virtualizzazione FlexArray per lo storage NetApp e-Series"](#)

["Implementazione della virtualizzazione FlexArray per storage di terze parti"](#)

- I tipi di dischi (ad esempio SATA, SSD o SAS) utilizzati per lo storage mirrorato devono essere gli stessi su entrambi gli array di storage.
- I parametri per la configurazione degli array di storage, come il tipo RAID e il tiering, devono essere gli stessi in entrambi i siti.

### Requisiti per gli switch FC

- Gli switch e il firmware dello switch devono essere identificati come supportati per le configurazioni MetroCluster.

["Tool di matrice di interoperabilità NetApp"](#)

- Ogni fabric deve disporre di due switch FC.



- Ogni sistema ONTAP deve essere collegato allo storage utilizzando componenti ridondanti in modo da garantire la ridondanza in caso di guasti al dispositivo e al percorso.
- I sistemi storage AFF A700, FAS9000, AFF A900 e FAS9500 supportano fino a otto ISL per fabric. Altri modelli di sistemi storage supportano fino a quattro ISL per fabric.
- Gli switch devono utilizzare la configurazione di base dello switch MetroCluster, le impostazioni ISL e le configurazioni FC-VI.

["Configurare manualmente gli switch Cisco FC"](#)

["Configurare manualmente gli switch FC Brocade"](#)

## Requisiti SyncMirror

- SyncMirror è necessario per una configurazione MetroCluster.
- Per lo storage mirrorato sono necessari due storage array separati, uno per sito.
- Sono necessari due set di LUN array.

Un set è richiesto per l'aggregato sull'array di storage locale (pool0) e un altro set è richiesto sull'array di storage remoto per il mirror dell'aggregato (l'altro plex dell'aggregato, pool1).

Per eseguire il mirroring dell'aggregato, i LUN dell'array devono avere le stesse dimensioni.

- Nella configurazione di MetroCluster sono supportati anche gli aggregati senza mirror.

Non sono protetti in caso di disastro del sito.



Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

## Installare e collegare i componenti MetroCluster in una configurazione con LUN array

### Montaggio in rack dei componenti hardware in una configurazione MetroCluster con LUN array

È necessario assicurarsi che i componenti hardware necessari per configurare una configurazione MetroCluster con i LUN degli array siano montati in rack correttamente.

#### A proposito di questa attività

È necessario eseguire questa attività su entrambi i siti MetroCluster.

#### Fasi

1. Pianificare il posizionamento dei componenti di MetroCluster.

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

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



I sistemi AFF non sono supportati con i LUN degli array.

["Procedure di installazione per il sistema AFF o FAS"](#)

4. Installare gli switch FC nel rack o nell'armadietto.

## Preparazione di uno storage array per l'utilizzo con i sistemi ONTAP

Prima di iniziare a configurare i sistemi ONTAP in una configurazione MetroCluster con LUN array, l'amministratore dello storage array deve preparare lo storage per l'utilizzo con ONTAP.

### Prima di iniziare

Gli array di storage, il firmware e gli switch che si intende utilizzare nella configurazione devono essere supportati dalla versione specifica di ONTAP.

- ["Interoperabilità NetApp \(IMT\)"](#)

In IMT, è possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

- ["NetApp Hardware Universe"](#)

### A proposito di questa attività

Per eseguire questa attività sull'array di storage, è necessario coordinarsi con l'amministratore dell'array di storage.

### Fasi

1. Creare LUN sull'array di storage in base al numero di nodi nella configurazione MetroCluster.

Ogni nodo della configurazione MetroCluster richiede LUN array per l'aggregato root, l'aggregato di dati e le parti di ricambio.

2. Configurare i parametri sull'array di storage necessari per lavorare con ONTAP.
  - ["Implementazione della virtualizzazione FlexArray per storage di terze parti"](#)
  - ["Implementazione della virtualizzazione FlexArray per lo storage NetApp e-Series"](#)

## Porte switch richieste per una configurazione MetroCluster con LUN array

Quando si collegano sistemi ONTAP a switch FC per configurare una configurazione MetroCluster con LUN array, è necessario collegare le porte FC-VI e HBA da ciascun controller a porte switch specifiche.

Se si utilizzano sia LUN di array che dischi nella configurazione MetroCluster, assicurarsi che le porte del controller siano collegate alle porte dello switch consigliate per la configurazione con dischi, quindi utilizzare le porte rimanenti per la configurazione con LUN di array.

La tabella seguente elenca le porte specifiche degli switch FC a cui è necessario collegare le diverse porte dei controller in una configurazione MetroCluster a otto nodi con LUN degli array.

**Linee guida generali per il cablaggio con LUN array**

Quando si utilizzano le tabelle di cablaggio, è necessario conoscere le seguenti linee guida:


- Gli switch Brocade e Cisco utilizzano diverse numerazioni delle porte:
  - Negli switch Brocade, la prima porta è numerata 0.
  - Sugli switch Cisco, la prima porta è numerata 1.
- Il cablaggio è lo stesso per ogni switch FC nel fabric dello switch.
- I sistemi storage FAS8200 possono essere ordinati con una delle due opzioni per la connettività FC-VI:
  - Porte integrate 0e e 0f configurate in modalità FC-VI.
  - Porte 1a e 1b su una scheda FC-VI nello slot 1.
- I sistemi storage FAS9000 richiedono quattro porte FC-VI. Le seguenti tabelle mostrano il cablaggio degli switch FC con quattro porte FC-VI su ciascun controller.

Per gli altri sistemi storage, utilizzare i cavi mostrati nelle tabelle ma ignorare i cavi delle porte FC-VI c e d.

È possibile lasciare vuote queste porte.

**Utilizzo della porta Brocade per i controller in una configurazione MetroCluster**

Le seguenti tabelle mostrano l'utilizzo delle porte sugli switch Brocade. Le tabelle mostrano la configurazione massima supportata, con otto moduli controller in due gruppi DR. Per le configurazioni più piccole, ignorare le righe dei moduli controller aggiuntivi. Gli switch Brocade 6510 e G620 supportano otto ISL.



L'utilizzo delle porte per lo switch Brocade 6505 in una configurazione MetroCluster a otto nodi non viene visualizzato. A causa del numero limitato di porte, le assegnazioni delle porte devono essere effettuate sito per sito, a seconda del modello di modulo controller e del numero di ISL e coppie di bridge in uso.

La seguente tabella mostra i cavi per il primo gruppo DR:

		Brocade 6520, 6510, 6505, G620, G610, switch or 7840	
Componente	Porta	Switch 1	Switch 2

controller_x_1	Porta FC-VI A.	0	
	Porta FC-VI b	-	0
	Porta FC-VI c	1	-
	Porta FC-VI d	-	1
	Porta HBA a	2	-
	Porta HBA b	-	2
	Porta HBA c	3	-
	Porta HBA d	-	3
controller_x_2	Porta FC-VI A.	4	-
	Porta FC-VI b	-	4
	Porta FC-VI c	5	-
	Porta FC-VI d	-	5
	Porta HBA a	6	-
	Porta HBA b	-	6
	Porta HBA c	7	-
	Porta HBA d	-	7

La seguente tabella mostra i cavi per il secondo gruppo DR:

		Brocade 6510		Brocade 6520		Brocade G620	
Componente	Porta	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2

controller_x _3	Porta FC-VI A.	24	-	48	-	18	-
	Porta FC-VI b	-	24	-	48	-	18
	Porta FC-VI c	25	-	49	-	19	-
	Porta FC-VI d	-	25	-	49	-	19
	Porta HBA a	26	-	50	-	24	-
	Porta HBA b	-	26	-	50	-	24
	Porta HBA c	27	-	51	-	25	-
	Porta HBA d	-	27	-	51	-	25
controller_x _4	Porta FC-VI A.	28	-	52	-	22	-
	Porta FC-VI b	-	28	-	52	-	22
	Porta FC-VI c	29	-	53	-	23	-
	Porta FC-VI d	-	29	-	53	-	23
	Porta HBA a	30	-	54	-	28	-
	Porta HBA b	-	30	-	54	-	28
	Porta HBA c	31	-	55	-	29	-
	Porta HBA d	-	31	-	55	-	29
<b>ISL</b>							
ISL 1	40	40	23	23	40	40	ISL 2
41	41	47	47	41	41	ISL 3	42

42	71	71	42	42	ISL 4	43	43
----	----	----	----	----	-------	----	----

#### Utilizzo della porta Cisco per i controller in una configurazione MetroCluster con ONTAP 9.4 o versione successiva

Le tabelle mostrano la configurazione massima supportata, con otto moduli controller in due gruppi DR. Per le configurazioni più piccole, ignorare le righe dei moduli controller aggiuntivi.

#### Utilizzo della porta Cisco 9396S

Cisco 9396S			
Componente	Porta	Switch 1	Switch 2
controller_x_1	Porta FC-VI A.	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta FC-VI d	-	2
	Porta HBA a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta HBA d	-	4
controller_x_2	Porta FC-VI A.	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta FC-VI d	-	6
	Porta HBA a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta HBA d	-	8

controller_x_3	Porta FC-VI A.	49	
	Porta FC-VI b	-	49
	Porta FC-VI c	50	
	Porta FC-VI d	-	50
	Porta HBA a	51	
	Porta HBA b	-	51
	Porta HBA c	52	
	Porta HBA d	-	52
controller_x_4	Porta FC-VI A.	53	-
	Porta FC-VI b	-	53
	Porta FC-VI c	54	-
	Porta FC-VI d	-	54
	Porta HBA a	55	-
	Porta HBA b	-	55
	Porta HBA c	56	-
	Porta HBA d	-	56

### Utilizzo della porta Cisco 9148S

Cisco 9148S			
Componente	Porta	Switch 1	Switch 2

controller_x_1	Porta FC-VI A.	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta FC-VI d	-	2
	Porta HBA a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta HBA d	-	4
controller_x_2	Porta FC-VI A.	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta FC-VI d	-	6
	Porta HBA a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta HBA d	-	8



controller_x_3	Porta FC-VI A.	25	
	Porta FC-VI b	-	25
	Porta FC-VI c	26	-
	Porta FC-VI d	-	26
	Porta HBA a	27	-
	Porta HBA b	-	27
	Porta HBA c	28	-
	Porta HBA d	-	28
controller_x_4	Porta FC-VI A.	29	-
	Porta FC-VI b	-	29
	Porta FC-VI c	30	-
	Porta FC-VI d	-	30
	Porta HBA a	31	-
	Porta HBA b	-	31
	Porta HBA c	32	-
	Porta HBA d	-	32

### Utilizzo della porta Cisco 9132T

Cisco 9132T			
Modulo MDS 1			
Componente	Porta	Switch 1	Switch 2

controller_x_1	Porta FC-VI A.	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta FC-VI d	-	2
	Porta HBA a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta HBA d	-	4
controller_x_2	Porta FC-VI A.	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta FC-VI d	-	6
	Porta HBA a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta HBA d	-	8
<b>Modulo MDS 2</b>			
<b>Componente</b>	<b>Porta</b>	<b>Switch 1</b>	<b>Switch 2</b>

controller_x_3	Porta FC-VI A.	1	-
	Porta FC-VI b	-	1
	Porta FC-VI c	2	-
	Porta FC-VI d	-	2
	Porta HBA a	3	-
	Porta HBA b	-	3
	Porta HBA c	4	-
	Porta HBA d	-	4
controller_x_4	Porta FC-VI A.	5	-
	Porta FC-VI b	-	5
	Porta FC-VI c	6	-
	Porta FC-VI d	-	6
	Porta HBA a	7	-
	Porta HBA b	-	7
	Porta HBA c	8	-
	Porta HBA d	-	8

### Utilizzo delle porte Cisco 9250



La seguente tabella mostra i sistemi con due porte FC-VI. I sistemi AFF A700 e FAS9000 dispongono di quattro porte FC-VI (a, b, c e d). Se si utilizza un sistema AFF A700 o FAS9000, le assegnazioni delle porte si spostano di una posizione. Ad esempio, le porte FC-VI c e d vanno alla porta dello switch 2 e alle porte HBA a e b vanno alla porta dello switch 3.

Cisco 9250i			
Lo switch Cisco 9250i non è supportato per le configurazioni MetroCluster a otto nodi.			
Componente	Porta	Switch 1	Switch 2

controller_x_1	Porta FC-VI A.	1	-
	Porta FC-VI b	-	1
	Porta HBA a	2	-
	Porta HBA b	-	2
	Porta HBA c	3	-
	Porta HBA d	-	3
controller_x_2	Porta FC-VI A.	4	-
	Porta FC-VI b	-	4
	Porta HBA a	5	-
	Porta HBA b	-	5
	Porta HBA c	6	-
	Porta HBA d	-	6
controller_x_3	Porta FC-VI A.	7	-
	Porta FC-VI b	-	7
	Porta HBA a	8	-
	Porta HBA b	-	8
	Porta HBA c	9	-
	Porta HBA d	-	9

controller_x_4	Porta FC-VI A.	10	-
	Porta FC-VI b	-	10
	Porta HBA a	11	-
	Porta HBA b	-	11
	Porta HBA c	13	-
	Porta HBA d	-	13

### Supporto di iniziatore condiviso e destinazione condivisa per la configurazione MetroCluster con LUN array

La possibilità di condividere una data porta FC Initiator o una data porta di destinazione è utile per le organizzazioni che desiderano ridurre al minimo il numero di porte initiator o di destinazione utilizzate. Ad esempio, un'organizzazione che prevede un basso utilizzo di i/o su una porta FC Initiator o su porte di destinazione potrebbe preferire condividere la porta FC Initiator o le porte di destinazione invece di dedicare ciascuna porta FC Initiator a una singola porta di destinazione.

Tuttavia, la condivisione delle porte iniziatore o di destinazione può influire negativamente sulle prestazioni.

["Come supportare la configurazione Shared Initiator e Shared Target con LUN array in un ambiente MetroCluster"](#)

### Collegare le porte FC-VI e HBA in una configurazione MetroCluster con i LUN degli array

#### Cablaggio delle porte FC-VI e HBA in una configurazione Fabric-Attached MetroCluster a due nodi con LUN array

Se si sta configurando una configurazione Fabric-Attached MetroCluster a due nodi con LUN array, è necessario collegare le porte FC-VI e HBA alle porte dello switch.

#### A proposito di questa attività

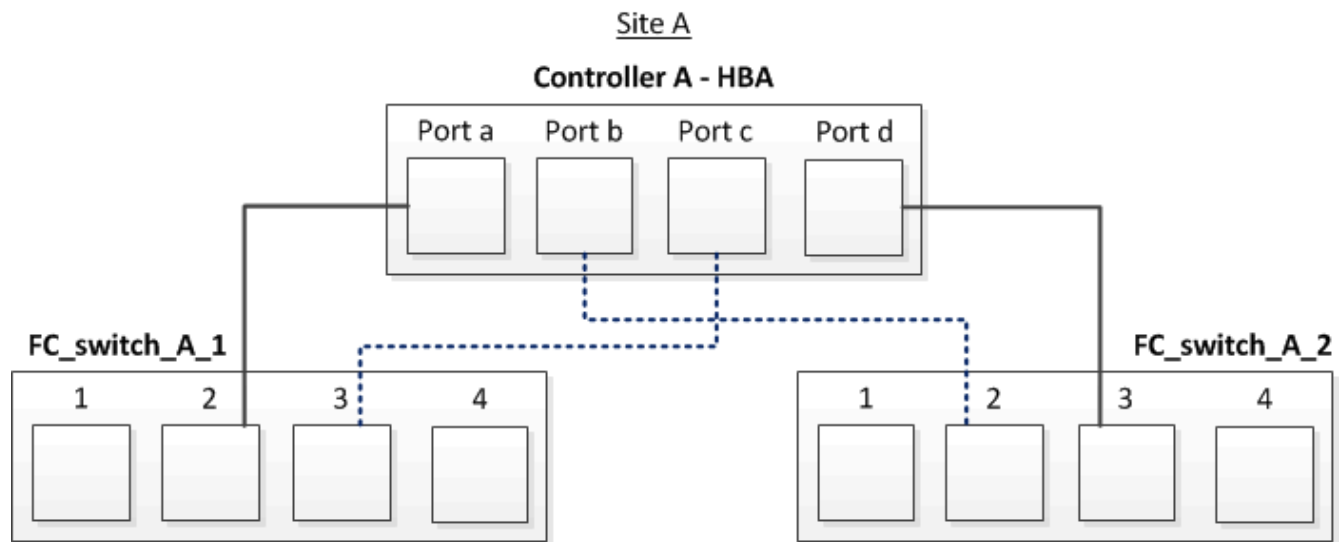
- È necessario ripetere questa attività per ciascun controller in entrambi i siti MetroCluster.
- Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte HBA e le porte dello switch specificate per la configurazione con i dischi.
  - ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)
  - ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

#### Fasi

1. Collegare le porte FC-VI dal controller alle porte switch alternative.
2. Eseguire il cablaggio controller-switch su entrambi i siti MetroCluster.

È necessario garantire la ridondanza nelle connessioni dal controller agli switch. Pertanto, per ciascun controller di un sito, è necessario assicurarsi che entrambe le porte HBA della stessa coppia di porte siano collegate a switch FC alternativi.

L'esempio seguente mostra le connessioni tra le porte HBA sul controller A e le porte su FC\_switch\_A\_1 e FC\_switch\_A\_2:



La seguente tabella elenca le connessioni tra le porte HBA e le porte dello switch FC nell'illustrazione:

Porte HBA	Porte dello switch
<b>Coppia di porte</b>	
Porta A.	FC_switch_A_1, porta 2
Porta d	FC_switch_A_2, porta 3
<b>Coppia di porte</b>	
Porta b	FC_switch_A_2, porta 2
Porta c	FC_switch_A_1, porta 3

#### Al termine

È necessario collegare gli ISL tra gli switch FC nei siti MetroCluster.

#### Cablaggio delle porte FC-VI e HBA in una configurazione Fabric-Attached MetroCluster a quattro nodi con LUN array

Se si sta configurando una configurazione Fabric-Attached MetroCluster a quattro nodi con LUN array, è necessario collegare le porte FC-VI e HBA alle porte dello switch.

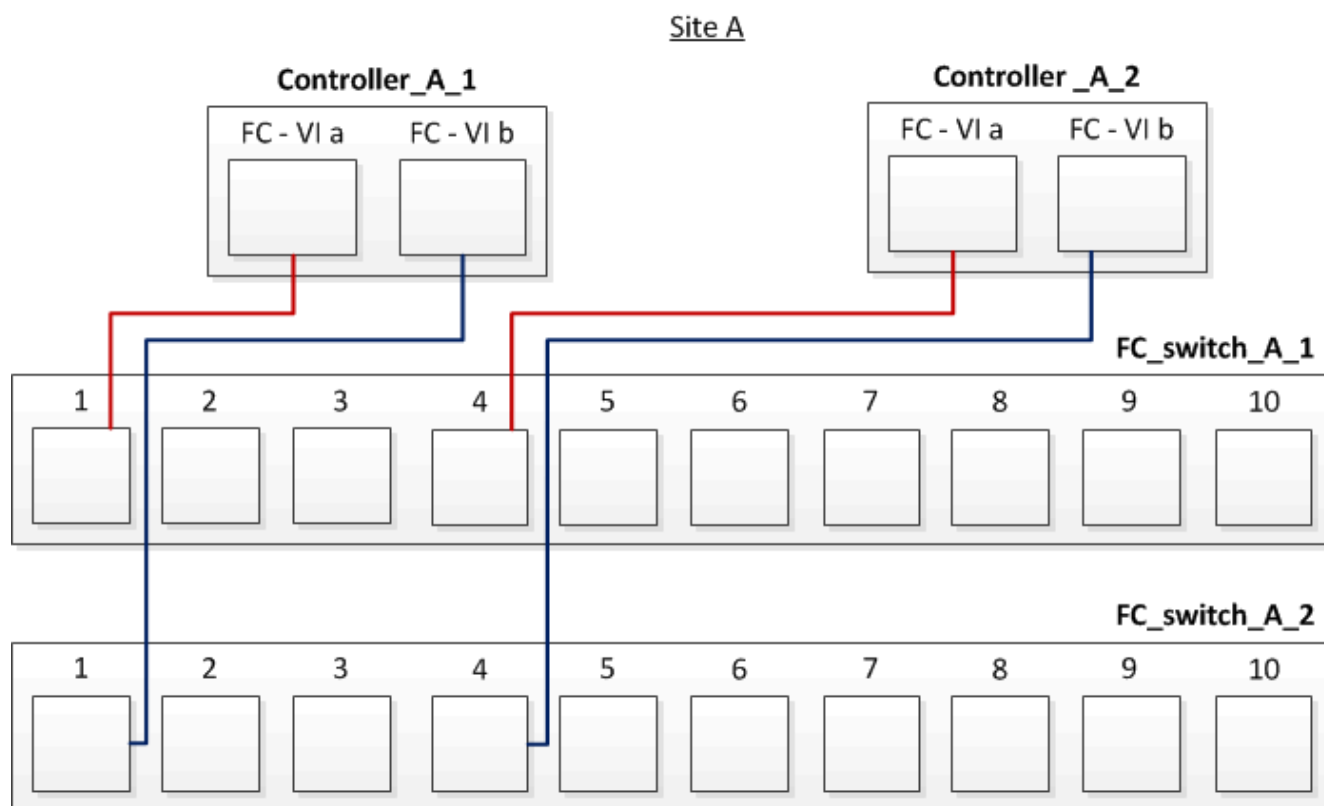
#### A proposito di questa attività

- È necessario ripetere questa attività per ciascun controller in entrambi i siti MetroCluster.
- Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte HBA e le porte dello switch specificate per la configurazione con i dischi.
  - ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)
  - ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

#### Fasi

1. Collegare le porte FC-VI da ciascun controller alle porte degli switch FC alternativi.

L'esempio seguente mostra le connessioni tra le porte FC-VI e le porte dello switch nel sito A:

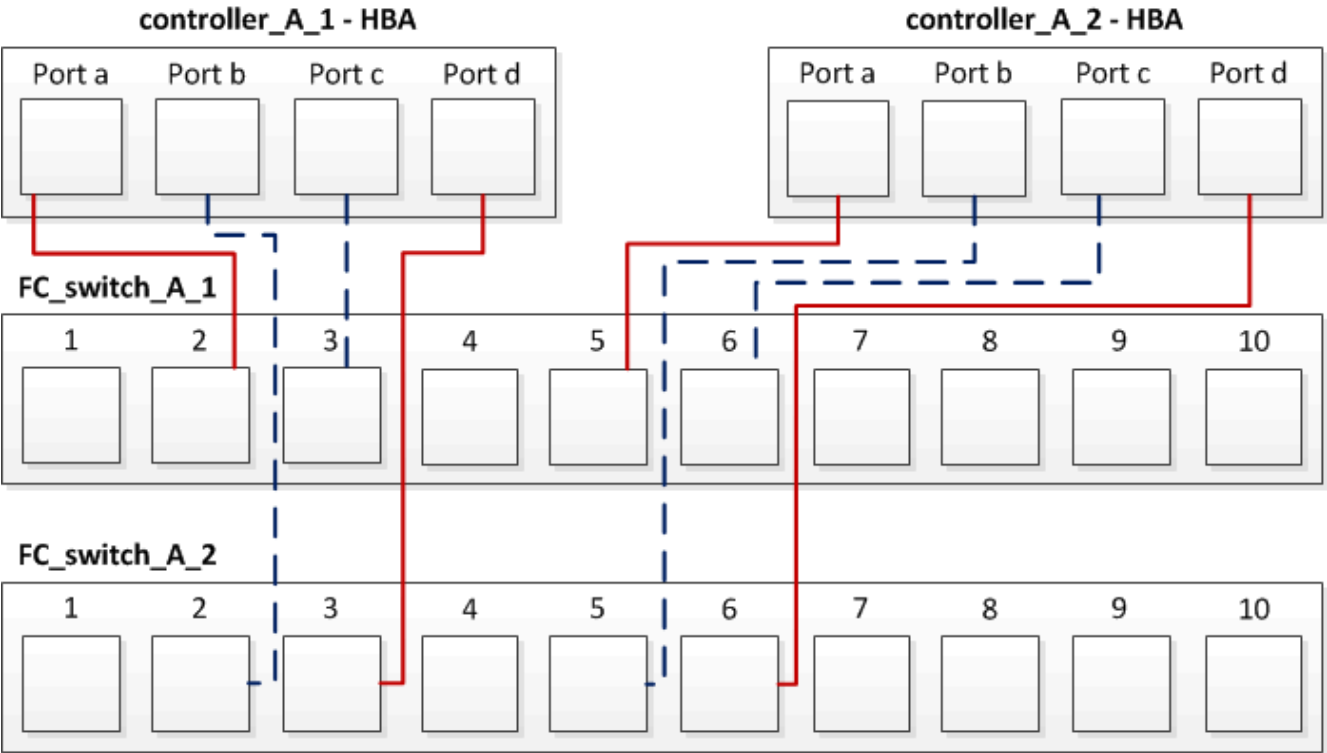


2. Eseguire il cablaggio controller-switch su entrambi i siti MetroCluster.

È necessario garantire la ridondanza nelle connessioni dal controller agli switch. Pertanto, per ciascun controller di un sito, è necessario assicurarsi che entrambe le porte HBA della stessa coppia di porte siano collegate a switch FC alternativi.

L'esempio seguente mostra le connessioni tra le porte HBA e le porte dello switch nel sito A:

Site A



La seguente tabella elenca le connessioni tra le porte HBA sul controller\_A\_1 e le porte dello switch FC nell'illustrazione:

Porte HBA	Porte dello switch
<b>Coppia di porte</b>	
Porta A.	FC_switch_A_1, porta 2
Porta d	FC_switch_A_2, porta 3
<b>Coppia di porte</b>	
Porta b	FC_switch_A_2, porta 2
Porta c	FC_switch_A_1, porta 3

La seguente tabella elenca le connessioni tra le porte HBA sul controller\_A\_2 e le porte dello switch FC nell'illustrazione:

Porte HBA	Porte dello switch
<b>Coppia di porte</b>	
Porta A.	FC_switch_A_1, porta 5
Porta d	FC_switch_A_2, porta 6



Coppia di porte	
Porta b	FC_switch_A_2, porta 5
Porta c	FC_switch_A_1, porta 6

### Al termine

È necessario collegare gli ISL tra gli switch FC nei siti MetroCluster.

### Informazioni correlate

Quando si collegano sistemi ONTAP a switch FC per configurare una configurazione MetroCluster con LUN array, è necessario collegare le porte FC-VI e HBA da ciascun controller a porte switch specifiche.

["Porte switch richieste per una configurazione MetroCluster con LUN array"](#)

### Cablaggio delle porte FC-VI e HBA in una configurazione Fabric-Attached MetroCluster a otto nodi con LUN array

Se si sta configurando una configurazione Fabric-Attached MetroCluster a otto nodi con LUN array, è necessario collegare le porte FC-VI e HBA alle porte dello switch.

### A proposito di questa attività

- È necessario ripetere questa attività per ciascun controller in entrambi i siti MetroCluster.
- Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte HBA e le porte dello switch specificate per la configurazione con i dischi.
  - ["Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"](#)
  - ["Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"](#)

### Fase

1. Collegare le porte FC-VI e HBA da ciascun controller alle porte degli switch FC alternativi. Fare riferimento alle seguenti tabelle:

### Configurazioni di cablaggio per FibreBridge 7500N o 7600N utilizzando entrambe le porte FC

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)					
MetroCluster 1 o DR Group 1					
Componente		Porta	Switch Brocade modelli 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, E DCX 8510-8		Switch Brocade G720
			Si connette a FC_switch...	Si collega alla porta dello switch...	Si collega alla porta dello switch...
controller_x_1	Porta FC-VI A.	1	0	0	Porta FC-VI b
2	0	0	Porta FC-VI c	1	1

1	Porta FC-VI d	2	1	1	Porta HBA a
1	2	8	Porta HBA b	2	2
8	Porta HBA c	1	3	9	Porta HBA d
2	3	9	controller_x_2	Porta FC-VI A.	1
4	4	Porta FC-VI b	2	4	4
Porta FC-VI c	1	5	5	Porta FC-VI d	2
5	5	Porta HBA a	1	6	12
Porta HBA b	2	6	12	Porta HBA c	1
7	13	Porta HBA d	2	7	13
Stack 1	bridge_x_1a	FC1	1	8	10
	FC2	2	8	10	bridge_x_1B
	FC1	1	9	11	FC2
	2	9	11	Stack 2	bridge_x_2a
FC1	1	10	14	FC2	2
10	14	bridge_x_2B	FC1	1	11
15	FC2	2	11	15	Stack 3
bridge_x_3a	FC1	1	12*	16	FC2
2	12*	16	bridge_x_3B	FC1	1
13*	17	FC2	2	13*	17
Stack y	bridge_x_ya	FC1	1	14*	20
FC2	2	14*	20	bridge_x_yb	FC1
1	15*	21	FC2	2	15*

**Al termine**

È necessario collegare gli ISL tra gli switch FC nei siti MetroCluster.

### Configurazioni di cablaggio per Cisco 9250i

Cisco 9250i*			
Componente	Porta	Interruttore 1	Interruttore 2
controller_x_1	Porta FC-VI A.	1	-
Porta FC-VI b	-	1	Porta HBA a
2	-	Porta HBA b	-
2	Porta HBA c	3	-
Porta HBA d	-	3	controller_x_2
Porta FC-VI A.	4	-	Porta FC-VI b
-	4	Porta HBA a	5
-	Porta HBA b	-	5
Porta HBA c	6	-	Porta HBA d
-	6	controller_x_3	Porta FC-VI A.
7	-	Porta FC-VI b	-
7	Porta HBA a	8	-
Porta HBA b	-	8	Porta HBA c
9	-	Porta HBA d	-
9	controller_x_4	Porta FC-VI A.	10
-	Porta FC-VI b	-	10
Porta HBA a	11	-	Porta HBA b
-	11	Porta HBA c	13
-	Porta HBA d	-	13

**Al termine**

È necessario collegare gli ISL tra gli switch FC nei siti MetroCluster.

### Cablaggio degli ISL in una configurazione MetroCluster con LUN array

È necessario collegare gli switch FC attraverso i siti attraverso i collegamenti interswitch (ISL) per formare fabric switch nella configurazione MetroCluster con LUN array.

#### Fasi

1. Collegare gli switch di ogni sito agli ISL o agli ISL, utilizzando il cablaggio nella tabella corrispondente alla configurazione e al modello di switch in uso.

I numeri di porta dello switch che è possibile utilizzare per gli ISL FC sono i seguenti:

Modello di switch	Porta ISL	Porta dello switch
Brocade 6520	Porta ISL 1	23
Porta ISL 2	47	Porta ISL 3
71	Porta ISL 4	95
Brocade 6505	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
Brocade 6510 e Brocade DCX 8510-8	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46
Porta ISL 8	47	Brocade 7810
Porta ISL 1	ge2 (10 Gbps)	Porta ISL 2
ge3 (10 Gbps)	Porta ISL 3	ge4 (10 Gbps)
Porta ISL 4	Ge5 (10 Gbps)	Porta ISL 5
Ge6 (10 Gbps)	Porta ISL 6	Ge7 (10 Gbps)

Brocade 7840  <b>Nota:</b> Lo switch Brocade 7840 supporta due porte VE da 40 Gbps o fino a quattro porte VE da 10 Gbps per switch per la creazione di ISL FCIP.	Porta ISL 1	ge0 (40 Gbps) o ge2 (10 Gbps)
Porta ISL 2	ge1 (40 Gbps) o ge3 (10 Gbps)	Porta ISL 3
Ge10 (10 Gbps)	Porta ISL 4	Ge11 (10 Gbps)
Brocade G610	Porta ISL 1	20
Porta ISL 2	21	Porta ISL 3
22	Porta ISL 4	23
BROCADE G620, G620-1, G630, G630-1, G720	Porta ISL 1	40
Porta ISL 2	41	Porta ISL 3
42	Porta ISL 4	43
Porta ISL 5	44	Porta ISL 6
45	Porta ISL 7	46

## Cablaggio dell'interconnessione del cluster in configurazioni a otto o quattro nodi

Nelle configurazioni MetroCluster a otto o quattro nodi, è necessario collegare l'interconnessione del cluster tra i moduli controller locali di ciascun sito.

### A proposito di questa attività

Questa attività non è richiesta nelle configurazioni MetroCluster a due nodi.

Questa attività deve essere eseguita in entrambi i siti MetroCluster.

### Fase

1. Collegare l'interconnessione del cluster da un modulo controller all'altro o, se si utilizzano switch di interconnessione del cluster, da ciascun modulo controller agli switch.

### Informazioni correlate

["Documentazione dei sistemi hardware ONTAP"](#)

["Gestione di rete e LIF"](#)

## Cablaggio delle connessioni di peering del cluster

È necessario collegare le porte del modulo controller utilizzate per il peering del cluster in modo che siano connessi al cluster sul sito del partner.

### A proposito di questa attività

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.

### Fase

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.

### Informazioni correlate

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

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 e decidere se utilizzare porte condivise o dedicate per tali relazioni.

["Peering dei cluster"](#)

## Cablaggio dell'interconnessione ha

Se si dispone di una configurazione MetroCluster a otto o quattro nodi e i controller storage all'interno delle coppie ha si trovano in uno chassis separato, è necessario collegare l'interconnessione ha tra i controller.

### A proposito di questa attività

- Questa attività non si applica alle configurazioni MetroCluster a due nodi.
- Questa attività deve essere eseguita in entrambi i siti MetroCluster.
- L'interconnessione ha deve essere cablata solo se i controller storage all'interno della coppia ha si trovano in uno chassis separato.

Alcuni modelli di storage controller supportano due controller in un unico chassis, nel qual caso utilizzano un'interconnessione ha interna.

### Fasi

1. Collegare l'interconnessione ha se il partner ha del controller di storage si trova in uno chassis separato.

["Documentazione dei sistemi hardware ONTAP"](#)

2. Se il sito MetroCluster include due coppie ha, ripetere i passaggi precedenti sulla seconda coppia ha.
3. Ripetere questa operazione sul sito del partner MetroCluster.

## Cablaggio della gestione e delle connessioni dati

È necessario collegare le porte di gestione e dati di ciascun controller di storage alle reti del sito.

### A proposito di questa attività

Questa attività deve essere ripetuta per ogni nuovo controller in entrambi i siti MetroCluster.

È possibile collegare le porte di gestione del controller e dello switch del cluster agli switch esistenti nella rete o a nuovi switch di rete dedicati, come gli switch di gestione del cluster NetApp CN1601.

### Fase

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

["Documentazione dei sistemi hardware ONTAP"](#)

## Cablare gli array storage agli switch FC in una configurazione MetroCluster

### Cablaggio degli array di storage agli switch FC in una configurazione MetroCluster

È necessario collegare gli array di storage agli switch FC in modo che i sistemi ONTAP nella configurazione MetroCluster possano accedere a un LUN di array specifico attraverso almeno due percorsi.

### Prima di iniziare

- Gli array di storage devono essere configurati per presentare le LUN degli array a ONTAP.
- I controller ONTAP devono essere collegati agli switch FC.
- Gli ISL devono essere cablati tra gli switch FC nei siti MetroCluster.
- È necessario ripetere questa attività per ciascun array di storage in entrambi i siti MetroCluster.
- È necessario collegare i controller in una configurazione MetroCluster agli array di storage tramite switch FC.

### Fasi

1. Collegare le porte dello storage array alle porte dello switch FC.

In ogni sito, collegare le coppie di porte ridondanti nell'array di storage agli switch FC su fabric alternativi. Ciò fornisce ridondanza nei percorsi per l'accesso alle LUN dell'array.

### Informazioni correlate

- La configurazione dello zoning dello switch consente di definire quali LUN di array possono essere visualizzati da uno specifico sistema ONTAP nella configurazione MetroCluster.

["Zoning dello switch in una configurazione MetroCluster con LUN array"](#)

- In una configurazione MetroCluster con LUN array, è necessario collegare le porte dello storage array che formano una coppia di porte ridondanti a switch FC alternativi.

["Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a due nodi"](#)

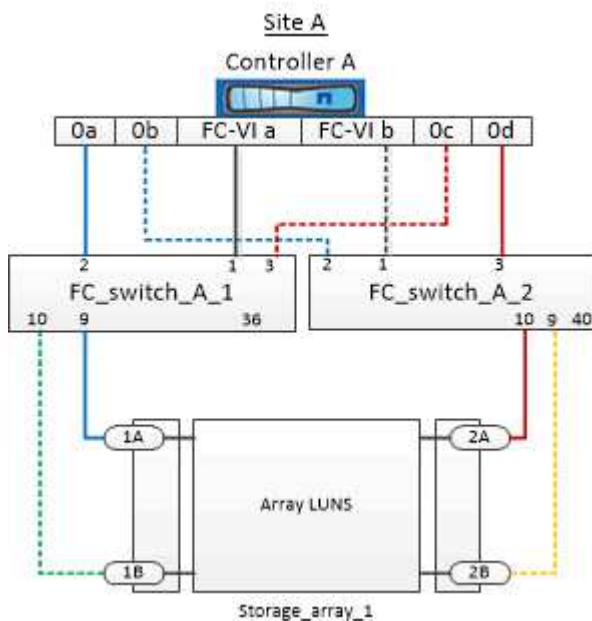
"Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a quattro nodi"

"Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a otto nodi"

#### Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a due nodi

In una configurazione MetroCluster con LUN array, è necessario collegare le porte dello storage array che formano una coppia di porte ridondanti a switch FC alternativi.

La figura seguente mostra le connessioni tra array di storage e switch FC in una configurazione MetroCluster fabric-attached a due nodi con LUN array:



Le connessioni tra le porte dello storage array e le porte dello switch FC sono simili sia per le varianti estensibile che per quelle collegate al fabric delle configurazioni MetroCluster a due nodi con LUN degli array.



Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte dello switch specificate per la configurazione con i dischi.

"Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Nell'illustrazione, le coppie di porte di array ridondanti per entrambi i siti sono le seguenti:

- Storage array presso il sito A:
  - Porte 1A e 2A
  - Porte 1B e 2B
- Storage array presso il sito B:
  - Porte 1A' e 2A'
  - Porte 1B' e 2B'



FC\_switch\_A\_1 nel sito A e FC\_switch\_B\_1 nel sito B sono collegati a Form Fabric\_1. Allo stesso modo, FC\_switch\_A\_2 nel sito A e FC\_switch\_B\_2 sono collegati al modulo Fabric\_2.

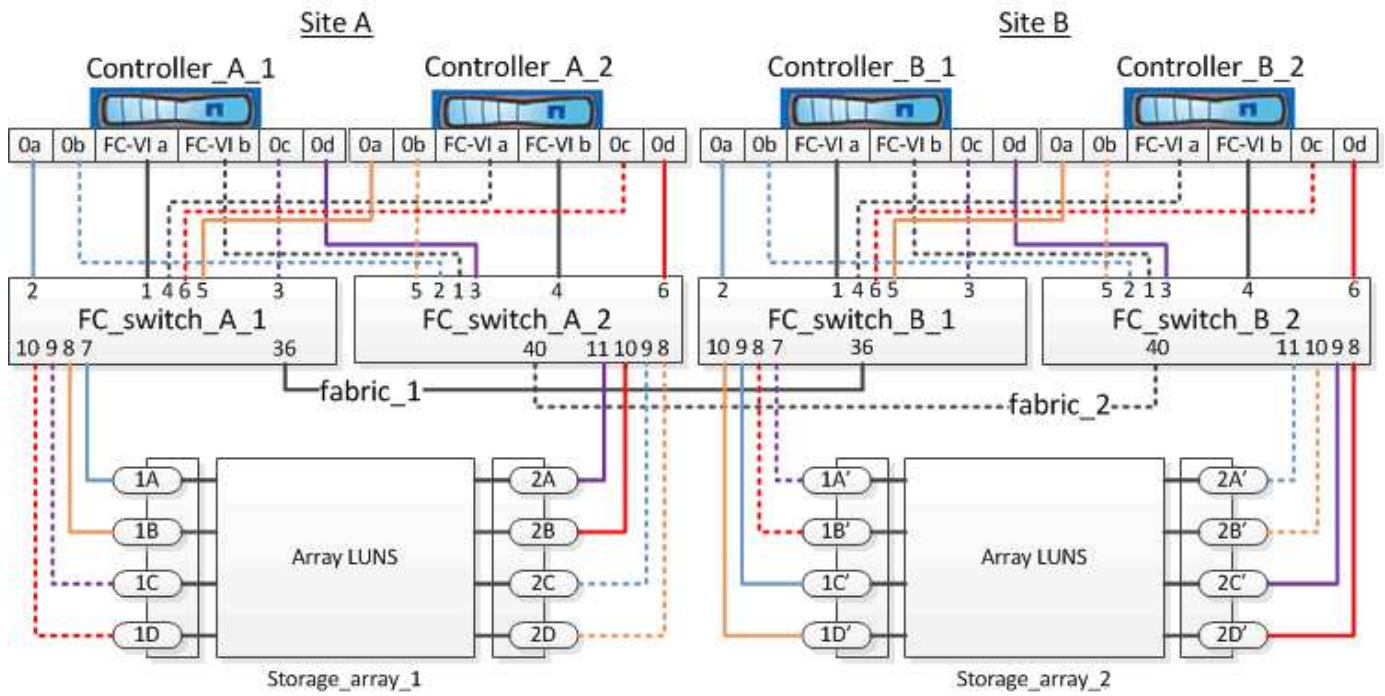
La seguente tabella elenca le connessioni tra le porte dello storage array e gli switch FC, come illustrato nell'esempio MetroCluster:

Porte LUN dell'array	Porte switch FC	Switch fabric
<b>Sito A</b>		
1A	FC_switch_A_1, porta 9	fabric_1
2A	FC_switch_A_2, porta 10	fabric_2
1B	FC_switch_A_1, porta 10	fabric_1
2B	FC_switch_A_2, porta 9	fabric_2
<b>Sito B</b>		
1 A'	FC_switch_B_1, porta 9	fabric_1
2'	FC_switch_B_2, porta 10	fabric_2
1B'	FC_switch_B_1, porta 10	fabric_1
2B'	FC_switch_B_2, porta 9	fabric_2

**Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a quattro nodi**

In una configurazione MetroCluster con LUN array, è necessario collegare le porte dello storage array che formano una coppia di porte ridondanti a switch FC alternativi.

La seguente illustrazione di riferimento mostra le connessioni tra array di storage e switch FC in una configurazione MetroCluster a quattro nodi con LUN di array:



Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte dello switch specificate per la configurazione con i dischi.

"Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Nell'illustrazione, le coppie di porte di array ridondanti per entrambi i siti sono le seguenti:

- Storage array presso il sito A:
  - Porte 1A e 2A
  - Porte 1B e 2B
  - Porte 1C e 2C
  - Porte 1D e 2D
- Storage array presso il sito B:
  - Porte 1A' e 2A'
  - Porte 1B' e 2B'
  - Porte 1C' e 2C'
  - Porte 1D' e 2D'

FC\_switch\_A\_1 nel sito A e FC\_switch\_B\_1 nel sito B sono collegati a Form Fabric\_1. Allo stesso modo, FC\_switch\_A\_2 nel sito A e FC\_switch\_B\_2 sono collegati al modulo Fabric\_2.

La seguente tabella elenca le connessioni tra le porte dello storage array e gli switch FC per l'illustrazione MetroCluster:

Porte LUN dell'array	Porte switch FC	Switch fabric
<b>Sito A</b>		

1A	FC_switch_A_1, porta 7	fabric_1
2A	FC_switch_A_2, porta 11	fabric_2
1B	FC_switch_A_1, porta 8	fabric_1
2B	FC_switch_A_2, porta 10	fabric_2
1C	FC_switch_A_1, porta 9	fabric_1
2C	FC_switch_A_2, porta 9	fabric_2
1D	FC_switch_A_1, porta 10	fabric_1
2D	FC_switch_A_2, porta 8	fabric_2
<b>Sito B</b>		
1 A'	FC_switch_B_1, porta 7	fabric_1
2'	FC_switch_B_2, porta 11	fabric_2
1B'	FC_switch_B_1, porta 8	fabric_1
2B'	FC_switch_B_2, porta 10	fabric_2
1"	FC_switch_B_1, porta 9	fabric_1
2C'	FC_switch_B_2, porta 9	fabric_2
1D'	FC_switch_B_1, porta 10	fabric_1
2D"	FC_switch_B_2, porta 8	fabric_2

#### **Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a otto nodi**

In una configurazione MetroCluster con LUN array, è necessario collegare le porte dello storage array che formano una coppia di porte ridondanti a switch FC alternativi.

Una configurazione MetroCluster a otto nodi è costituita da due gruppi DR a quattro nodi. Il primo gruppo di DR è costituito dai seguenti nodi:

- Controller\_A\_1
- Controller\_A\_2
- Controller\_B\_1
- Controller\_B\_2

Il secondo gruppo di DR è costituito dai seguenti nodi:

- Controller\_A\_3
- Controller\_A\_4
- Controller\_B\_3
- Controller\_B\_4

Per collegare le porte dell'array per il primo gruppo DR, è possibile utilizzare gli esempi di cablaggio per una configurazione MetroCluster a quattro nodi per il primo gruppo DR.

["Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a quattro nodi"](#)

Per collegare le porte dell'array per il secondo gruppo DR, seguire gli stessi esempi ed estrapolare le porte FC-VI e le porte FC Initiator appartenenti ai controller del secondo gruppo DR.

## **Zoning dello switch in una configurazione MetroCluster con LUN array**

### **Requisiti per lo zoning dello switch in una configurazione MetroCluster con LUN array**

Quando si utilizza lo zoning dello switch in una configurazione MetroCluster con LUN array, è necessario assicurarsi che vengano rispettati alcuni requisiti di base.

I requisiti per lo zoning dello switch in una configurazione MetroCluster con LUN array sono i seguenti:

- La configurazione di MetroCluster deve seguire lo schema di zoning da singolo iniziatore a destinazione singola.

La zoning da singolo iniziatore a destinazione singola limita ogni zona a una singola porta FC Initiator e a una singola porta di destinazione.

- Le porte FC-VI devono essere zonate end-to-end nel fabric.
- La condivisione di più porte initiator con una singola porta di destinazione può causare problemi di performance.

Analogamente, la condivisione di più porte di destinazione con una singola porta iniziatore può causare problemi di performance.

- È necessario aver eseguito una configurazione di base degli switch FC utilizzati nella configurazione MetroCluster.
  - ["Configurare manualmente gli switch Cisco FC"](#)
  - ["Configurare manualmente gli switch FC Brocade"](#)

### **Supporto di iniziatore condiviso e destinazione condivisa per la configurazione MetroCluster con LUN array**

La possibilità di condividere una data porta FC Initiator o una data porta di destinazione è utile per le organizzazioni che desiderano ridurre al minimo il numero di porte initiator o di destinazione utilizzate. Ad esempio, un'organizzazione che prevede un basso utilizzo di i/o su una porta FC Initiator o su porte di destinazione potrebbe preferire condividere la porta FC Initiator o le porte di destinazione invece di dedicare ciascuna porta FC Initiator a una singola porta di destinazione.

Tuttavia, la condivisione delle porte iniziatore o di destinazione può influire negativamente sulle prestazioni.

## Informazioni correlate

["Come supportare la configurazione Shared Initiator e Shared Target con LUN array in un ambiente MetroCluster"](#)

- Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da specifici sistemi ONTAP.

["Esempio di zoning dello switch in una configurazione MetroCluster a due nodi con LUN array"](#)

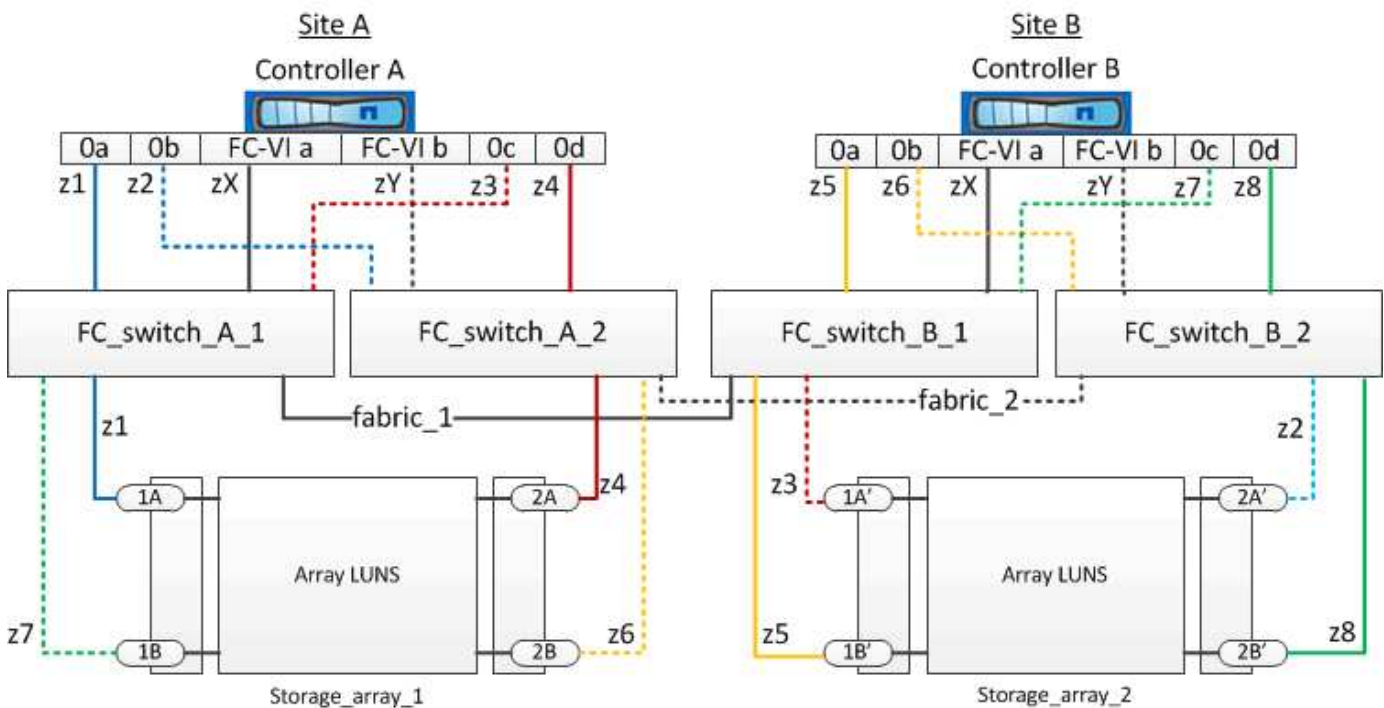
["Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"](#)

["Esempio di zoning dello switch in una configurazione MetroCluster a otto nodi con LUN array"](#)

## Esempio di zoning dello switch in una configurazione MetroCluster a due nodi con LUN array

Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da specifici sistemi ONTAP.

È possibile utilizzare il seguente esempio come riferimento per determinare lo zoning per una configurazione MetroCluster a due nodi collegata al fabric con LUN di array:



L'esempio mostra lo zoning da singolo iniziatore a destinazione singola per le configurazioni MetroCluster. Le linee dell'esempio rappresentano zone piuttosto che connessioni; ciascuna linea è etichettata con il relativo numero di zona.

Nell'esempio, le LUN degli array sono allocate su ciascun array di storage. I LUN di pari dimensione vengono forniti sugli array di storage di entrambi i siti, un requisito SyncMirror. Ogni sistema ONTAP dispone di due percorsi per l'array LUN. Le porte dell'array di storage sono ridondanti.

Le coppie di porte array ridondanti per entrambi i siti sono le seguenti:

- Storage array presso il sito A:
  - Porte 1A e 2A
  - Porte 1B e 2B
- Storage array presso il sito B:
  - Porte 1A' e 2A'
  - Porte 1B' e 2B'

Le coppie di porte ridondanti su ciascun array di storage formano percorsi alternativi. Pertanto, entrambe le porte delle coppie di porte possono accedere alle LUN sui rispettivi array di storage.

La seguente tabella mostra le zone per le illustrazioni:

Zona	Controller ONTAP e porta iniziatore	Porta dello storage array
<b>FC_switch_A_1</b>		
z1	Controller A: Porta 0a	Porta 1A
z3	Controller A: Porta 0c	Porta 1A'
<b>FC_switch_A_2</b>		
z2	Controller A: Porta 0b	Porta 2A'
z4	Controller A: Porta 0d	Porta 2A
<b>FC_switch_B_1</b>		
z5	Controller B: Porta 0a	Porta 1B'
z7	Controller B: Porta 0c	Porta 1B
<b>FC_switch_B_2</b>		
z6	Controller B: Porta 0b	Porta 2B
z8	Controller B: Porta 0d	Porta 2B'

La seguente tabella mostra le zone per le connessioni FC-VI:

Zona	Controller ONTAP e porta iniziatore	Switch
<b>Sito A</b>		
ZX	Controller A: Porta FC-VI A.	Switch_FC_A_1
ZY	Controller A: Porta FC-VI b	Switch_FC_A_2
<b>Sito B</b>		

ZX	Controller B: Porta FC-VI a	Switch_FC_B_1
ZY	Controller B: Porta FC-VI b	Switch_FC_B_2

### Informazioni correlate

- Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da un sistema ONTAP specifico.

["Requisiti per lo zoning dello switch in una configurazione MetroCluster con LUN array"](#)

["Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"](#)

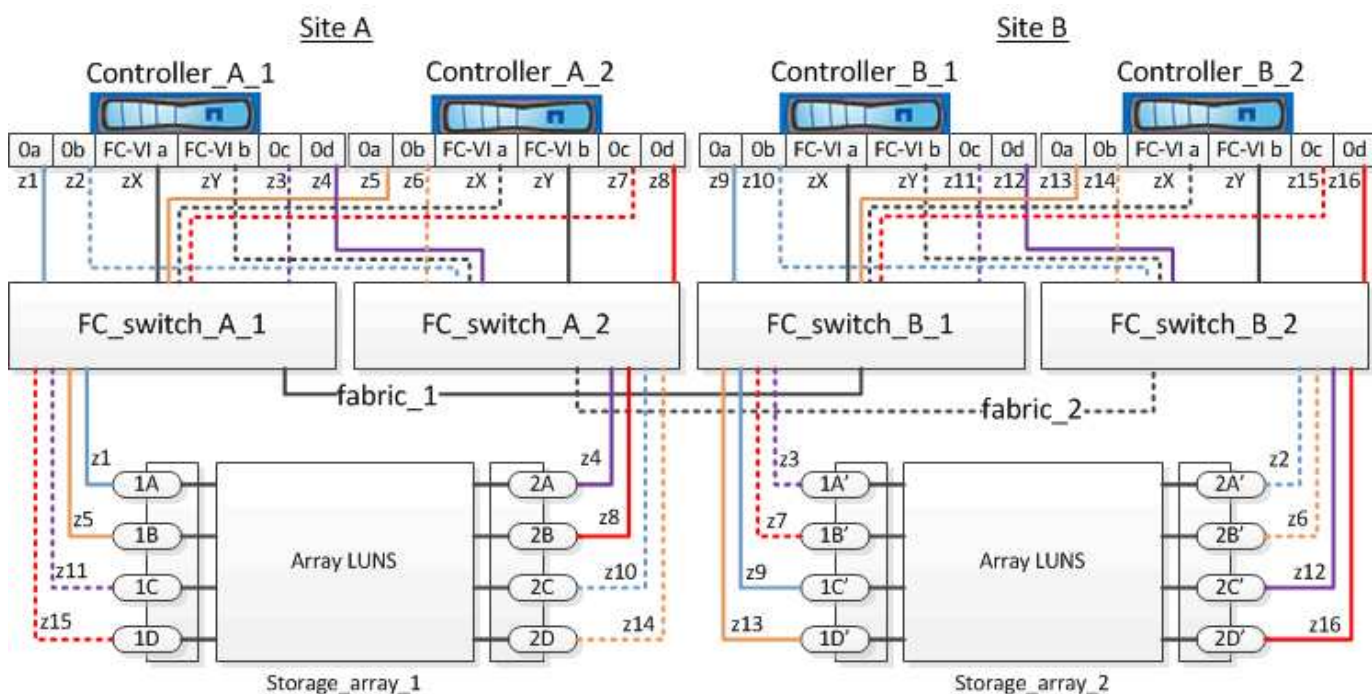
- Quando si utilizza lo zoning dello switch in una configurazione MetroCluster con LUN array, è necessario assicurarsi che vengano rispettati alcuni requisiti di base.

["Esempio di zoning dello switch in una configurazione MetroCluster a otto nodi con LUN array"](#)

### Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array

Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da uno specifico sistema ONTAP.

È possibile utilizzare il seguente esempio come riferimento per determinare lo zoning per una configurazione MetroCluster a quattro nodi con LUN di array. L'esempio mostra lo zoning da singolo iniziatore a destinazione singola per una configurazione MetroCluster. Le linee nell'esempio seguente rappresentano zone anziché connessioni; ciascuna linea è contrassegnata dal relativo numero di zona:



Nella figura, le LUN degli array sono allocate su ciascun array di storage per la configurazione MetroCluster. I LUN di pari dimensione vengono forniti sugli array di storage di entrambi i siti, un requisito SyncMirror. Ogni sistema ONTAP dispone di due percorsi per l'array LUN. Le porte dell'array di storage sono ridondanti.

Nell'illustrazione, le coppie di porte di array ridondanti per entrambi i siti sono le seguenti:

- Storage array presso il sito A:
  - Porte 1A e 2A
  - Porte 1B e 2B
  - Porte 1C e 2C
  - Porte 1D e 2D
- Storage array presso il sito B:
  - Porte 1A' e 2A'
  - Porte 1B' e 2B'
  - Porte 1C' e 2C'
  - Porte 1D' e 2D'

Le coppie di porte ridondanti su ciascun array di storage formano percorsi alternativi. Pertanto, entrambe le porte delle coppie di porte possono accedere alle LUN sui rispettivi array di storage.

Le seguenti tabelle mostrano le zone di questo esempio:

**Zone per FC\_switch\_A\_1**

Zona	Controller ONTAP e porta iniziatore	Porta dello storage array
z1	Controller_A_1: Porta 0a	Porta 1A
z3	Controller_A_1: Porta 0c	Porta 1A'
z5	Controller_A_2: Porta 0a	Porta 1B
z7	Controller_A_2: Porta 0c	Porta 1B'

**Zone per FC\_switch\_A\_2**

Zona	Controller ONTAP e porta iniziatore	Porta dello storage array
z2	Controller_A_1: Porta 0b	Porta 2A'
z4	Controller_A_1: Porta 0d	Porta 2A
z6	Controller_A_2: Porta 0b	Porta 2B'
z8	Controller_A_2: Porta 0d	Porta 2B

**Zone per FC\_switch\_B\_1**

Zona	Controller ONTAP e porta iniziatore	Porta dello storage array
------	-------------------------------------	---------------------------



z9	Controller_B_1: Porta 0a	Porta 1C'
z11	Controller_B_1: Porta 0c	Porta 1C
z13	Controller_B_2: Porta 0a	Porta 1D'
z15	Controller_B_2: Porta 0c	Porta 1D

#### **Zone per FC\_switch\_B\_2**

Zona	Controller ONTAP e porta iniziatore	Porta dello storage array
z10	Controller_B_1: Porta 0b	Porta 2C
z12	Controller_B_1: Porta 0d	Porta 2C'
z14	Controller_B_2: Porta 0b	Porta 2D
z16	Controller_B_2: Porta 0d	Porta 2D"

#### **Zone per le connessioni FC-VI nel sito A.**

Zona	Controller ONTAP e porta iniziatore FC	Switch
ZX	Controller_A_1: Porta FC-VI A.	Switch_FC_A_1
ZY	Controller_A_1: Porta FC-VI b	Switch_FC_A_2
ZX	Controller_A_2: Porta FC-VI A.	Switch_FC_A_1
ZY	Controller_A_2: Porta FC-VI b	Switch_FC_A_2

#### **Zone per le connessioni FC-VI nel sito B**

Zona	Controller ONTAP e porta iniziatore FC	Switch
ZX	Controller_B_1: Porta FC-VI A.	Switch_FC_B_1
ZY	Controller_B_1: Porta FC-VI b	Switch_FC_B_2
ZX	Controller_B_2: Porta FC-VI A.	Switch_FC_B_1
ZY	Controller_B_2: Porta FC-VI b	Switch_FC_B_2

## Informazioni correlate

- Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da specifici sistemi ONTAP.

["Esempio di zoning dello switch in una configurazione MetroCluster a due nodi con LUN array"](#)

["Esempio di zoning dello switch in una configurazione MetroCluster a otto nodi con LUN array"](#)

- Quando si utilizza lo zoning dello switch in una configurazione MetroCluster con LUN array, è necessario assicurarsi che vengano rispettati alcuni requisiti di base.

["Requisiti per lo zoning dello switch in una configurazione MetroCluster con LUN array"](#)

## Esempio di zoning dello switch in una configurazione MetroCluster a otto nodi con LUN array

Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da specifici sistemi ONTAP.

Una configurazione MetroCluster a otto nodi è costituita da due gruppi DR a quattro nodi. Il primo gruppo di DR è costituito dai seguenti nodi:

- Controller\_A\_1
- Controller\_A\_2
- Controller\_B\_1
- Controller\_B\_2

Il secondo gruppo di DR è costituito dai seguenti nodi:

- Controller\_A\_3
- Controller\_A\_4
- Controller\_B\_3
- Controller\_B\_4

Per configurare lo zoning dello switch, è possibile utilizzare gli esempi di zoning per una configurazione MetroCluster a quattro nodi per il primo gruppo DR.

["Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"](#)

Per configurare lo zoning per il secondo gruppo DR, seguire gli stessi esempi e requisiti per le porte FC Initiator e le LUN array appartenenti ai controller del secondo gruppo DR.

## Informazioni correlate

- Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da specifici sistemi ONTAP.

["Esempio di zoning dello switch in una configurazione MetroCluster a due nodi con LUN array"](#)

["Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"](#)

- Quando si utilizza lo zoning dello switch in una configurazione MetroCluster con LUN array, è necessario

assicurarsi che vengano rispettati alcuni requisiti di base.

["Requisiti per lo zoning dello switch in una configurazione MetroCluster con LUN array"](#)

## Configurare ONTAP in una configurazione MetroCluster con LUN array

### Verifica e configurazione dello stato ha dei componenti in modalità manutenzione

Quando si configura un sistema storage in una configurazione MetroCluster, è necessario assicurarsi che lo stato di alta disponibilità (ha) del modulo controller e dei componenti dello chassis sia "mcc" o "mcc-2n" in modo che questi componenti si avviino correttamente.

#### Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

#### A proposito di questa attività

Questa attività non è richiesta sui sistemi ricevuti dalla fabbrica.

#### Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

```
ha-config show
```

Lo stato ha corretto dipende dalla configurazione di MetroCluster.

Numero di controller nella configurazione MetroCluster	Lo stato HA per tutti i componenti deve essere...
Configurazione MetroCluster FC a otto o quattro nodi	mcc
Configurazione MetroCluster FC a due nodi	mcc-2n
Configurazione IP MetroCluster	mccip

2. Se lo stato di sistema visualizzato del controller non è corretto, impostare lo stato ha per il modulo controller:

Numero di controller nella configurazione MetroCluster	Comando
Configurazione MetroCluster FC a otto o quattro nodi	ha-config modify controller mcc
Configurazione MetroCluster FC a due nodi	ha-config modify controller mcc-2n
Configurazione IP MetroCluster	ha-config modify controller mccip

3. Se lo stato di sistema visualizzato dello chassis non è corretto, impostare lo stato ha per lo chassis:

Numero di controller nella configurazione MetroCluster	Comando
Configurazione MetroCluster FC a otto o quattro nodi	<code>ha-config modify chassis mcc</code>
Configurazione MetroCluster FC a due nodi	<code>ha-config modify chassis mcc-2n</code>
Configurazione IP MetroCluster	<code>ha-config modify chassis mccip</code>

4. Avviare il nodo su ONTAP:

```
boot_ontap
```

5. Ripetere questi passaggi su ciascun nodo della configurazione MetroCluster.

### Configurazione di ONTAP su un sistema che utilizza solo LUN di array

Se si desidera configurare ONTAP per l'utilizzo con le LUN degli array, è necessario configurare l'aggregato root e il volume root, riservare spazio per le operazioni di diagnostica e ripristino e impostare il cluster.

#### Prima di iniziare

- Il sistema ONTAP deve essere collegato allo storage array.
- L'amministratore dell'array di storage deve aver creato i LUN e presentarli a ONTAP.
- L'amministratore dell'array di storage deve aver configurato la protezione LUN.

#### A proposito di questa attività

È necessario configurare ciascun nodo che si desidera utilizzare con le LUN degli array. Se il nodo si trova in una coppia ha, è necessario completare il processo di configurazione su un nodo prima di procedere con la configurazione sul nodo partner.

#### Fasi

1. Accendere il nodo primario e interrompere il processo di avvio premendo Ctrl-C quando viene visualizzato il seguente messaggio sulla console:

```
Press CTRL-C for special boot menu.
```

2. Selezionare l'opzione **4 (pulizia della configurazione e inizializzazione di tutti i dischi)** nel menu di avvio.

Viene visualizzato l'elenco dei LUN degli array resi disponibili per ONTAP. Inoltre, viene specificata anche la dimensione del LUN dell'array richiesta per la creazione del volume root. Le dimensioni richieste per la creazione del volume root variano da un sistema ONTAP all'altro.

- Se in precedenza non sono stati assegnati LUN di array, ONTAP rileva e visualizza i LUN di array disponibili, come illustrato nell'esempio seguente:

```

mcc8040-ams1:> disk show NET-1.6 -instance
      Disk: NET-1.6
      Container Type: aggregate
      Owner/Home: mcc8040-ams1-01 / mcc8040-ams1-01
      DR Home: -
      Stack ID/Shelf/Bay: - / - / -
      LUN: 0
      Array: NETAPP_INF_1
      Vendor: NETAPP
      Model: INF-01-00
      Serial Number: 60080E50004317B40000003B158E35974
      UID:
60080E50:004317B4:0000003B1:58E35974:00000000:00000000:00000000:000000
00:00000000:00000000
      BPS: 512
      Physical Size: 87.50GB
      Position: data
      Checksum Compatibility: block
      Aggregate: eseries
      Plex: plex0

Paths:

      LUN  Initiator Side      Target
Side                               Link
Controller      Initiator      ID  Switch Port      Switch
Port            Acc Use  Target Port      TPGN      Speed
I/O KB/s            IOPS
-----
mcc8040-ams1-01    2c                0  mccb6505-ams1:16  mccb6505-
ams1:18          AO  INU  20330080e54317b4      1  4 Gb/S
0                0
mcc8040-ams1-01    2a                0  mccb6505-ams1:17  mccb6505-
ams1:19          ANO RDY  20320080e54317b4      0  4 Gb/S
0                0

Errors:
-
```

- Se le LUN degli array sono state assegnate in precedenza, ad esempio, tramite la modalità di manutenzione, vengono contrassegnate come locali o partner nell'elenco delle LUN degli array disponibili, a seconda che siano state selezionate o meno le LUN degli array dal nodo su cui si sta installando ONTAP o il partner ha:

In questo esempio, le LUN degli array con i numeri di indice 3 e 6 sono contrassegnate come "local" perché erano state precedentemente assegnate da questo nodo particolare:

```
*****
* No disks are owned by this node, but array LUNs are assigned.      *
* You can use the following information to verify connectivity from   *
* HBAs to switch ports.  If the connectivity of HBAs to switch ports *
* does not match your expectations, configure your SAN and rescan.    *
* You can rescan by entering 'r' at the prompt for selecting         *
* array LUNs below.                                                  *
```

```
*****
```

	HBA	HBA WWPN	Switch port	Switch port WWPN
	---	-----	-----	-----
	0e	500a098001baf8e0	vgbr6510s203:25	20190027f88948dd
	0f	500a098101baf8e0	vgci9710s202:1-17	
2011547feeead680				
	0g	500a098201baf8e0	vgbr6510s203:27	201b0027f88948dd
	0h	500a098301baf8e0	vgci9710s202:1-18	
2012547feeead680				

No native disks were detected, but array LUNs were detected.  
You will need to select an array LUN to be used to create the root  
aggregate and root volume.

The array LUNs visible to the system are listed below. Select one array  
LUN to be used to  
create the root aggregate and root volume. \*\*The root volume requires  
350.0 GB of space.\*\*

Warning: The contents of the array LUN you select will be erased by  
ONTAP prior to their use.

Index	Array LUN Name	Model	Vendor	Size	Owner
Checksum	Serial Number				
-----	-----	-----	-----	-----	-----
0	vgci9710s202:2-24.0L19	RAID5	DGC	217.3 GB	Block
6006016083402B0048E576D7					
1	vgbr6510s203:30.126L20	RAID5	DGC	217.3 GB	Block
6006016083402B0049E576D7					
2	vgci9710s202:2-24.0L21	RAID5	DGC	217.3 GB	Block
6006016083402B004AE576D7					
3	vgbr6510s203:30.126L22	RAID5	DGC	405.4 GB	local Block
6006016083402B004BE576D7					
4	vgci9710s202:2-24.0L23	RAID5	DGC	217.3 GB	Block
6006016083402B004CE576D7					
5	vgbr6510s203:30.126L24	RAID5	DGC	217.3 GB	Block

```
6006016083402B004DE576D7
```

```
6    vgbr6510s203:30.126L25    RAID5    DGC    423.5 GB    local    Block
```

```
6006016083402B003CF93694
```

```
7    vgci9710s202:2-24.0L26    RAID5    DGC    423.5 GB    Block
```

```
6006016083402B003DF93694
```

3. Selezionare il numero di indice corrispondente al LUN dell'array che si desidera assegnare come volume root.

Il LUN dell'array deve essere di dimensioni sufficienti per creare il volume root.

Il LUN dell'array selezionato per la creazione del volume root è contrassegnato come "locale (root)".

Nell'esempio seguente, il LUN dell'array con il numero di indice 3 è contrassegnato per la creazione del volume root:

The root volume will be created on switch 0:5.183L33.

**\*\*ONTAP requires that 11.0 GB of space be reserved for use in diagnostic and recovery operations.\*\*** Select one array LUN to be used as spare for diagnostic and recovery operations.

Index	Array LUN Name	Model	Vendor	Size	Owner
Checksum	Serial Number				
-----	-----	-----	-----	-----	-----
0	switch0:5.183L1	SYMMETRIX	EMC	266.1 GB	
Block	600604803436313734316631				
1	switch0:5.183L3	SYMMETRIX	EMC	266.1 GB	
Block	600604803436316333353837				
2	switch0:5.183L31	SYMMETRIX	EMC	266.1 GB	
Block	600604803436313237643666				
3	switch0:5.183L33	SYMMETRIX	EMC	658.3 GB	local (root)
Block	600604803436316263613066				
4	switch0:7.183L0	SYMMETRIX	EMC	173.6 GB	
Block	600604803436313261356235				
5	switch0:7.183L2	SYMMETRIX	EMC	173.6 GB	
Block	600604803436313438396431				
6	switch0:7.183L4	SYMMETRIX	EMC	658.3 GB	
Block	600604803436313161663031				
7	switch0:7.183L30	SYMMETRIX	EMC	173.6 GB	
Block	600604803436316538353834				
8	switch0:7.183L32	SYMMETRIX	EMC	266.1 GB	
Block	600604803436313237353738				
9	switch0:7.183L34	SYMMETRIX	EMC	658.3 GB	
Block	600604803436313737333662				

4. Selezionare il numero di indice corrispondente al LUN dell'array che si desidera assegnare per l'utilizzo nelle opzioni di diagnostica e ripristino.

Il LUN dell'array deve essere di dimensioni sufficienti per l'utilizzo nelle opzioni di diagnostica e ripristino. Se necessario, è anche possibile selezionare più LUN di array con una dimensione combinata maggiore o uguale alla dimensione specificata. Per selezionare più voci, è necessario immettere i valori separati da virgole di tutti i numeri di indice corrispondenti ai LUN dell'array che si desidera selezionare per le opzioni di diagnostica e ripristino.

L'esempio seguente mostra un elenco di LUN array selezionati per la creazione del volume root e per le opzioni di diagnostica e ripristino:



Here is a list of the selected array LUNs

Index	Array LUN Name	Model	Vendor	Size	Owner
Checksum	Serial Number				
-----	-----	-----	-----	-----	-----
2	switch0:5.183L31	SYMMETRIX	EMC	266.1 GB	local
Block	600604803436313237643666				
3	switch0:5.183L33	SYMMETRIX	EMC	658.3 GB	local (root)
Block	600604803436316263613066				
4	switch0:7.183L0	SYMMETRIX	EMC	173.6 GB	local
Block	600604803436313261356235				
5	switch0:7.183L2	SYMMETRIX	EMC	173.6 GB	local
Block	600604803436313438396431				

Do you want to continue (yes|no)?



Selezionando “no” si cancella la selezione del LUN.

5. Invio **y** quando richiesto dal sistema per continuare il processo di installazione.

Vengono creati l'aggregato root e il volume root e il resto del processo di installazione continua.

6. Inserire i dettagli richiesti per creare l'interfaccia di gestione dei nodi.

L'esempio seguente mostra la schermata dell'interfaccia di gestione dei nodi con un messaggio che conferma la creazione dell'interfaccia di gestione dei nodi:

Welcome to node setup.

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 setup wizard.  
Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

Enter the node management interface port [e0M]:

Enter the node management interface IP address: 192.0.2.66

Enter the node management interface netmask: 255.255.255.192

Enter the node management interface default gateway: 192.0.2.7

A node management interface on port e0M with IP address 192.0.2.66 has been created.

This node has its management address assigned and is ready for cluster setup.

## Al termine

Dopo aver configurato ONTAP su tutti i nodi che si desidera utilizzare con le LUN degli array, completare il <https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-ssg/home.html> ["Processo di installazione del cluster"]

## Informazioni correlate

["Requisiti e riferimenti per l'installazione della virtualizzazione FlexArray"](#)

## Configurazione del cluster

La configurazione del cluster comporta la configurazione di ciascun nodo, la creazione del cluster sul primo nodo e l'Unione di eventuali nodi rimanenti al cluster.

## Informazioni correlate

["Installazione del software"](#)

## Installazione della licenza per l'utilizzo di LUN array in una configurazione MetroCluster

È necessario installare la licenza V\_StorageAttach su ogni nodo MetroCluster che si desidera utilizzare con le LUN degli array. Non è possibile utilizzare le LUN degli array in un aggregato fino a quando la licenza non viene installata.

## Prima di iniziare

- Il cluster deve essere installato.
- È necessario disporre della chiave di licenza per la licenza V\_StorageAttach.

### A proposito di questa attività

È necessario utilizzare una chiave di licenza separata per ciascun nodo su cui si desidera installare la licenza V\_StorageAttach.

### Fasi

1. Installare la licenza V\_StorageAttach.

```
system license add
```

Ripetere questo passaggio per ogni nodo del cluster su cui si desidera installare la licenza.

2. Verificare che la licenza V\_StorageAttach sia installata su tutti i nodi richiesti in un cluster.

```
system license show
```

L'output di esempio seguente mostra che la licenza V\_StorageAttach è installata sui nodi di cluster\_A:

```
cluster_A::> system license show
Serial Number: nnnnnnnn
Owner: controller_A_1
Package      Type      Description      Expiration
-----
V_StorageAttach  license Virtual Attached Storage

Serial Number: 11111111
Owner: controller_A_2
Package      Type      Description      Expiration
-----
V_StorageAttach  license Virtual Attached Storage
```

### Configurazione delle porte FC-VI su una scheda X1132A-R6 quad-port su sistemi FAS8020

Se si utilizza la scheda a quattro porte X1132A-R6 su un sistema FAS8020, è possibile accedere alla modalità di manutenzione per configurare le porte 1a e 1b per l'utilizzo di FC-VI e Initiator. Questa operazione non è necessaria sui sistemi MetroCluster ricevuti dalla fabbrica, in cui le porte sono impostate in modo appropriato per la configurazione.

### A proposito di questa attività

Questa attività deve essere eseguita in modalità manutenzione.



Conversione di una porta FC in una porta FC-VI con `ucadmin` Il comando è supportato solo sui sistemi FAS8020 e AFF 8020. La conversione delle porte FC in porte FCVI non è supportata su altre piattaforme.

### Fasi

1. Disattivare le porte:

```
storage disable adapter 1a
```

```
storage disable adapter 1b
```

```
*> storage disable adapter 1a
Jun 03 02:17:57 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1a.
Host adapter 1a disable succeeded
Jun 03 02:17:57 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1a is now offline.
*> storage disable adapter 1b
Jun 03 02:18:43 [controller_B_1:fc.adapter.offlining:info]: Offlining
Fibre Channel adapter 1b.
Host adapter 1b disable succeeded
Jun 03 02:18:43 [controller_B_1:fc.adapter.offline:info]: Fibre Channel
adapter 1b is now offline.
*>
```

## 2. Verificare che le porte siano disattivate:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
-----	-----	-----	-----	-----	-----
...					
1a	fc	initiator	-	-	offline
1b	fc	initiator	-	-	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

## 3. Impostare le porte a e b sulla modalità FC-VI:

```
ucadmin modify -adapter 1a -type fcvi
```

Il comando imposta la modalità su entrambe le porte della coppia di porte, 1a e 1b (anche se solo 1a è specificata nel comando).

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1a. Reboot the controller for the changes to
take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has
changed to fcvi on adapter 1b. Reboot the controller for the changes to
take effect.
```

#### 4. Confermare che la modifica è in sospeso:

```
ucadmin show
```

```
*> ucadmin show
```

Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
...					
1a	fc	initiator	-	fcvi	offline
1b	fc	initiator	-	fcvi	offline
1c	fc	initiator	-	-	online
1d	fc	initiator	-	-	online

#### 5. Spegner il controller, quindi riavviarlo in modalità di manutenzione.

#### 6. Confermare la modifica della configurazione:

```
ucadmin show local
```

Node	Adapter	Mode	Type	Mode	Type	Status
...						
controller_B_1	1a	fc	fcvi	-	-	online
controller_B_1	1b	fc	fcvi	-	-	online
controller_B_1	1c	fc	initiator	-	-	online
controller_B_1	1d	fc	initiator	-	-	online
6 entries were displayed.						

## Assegnazione della proprietà delle LUN degli array

Le LUN degli array devono essere di proprietà di un nodo prima di poter essere aggiunte a un aggregato per essere utilizzate come storage.

### Prima di iniziare

- Il test della configurazione back-end (test della connettività e della configurazione dei dispositivi dietro i sistemi ONTAP) deve essere completato.
- I LUN degli array che si desidera assegnare devono essere presentati ai sistemi ONTAP.

### A proposito di questa attività

È possibile assegnare la proprietà di LUN array con le seguenti caratteristiche:

- Non sono di proprietà.
- Non presentano errori di configurazione degli array di storage, come ad esempio:
  - Il LUN dell'array è inferiore o superiore alle dimensioni supportate da ONTAP.
  - LDEV è mappato su una sola porta.
  - All'LDEV sono assegnati ID LUN non coerenti.
  - Il LUN è disponibile su un solo percorso.

ONTAP genera un messaggio di errore se si tenta di assegnare la proprietà di un LUN dell'array con errori di configurazione back-end che interferirebbero con il sistema ONTAP e l'array di storage che funzionano insieme. È necessario correggere tali errori prima di procedere con l'assegnazione del LUN dell'array.

ONTAP avvisa l'utente se si tenta di assegnare un LUN di array con un errore di ridondanza: Ad esempio, tutti i percorsi a questo LUN di array sono collegati allo stesso controller o solo a un percorso del LUN di array. È possibile correggere un errore di ridondanza prima o dopo l'assegnazione della proprietà del LUN.

### Fasi

1. Visualizzare le LUN degli array non ancora assegnate a un nodo:

```
storage disk show -container-type unassigned
```

2. Assegnare un LUN di array a questo nodo:

```
storage disk assign -disk array_LUN_name -owner nodename
```

Se si desidera correggere un errore di ridondanza dopo l'assegnazione del disco anziché in precedenza, è necessario utilizzare `-force` con il comando di assegnazione del disco di storage.

### Informazioni correlate

["Requisiti e riferimenti per l'installazione della virtualizzazione FlexArray"](#)

### 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.

### Fasi

1. Configurare le LIF tra cluster utilizzando la procedura descritta in:

["Configurazione delle LIF tra cluster"](#)

2. Creare una relazione peer del cluster utilizzando la procedura descritta in:

["Peering dei cluster"](#)

## Mirroring degli aggregati root

È necessario eseguire il mirroring degli aggregati root nella configurazione MetroCluster per garantire la protezione dei dati.

### Prima di iniziare

È necessario assicurarsi che i requisiti SyncMirror per la configurazione MetroCluster con le LUN degli array siano soddisfatti. Fare riferimento a ["Requisiti per una configurazione MetroCluster con LUN array"](#).

### A proposito di questa attività

Ripetere questa operazione per ogni controller nella configurazione MetroCluster.

### Fase

1. Eseguire il mirroring dell'aggregato root senza mirror:

```
storage aggregate mirror
```

Il seguente comando esegue il mirroring dell'aggregato root per controller\_A\_1:

```
controller_A_1::> storage aggregate mirror aggr0_controller_A_1
```

L'aggregato root viene mirrorato con LUN di array dal pool1.

## Creazione di aggregati di dati, implementazione e verifica della configurazione MetroCluster

È necessario creare aggregati di dati su ciascun nodo, implementare e verificare la configurazione di MetroCluster.

### Fasi

1. Creare aggregati di dati su ciascun nodo:
  - a. Creare un aggregato di dati mirrorato su ciascun nodo:

["Eseguire il mirroring degli aggregati root"](#).

- b. Se necessario, creare aggregati di dati senza mirroring:

["Creare un aggregato di dati mirrorato su ciascun nodo"](#).

2. ["Implementare la configurazione MetroCluster"](#).
3. ["Configurare gli switch MetroCluster FC per il monitoraggio dello stato di salute"](#).
4. Controllare e verificare la configurazione:

- a. ["Controllare la configurazione MetroCluster"](#).
  - b. ["Verificare la presenza di errori di configurazione MetroCluster con Config Advisor"](#).
  - c. ["Verificare lo switchover, la riparazione e lo switchback"](#).
5. Installare e configurare il software MetroCluster Tiebreaker:
  - a. ["Installare il software Tiebreaker"](#).
  - b. ["Configurare il software Tiebreaker"](#).
6. Impostare la destinazione dei file di backup della configurazione:  
["Proteggere i file di backup della configurazione"](#).

## Implementare una configurazione MetroCluster con dischi e LUN di array

### Implementazione di una configurazione MetroCluster con dischi e LUN di array

Per implementare una configurazione MetroCluster con dischi e LUN di array nativi, è necessario assicurarsi che i sistemi ONTAP utilizzati nella configurazione possano essere collegati agli array di storage.

Una configurazione MetroCluster con dischi e LUN di array può avere due o quattro nodi. Sebbene la configurazione MetroCluster a quattro nodi debba essere fabric-attached, la configurazione a due nodi può essere estensibile o fabric-attached.

In ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#), È possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster. Utilizzare **Esplora componenti** per selezionare i componenti e la versione di ONTAP per perfezionare la ricerca. È possibile fare clic su **Mostra risultati** per visualizzare l'elenco delle configurazioni supportate che corrispondono ai criteri.

#### Informazioni correlate

Per configurare una configurazione MetroCluster con collegamento a fabric a due nodi o una configurazione MetroCluster a quattro nodi con dischi e LUN di array nativi, è necessario utilizzare bridge FC-SAS per collegare i sistemi ONTAP agli shelf di dischi attraverso gli switch FC. È possibile collegare i LUN degli array ai sistemi ONTAP attraverso gli switch FC.

["Esempio di una configurazione MetroCluster a due nodi collegata al fabric con dischi e LUN di array"](#)

["Esempio di configurazione MetroCluster a quattro nodi con dischi e LUN di array"](#)

### Considerazioni sull'implementazione di una configurazione MetroCluster con dischi e LUN di array

Quando si pianifica la configurazione MetroCluster per l'utilizzo con dischi e LUN di array, è necessario prendere in considerazione diversi fattori, come l'ordine di impostazione dell'accesso allo storage, la posizione dell'aggregato root e l'utilizzo di porte, switch e bridge FC-SAS.

Per pianificare la configurazione, prendere in considerazione le informazioni riportate nella seguente tabella:

Considerazione	Linee guida
----------------	-------------



Ordine di impostazione dell'accesso allo storage	È possibile impostare prima l'accesso a dischi o LUN di array. Prima di configurare l'altro tipo di storage, è necessario completare tutte le operazioni di configurazione per quel tipo di storage e verificare che siano state configurate correttamente.
Posizione dell'aggregato root	<ul style="list-style-type: none"> <li>Se si sta configurando un'implementazione di <i>new</i> MetroCluster con dischi e LUN di array, è necessario creare l'aggregato root sui dischi nativi.</li> </ul> <p>Durante questa operazione, assicurarsi che <i>almeno un shelf</i> di dischi (con 24 dischi) sia configurato in ciascuno dei siti.</p> <ul style="list-style-type: none"> <li>Se si aggiungono dischi nativi a una configurazione MetroCluster <i>esistente</i> che utilizza LUN di array, l'aggregato root può rimanere su un LUN di array.</li> </ul>
Utilizzo di switch e bridge FC-SAS	<p>I bridge FC-SAS sono richiesti in configurazioni a quattro nodi e due nodi fabric-attached per collegare i sistemi ONTAP agli shelf di dischi attraverso gli switch.</p> <p>È necessario utilizzare gli stessi switch per connettersi agli array di storage e ai bridge FC-SAS.</p>
Utilizzando le porte FC Initiator	<p>Le porte iniziatore utilizzate per il collegamento a un bridge FC-SAS devono essere diverse dalle porte utilizzate per il collegamento agli switch, che si collegano agli array di storage.</p> <p>Per collegare un sistema ONTAP a dischi e LUN di array sono necessarie almeno otto porte di iniziatore.</p>

#### Informazioni correlate

- Le procedure e i comandi di configurazione dello switch sono diversi, a seconda del vendor dello switch.
  - ["Configurazione manuale degli switch Brocade FC"](#)
  - ["Configurazione manuale degli switch Cisco FC"](#)
- Quando si aggiunge nuovo storage alla configurazione, si installano e cablano i bridge RTO FibreBridge e gli shelf di dischi SAS.
  - ["Installazione di bridge FC-SAS e shelf di dischi SAS"](#)
- Lo zoning dello switch definisce i percorsi tra i nodi connessi. La configurazione dello zoning consente di definire quali LUN di array possono essere visualizzati da un sistema ONTAP specifico.
  - ["Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"](#)

## "Esempio di zoning dello switch in una configurazione MetroCluster a otto nodi con LUN array"

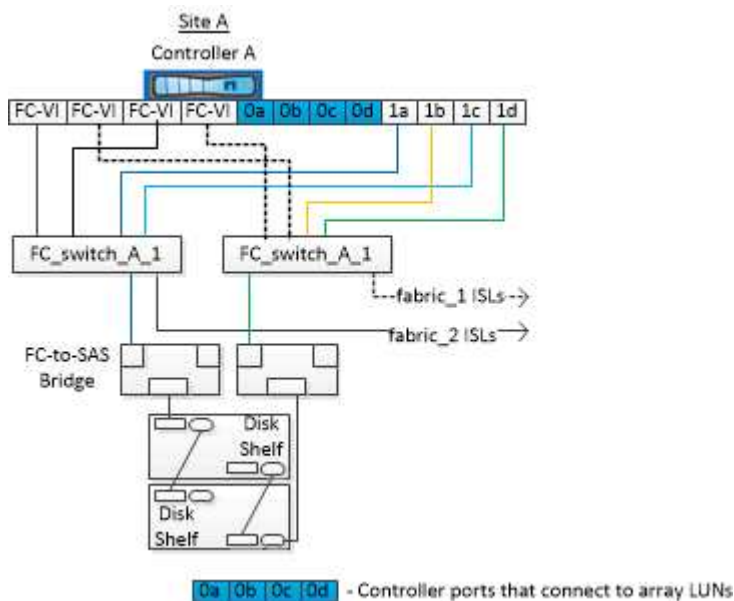
- "NetApp Hardware Universe"

### Esempio di una configurazione MetroCluster a due nodi collegata al fabric con dischi e LUN di array

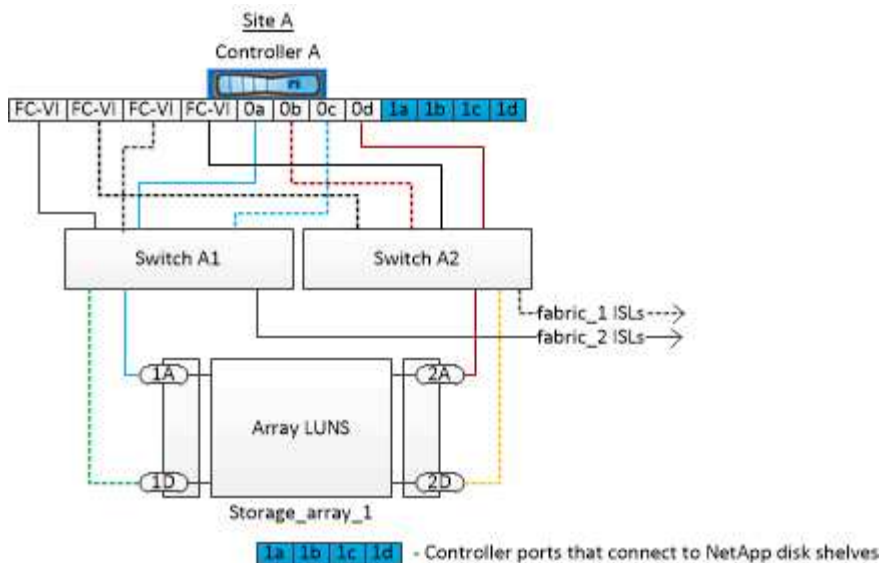
Per configurare una configurazione MetroCluster a due nodi con fabric-attached con dischi e LUN di array nativi, è necessario utilizzare bridge FC-SAS per collegare i sistemi ONTAP con gli shelf di dischi attraverso gli switch FC. È possibile collegare i LUN degli array ai sistemi ONTAP attraverso gli switch FC.

Le seguenti illustrazioni rappresentano esempi di configurazione MetroCluster a due nodi con collegamento a fabric con dischi e LUN di array. Entrambi rappresentano la stessa configurazione MetroCluster; le rappresentazioni per i dischi e le LUN degli array sono separate solo per semplificazioni.

Nella seguente illustrazione che mostra la connettività tra i sistemi e i dischi ONTAP, le porte HBA da 1a a 1d vengono utilizzate per la connettività con i dischi attraverso i bridge FC-SAS:



Nella seguente illustrazione che mostra la connettività tra i sistemi ONTAP e i LUN degli array, le porte HBA da 0a a 0d vengono utilizzate per la connettività con i LUN degli array perché le porte da 1a a 1d vengono utilizzate per la connettività con i dischi:



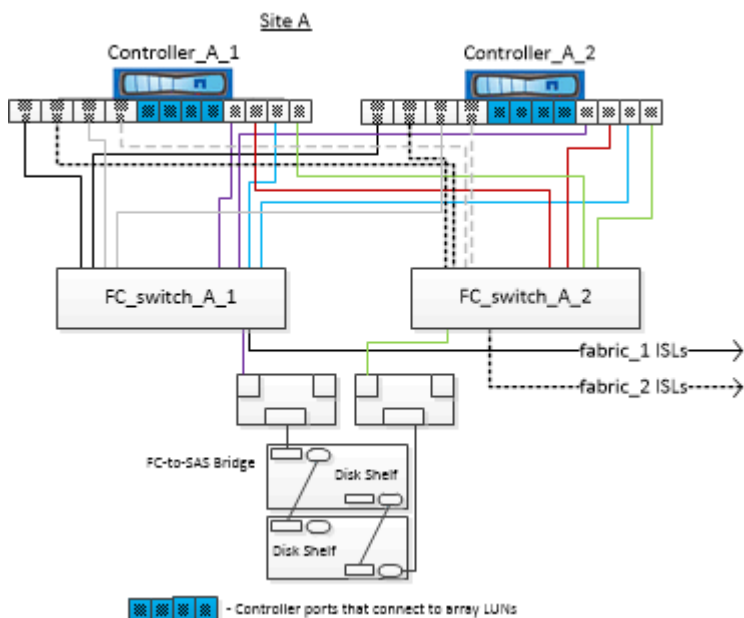
### Esempio di configurazione MetroCluster a quattro nodi con dischi e LUN di array

Per configurare una configurazione MetroCluster a quattro nodi con dischi e LUN di array nativi, è necessario utilizzare bridge FC-SAS per collegare i sistemi ONTAP con gli shelf di dischi attraverso gli switch FC. È possibile collegare i LUN degli array ai sistemi ONTAP attraverso gli switch FC.

Per la connessione a dischi nativi e LUN di array, un sistema ONTAP richiede almeno otto porte di iniziatore.

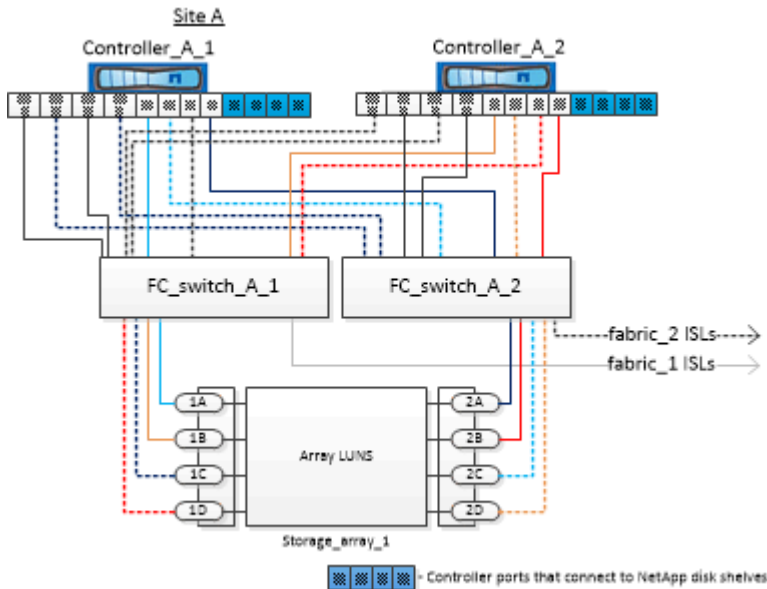
Le figure seguenti rappresentano esempi di configurazione MetroCluster con dischi e LUN di array. Entrambi rappresentano la stessa configurazione MetroCluster; le rappresentazioni per i dischi e le LUN degli array sono separate solo per semplificazioni.

Nella seguente illustrazione che mostra la connettività tra sistemi e dischi ONTAP, le porte HBA da 1a a 1d vengono utilizzate per la connettività con i dischi attraverso i bridge FC-SAS:



Nella seguente illustrazione, che mostra la connettività tra i sistemi ONTAP e i LUN degli array, le porte HBA

da 0a a 0d vengono utilizzate per la connettività con i LUN degli array perché le porte da 1a a 1d vengono utilizzate per la connettività con i dischi:



## Come utilizzare Active IQ Unified Manager e Gestore di sistema di ONTAP per ulteriori configurazioni e monitoraggi

### Sincronizzazione dell'ora di sistema mediante NTP

Ogni cluster necessita di un proprio server NTP (Network Time Protocol) per sincronizzare l'ora tra i nodi e i relativi client. È possibile utilizzare la finestra di dialogo Edit DateTime (Modifica data) in System Manager per configurare il server NTP.

#### Prima di iniziare

È necessario aver scaricato e installato System Manager. System Manager è disponibile sul sito di supporto NetApp.

#### A proposito di questa attività

- Non è possibile modificare le impostazioni del fuso orario per un nodo guasto o per il nodo partner dopo un Takeover.
- Ogni cluster nella configurazione MetroCluster FC deve disporre di uno o più server NTP separati utilizzati dai nodi, dagli switch FC e dai bridge FC-SAS in quel sito MetroCluster.

Se si utilizza il software MetroCluster Tiebreaker, deve disporre anche di un server NTP separato.

#### Fasi

1. Dalla home page, fare doppio clic sul sistema di storage appropriato.
2. Espandere la gerarchia **Cluster** nel riquadro di navigazione a sinistra.
3. Nel riquadro di navigazione, fare clic su **Configuration System Tools DateTime**.
4. Fare clic su **Edit** (Modifica).
5. Selezionare il fuso orario.

6. Specificare gli indirizzi IP dei server di riferimento orario, quindi fare clic su **Aggiungi**.

È necessario aggiungere un server NTP all'elenco dei server di riferimento orario. Il controller di dominio può essere un server autorevole.

7. Fare clic su **OK**.

8. Verificare le modifiche apportate alle impostazioni di data e ora nella finestra **Data e ora**.

## 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.

### 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.

## 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 per consentire a FlexCache di utilizzare `vserver peer repeer` comando.

### 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 sul sito MetroCluster\_A.

- 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 `vserver peer repeer` comando 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 un IPSpace 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 impostare gli archivi di oggetti come descritto in ["Impostare gli archivi di oggetti per FabricPool in una configurazione MetroCluster"](#).

#### 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.



Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

## Supporto FlexGroup nelle configurazioni MetroCluster

A partire da ONTAP 9.6, le configurazioni MetroCluster supportano i volumi FlexGroup.

## Supporto dei gruppi di coerenza nelle configurazioni MetroCluster

A partire da ONTAP 9.11.1, ["gruppi di coerenza"](#) Sono supportati nelle configurazioni MetroCluster.

## 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"](#)
- 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 oggetti IPSpace e requisiti di configurazione della subnet](#)

- Quando si configura la rete in una configurazione MetroCluster, è necessario conoscere i requisiti per la creazione di LIF.

### [Requisiti per la creazione di LIF in una configurazione MetroCluster](#)

- 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.

### [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

- Quando si configura la rete in una configurazione MetroCluster, è necessario conoscere i requisiti per la creazione di LIF.

### [Requisiti per la creazione di LIF in una configurazione MetroCluster](#)

- 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.

### [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 corretta creazione di una LIF in una configurazione MetroCluster eseguendo `metrocluster check lif show` comando. In caso di problemi durante la creazione della LIF, è possibile utilizzare `metrocluster check lif repair-placement` per risolvere i problemi.

## Informazioni correlate

- 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 oggetti IPSpace e requisiti di configurazione della subnet](#)

- 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.

### [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	<p>ONTAP identifica le porte di destinazione FC collegate sul cluster DR.</p>	<p>Le porte del cluster DR che si trovano nello stesso IPspace del LIF di origine vengono selezionate per un controllo di raggiungibilità.</p> <p>Se non sono presenti porte nel cluster DR nello stesso IPspace, non è possibile posizionare la LIF.</p> <p>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.</p>
Controllo della raggiungibilità	<p>La raggiungibilità viene determinata verificando la connettività del WWN del fabric di origine sulle porte del cluster DR.</p> <p>Se lo stesso fabric non è presente nel sito di DR, il LIF viene posizionato su una porta casuale del partner di DR.</p>	<p>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.</p> <p>Per il successo dei controlli di raggiungibilità, le trasmissioni ARP devono essere consentite tra i due cluster.</p> <p>Ogni porta che riceve una risposta dalla LIF di origine verrà contrassegnata come possibile per il posizionamento.</p>

Selezione della porta	<p>ONTAP classifica le porte in base ad attributi quali tipo di adattatore e velocità, quindi seleziona le porte con attributi corrispondenti.</p> <p>Se non vengono trovate porte con attributi corrispondenti, la LIF viene posizionata su una porta connessa in modo casuale del partner DR.</p>	<p>Dalle porte contrassegnate come raggiungibili durante il controllo di raggiungibilità, ONTAP preferisce le porte che si trovano nel dominio di broadcast associato alla subnet della LIF.</p> <p>Se nel cluster DR non sono disponibili porte di rete che si trovano nel dominio di trasmissione associato alla subnet della LIF, ONTAP seleziona le porte che hanno la raggiungibilità della 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.

## Le LIF non sono accessibili dopo uno switchover

Se viene apportata una modifica al fabric dello switch FC a cui sono collegate le porte di destinazione FC dei nodi di origine e DR, i LIF FC posizionati presso il partner DR potrebbero diventare inaccessibili agli host dopo un'operazione di switchover.

Eseguire il `metrocluster check lif repair-placement` Comando sul nodo di origine e sui nodi DR dopo una modifica apportata al fabric dello switch FC per verificare la connettività host delle LIF. Le modifiche apportate al fabric dello switch potrebbero causare il posizionamento di LIF in diverse porte FC di destinazione nel nodo partner DR.

## Informazioni correlate

- 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 oggetti IPspace e requisiti di configurazione della subnet](#)

- Quando si configura la rete in una configurazione MetroCluster, è necessario conoscere i requisiti per la creazione di LIF.

[Requisiti per la creazione di LIF in una configurazione MetroCluster](#)

## Creazione di un volume su un aggregato root

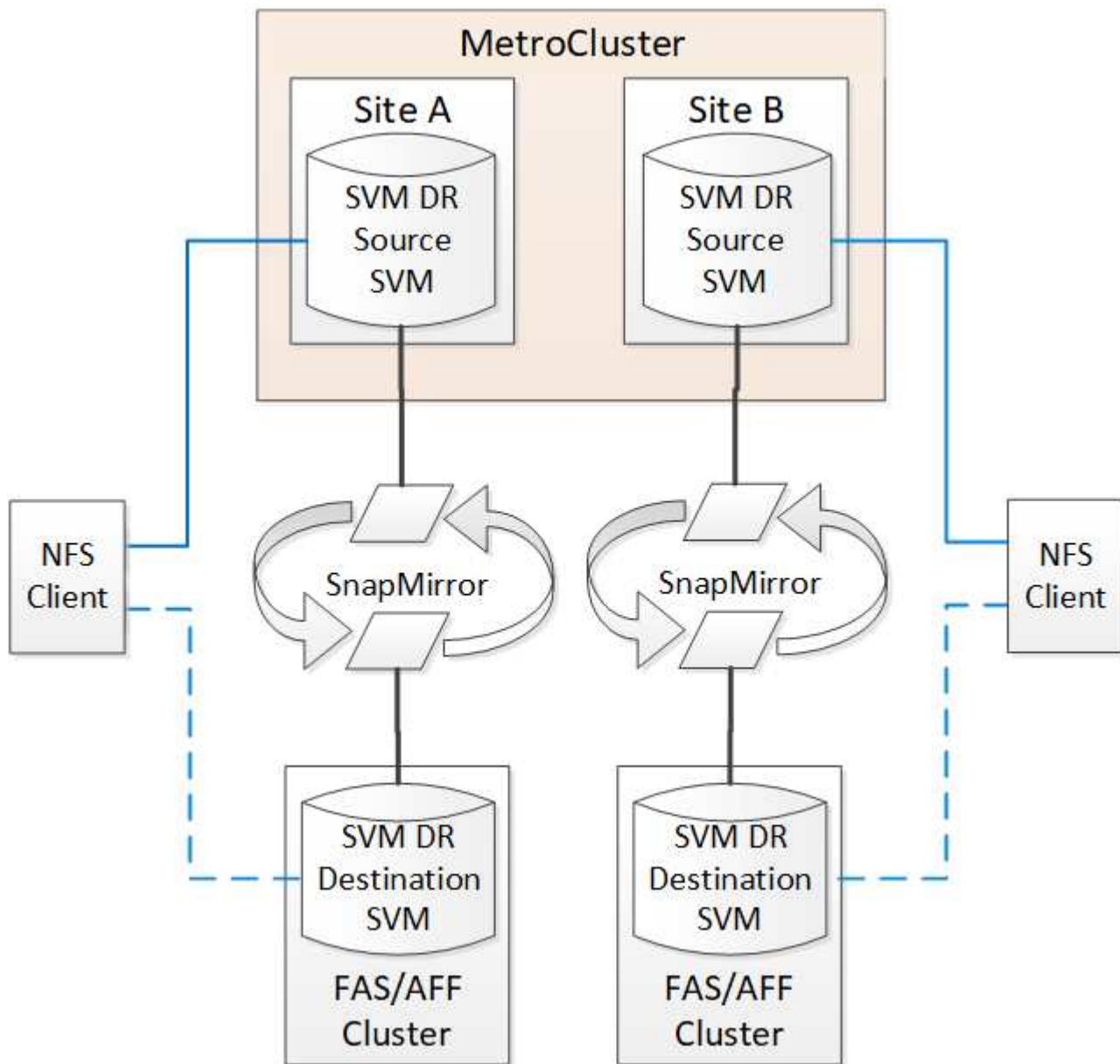
Il sistema non consente la creazione di nuovi volumi nell'aggregato root (un aggregato con un criterio ha di CFO) di un nodo in una configurazione MetroCluster.

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.

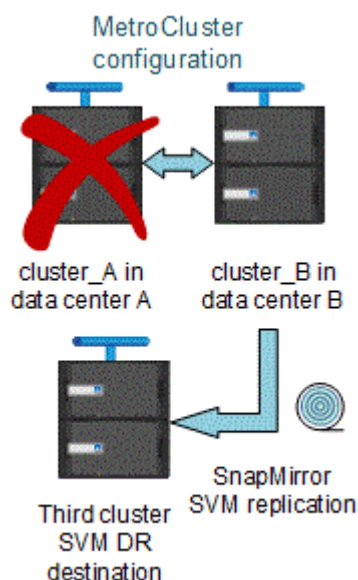
- Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.

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.

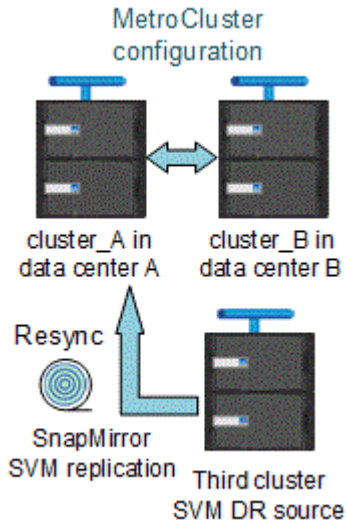
Tuttavia, una volta completato il processo di switchover o switchback, gli aggiornamenti pianificati per il DR SVM successivi avranno esito positivo.

Vedere la sezione “Replica della configurazione SVM” nel ["Protezione dei dati con la CLI"](#) 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 del comando "storage aggregate plex show" è indeterminato dopo uno switchover MetroCluster

Quando si esegue `storage aggregate plex show` Comando dopo uno switchover MetroCluster, lo stato di plex0 dell'aggregato root commutato è indeterminato e viene visualizzato come "failed". 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.

#### A proposito di questa attività





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 e sul funzionamento di MetroCluster.

### MetroCluster e informazioni varie

Informazioni	Soggetto
<a href="#">"Documentazione di ONTAP 9"</a>	<ul style="list-style-type: none"><li>• Tutte le informazioni MetroCluster</li></ul>
<a href="#">"Architettura e progettazione della soluzione NetApp MetroCluster, TR-4705"</a>	<ul style="list-style-type: none"><li>• Panoramica tecnica della configurazione e del funzionamento del MetroCluster FC.</li><li>• Best practice per la configurazione MetroCluster FC.</li></ul>
<a href="#">"Architettura e progettazione della soluzione IP MetroCluster, TR-4689"</a>	<ul style="list-style-type: none"><li>• Panoramica tecnica della configurazione e del funzionamento dell'IP MetroCluster.</li><li>• Best practice per la configurazione IP di MetroCluster.</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="#">"Installazione e configurazione di MetroCluster IP: Differenze tra le configurazioni di ONTAP MetroCluster"</a>	<ul style="list-style-type: none"><li>• Architettura IP di MetroCluster</li><li>• Cablaggio della configurazione</li><li>• Configurazione di MetroCluster in ONTAP</li></ul>
<a href="#">"Gestione MetroCluster e disaster recovery"</a>	<ul style="list-style-type: none"><li>• Informazioni sulla configurazione di MetroCluster</li><li>• Switchover, healing e switchback</li><li>• Disaster recovery</li></ul>

<p>"Gestire i componenti di MetroCluster"</p>	<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>
<p>"Transizione da MetroCluster FC a MetroCluster IP"</p> <p>"Guida all'upgrade e all'espansione di MetroCluster"</p>	<ul style="list-style-type: none"> <li>• Aggiornamento o aggiornamento di una configurazione MetroCluster</li> <li>• Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP</li> <li>• Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi</li> </ul>
<p>"Installazione e configurazione del software MetroCluster Tiebreaker"</p>	<ul style="list-style-type: none"> <li>• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker</li> </ul>
<p>Documentazione di Active IQ Digital Advisor</p> <p>"Documentazione NetApp: Guide e risorse sui prodotti"</p>	<ul style="list-style-type: none"> <li>• Monitoraggio della configurazione e delle prestazioni di MetroCluster</li> </ul>
<p>"Transizione basata sulla copia"</p>	<ul style="list-style-type: none"> <li>• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster</li> </ul>
<p>"Concetti di ONTAP"</p>	<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.