Documentazione MetroCluster

ONTAP MetroCluster

NetApp
April 25, 2024

Sommario

Documentazione MetroCluster

Note di rilascio di MetroCluster

Il "Note sulla versione di ONTAP 9" descrivere nuove funzionalità, note sull'aggiornamento, problemi risolti, limitazioni note e problemi noti.

Per accedere alle Note sulla versione, devi accedere al sito di supporto NetApp.

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 Tutti gli array SAN	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 (OOOD) 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	• AptPolicy deve essere impostato su 1 • DLS deve essere impostato su Off • IOD deve essere impostato su ON	• AptPolicy deve essere impostato su 3 • DLS deve essere impostato su ON • IOD deve essere impostato su Off

Cisco	Policy per il VSAN designato da FCVI: • Policy per il bilanciamento del carico: Srcid e dstid • IOD deve essere impostato su ON Policy per il VSAN designato per lo storage: • Policy per il bilanciamento del carico: Srcid, dstid e oxid • VSAN non deve avere l'opzione di garanzia in-order impostata	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.

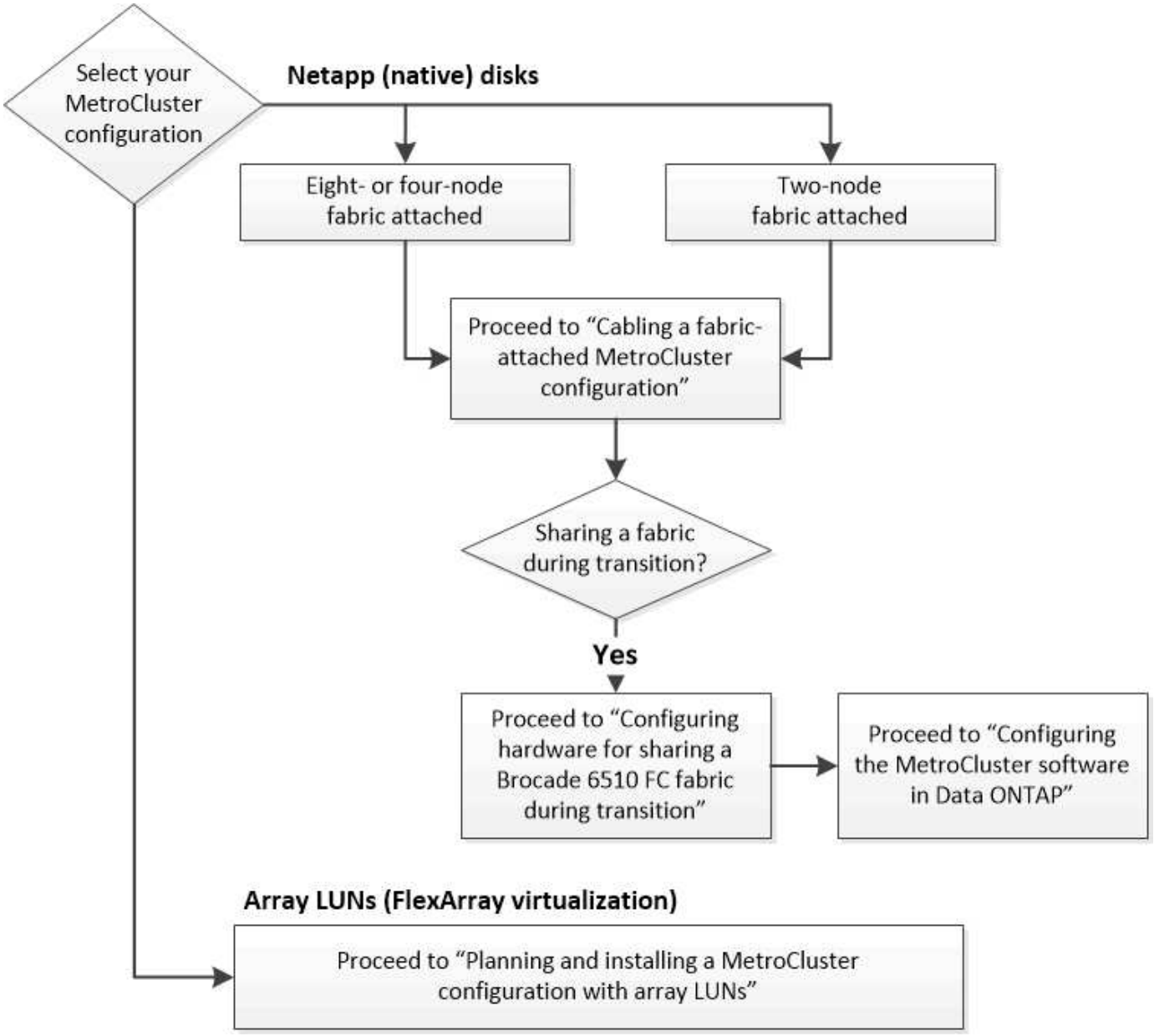
La seguente tabella mostra l'utilizzo della porta TCP/UDP in un firewall esterno posizionato tra due siti MetroCluster.

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.

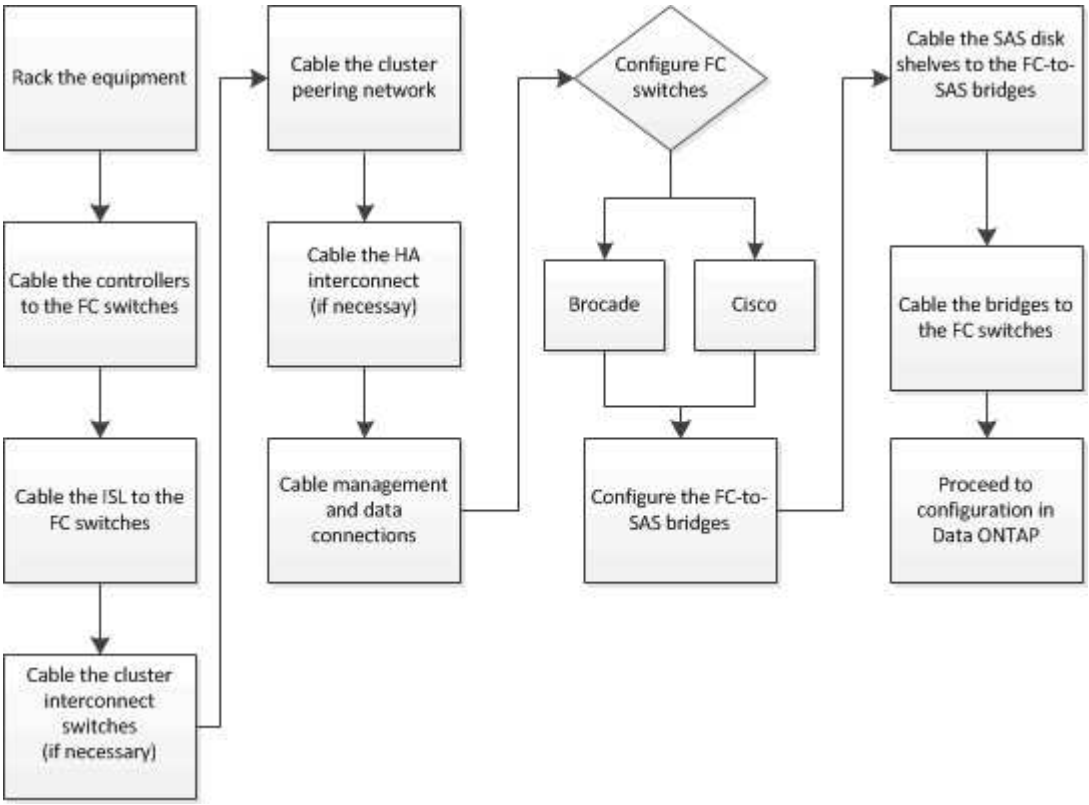


Per questo tipo di installazione…	Utilizzare queste procedure…
Configurazione fabric-attached con dischi NetApp (nativi)	1. "Cablaggio di una configurazione MetroCluster collegata al fabric" 2. "Configurazione del software MetroCluster in ONTAP"
Configurazione fabric-attached durante la condivisione 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.	1. "Cablaggio di una configurazione MetroCluster collegata al fabric" 2. "Configurazione dell'hardware MetroCluster per la condivisione di un fabric FC Brocade 6510 7-Mode durante la transizione" 3. "Configurazione del software MetroCluster in ONTAP"

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

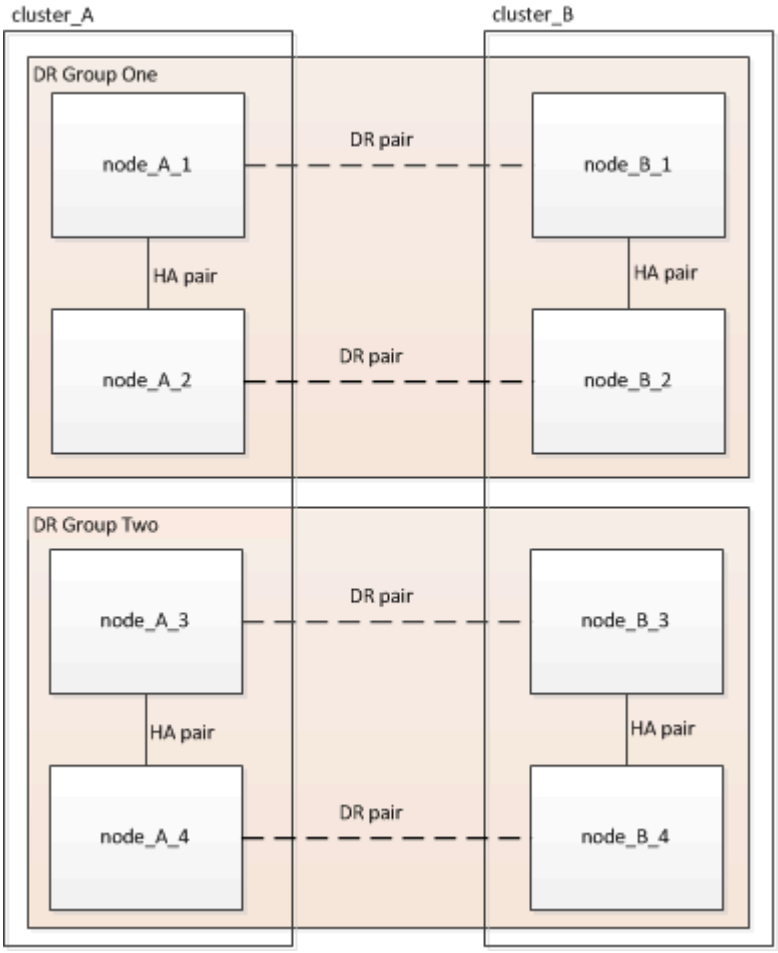
Durante la pianificazione della configurazione MetroCluster, è necessario comprendere i componenti hardware e il modo in cui si collegano.

Gruppi di disaster recovery (DR)

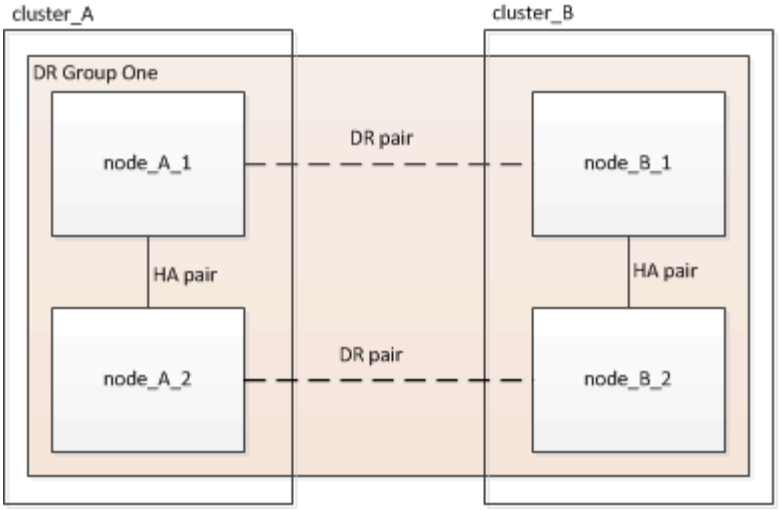
Una configurazione Fabric MetroCluster è costituita da uno o due gruppi DR, a seconda del numero di nodi nella configurazione MetroCluster. Ciascun gruppo di DR è costituito da quattro nodi.

- 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.

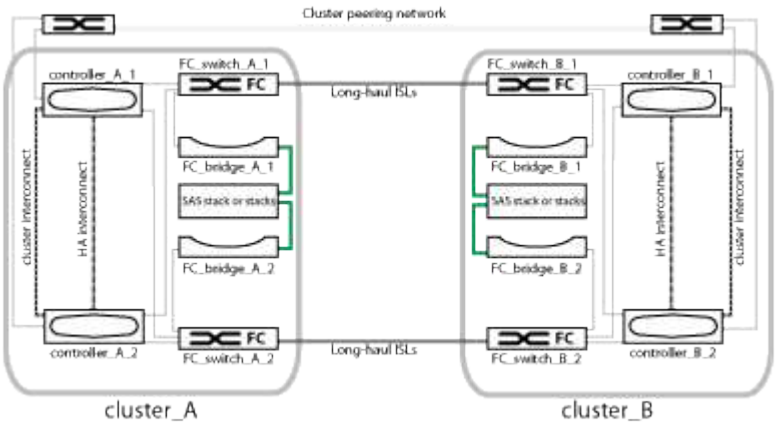
- Connessioni Ethernet dai controller alla rete fornita dal cliente utilizzata per il peering del cluster

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

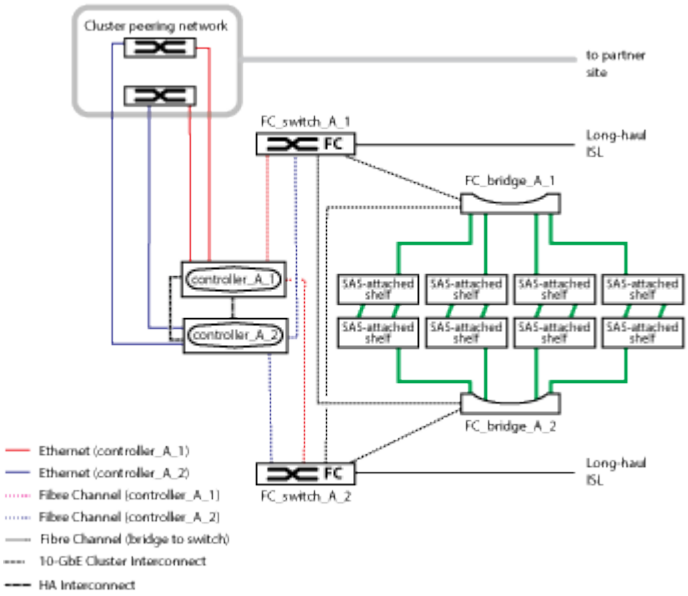
- Un'interconnessione del cluster tra ciascun controller del cluster locale

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.

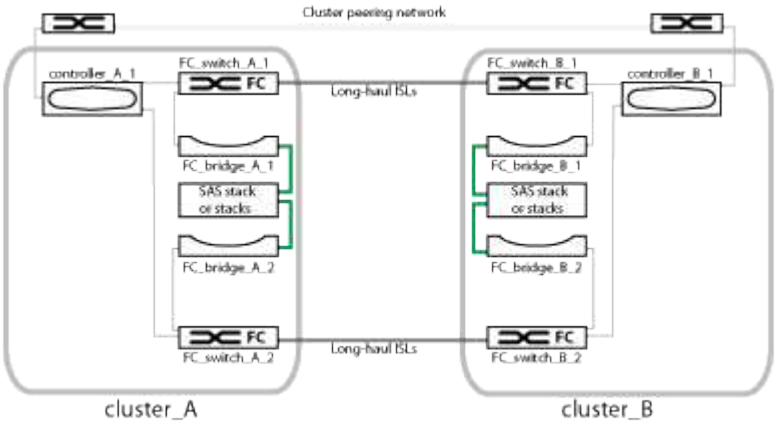


La seguente illustrazione mostra una vista più dettagliata della connettività in un singolo cluster MetroCluster (entrambi i cluster hanno la stessa configurazione):



Configurazione Fabric MetroCluster a due nodi

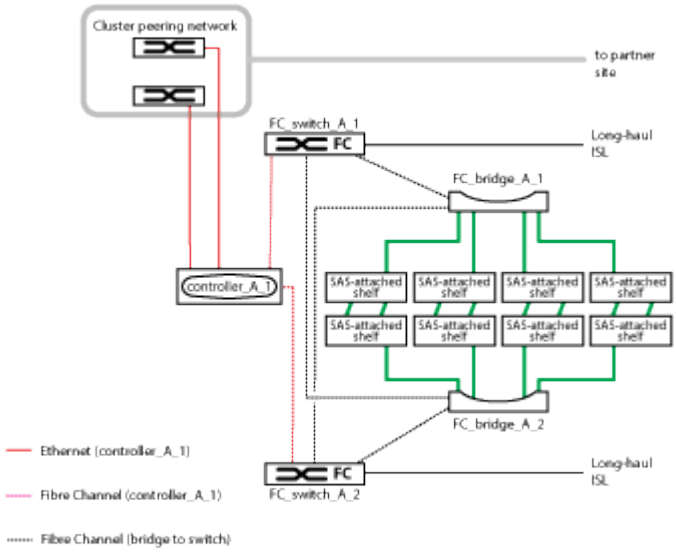
La figura seguente mostra una vista semplificata di una configurazione MetroCluster fabric a due nodi. Per alcune connessioni, una singola linea rappresenta connessioni multiple e ridondanti tra i componenti. Le connessioni di rete per dati e gestione non vengono visualizzate.



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:

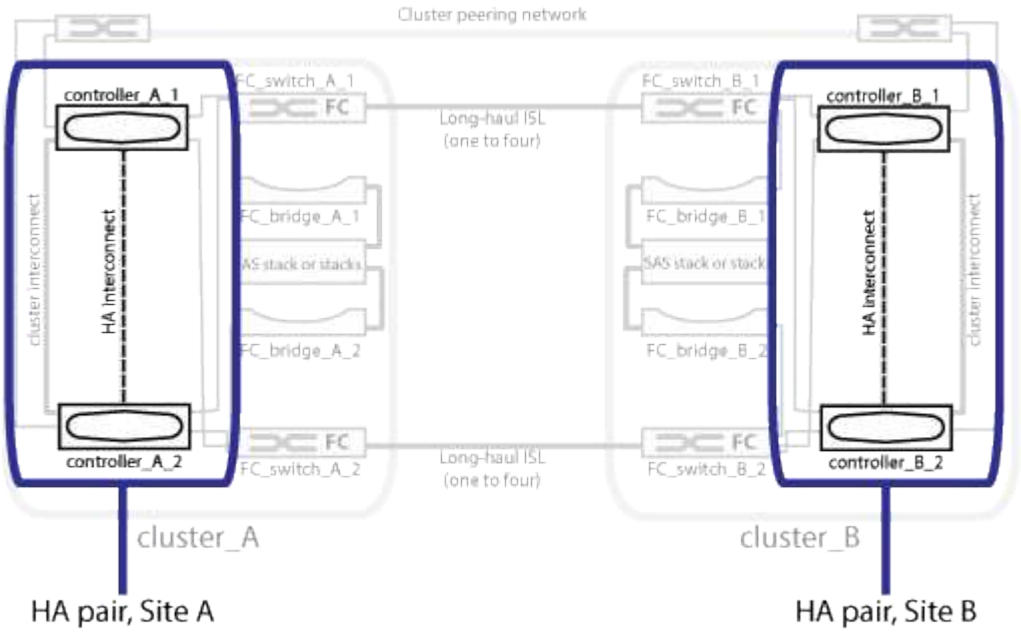
- Connessioni FC tra l'adattatore FC-VI su ciascun modulo controller
- Connessioni FC dagli HBA di ciascun modulo controller al bridge FC-SAS per ogni shelf stack SAS
- Connessioni SAS tra ogni shelf SAS e dalla parte superiore e inferiore di ogni stack a un bridge FC-SAS
- Connessioni Ethernet dai controller 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"

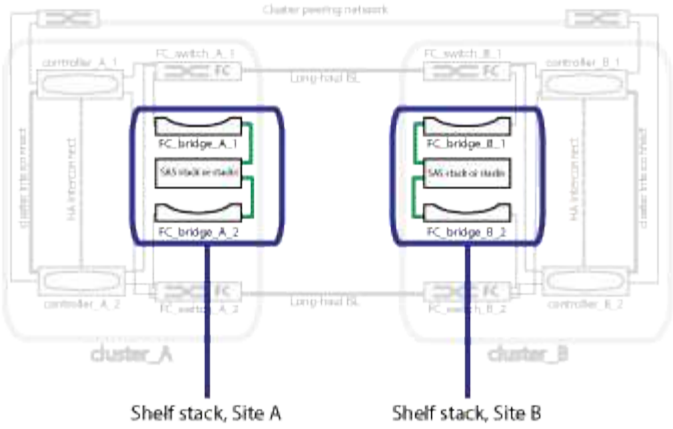
"Fabric switch FC ridondanti"

"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

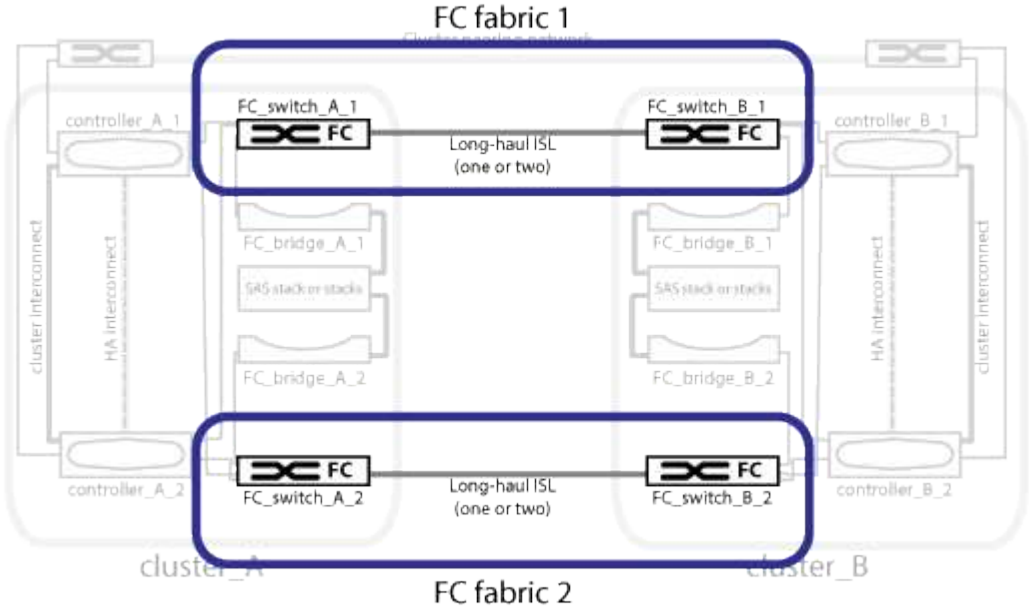
"Immagine delle coppie ha locali in una configurazione MetroCluster"

"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"

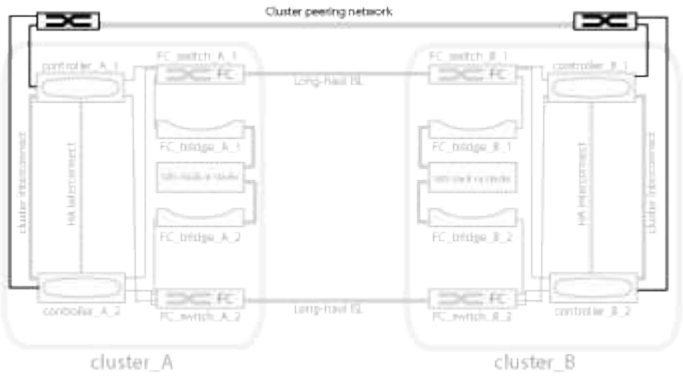
"Immagine di bridge FC-SAS ridondanti"

"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 ha. 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	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

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		Switch Brocade modello G720
		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		Switch Brocade modello G720
		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_51a	1	32	56	20
26	32	bridge_x_51b	2	32	56	20	26
32	Stack 2	bridge_x_52a	1	33	57	21	27
33	bridge_x_52b	2	33	57	21	27	33
Stack 3	bridge_x_53a	1	34	58	22	30	34
bridge_x_54b	2	34	58	22	30	34	Stack y
bridge_x_ya	1	35	59	23	31	35	bridge_x_yb

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 **Nota**: 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_51a	FC1	1	32	-	26	26	32
		FC2	2	32	-	26	26	32
	bridge_x_51b	FC1	1	33	-	27	27	33
		FC2	2	33	-	27	27	33
Stack 2	bridge_x_52a	FC1	1	34	-	30	30	34
		FC2	2	34	-	30	30	34
	bridge_x_52b	FC1	1	35	-	31	31	35
		FC2	2	35	-	31	31	35
Stack 3	bridge_x_53a	FC1	1	-	-	32	32	36
		FC2	2	-	-	32	32	36
	bridge_x_53b	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	• "Configurare gli switch Brocade FC con i file RCF" • "Configurare gli switch FC Cisco con i file RCF"
Non disporre di un RCF o di un RCF che non soddisfi i requisiti dell'utente	• "Configurare manualmente gli switch Brocade FC" • "Configurare manualmente gli switch Cisco FC"

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 × distanza reale = distanza.

   Se la distanza è di 3 km, 1.5 × 3 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 × 20 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.

Download e installazione del software NX-OS dello switch FC Cisco

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

seguente:

```
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:

   `switchcfgpersistentenable`

   Su FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

   Su FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgpersistentenable
   ```

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 **Nota:** 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-numbernumber 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
25  26  27
----------------+---+---+---+---+-----+---+---+---+----+---+---+---+
-----+---+---+---
Speed             AN  AN  AN  AN    AN  AN  8G  AN   AN  AN  16G  16G
AN  AN  AN  AN
Fill Word         0   0   0   0     0   0   3   0    0   0   3   3     3
0   0   0
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
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
Mirror Port       ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Rate Limit        ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Credit Recovery   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
```

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 × real_distance = distanza

   Se la distanza è di 3 km, allora 1.5 × 3 km = 4.5 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 × 20 km = 30 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     Lx      Max/Resv    Buffer Needed    Link      Remaining
Port  Type    Mode     Buffers     Usage  Buffers   Distance  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 fciptunnel 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:

   ```
   portcfig 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           Config
Port   Configured    Active   Configured   Active  Speed
----   ----------    -------  ----------   ------  -----
  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

Zona nel fabric_1	**Porte dei membri**
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

Zona nel fabric_2	Porte dei membri
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 Encryption
Port  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:
   a. Accedere alla modalità di configurazione, se non è già stata eseguita questa operazione:

      ```
      config t
      ```

   b. Modificare il database VSAN:

      ```
      vsan database
      ```

   c. Impostare l'ID VSAN:

      ```
      vsan vsan-ID
      ```

   d. Impostare il nome VSAN:

      ```
      vsan vsan-ID name vsan_name
      ```

2. Aggiunta di porte a FC-VI VSAN:
   a. 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.

   b. Uscire dalla modalità di configurazione:

      ```
      end
      ```

   c. 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 x 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.

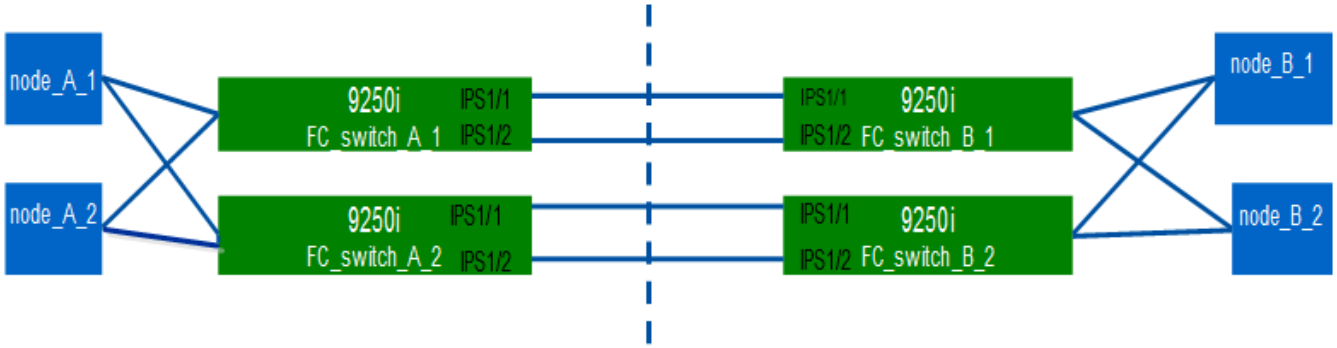
Configurazione delle porte FCIP per un ISL doppio sugli switch FC Cisco 9250i

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 pmtu-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 pmtu-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:

   Eseguire 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

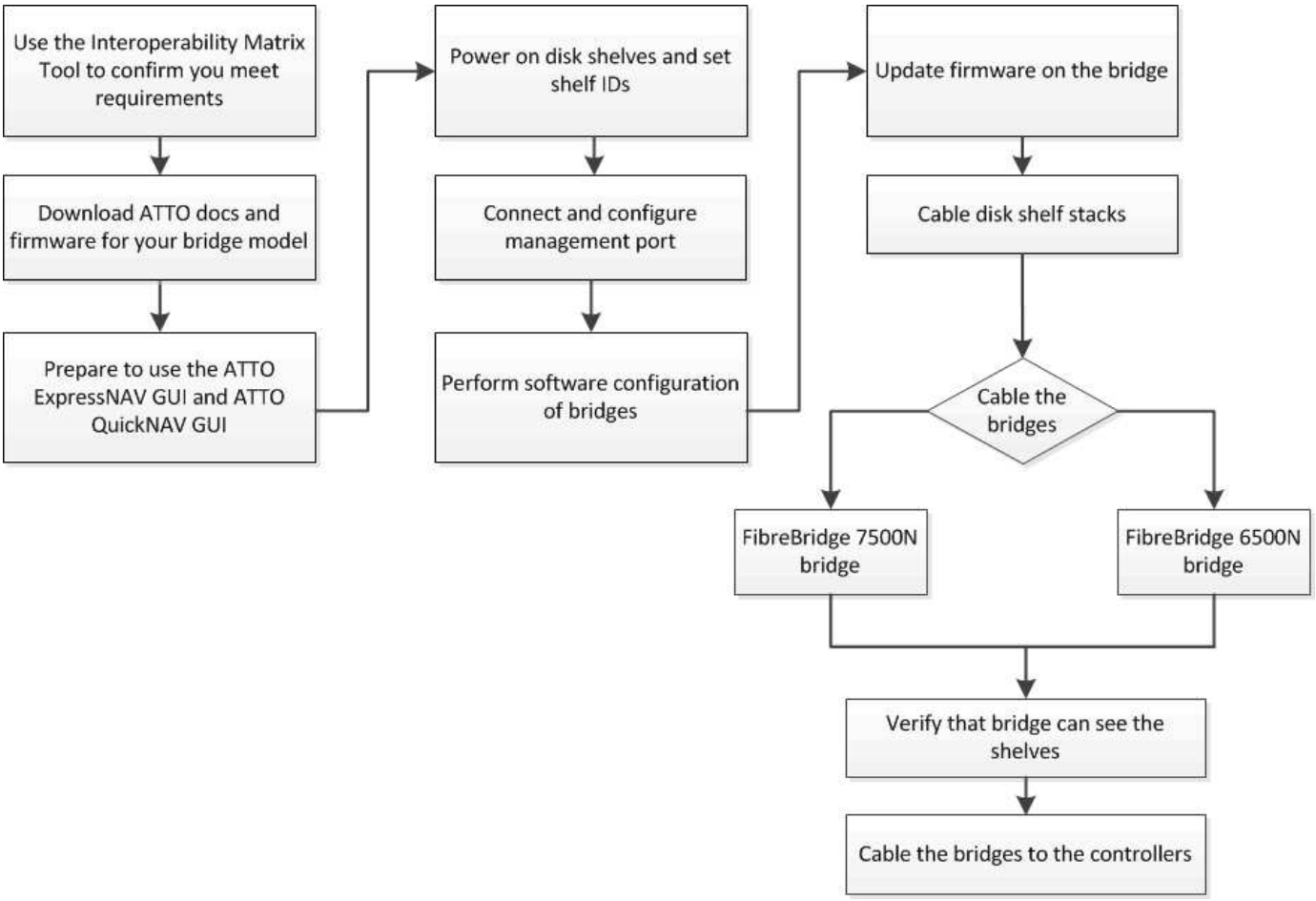
Per i sistemi ricevuti in fabbrica, i bridge FC-SAS sono preconfigurati e non richiedono alcuna configurazione aggiuntiva.

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

ONTAP 9.5 o versione successiva	a. Visualizzare lo stato dei bridge:
	`storage bridge show`
	L'output mostra quale bridge non è protetto.
	b. Fissare il bridge:
	`securebridge`

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.

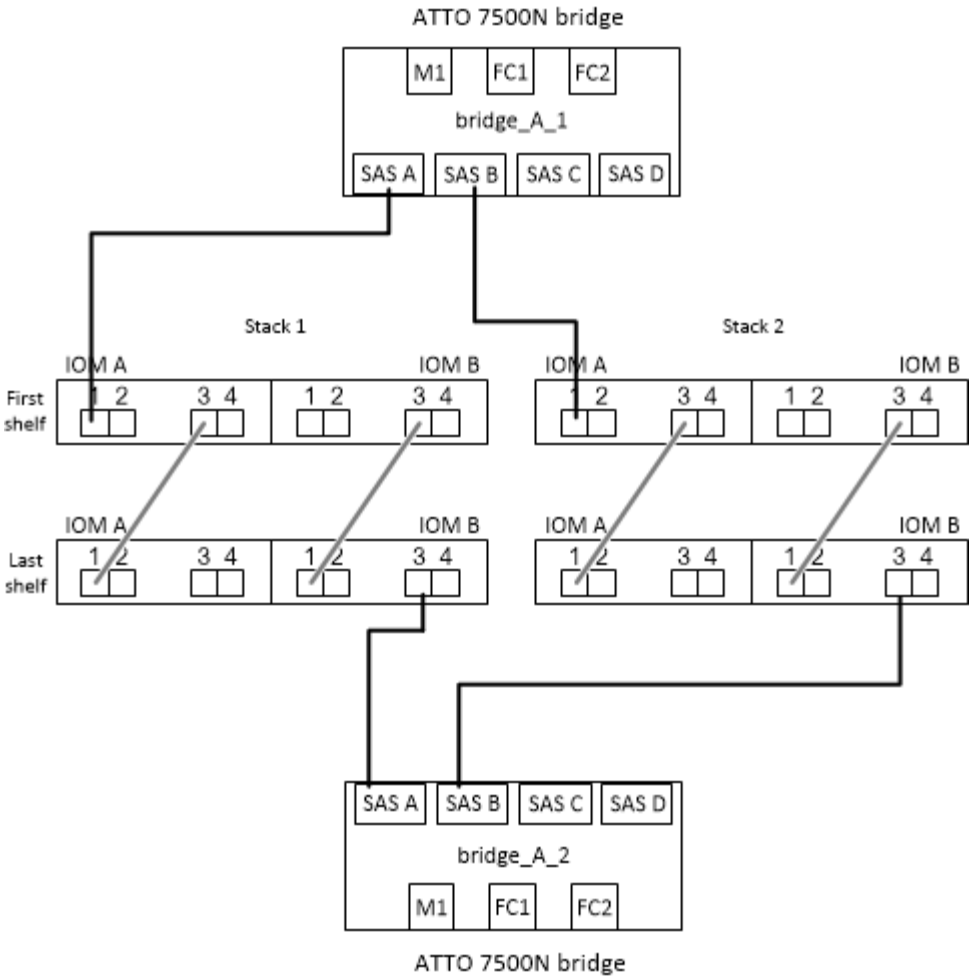
   a. Per il primo stack di shelf di dischi, collegare il cavo IOM A del primo shelf alla porta SAS A su FibreBridge A e il cavo IOM B dell'ultimo shelf alla porta SAS A su FibreBridge B.

   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.

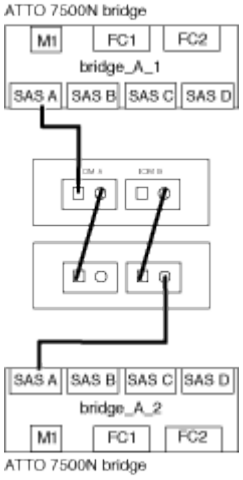
   a. Per il primo stack di shelf, collegare IOM A una porta quadrata del primo shelf alla porta SAS A su FibreBridge A.

   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.

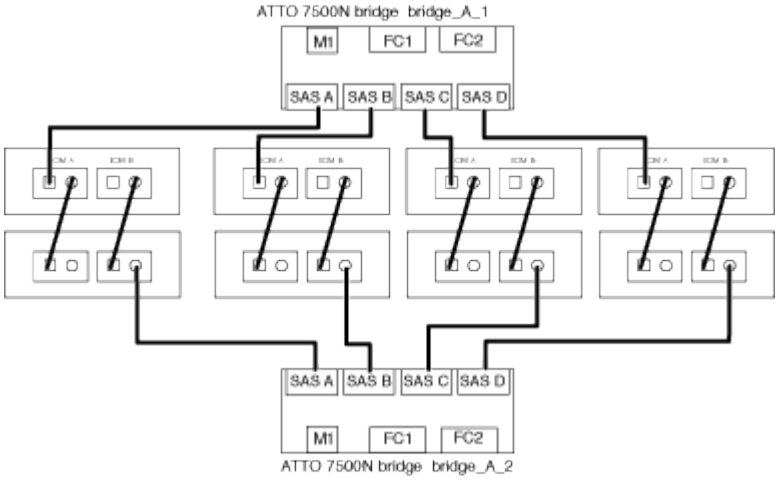
   "Guida all'installazione e al servizio degli shelf di dischi SAS per DS4243, DS2246, DS4486 e DS4246"

La figura seguente mostra un set di bridge collegati a una pila di shelf:



2. 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

1. 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	a. In un browser Web supportato, inserire l'indirizzo IP di un bridge nella casella del browser. Viene visualizzato il sito Web di ATTO FibreBridge del bridge per il quale è stato immesso l'indirizzo IP, che dispone di un collegamento. b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge. Viene visualizzata la pagina di stato di ATTO FibreBridge del bridge con un menu a sinistra. c. Fare clic su **Avanzate**. d. Visualizzare i dispositivi collegati utilizzando il comando sastargets, quindi fare clic su **Submit** (Invia).
Connessione alla porta seriale	Visualizzare i dispositivi connessi: `sastargets`

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        3QP1G7A900009939FNTT
  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.

2. 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 Fase 1 per ogni bridge rimanente.

Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo il cablaggio. Collegamento degli shelf di dischi ai bridge b. Ripetere Fase 1.

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 sprotegge 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       root, nosnap=on
                                mirrored
                                64-bit
```

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> 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] 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
   ```

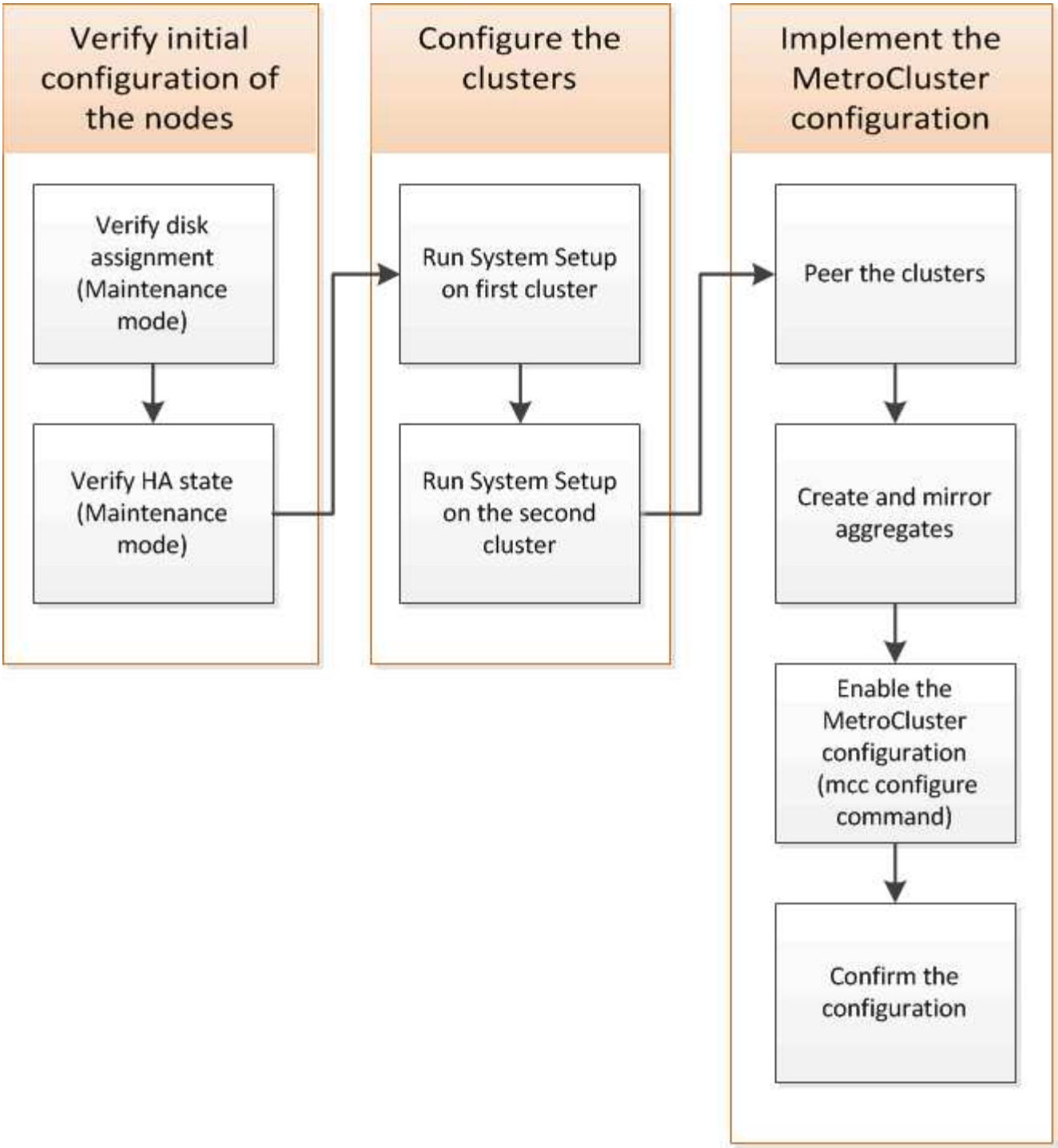
3. Eseguire l'utility fmc_DC per assicurarsi che 7-Mode Fabric MetroCluster funzioni correttamente.

   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				

Nodo 2 Non richiesto se si utilizza una configurazione MetroCluster a due nodi (un nodo per ogni sito). Esempio utilizzato in questa guida: Controller_A_2				

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				
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 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 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	

Sito A nbsp; 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 nbsp;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	`ucadmin modify -m fc -t initiator` *`adapter_name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter_name`*
Destinazione FC	`fcadmin config -t target` *`adapter_name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter_name`*

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	`ucadmin show`
FC	`fcadmin show`

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
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       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
         Current  Current    Pending  Pending    Admin
   Adapter  Mode     Type       Mode     Type       Status
   -------  -------  ---------  -------  ---------  -------
     ...
     1a     fc       initiator  -        fcvi       offline
     1b     fc       initiator  -        fcvi       offline
     1c     fc       initiator  -        -          online
     1d     fc       initiator  -        -          online
   ```

5. Spegnere 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-nameshelf-name -p pool`

      Se lo storage 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 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 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
                                                                  Speed
(Mbps)
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
                                  Failover
Vserver          Group            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          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

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
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Creazione di LIF intercluster sulla SVM di sistema:

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          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

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-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Se si specificano entrambi `-generate-passphrase` e. `-peer-addrs`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addrs` 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-addrs 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-addrs
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-addrs` *`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-addrs 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-addrs 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-addrs 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
             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
```

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	Dal prompt di qualsiasi nodo, configurare MetroCluster: `metrocluster configure node-name`

Un singolo aggregato di dati mirrorato	a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
	
	`set -privilege advanced`
	
	Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (*).
	
	b. Configurare MetroCluster con `-allow-with -one-aggregate true` parametro:
	
	`metrocluster configure -allow-with -one-aggregate true` *`node-name`*
	
	c. Tornare al livello di privilegio admin:
	
	`set -privilege admin`

> La Best practice consiste nell'avere più aggregati di dati. Se il primo gruppo DR dispone di un solo aggregato e si desidera aggiungere un gruppo DR con un aggregato, è necessario spostare il volume di metadati dal singolo aggregato di dati. Per ulteriori informazioni su questa procedura, vedere "Spostamento di un volume di metadati nelle configurazioni MetroCluster".

Il seguente comando abilita la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene controller_A_1:

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verificare lo stato della rete sul sito A:

```
network port show
```

L'esempio seguente mostra l'utilizzo della porta di rete in una configurazione MetroCluster a quattro nodi:

```
cluster_A::> network port show
                                                         Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    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
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    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    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    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.
```

- 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
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    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    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    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.
```

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
                              Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address  Port
Number
------------ --------------- ------- ------ -------- -----------
-----------
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: [00:00:00:00:00:00:00:00:00]
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_adddress> -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	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   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              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr2
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
```

```
controller_A_2        controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                      controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                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
                              Takeover
Node           Partner        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
                              Takeover
Node           Partner        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
                                Takeover
Node            Partner         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:

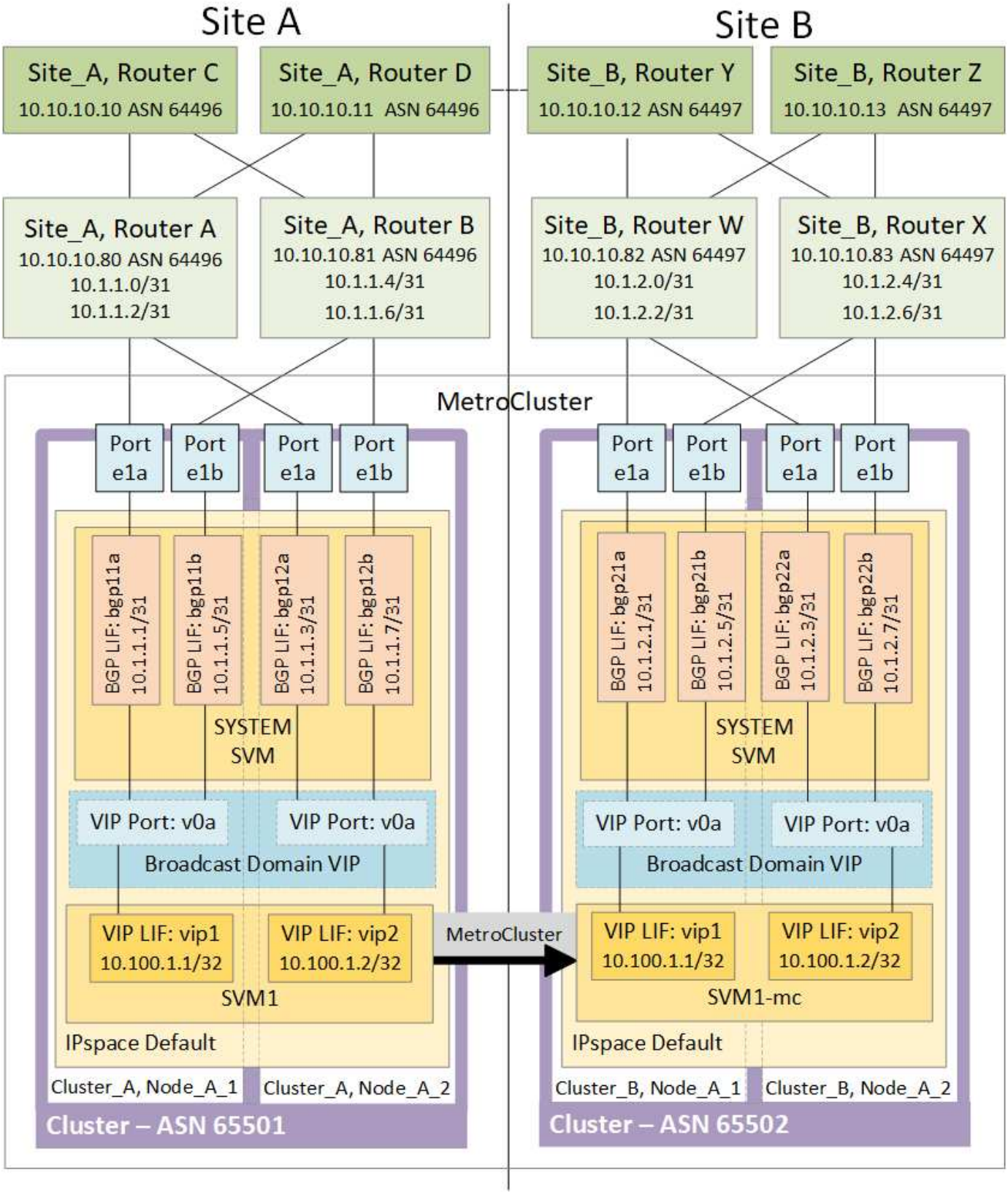
   ```
   system configuration backup settings modify URL-of-destination
   ```

   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 ridistribuzione del percorso sui router. Il BGP interno (IBGP) e l'utilizzo dei riflettori di percorso non sono impossibili, ma non rientrano nell'ambito di una semplice configurazione VIP.

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

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

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                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   heal roots
   completed
         cluster_B
                 node_B_2         unreachable    -         switched over
   42 entries were displayed.metrocluster operation show
   ```

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                              Configuration  DR
Group Cluster Node              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                              Configuration  DR
   Group Cluster Node              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. Spegnere gli alimentatori del bridge.
2. Verificare che il monitoraggio del bridge indichi un errore:

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                                  Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
   Status
   ---------- ------------- ------- --------- ---------------- ---------
   -------
   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. Spegnere le PDU sul lato sinistro del rack contenente i componenti MetroCluster.
2. Monitorare il risultato sulla console:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Riaccendere le PDU di sinistra.
4. Assicurarsi che ONTAP cancella la condizione di errore.
5. Ripetere i passaggi precedenti con le PDU di destra.

Verifica del funzionamento 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::> vserver show -type data

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       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. Spegnere 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::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       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
ISL							
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
Modulo MDS 2			
Componente	**Porta**	**Switch 1**	**Switch 2**

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

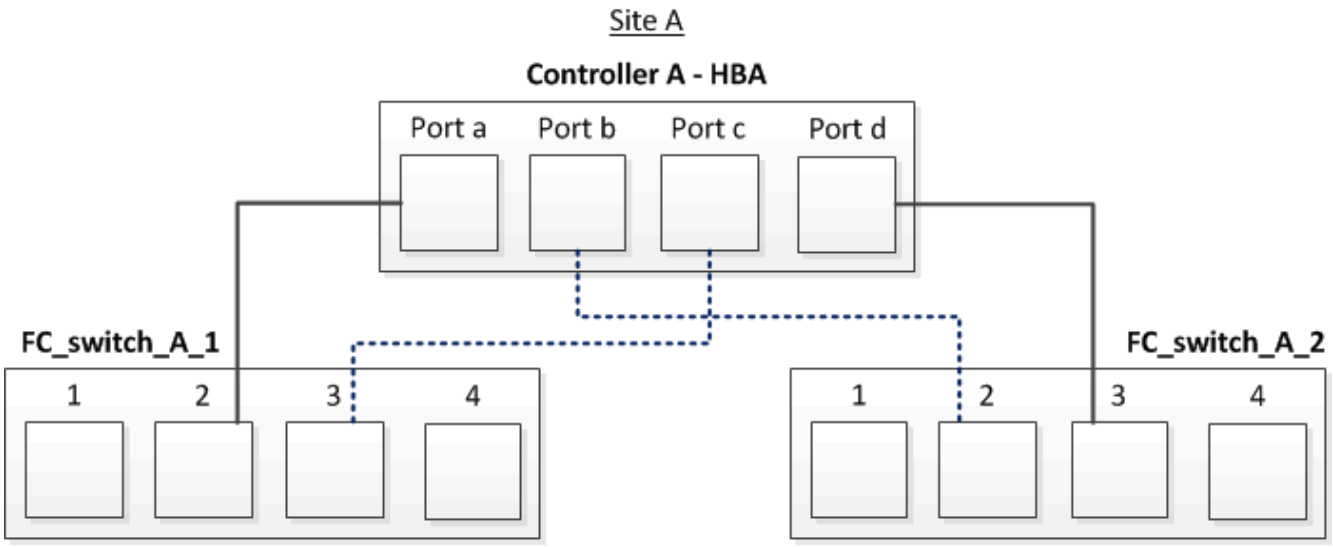
- È necessario ripetere questa attività per ciascun controller in entrambi i siti MetroCluster.
- Se si prevede di utilizzare dischi in aggiunta alle LUN degli array nella configurazione MetroCluster, è necessario utilizzare le porte HBA e le porte dello switch specificate per la configurazione con i 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
Coppia di porte	
Porta A.	FC_switch_A_1, porta 2
Porta d	FC_switch_A_2, porta 3
Coppia di porte	
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.

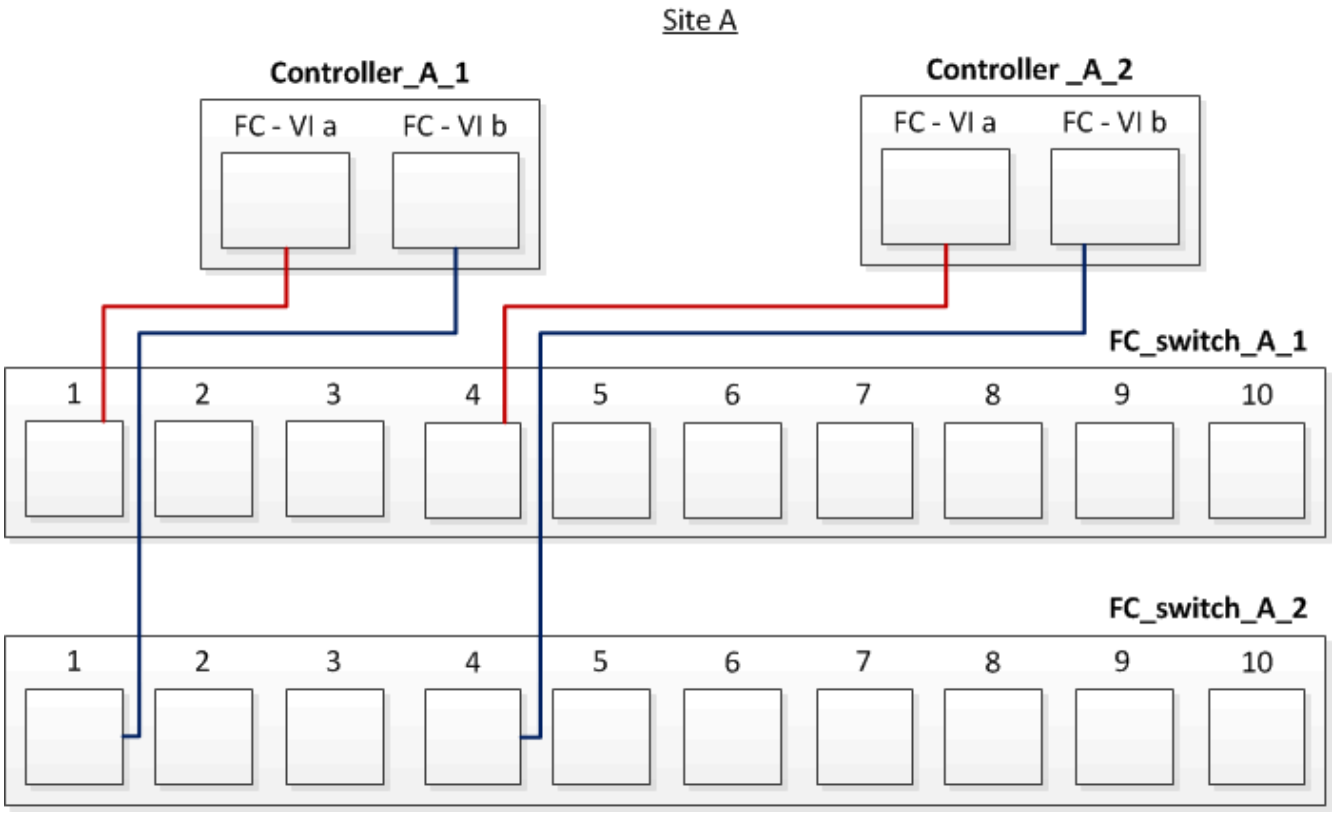
A proposito di questa attività

- 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.

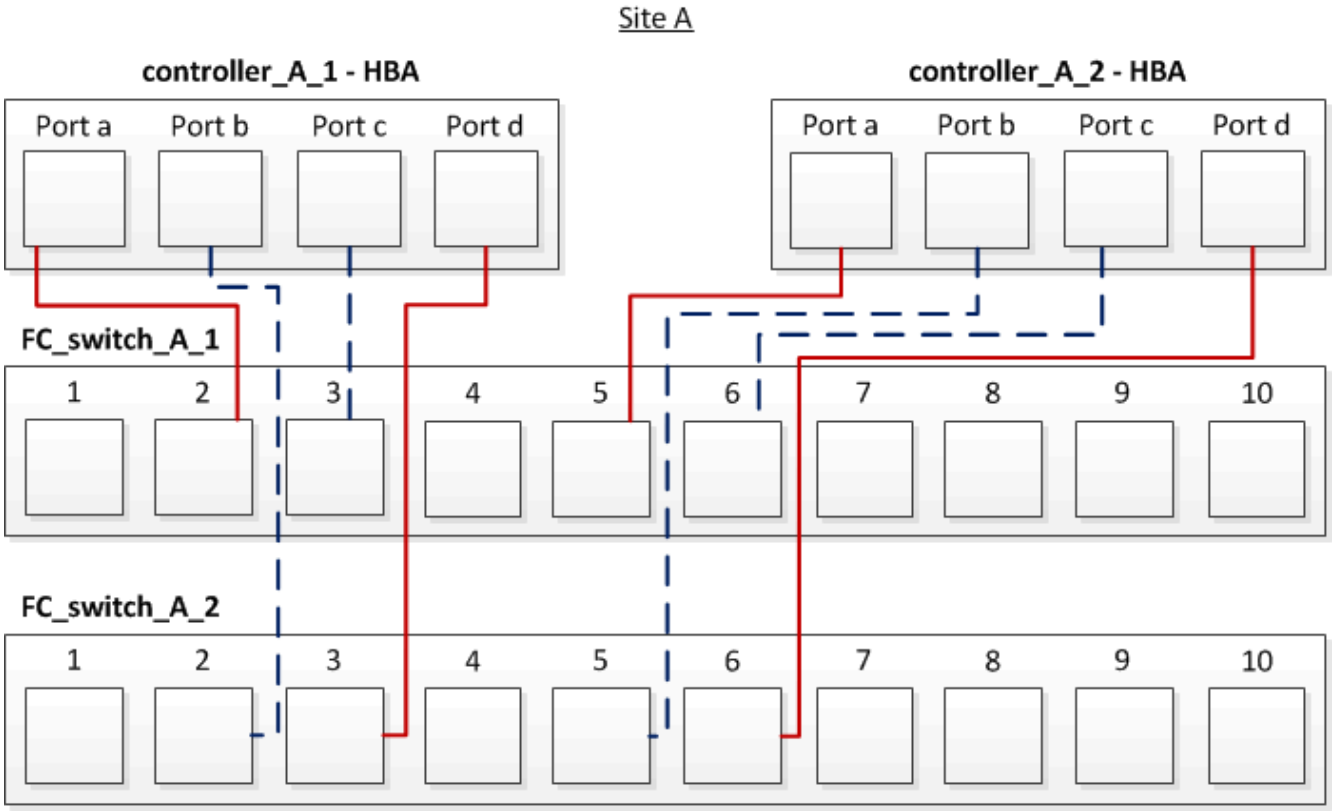
L'esempio seguente mostra le connessioni tra le porte FC-VI e le porte dello switch nel sito A:



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:



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
Coppia di porte	
Porta A.	FC_switch_A_1, porta 2
Porta d	FC_switch_A_2, porta 3
Coppia di porte	
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
Coppia di porte	
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 **Nota**: 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"

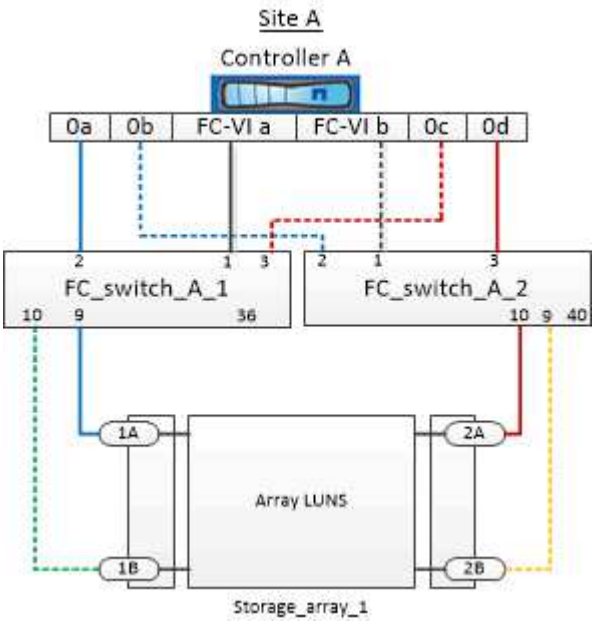
"Esempio di collegamento delle porte dello storage array agli switch FC in una configurazione MetroCluster a quattro nodi"

"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.

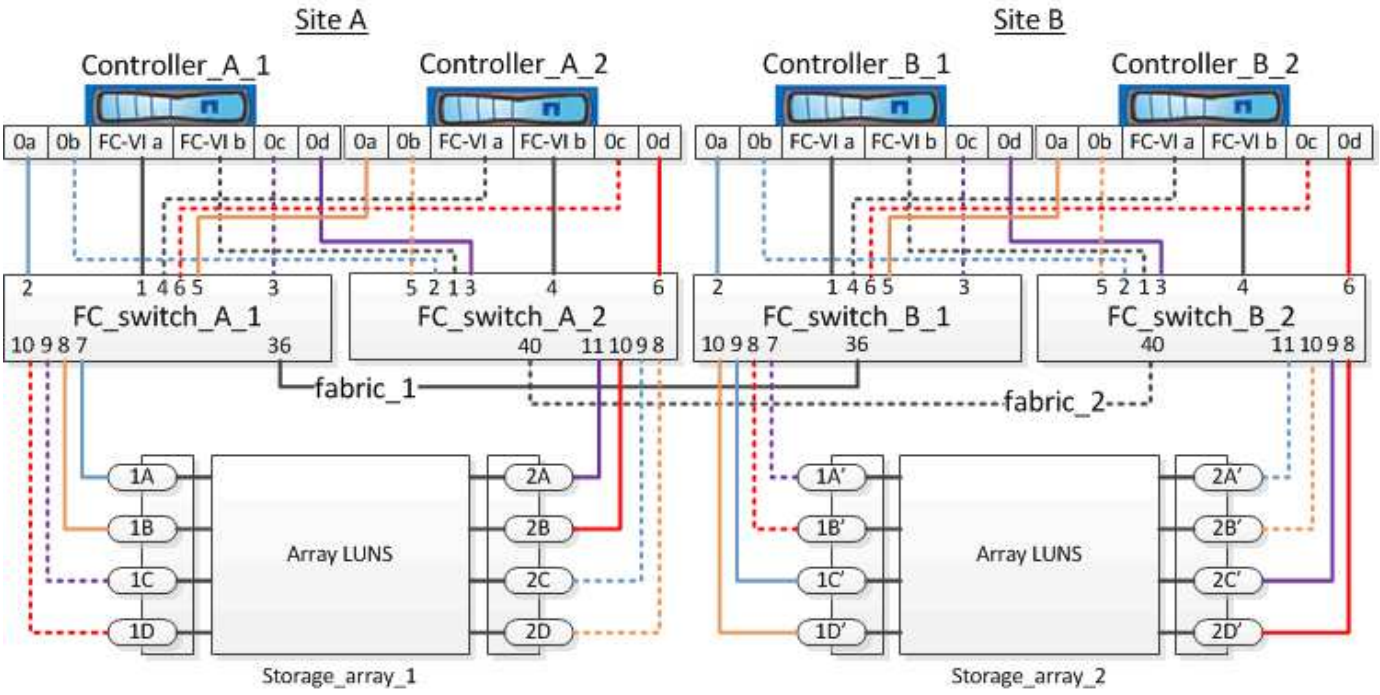
La seguente tabella elenca le connessioni tra le porte dello storage array e gli switch FC, come illustrato nell'esempio MetroCluster:

Porte LUN dell'array	Porte switch FC	Switch fabric
Sito A		
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
Sito 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
Sito A		

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
Sito 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"

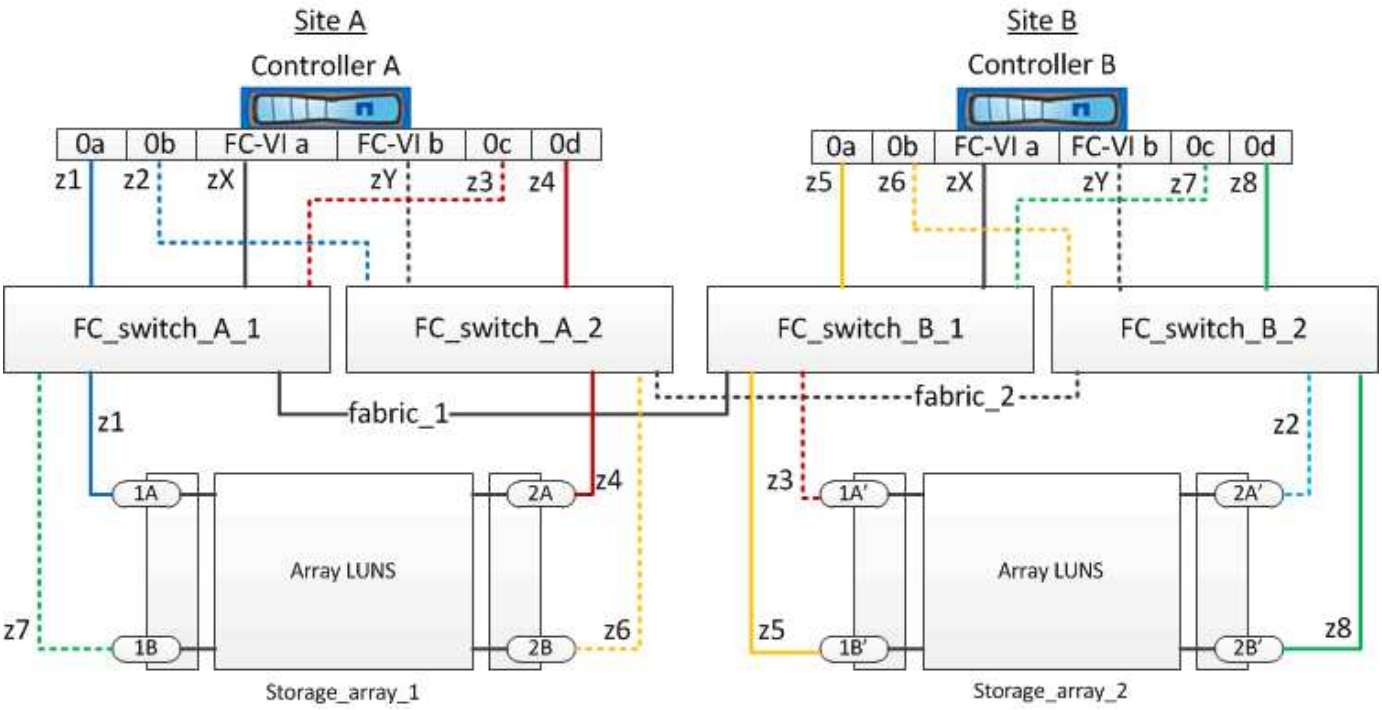
  "Esempio di zoning dello switch in una configurazione MetroCluster a quattro nodi con LUN array"

  "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
FC_switch_A_1		
z1	Controller A: Porta 0a	Porta 1A
z3	Controller A: Porta 0c	Porta 1A'
FC_switch_A_2		
z2	Controller A: Porta 0b	Porta 2A'
z4	Controller A: Porta 0d	Porta 2A
FC_switch_B_1		
z5	Controller B: Porta 0a	Porta 1B'
z7	Controller B: Porta 0c	Porta 1B
FC_switch_B_2		
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
Sito A		
ZX	Controller A: Porta FC-VI A.	Switch_FC_A_1
ZY	Controller A: Porta FC-VI b	Switch_FC_A_2
Sito 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"

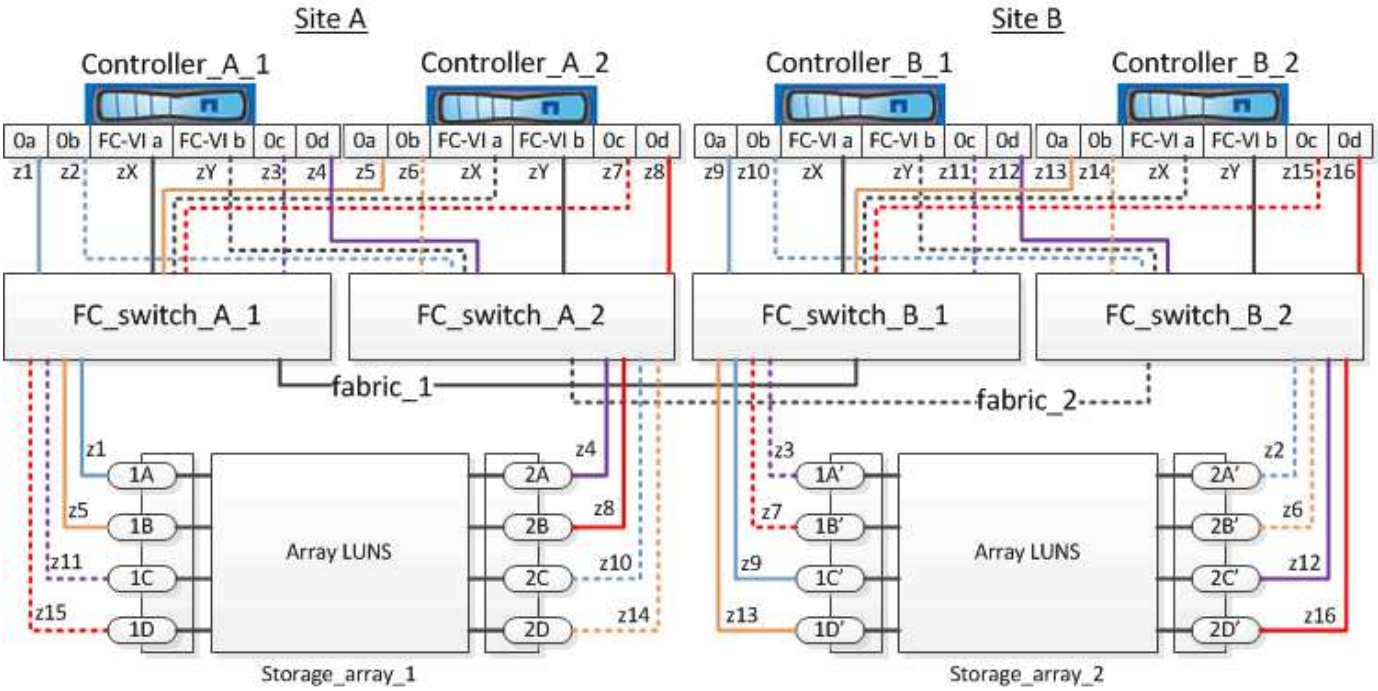
- Quando si utilizza lo zoning dello switch in una configurazione MetroCluster con LUN array, è necessario assicurarsi che vengano rispettati alcuni requisiti di base.

  "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	`ha-config modify chassis mcc`
Configurazione MetroCluster FC a due nodi	`ha-config modify chassis 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 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: 60080E50004317B4000003B158E35974
                   UID:
60080E50:004317B4:000003B1:58E35974:00000000:00000000:00000000:000000
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     60060480343631373431663 1
   1  switch0:5.183L3   SYMMETRIX   EMC     266.1 GB
Block     60060480343631633335383 7
   2  switch0:5.183L31  SYMMETRIX   EMC     266.1 GB
Block     60060480343631323764366 6
   3  switch0:5.183L33  SYMMETRIX   EMC     658.3 GB local  (root)
Block     60060480343631626361306 6
   4  switch0:7.183L0   SYMMETRIX   EMC     173.6 GB
Block     60060480343631326135623 5
   5  switch0:7.183L2   SYMMETRIX   EMC     173.6 GB
Block     60060480343631343839643 1
   6  switch0:7.183L4   SYMMETRIX   EMC     658.3 GB
Block     60060480343631316166303 1
   7  switch0:7.183L30  SYMMETRIX   EMC     173.6 GB
Block     60060480343631653885383 4
   8  switch0:7.183L32  SYMMETRIX   EMC     266.1 GB
Block     60060480343631323735373 8
   9  switch0:7.183L34  SYMMETRIX   EMC     658.3 GB
Block     60060480343631373733366 2
```

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     60060480343631323764366 6
   3  switch0:5.183L33   SYMMETRIX  EMC     658.3 GB  local   (root)
Block     60060480343631626361306 6
   4  switch0:7.183L0    SYMMETRIX  EMC     173.6 GB  local
Block     60060480343631326135623 5
   5  switch0:7.183L2    SYMMETRIX  EMC     173.6 GB  local
Block     60060480343631343839643 1
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 ilhttps://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: llllllll
   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: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
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       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
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Spegnere 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	• Se si sta configurando un'implementazione di *new* MetroCluster con dischi e LUN di array, è necessario creare l'aggregato root sui dischi nativi. Durante questa operazione, assicurarsi che *almeno un* shelf di dischi (con 24 dischi) sia configurato in ciascuno dei siti. • Se si aggiungono dischi nativi a una configurazione MetroCluster *esistente* che utilizza LUN di array, l'aggregato root può rimanere su un LUN di array.
Utilizzo di switch e bridge FC-SAS	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. È necessario utilizzare gli stessi switch per connettersi agli array di storage e ai bridge FC-SAS.
Utilizzando le porte FC Initiator	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. Per collegare un sistema ONTAP a dischi e LUN di array sono necessarie almeno otto porte di iniziatore.

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"

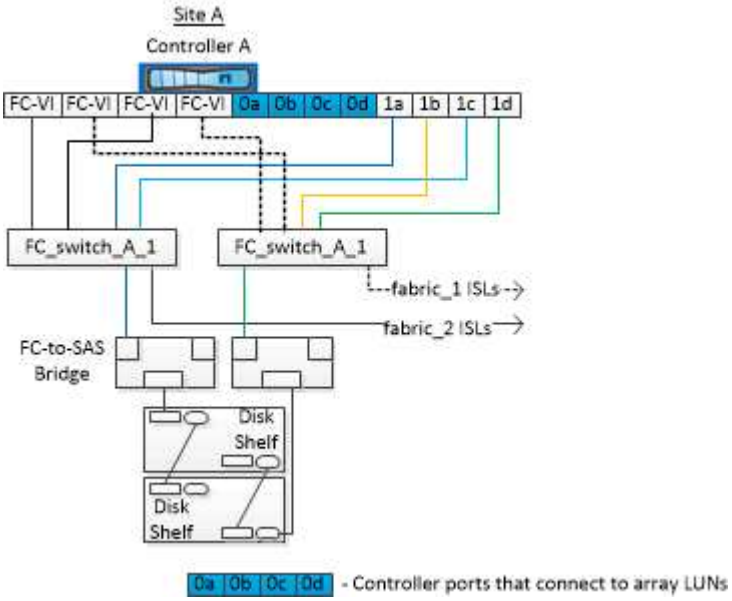
- "NetApp Hardware Universe"

Esempio di una configurazione MetroCluster a due nodi collegata al fabric con dischi e LUN di array

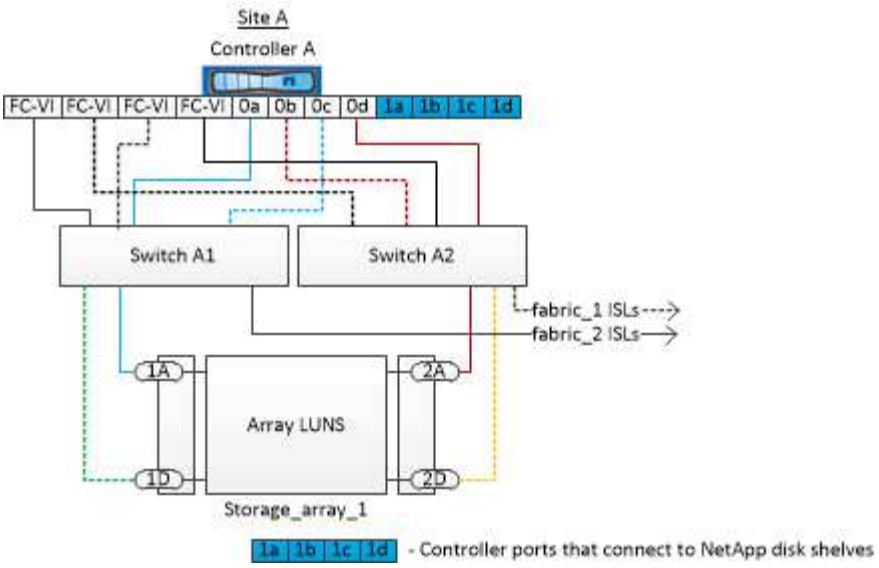
Per configurare una configurazione MetroCluster a due nodi con fabric-attached con dischi e LUN di array nativi, è necessario utilizzare bridge FC-SAS per collegare i sistemi ONTAP con gli shelf di dischi attraverso gli switch FC. È possibile collegare i LUN degli array ai sistemi ONTAP attraverso gli 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:



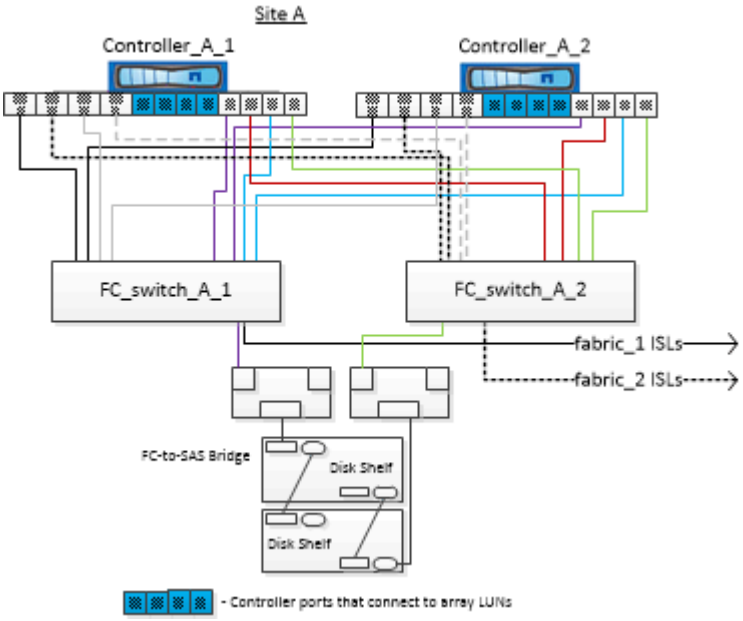
Esempio di configurazione MetroCluster a quattro nodi con dischi e LUN di array

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.

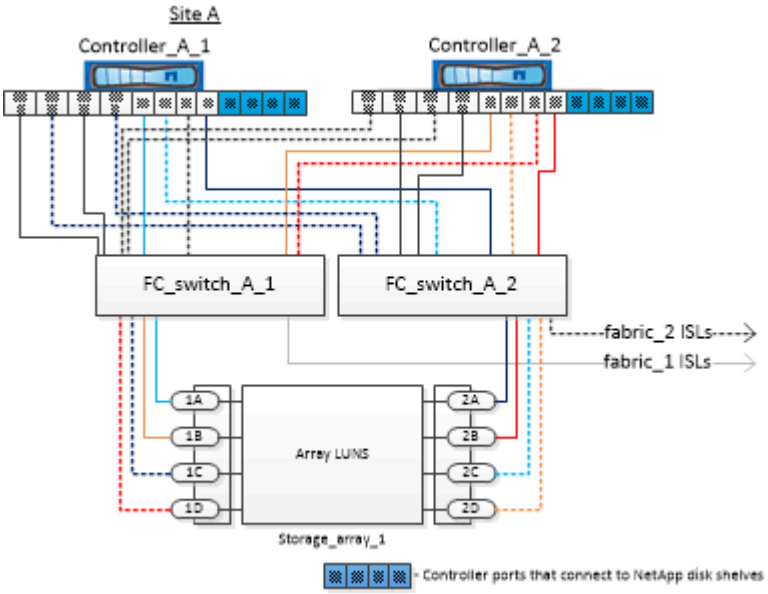
Le figure seguenti rappresentano esempi di configurazione MetroCluster con dischi e LUN di array. Entrambi rappresentano la stessa configurazione MetroCluster; le rappresentazioni per i dischi e le LUN degli array sono separate solo per semplificazioni.

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	ONTAP identifica le porte di destinazione FC collegate sul cluster DR.	Le porte del cluster DR che si trovano nello stesso IPSpace del LIF di origine vengono selezionate per un controllo di raggiungibilità. Se non sono presenti porte nel cluster DR nello stesso IPSpace, non è possibile posizionare la LIF. Tutte le porte del cluster di DR che ospitano già una LIF nello stesso IPSpace e nella stessa subnet vengono automaticamente contrassegnate come raggiungibili e possono essere utilizzate per il posizionamento. Queste porte non sono incluse nel controllo di raggiungibilità.
Controllo della raggiungibilità	La raggiungibilità viene determinata verificando la connettività del WWN del fabric di origine sulle porte del cluster DR. Se lo stesso fabric non è presente nel sito di DR, il LIF viene posizionato su una porta casuale del partner di DR.	La raggiungibilità è determinata dalla risposta a una trasmissione ARP (Address Resolution Protocol) da ciascuna porta precedentemente identificata sul cluster DR all'indirizzo IP di origine della LIF da posizionare. Per il successo dei controlli di raggiungibilità, le trasmissioni ARP devono essere consentite tra i due cluster. Ogni porta che riceve una risposta dalla LIF di origine verrà contrassegnata come possibile per il posizionamento.

Selezione della porta	ONTAP classifica le porte in base ad attributi quali tipo di adattatore e velocità, quindi seleziona le porte con attributi corrispondenti. Se non vengono trovate porte con attributi corrispondenti, la LIF viene posizionata su una porta connessa in modo casuale del partner DR.	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. 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. 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. ONTAP classifica le porte in base ad attributi quali tipo di adattatore, tipo di interfaccia e velocità, quindi seleziona le porte con attributi corrispondenti.
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

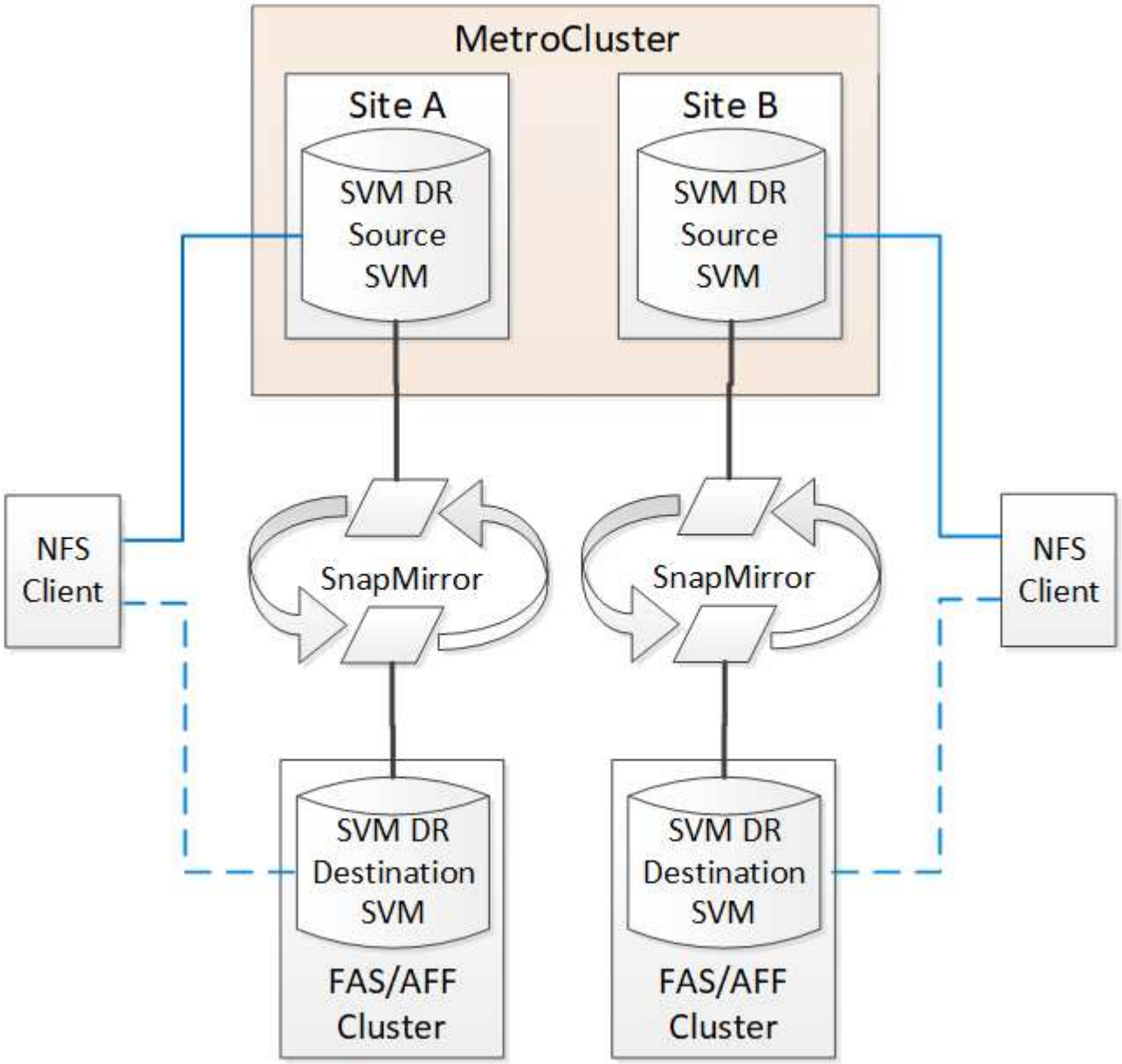
Il sistema non consente la creazione di nuovi volumi nell'aggregato root (un aggregato con un criterio ha di CFO) di un nodo in una configurazione MetroCluster.

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.



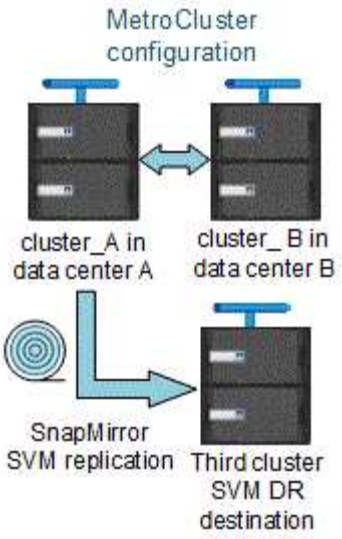
È necessario conoscere i seguenti requisiti e limitazioni dell'utilizzo di SVM con il disaster recovery SnapMirror:

- 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.

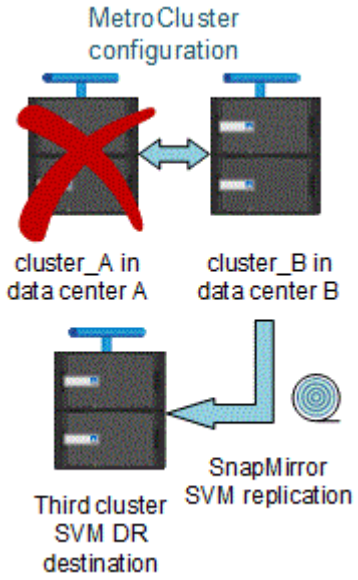
- Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.

  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.

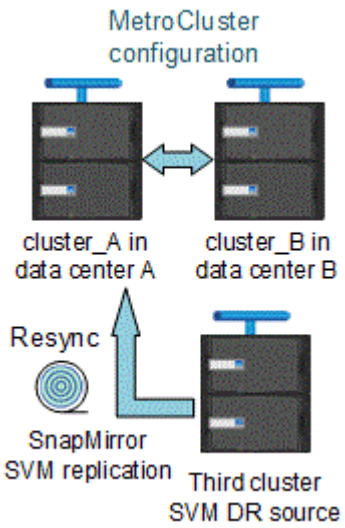
  Tuttavia, una volta completato il processo di switchover o switchback, gli aggiornamenti pianificati per il DR SVM successivi avranno esito positivo.

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
"Documentazione di ONTAP 9"	• Tutte le informazioni MetroCluster
"Architettura e progettazione della soluzione NetApp MetroCluster, TR-4705"	• Panoramica tecnica della configurazione e del funzionamento del MetroCluster FC. • Best practice per la configurazione MetroCluster FC.
"Architettura e progettazione della soluzione IP MetroCluster, TR-4689"	• Panoramica tecnica della configurazione e del funzionamento dell'IP MetroCluster. • Best practice per la configurazione IP di MetroCluster.
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Installazione e configurazione di MetroCluster IP: Differenze tra le configurazioni di ONTAP MetroCluster"	• Architettura IP di MetroCluster • Cablaggio della configurazione • Configurazione di MetroCluster in ONTAP
"Gestione MetroCluster e disaster recovery"	• Informazioni sulla configurazione di MetroCluster • Switchover, healing e switchback • Disaster recovery

"Gestire i componenti di MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster FC • Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch • Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch • Sostituzione dell'hardware in un sito di emergenza in una configurazione FC MetroCluster Fabric-Attached o Stretch • Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.
"Transizione da MetroCluster FC a MetroCluster IP" "Guida all'upgrade e all'espansione di MetroCluster"	• Aggiornamento o aggiornamento di una configurazione MetroCluster • Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP • Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi
"Installazione e configurazione del software MetroCluster Tiebreaker"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
Documentazione di Active IQ Digital Advisor "Documentazione NetApp: Guide e risorse sui prodotti"	• Monitoraggio della configurazione e delle prestazioni di MetroCluster
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster
"Concetti di ONTAP"	• Come funzionano gli aggregati mirrorati

Installare una configurazione IP MetroCluster

Panoramica

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

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

Prepararsi per l'installazione di MetroCluster

Differenze tra le configurazioni ONTAP MetroCluster

Le varie configurazioni MetroCluster presentano differenze chiave nei componenti richiesti.

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

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

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

Importante

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

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

Supporto per tutti i sistemi array SAN nelle configurazioni MetroCluster

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

Le configurazioni di piattaforma supportate sono elencate nella "NetApp Hardware Universe".

Differenze tra ONTAP Mediator e MetroCluster Tiebreaker

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

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

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

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

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

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

  "Scoprite in che modo ONTAP Mediator supporta lo switchover non pianificato automatico".

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

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

  Prima di utilizzare il software Tiebreaker, consultare "Installazione e configurazione del software MetroCluster Tiebreaker"

Interoperabilità di ONTAP Mediator con altre applicazioni e appliance

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

Considerazioni per le configurazioni MetroCluster IP

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

Accesso allo storage remoto nelle configurazioni MetroCluster IP

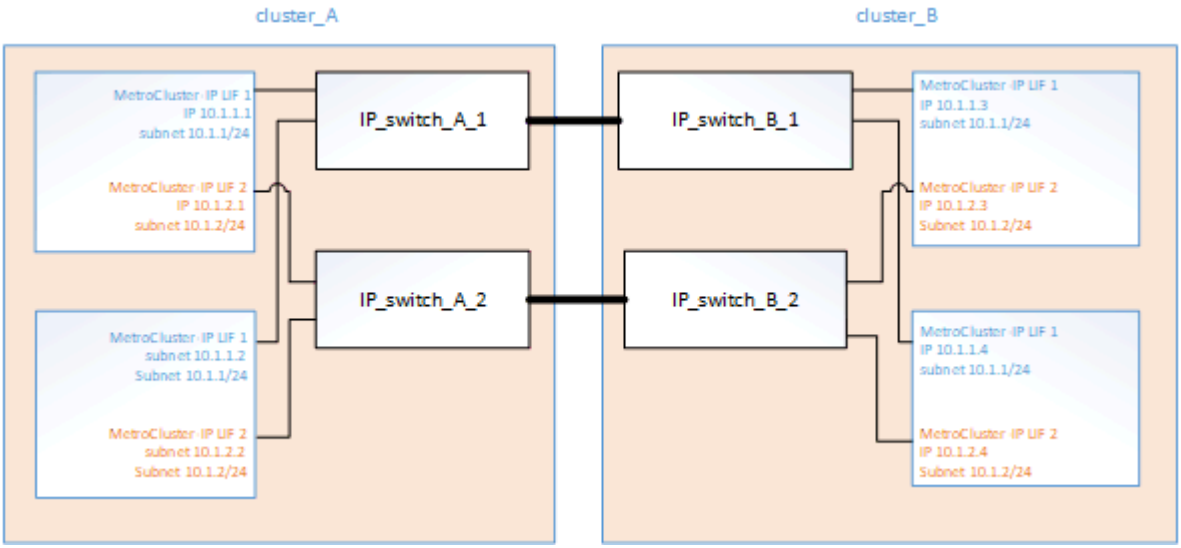
Nelle configurazioni MetroCluster IP, l'unico modo in cui i controller locali possono raggiungere i pool di storage remoti è tramite i controller remoti. Gli switch IP sono collegati alle porte Ethernet dei controller e non dispongono di connessioni dirette agli shelf di dischi. Se il controller remoto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

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

Indirizzi IP MetroCluster

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

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



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

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

- Devono rientrare in un intervallo IP univoco.

  Non devono sovrapporsi a nessuno spazio IP nell'ambiente.

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

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

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

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

Caratteristiche delle interfacce IP MetroCluster

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

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

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

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

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

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

A partire da ONTAP 9,4, le configurazioni IP di MetroCluster supportano nuove installazioni con ADP (partizione avanzata dei dischi).

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

- Per utilizzare ADP con le configurazioni IP di MetroCluster, è necessario ONTAP 9,4 e versioni successive.
- ADPv2 è supportato nelle configurazioni IP di MetroCluster.

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

  Esempio di configurazione supportata:

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

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

Partizione automatica

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

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

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

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

> Se si utilizzano unità interne ed esterne, è necessario innanzitutto inizializzare MetroCluster con le sole unità interne che utilizzano ADP. Dopo aver completato l'installazione o l'installazione, collegare manualmente lo shelf esterno.
>
> Devi assicurarti che gli shelf interni dispongano del numero minimo di dischi consigliato, come descritto in Differenze tra ADP e assegnazione del disco per sistema.
>
> Per i dischi interni ed esterni, è necessario popolare gli shelf parzialmente pieni, come descritto in Come popolare gli shelf parzialmente completi.

Come funziona l'assegnazione automatica shelf-by-shelf

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

- Tutti i dischi sul sito_A-shelf_1 vengono assegnati automaticamente al pool 0 del nodo_A_1
- Tutti i dischi sul sito_A-shelf_3 vengono assegnati automaticamente al pool 0 del nodo_A_2
- Tutti i dischi sul sito_B-shelf_1 vengono assegnati automaticamente al pool 0 del nodo_B_1
- Tutti i dischi sul sito_B-shelf_3 vengono assegnati automaticamente al pool 0 del nodo_B_2
- Tutti i dischi sul sito_B-shelf_2 vengono assegnati automaticamente al pool 1 del nodo_A_1
- Tutti i dischi sul sito_B-shelf_4 vengono assegnati automaticamente al pool 1 del nodo_A_2
- Tutti i dischi sul sito_A-shelf_2 vengono assegnati automaticamente al pool 1 del nodo_B_1
- Tutti i dischi sul sito_A-shelf_4 vengono assegnati automaticamente al pool 1 del nodo_B_2

Come popolare gli shelf parzialmente completi

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

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

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

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

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

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

Trimestre 4: Baie 18-23	Vani 18-21

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

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

Assegnazione manuale del disco (ONTAP 9.5)

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

- Tre shelf esterni per sito.

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

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

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

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

Assegnazione manuale del disco (ONTAP 9.4)

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

- Meno di quattro shelf esterni per sito.

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

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

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

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

- Assegnare metà dei dischi sul sito_A-shelf_1 al pool 0 del nodo_A_1.
- Assegnare metà dei dischi sul sito_A-shelf_1 al pool 0 del nodo_A_2.
- Assegnare metà dei dischi sul sito_A-shelf_2 al pool 1 del nodo_B_1.
- Assegnare metà dei dischi sul sito_A-shelf_2 al pool 1 del nodo_B_2.

- Assegnare metà dei dischi sul sito_B-shelf_1 al pool 0 del nodo_B_1.
- Assegnare metà dei dischi sul sito_B-shelf_1 al pool 0 del nodo_B_2.
- Assegnare metà dei dischi sul sito_B-shelf_2 al pool 1 del nodo_A_1.
- Assegnare metà dei dischi sul sito_B-shelf_2 al pool 1 del nodo_A_2.

Aggiunta di shelf a una configurazione esistente

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

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

Informazioni correlate

"Componenti IP MetroCluster richiesti e convenzioni di denominazione"

"Gestione di dischi e aggregati"

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

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

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

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

"NetApp Hardware Universe"

Assegnazione di ADP e dischi sui sistemi AFF A320

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

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota. **Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni** • Otto partizioni per i dati • Due partizioni di parità • Due partizioni di riserva
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

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

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

Numero minimo di dischi consigliati (per sito)	Solo dischi interni	I dischi interni sono divisi in quattro gruppi uguali. Ciascun gruppo viene assegnato automaticamente a un pool separato e ciascun pool viene assegnato a un controller separato nella configurazione. Metà delle unità interne rimane non assegnata prima della configurazione di MetroCluster.	Due quarti sono utilizzati dalla coppia ha locale. Gli altri due quarti vengono utilizzati dalla coppia ha remota. L'aggregato root include le seguenti partizioni in ogni plex: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

Numero minimo di dischi supportati (per sito)	16 dischi interni	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato. Due quarti su uno shelf possono avere lo stesso pool. Il pool viene scelto in base al nodo proprietario del trimestre: • Se di proprietà del nodo locale, viene utilizzato pool0. • Se di proprietà del nodo remoto, viene utilizzato pool1. Ad esempio: Uno shelf con trimestri da Q1 a Q4 può avere le seguenti assegnazioni: • Q1: Pool Node_A_1 0 • Q2: Pool Node_A_2 0 • D3: Pool Node_B_1 • D4:pool Node_B_2 1 ⓘ Metà delle unità interne rimane non assegnata prima della configurazione di MetroCluster.	Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni: • Due partizioni per i dati • Due partizioni di parità • Nessun ricambio

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

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

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota. Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. L'aggregato root include le seguenti partizioni in ogni plex: • Otto partizioni per i dati • Due partizioni di parità • Due partizioni di riserva
Numero minimo di dischi supportati (per sito)	16 dischi interni	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni: • Due partizioni per i dati • Due partizioni di parità • Nessuna partizione di riserva

Assegnazione di ADP e dischi sui sistemi AFF A300

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

Numero minimo di dischi consigliati (per sito)	48 dischi	I dischi su ogni shelf esterno sono divisi in due gruppi uguali (metà). Ogni half-shelf viene assegnato automaticamente a un pool separato.	Una shelf viene utilizzata dalla coppia ha locale. Il secondo shelf viene utilizzato dalla coppia ha remota. Le partizioni su ogni shelf vengono utilizzate per creare l'aggregato root. L'aggregato root include le seguenti partizioni in ogni plex: • Otto partizioni per i dati • Due partizioni di parità • Due partizioni di riserva
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali. Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include le seguenti partizioni: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

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

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Ciascuno dei due plessi nell'aggregato root include: • 20 partizioni per i dati • Due partizioni di parità • Due partizioni di riserva

Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

Assegnazione di ADP e dischi sui sistemi AFF A700

Linee guida	Dischi per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Ciascuno dei due plessi nell'aggregato root include: • 20 partizioni per i dati • Due partizioni di parità • Due partizioni di riserva
Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

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

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

Numero minimo di dischi consigliati (per sito)	Dischi interni e 96 dischi esterni	Le partizioni interne sono divise in quattro gruppi uguali (quarti). Ogni trimestre viene assegnato automaticamente a un pool separato. I dischi sugli shelf esterni vengono assegnati automaticamente shelf-by-shelf, con tutti i dischi su ogni shelf assegnati a uno dei quattro nodi nella configurazione MetroCluster.	L'aggregato root viene creato con 12 partizioni root sullo shelf interno. Ciascuno dei due plessi nell'aggregato root include: • Otto partizioni per i dati • Due partizioni di parità • Due partizioni di riserva
Numero minimo di dischi supportati (per sito)	24 dischi interni	Le partizioni interne sono divise in quattro gruppi uguali (quarti). Ogni trimestre viene assegnato automaticamente a un pool separato.	L'aggregato root viene creato con 12 partizioni root sullo shelf interno. Ciascuno dei due plessi nell'aggregato root include: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

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

Linee guida	Shelf per sito	Regole di assegnazione dei dischi	Layout ADP per la partizione root
Numero minimo di dischi consigliati (per sito)	96 dischi	I dischi vengono assegnati automaticamente shelf-by-shelf.	Ciascuno dei due plessi nell'aggregato root include: • 20 partizioni per i dati • Due partizioni di parità • Due partizioni di riserva

Numero minimo di dischi supportati (per sito)	24 dischi	I dischi sono divisi in quattro gruppi uguali (quarti). Ogni quarter-shelf viene assegnato automaticamente a un pool separato.	Ciascuno dei due plessi nell'aggregato root include: • Tre partizioni per i dati • Due partizioni di parità • Una partizione di riserva

Assegnazione dei dischi sui sistemi FAS2750

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

Assegnazione dei dischi sui sistemi FAS8200

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

Assegnazione dei dischi sui sistemi FAS500f

Le stesse linee guida e regole per l'assegnazione dei dischi per i sistemi AFF C250 e AFF A250 si applicano ai sistemi FAS500f. Per l'assegnazione dei dischi nei sistemi FAS500f, fare riferimento alla [ADP_FAS500f] tabella.

Assegnazione dei dischi sui sistemi FAS9000

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

Assegnazione dei dischi sui sistemi FAS9500

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

Peering dei cluster

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

Informazioni correlate

"Configurazione rapida del peering di cluster e SVM"

Prerequisiti per il peering del cluster

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

Requisiti di connettività

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

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

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

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

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

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

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

Requisiti delle porte

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

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

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

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

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

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

Requisiti del firewall

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

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

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

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

Considerazioni sull'utilizzo di porte dedicate

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

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

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

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

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

Considerazioni sulla condivisione delle porte dati

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

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

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

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

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

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

Requisiti ISL

Panoramica dei requisiti ISL

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

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

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

Switch NetApp validati e conformi a MetroCluster

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

Switch validati da NetApp

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

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

dischi NS224

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

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

Switch compatibili con MetroCluster

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

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

Considerazioni per gli ISL

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

Requisiti generali dell'ISL MetroCluster

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

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

Limiti di latenza e perdita di pacchetti negli ISL

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

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

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

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

Considerazioni sul ricetrasmettitore e sul cavo

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

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

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

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

Utilizzando dispositivi di crittografia xWDM, TDM e esterni

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

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

Numero di ISL e cavi di breakout supportati

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

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

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

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

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

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

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

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

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

implementare MetroCluster.

A partire da ONTAP 9,6, le configurazioni IP MetroCluster con switch Cisco supportati possono condividere le reti esistenti per i collegamenti interswitch (ISL) invece di utilizzare ISL MetroCluster dedicati. Questa topologia è nota come *reti Layer 2 condivise*.

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

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

Requisiti ISL per le reti Layer 2 e Layer 3

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

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

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

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

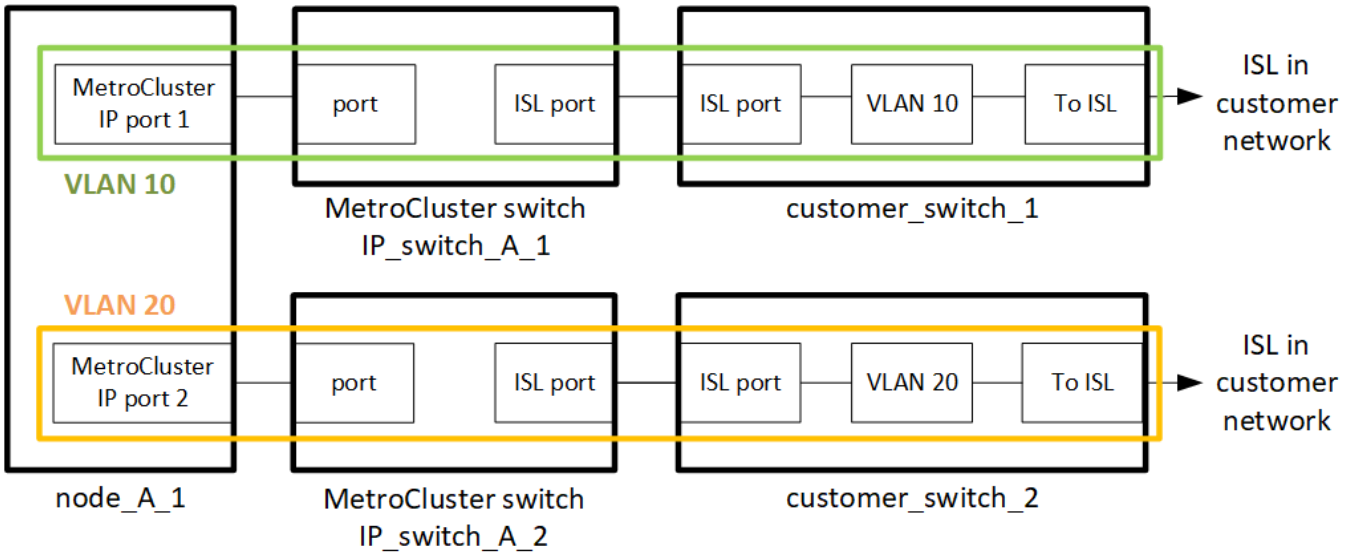
  I servizi di condivisione dei collegamenti, ad esempio i collegamenti MPLS (MultiProtocol Label Switching), non sono supportati.

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

- La VLAN predefinita dello switch non è consentita

Considerazioni per le reti di livello 2

Gli switch backend MetroCluster sono collegati alla rete del cliente.



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

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

Configurazione VLAN in ONTAP

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

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

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

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

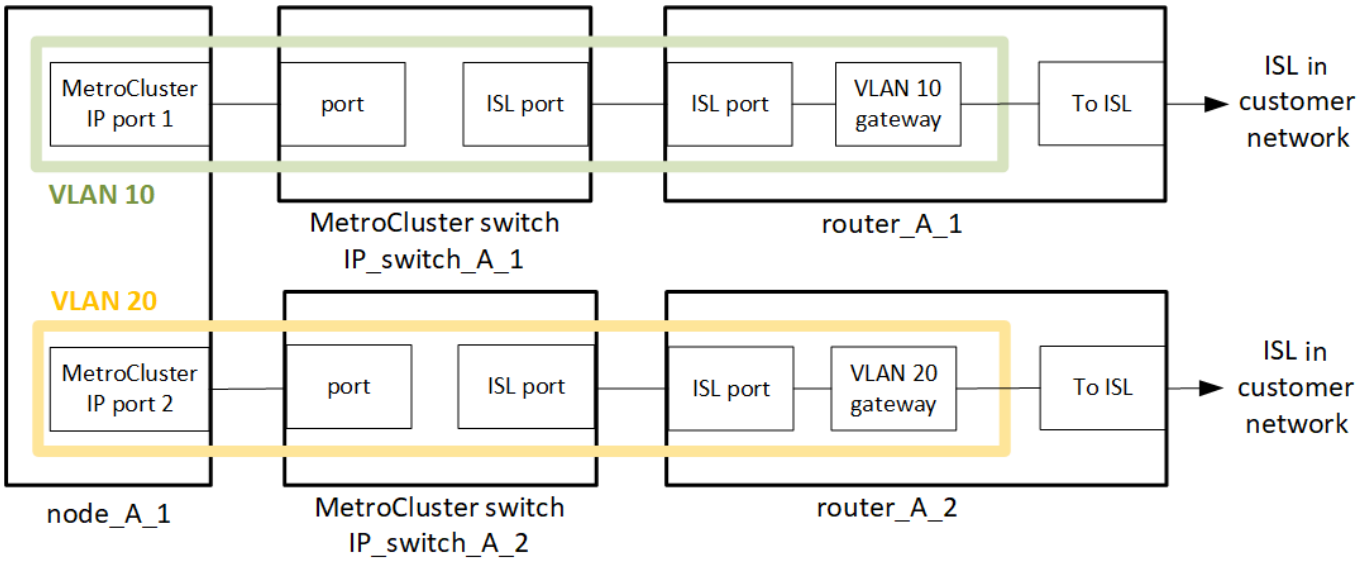
> I sistemi sopra elencati potrebbero essere configurati utilizzando VLAN 100 e versioni successive. Tuttavia, alcune VLAN in questo intervallo potrebbero essere riservate ad altri o ad uso futuro.

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

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

Considerazioni per le reti di livello 3

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



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

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

- Aggiornamento di una configurazione MetroCluster a quattro nodi
- Transizione da MetroCluster FC a MetroCluster IP

- Su ciascun sito MetroCluster sono necessarie due subnet, una per ogni rete.
- L'assegnazione Auto-IP non è supportata.

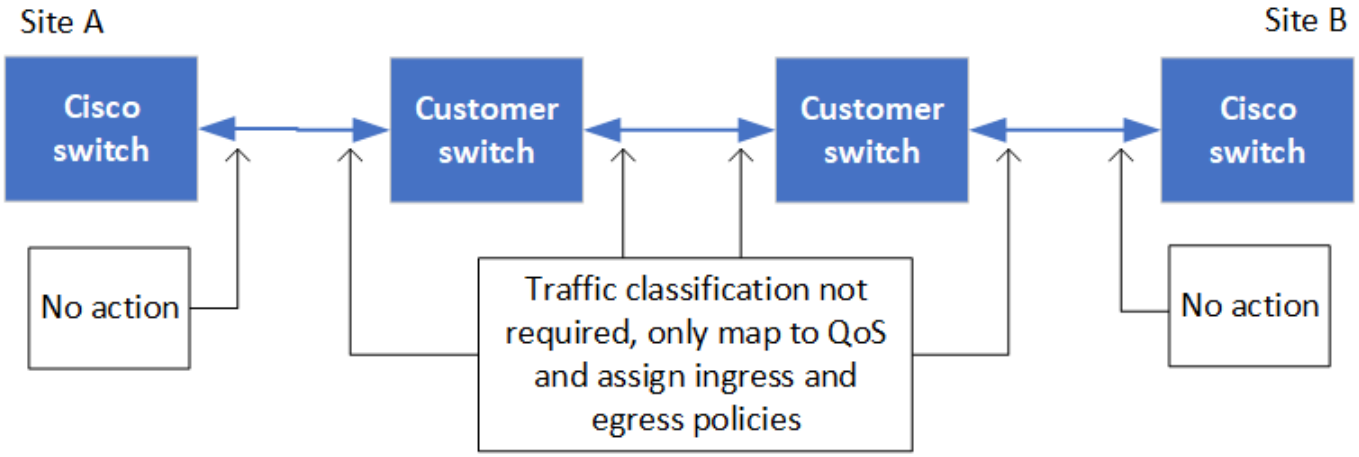
Quando si configurano gli indirizzi IP dei router e dei gateway, sono necessari i seguenti requisiti:

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

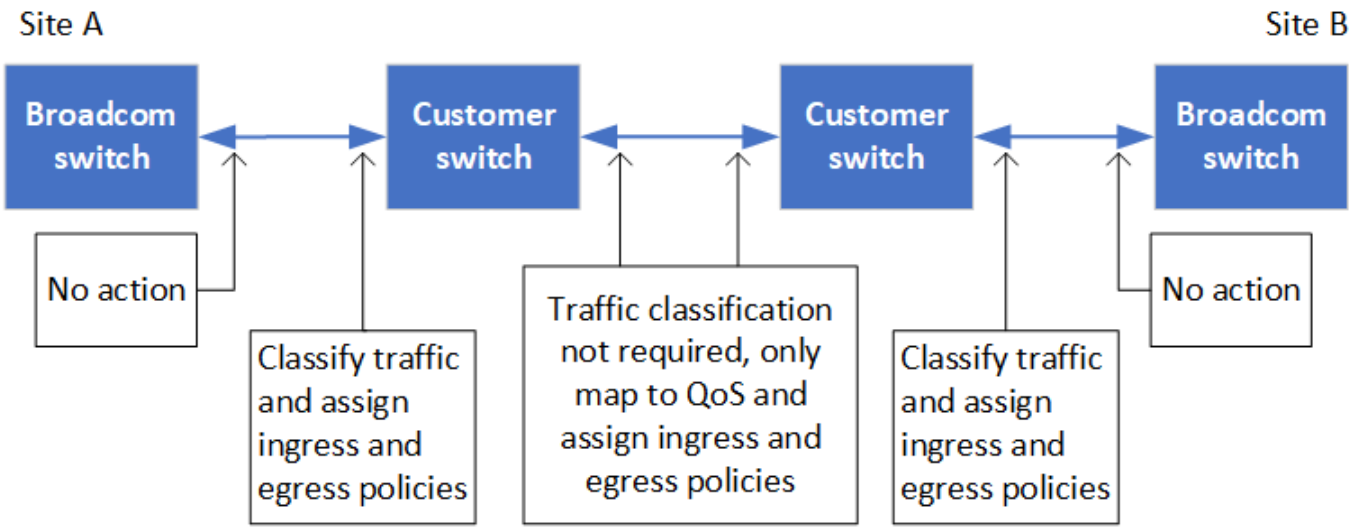
Impostazioni richieste per gli interruttori intermedi

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

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



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



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

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

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

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

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

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

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

Classificare il traffico in ingresso:

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

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

Corrispondenza del traffico all'ingresso:

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

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

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

Classificare il traffico in ingresso:

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

Far corrispondere il traffico all'ingresso:

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

Configurare il criterio di accodamento in uscita per le porte ISL

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

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

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

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

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

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

Esempio 1: Cisco

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

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

- `MetroClusterIP_ISL_Ingress_Match`

Viene assegnato il `MetroClusterIP_ISL_Ingress_Match` Policy map ai porti ISL che trasportano il traffico MetroCluster.

Esempio 2: Broadcom

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

- `ip access-list rdma`
- `ip access-list storage`
- `class-map type qos match-all rdma`
- `class-map type qos match-all storage`
- `MetroClusterIP_ISL_Ingress_Classify`
- `MetroClusterIP_ISL_Ingress_Match`

Assegnato dall'utente `the MetroClusterIP_ISL_Ingress_Classify` Mappa dei criteri alle porte ISL sullo switch intermedio che collega lo switch Broadcom.

Viene assegnato il `MetroClusterIP_ISL_Ingress_Match` La policy viene associata alle porte ISL sullo switch intermedio che trasporta il traffico MetroCluster ma non collega lo switch Broadcom.

Considerazioni sull'utilizzo di switch compatibili con MetroCluster

Requisiti e limitazioni quando si utilizzano switch compatibili con MetroCluster

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

Requisiti generali per gli switch compatibili con MetroCluster

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

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

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

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

Limitazioni relative all'utilizzo di switch compatibili con MetroCluster

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

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

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

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

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

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

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

Esempi di configurazione delle porte dello switch

Informazioni sulle varie configurazioni delle porte dello switch.

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

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

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

Porta dello switch che collega un'interfaccia MetroCluster

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

Porte ISL

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

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

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

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

- RDMA, COS 5 / DSCP 40: 60%

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

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

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

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

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

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

Configurazione di base

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

Esempio:

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

Esempio:

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

Esempi di configurazione della classificazione

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

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

Esempio:

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

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

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

Esempio:

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

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

Esempio:

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

Esempi di configurazione delle porte di nodo

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

Esempio:

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

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

Esempio:

```
    speed auto

    speed 40000
```

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

Esempio:

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

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

Esempio:

```
fec off
```

Esempi di configurazione delle porte ISL in tutta la rete

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

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

Esempi di topologie di rete MetroCluster

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

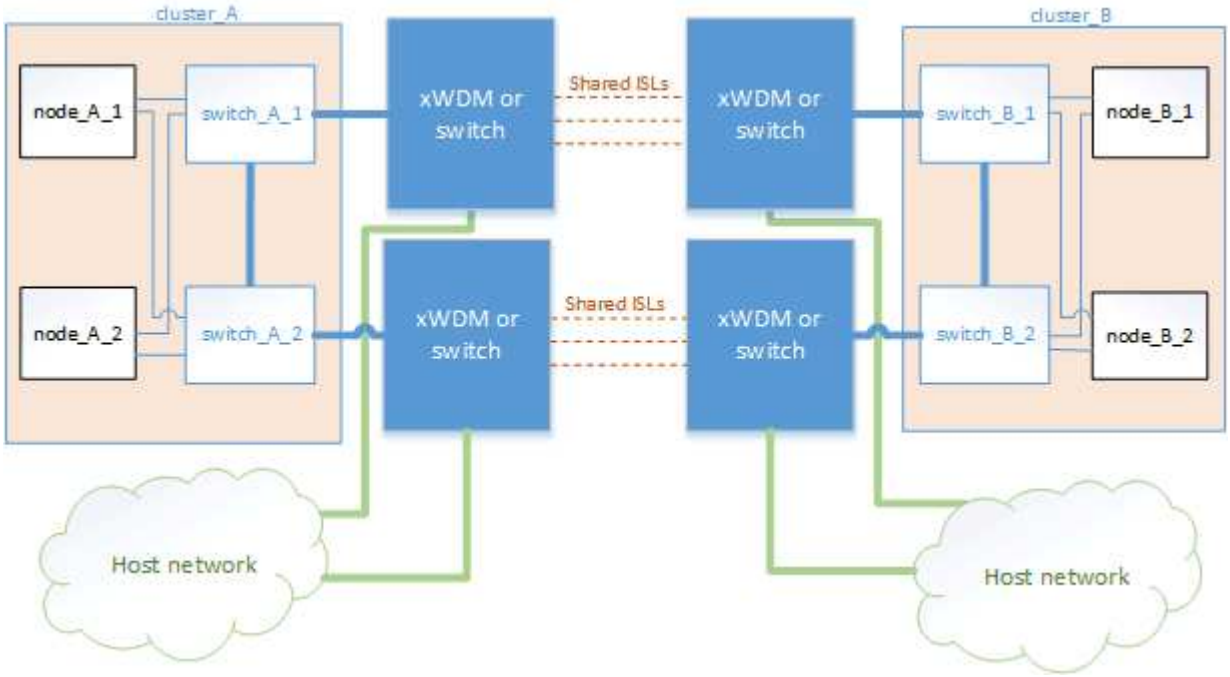
In queste topologie, si ipotizza che la rete ISL e intermedia sia configurata secondo i requisiti indicati nella "Considerazioni per gli ISL".

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

Configurazione di rete condivisa con collegamenti diretti

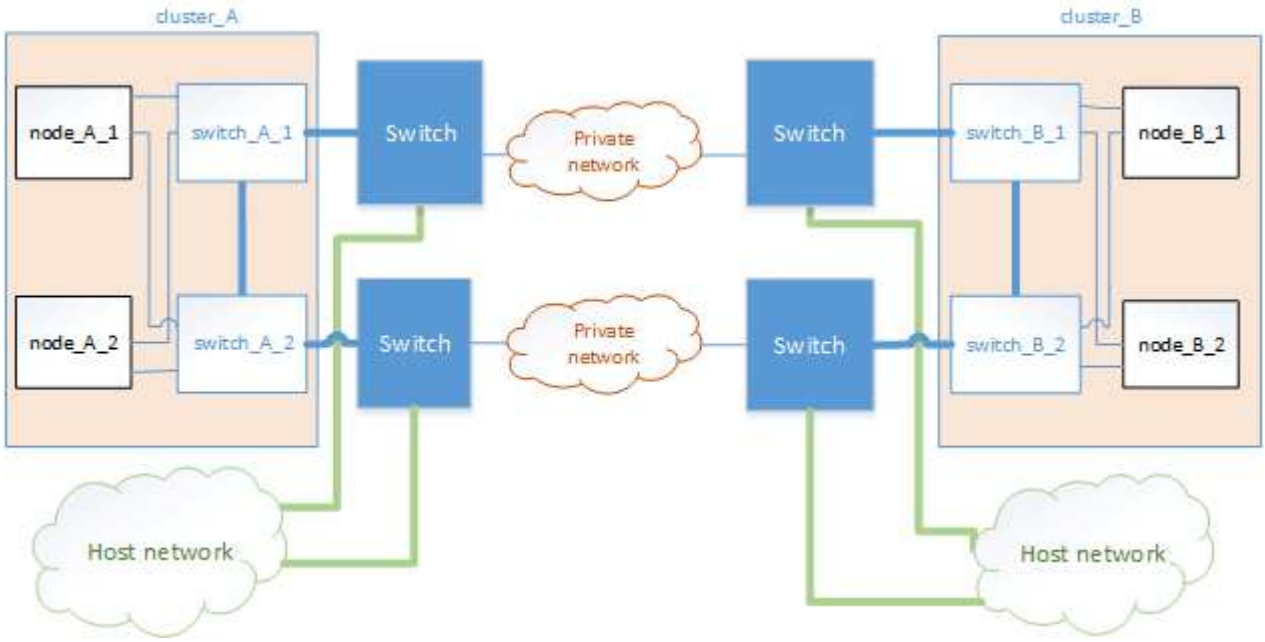
In questa topologia, due siti distinti sono collegati da collegamenti diretti. Questi collegamenti possono essere tra dispositivi o switch xWDM e TDM. La capacità degli ISL non è dedicata al traffico MetroCluster, ma è

condivisa con altro traffico non MetroCluster.



Infrastruttura condivisa con reti intermedie

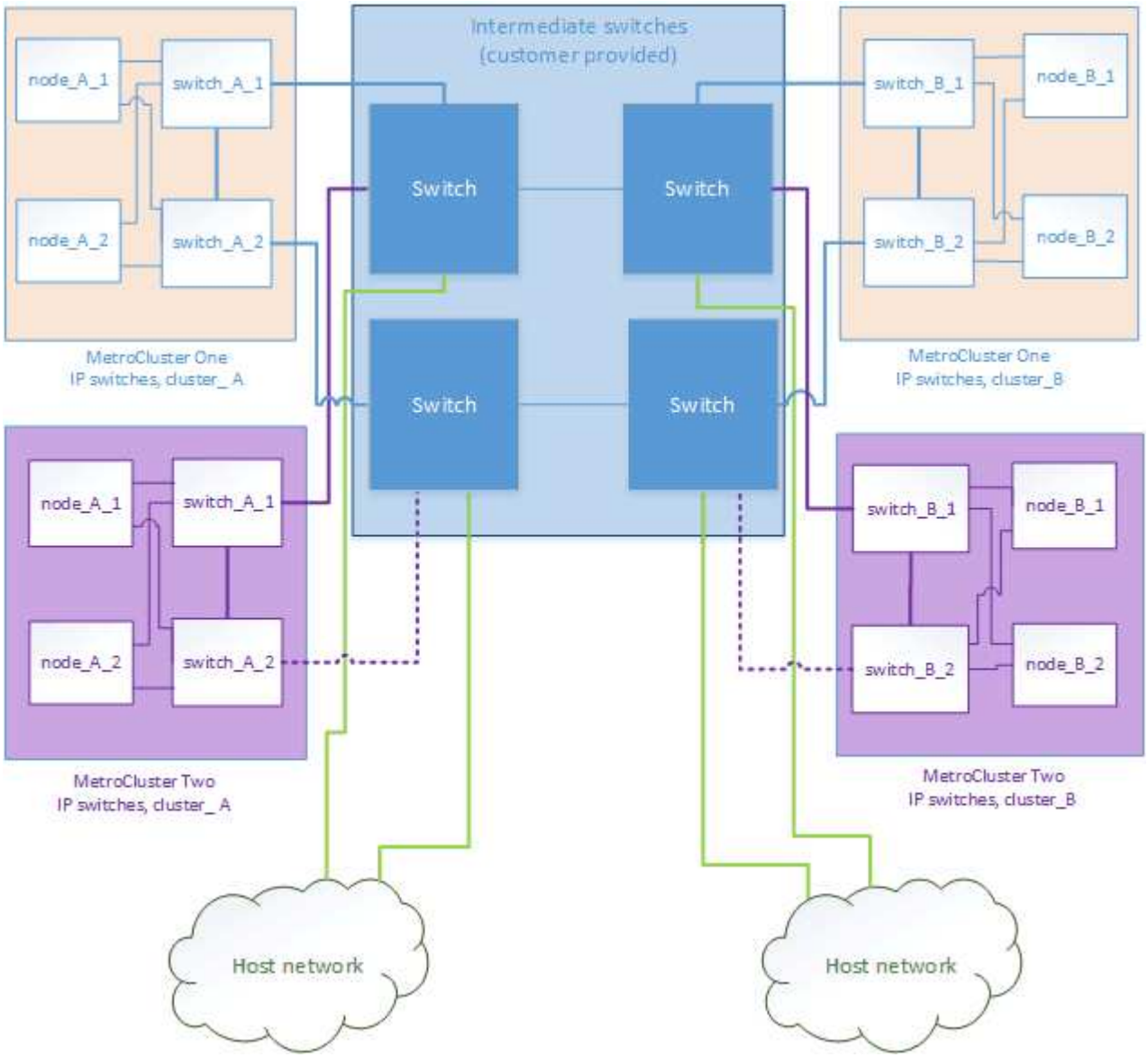
In questa topologia, i siti MetroCluster non sono collegati direttamente, ma MetroCluster e il traffico host viaggiano attraverso una rete. La rete può essere costituita da una serie di xWDM e TDM e switch, ma a differenza della configurazione condivisa con ISL diretti, i collegamenti non sono diretti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



Configurazioni MetroCluster multiple che condividono una rete intermedia

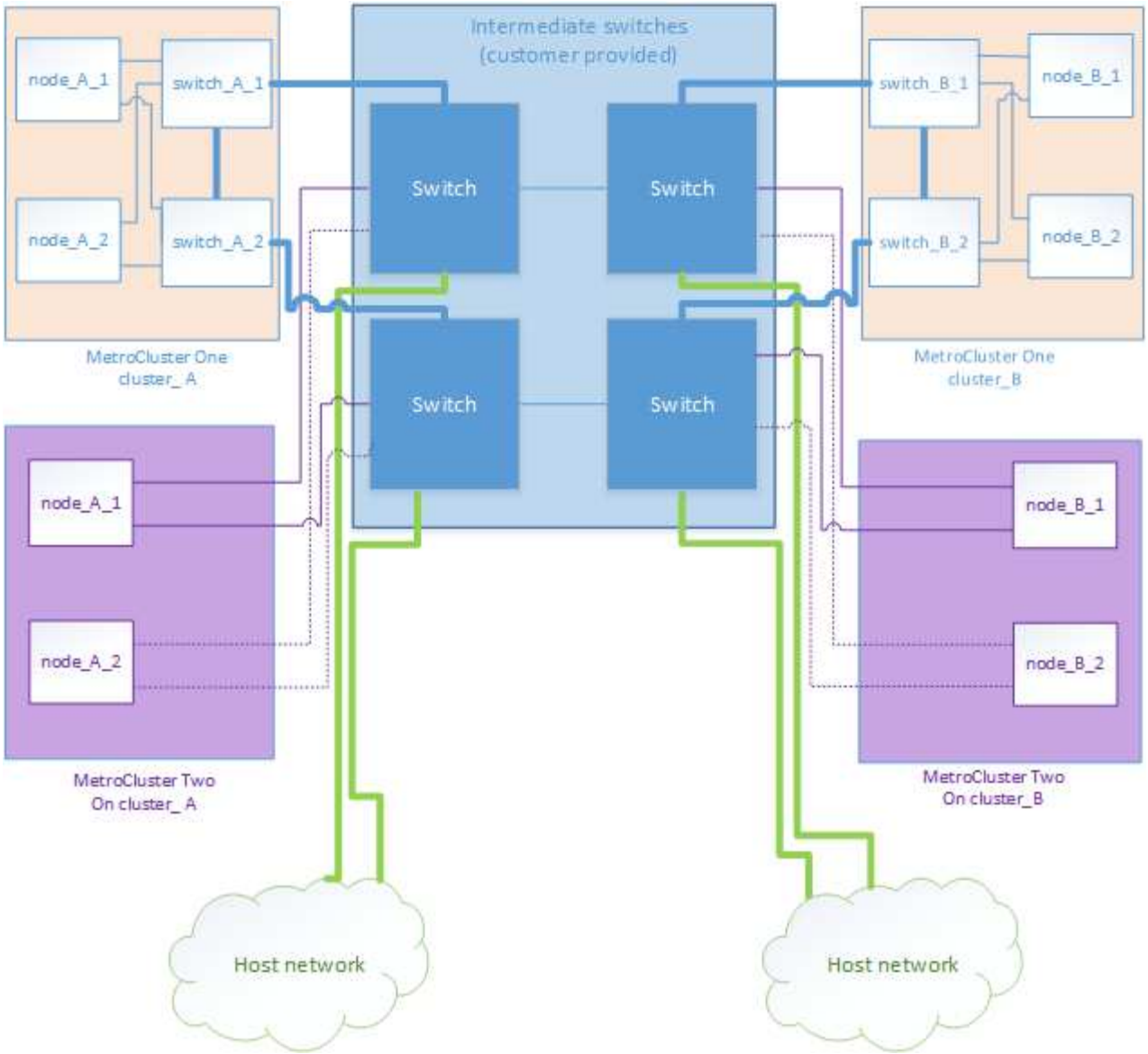
In questa topologia, due configurazioni MetroCluster separate condividono la stessa rete intermedia. Nell'esempio, MetroCluster ONE switch_A_1 e MetroCluster Two switch_A_1, entrambi si collegano allo stesso interruttore intermedio.

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



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

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



Utilizzo di aggregati senza mirror

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

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

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

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

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

Considerazioni per aggregati senza mirror e SVM

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

Considerazioni per aggregati senza mirror e SAN

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

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

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

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

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

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

   ```
   disk option show
   ```

3. Seguire i passaggi della procedura per aggiungere lo shelf.
4. Assegnare manualmente tutti i dischi dal nuovo shelf al nodo che sarà proprietario dell'aggregato o degli aggregati senza mirror.
5. Creare gli aggregati:

   ```
   storage aggregate create
   ```

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

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

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

   ```
   disk option show
   ```

Utilizzo del firewall nei siti MetroCluster

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

Considerazioni sull'utilizzo del firewall nei siti MetroCluster

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

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

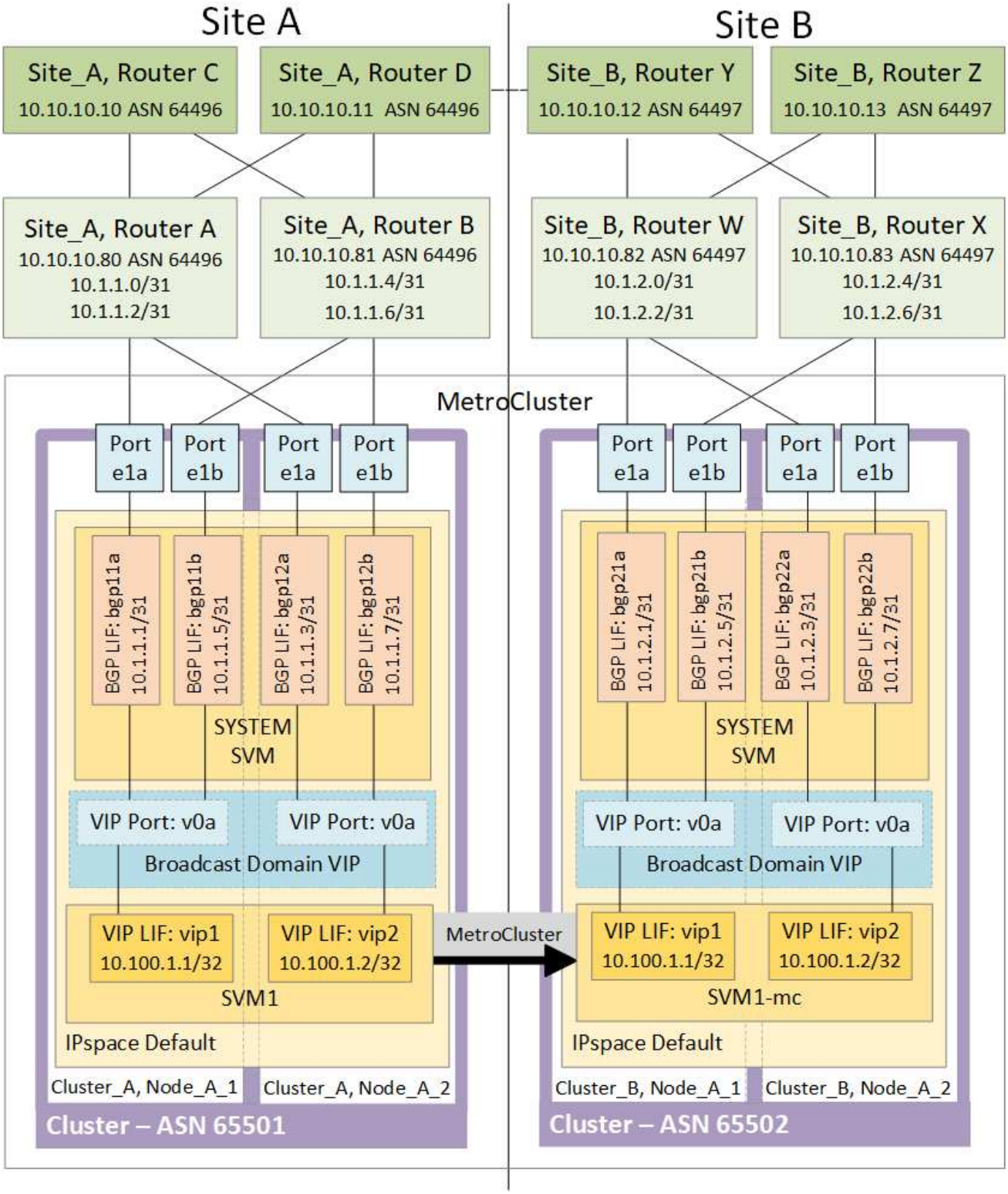
Tipo di traffico	Porta/servizi
Peering dei cluster	11104 / TCP 11105 / TCP
Gestore di sistema di ONTAP	443 / TCP
MetroCluster IP Intercluster LIF	65200 / TCP 10006 / TCP e UDP
Assistenza hardware	4444 / TCP

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

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

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

"Configurazione di LIF IP virtuali (VIP)"



Limitazioni ONTAP

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

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

in qualsiasi momento.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configurare i componenti hardware di MetroCluster

Parti di una configurazione IP MetroCluster

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

Elementi hardware chiave

Una configurazione MetroCluster IP include i seguenti elementi hardware principali:

- Controller di storage

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

- Rete IP

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

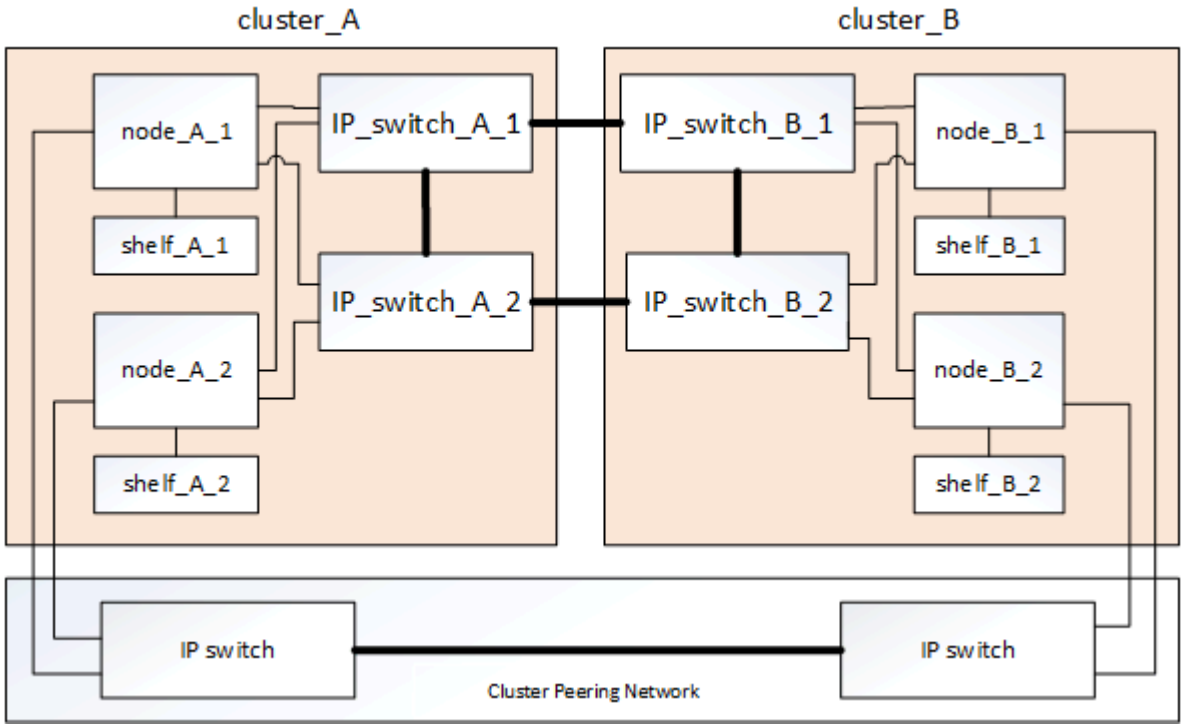
  - Connettività cluster standard per comunicazioni intra-cluster.

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

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

- Rete di peering del cluster

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



Gruppi di disaster recovery (DR)

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

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

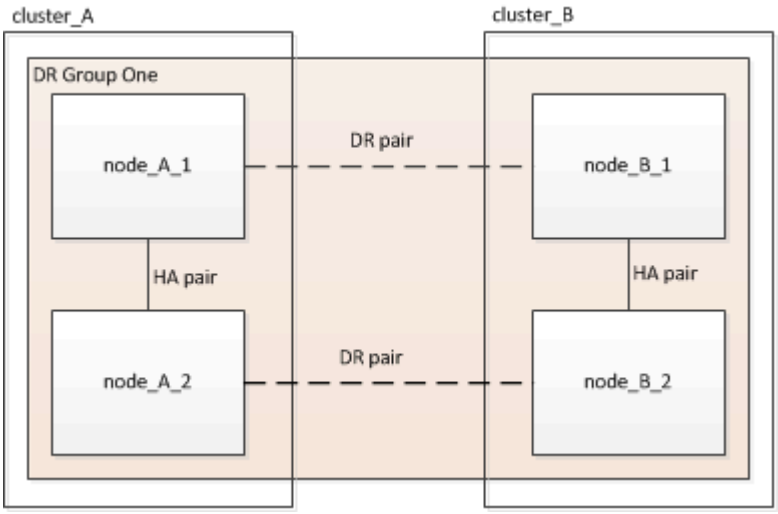
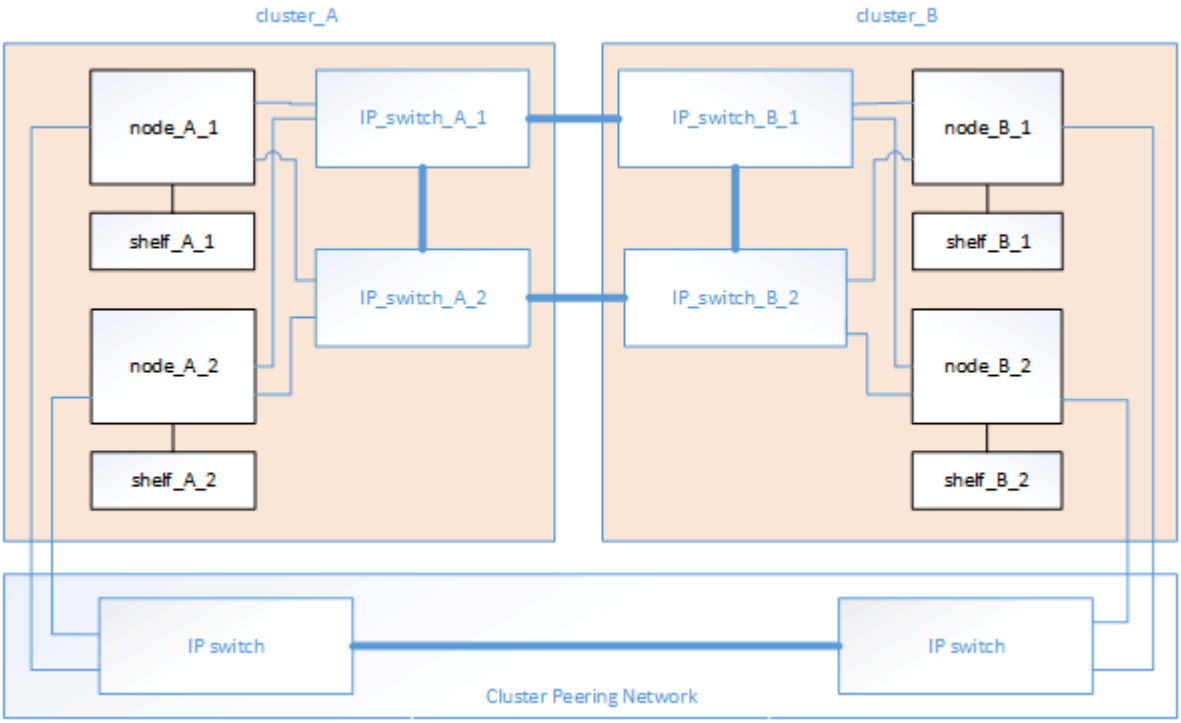


Immagine delle coppie ha locali in una configurazione MetroCluster

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

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

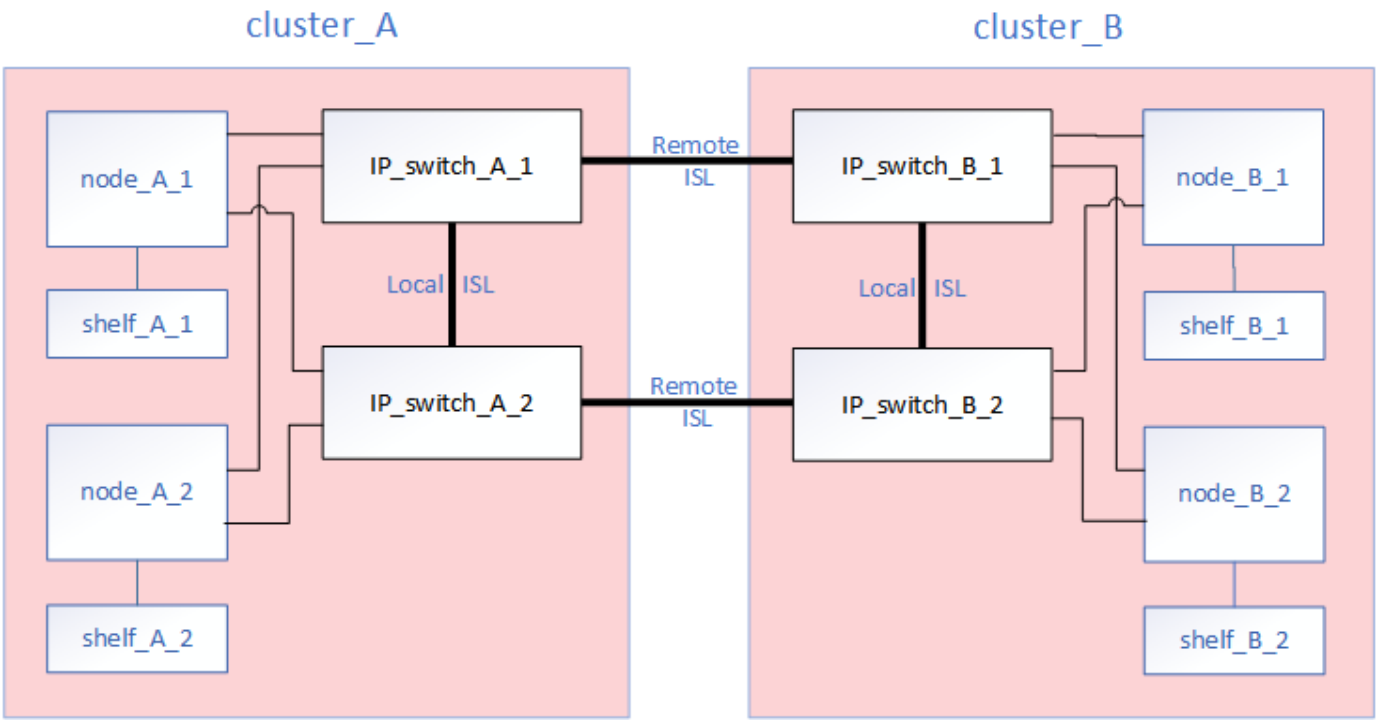


Informazioni correlate

"Concetti di ONTAP"

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

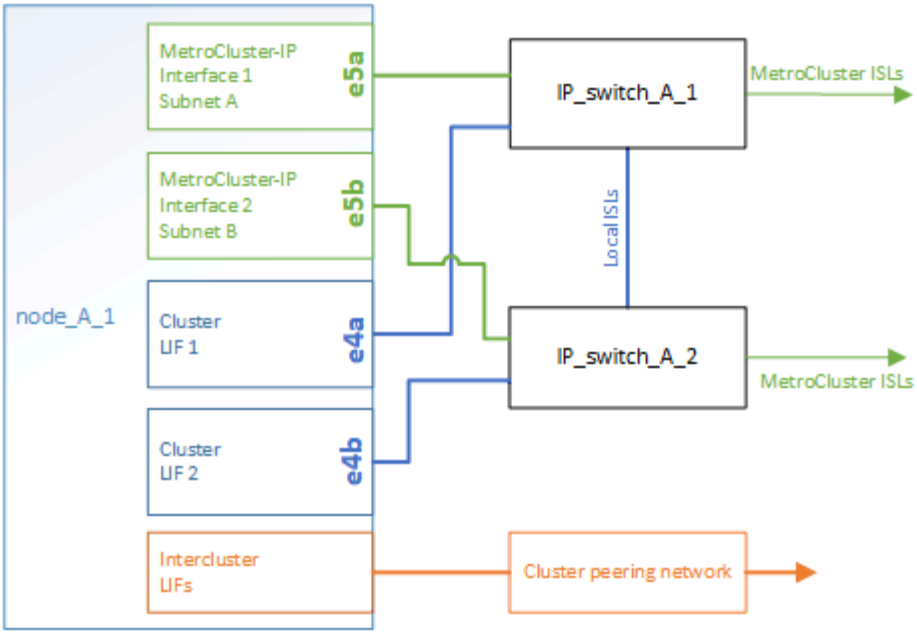
I cluster ONTAP in genere includono una rete di interconnessione cluster per il traffico tra i nodi del cluster. Nelle configurazioni MetroCluster IP, questa rete viene utilizzata anche per trasportare il traffico di replica dei dati tra i siti MetroCluster.



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

- Due interfacce IP MetroCluster
- Due interfacce cluster locali

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



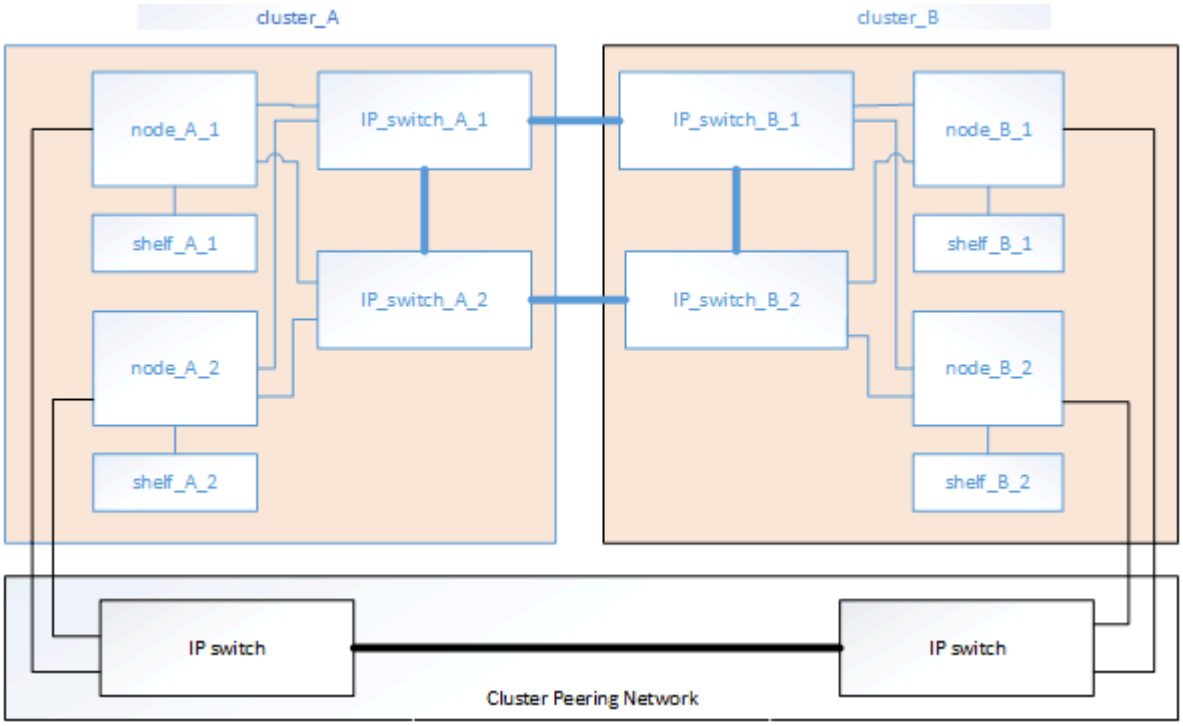
Informazioni correlate

"Considerazioni per le configurazioni MetroCluster IP"

Immagine della rete di peering del cluster

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

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



Informazioni correlate

"Configurazione rapida del peering di cluster e SVM"

"Considerazioni per la configurazione del peering del cluster"

"Cablaggio delle connessioni di peering del cluster"

"Peering dei cluster"

Componenti IP MetroCluster richiesti e convenzioni di denominazione

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

Software e hardware supportati

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

"NetApp Hardware Universe"

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

Requisiti di ridondanza dell'hardware in una configurazione MetroCluster IP

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

Requisiti del cluster ONTAP in una configurazione IP MetroCluster

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

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

Nomi di esempio:

- Sito A: Cluster_A
- Sito B: Cluster_B

Requisiti dello switch IP in una configurazione IP MetroCluster

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

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

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

Nomi di esempio:

- Sito A: Cluster_A
  - IP_switch_A_1
  - IP_switch_A_2
- Sito B: Cluster_B
  - IP_switch_B_1
  - IP_switch_B_2

Requisiti del modulo controller in una configurazione IP MetroCluster

Le configurazioni MetroCluster IP richiedono quattro o otto moduli controller.

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

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

- Le nuove installazioni MetroCluster IP sui sistemi FAS non sono supportate in ONTAP 9.4.

  Le configurazioni MetroCluster IP esistenti sui sistemi FAS possono essere aggiornate a ONTAP 9.4.

- A partire da ONTAP 9.5, sono supportate le nuove installazioni MetroCluster IP sui sistemi FAS.
- A partire da ONTAP 9.4, sono supportati i moduli controller configurati per ADP.

Nomi di esempio

Nella documentazione vengono utilizzati i seguenti nomi di esempio:

- Sito A: Cluster_A
  - Controller_A_1
  - Controller_A_2
- Sito B: Cluster_B
  - Controller_B_1
  - Controller_B_2

Requisiti dell'adattatore Gigabit Ethernet in una configurazione MetroCluster IP

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

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

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

"Scopri l'assegnazione automatica dei dischi e i sistemi ADP nelle configurazioni IP di MetroCluster".

Requisiti di pool e disco (supporto minimo)

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

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

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

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

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

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

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

Le configurazioni MetroCluster supportano RAID-DP e RAID4.

Considerazioni sulla posizione dei dischi per gli shelf parzialmente popolati

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

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

Considerazioni sulla posizione dei dischi interni di AFF A800

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

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

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

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

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

Combinazione di moduli IOM12 e IOM 6 in uno stack

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

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

Scaffalatura dei componenti hardware

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

A proposito di questa attività

Questa attività deve essere eseguita su entrambi i siti MetroCluster.

Fasi

1. Pianificare il posizionamento dei componenti di MetroCluster.

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

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

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A220/FAS2700"

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A250"

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A300"

   "Sistemi AFF A320: Installazione e configurazione"

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A400"

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A700"

   "Istruzioni per l'installazione e la configurazione dei sistemi AFF A800"

   "Istruzioni per l'installazione e la configurazione dei sistemi FAS500f"

   "Istruzioni per l'installazione e la configurazione dei sistemi FAS8200"

   "Istruzioni per l'installazione e la configurazione dei sistemi FAS8300 e FAS8700"

   "Istruzioni per l'installazione e la configurazione dei sistemi FAS9000"

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

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

Collegare via cavo gli switch IP MetroCluster

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

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

Prima di iniziare

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

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

Cablaggio di configurazioni MetroCluster a otto nodi

Per la configurazione di MetroCluster con ONTAP 9.8 e versioni precedenti, alcune procedure eseguite per la transizione di un aggiornamento richiedono l'aggiunta di un secondo gruppo di DR a quattro nodi alla configurazione per creare una configurazione temporanea a otto nodi. A partire da ONTAP 9,9.1, sono supportate le configurazioni permanenti di MetroCluster a otto nodi.

A proposito di questa attività

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

Ad esempio, la configurazione include quanto segue:

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

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

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

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

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

  Utilizzare questa panoramica dei cavi per verificare il cablaggio.

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

Collegamento di due configurazioni MetroCluster agli switch

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

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

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

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

Cabling a FAS8200 or AFF A300 to a Cisco 3232C or Cisco 9336C-FX2 switch			
Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, MetroCluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled	

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

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

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

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

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

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

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

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

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

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

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

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

Cabling an AFF A150, ASA A150, FAS2750 or AFF A220 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

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

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

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

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

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

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

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

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

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

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

Leggere queste informazioni prima di utilizzare le tabelle:

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

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

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

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

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

Note a cui si fa riferimento nelle tabelle:

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

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

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

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

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

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

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

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

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

Collegamento di un sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 o FAS8700 a uno switch Broadcom BES-53248

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

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

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

Configurazioni supportate

Le seguenti configurazioni non sono attualmente supportate:

- Transizione MetroCluster FC-IP

Esaminare queste considerazioni prima di utilizzare le tabelle di configurazione

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

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

Le sezioni seguenti descrivono il cablaggio fisico. Fare riferimento anche alla "RcfFileGenerator" per informazioni dettagliate sul cablaggio.

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

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

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

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

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

Cablaggio delle porte di peering, dati e gestione del controller

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

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

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

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

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

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

   "Configurazione rapida del peering di cluster e SVM"

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

   Seguire le istruzioni di installazione della piattaforma in "Documentazione dei sistemi hardware ONTAP".

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

Configurare gli switch IP di MetroCluster

Configurazione degli switch IP Broadcom

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

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

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

Ripristino delle impostazioni predefinite dello switch IP Broadcom

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

A proposito di questa attività

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

Fasi

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

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

2. Cancellare la configurazione di avvio e rimuovere il banner

a. Cancellare la configurazione di avvio:

`erase startup-config`

```
(IP_switch_A_1) #erase startup-config

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

(IP_switch_A_1) #
```

Questo comando non cancella il banner.

b. Rimuovere lo striscione:

`no set clibanner`

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

3. Riavviare lo switch:*`(IP_switch_A_1) #reload*`

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

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

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

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

```
(Routing)>
```

5. Passare al prompt dei comandi con privilegi elevati:

   `enable`

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

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

```
serviceport protocol none
```

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

(Routing) #
```

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

   `serviceport ip ip-address netmask gateway`

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

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

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

   `show serviceport`

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

```
(Routing) #show serviceport

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

(Routing) #
```

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

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

a. Generare chiavi RSA.

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

b. Generare chiavi DSA (opzionale)

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

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

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

d. Abilitare il server SSH.

Se necessario, uscire dal contesto di configurazione.

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

+

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

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

`configure`

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

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

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

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

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

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

```
> (Config)# ntp ?

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

>(Config)# ntp server ?

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

>(Config)# ntp server 10.99.99.5
```

12. Configurare il nome dello switch:

    `hostname IP_switch_A_1`

    Il prompt di switch visualizza il nuovo nome:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Salvare la configurazione:

    `write memory`

    Si ricevono messaggi e output simili al seguente esempio:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

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

Download e installazione del software EFOS dello switch Broadcom

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

A proposito di questa attività

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

Nota:

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

Fasi

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

   Esempio 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Esempio 2

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

IP_switch_A_2 #
```

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

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

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

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

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

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

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

Fasi

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

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

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

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

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

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


File transfer operation completed successfully.

(IP_switch_A_1) #
```

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

   `boot system backup`

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

(IP_switch_A_1) #
```

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

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Salvare la configurazione:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

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


Configuration Saved!

(IP_switch_A_1) #
```

5. Riavviare lo switch:

   `reload`

```
(IP_switch_A_1) #reload

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

6. Attendere il riavvio dello switch.

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

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

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

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

Fasi

1. Avviare lo switch in modalità di installazione ONIE.

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

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

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

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

Lo switch si avvia in modalità di installazione ONIE.

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

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

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

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

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

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

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

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

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

5. Installare il nuovo software dello switch

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

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

6. Verificare che il nuovo software dello switch sia installato

show bootvar

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

7. Completare l'installazione

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

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

Download e installazione dei file RCF Broadcom

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

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

Fasi

1. Generare i file RCF Broadcom per l'IP MetroCluster.
   a. Scaricare il "RcfFileGenerator per MetroCluster IP"
   b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.

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

2. Copiare i file RCF sugli switch:

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

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

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

Remote Password:*************

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

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

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


Validating configuration script...

config

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

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248



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


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

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

```
script list
```

```
(IP_switch_A_1) #script list

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

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

c. Applicare lo script RCF:

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

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

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


config

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

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

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

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

(IP_switch_A_1) #
```

d. Salvare la configurazione:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

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


Configuration Saved!

(IP_switch_A_1) #
```

e. Riavviare lo switch:

   `reload`

```
(IP_switch_A_1) #reload

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

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

3. Ricaricare lo switch:

   `reload`

```
IP_switch_A_1# reload
```

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

Disattivare le porte e i canali delle porte ISL non utilizzati

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

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

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

Per informazioni dettagliate sulla porta ISL

Eseguire il comando `show port all`.

Per i dettagli del canale della porta

Eseguire il comando `show port-channel all`.

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

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

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

Configurare gli switch IP Cisco

Configurazione degli switch IP Cisco

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

A proposito di questa attività

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

Ripristino delle impostazioni predefinite dello switch IP Cisco

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

A proposito di questa attività

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

Fasi

1. Ripristinare le impostazioni predefinite dello switch:

   a. Cancellare la configurazione esistente:

```
write erase
```

b. Ricaricare il software dello switch:

```
reload
```

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

c. Nella configurazione guidata, immettere le impostazioni di base dello switch:
   - Password amministratore
   - Nome dello switch
   - Configurazione della gestione fuori banda
   - Gateway predefinito
   - Servizio SSH (RSA)

     Al termine della configurazione guidata, lo switch si riavvia.

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

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

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

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

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

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

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

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

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

L’ultimo set di prompt completa la configurazione:

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

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

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

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

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

2. Salvare la configurazione:

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

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

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

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

Download e installazione del software NX-OS dello switch Cisco

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

A proposito di questa attività

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

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

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

Fasi

1. Scaricare il file software NX-OS supportato.

   "Download del software Cisco"

2. Copiare il software dello switch sullo switch:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

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

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

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

   ```
   dir bootflash:
   ```

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

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

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

4. Installare il software dello switch:

   `install all nxos bootflash:nxos.version-number.bin`

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

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

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

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

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

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

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

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

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

```
-- SUCCESS



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



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


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


Install is in progress, please wait.

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

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

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

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


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

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

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

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

The switch software is now installed.
```

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

   L'esempio seguente mostra l'output:

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

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


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

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

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

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

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

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

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

Download e installazione dei file Cisco IP RCF

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

A proposito di questa attività

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per

copiare i file sui centralini.

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

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

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

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

Fasi

1. Scaricare i file MetroCluster IP RCF.

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

2. Copiare i file RCF sugli switch:

   a. Copiare i file RCF sul primo switch:

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

   In questo esempio, il file RCF NX3232_v1.80_Switch-A1.txt viene copiato dal server SFTP all'indirizzo 10.10.99.99 alla flash di avvio locale. Utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

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

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

3. Verificare su ogni switch che il file RCF sia presente nella directory bootflash di ogni switch:

   ```
   dir bootflash:
   ```

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

   ```
   IP_switch_A_1# dir bootflash:
                     .
                     .
                     .
   5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                     .
                     .
                     .

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

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

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

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

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

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

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

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

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

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

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

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

   `copy running-config startup-config`

   L'output dovrebbe essere simile a quanto segue:

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

7. Ricaricare lo switch:

   `reload`

   ```
   IP_switch_A_1# reload
   ```

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

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

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

A proposito di questa attività

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

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

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

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

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

Fasi

1. Impostare il parametro fec su Off su ciascuna porta a 25 Gbps collegata a un modulo controller, quindi copiare la configurazione in esecuzione nella configurazione di avvio:

   a. Accedere alla modalità di configurazione: `config t`

   b. Specificare l'interfaccia a 25 Gbps da configurare: `interface interface-ID`

   c. Impostare fec su Off: `fec off`

   d. Ripetere i passaggi precedenti per ciascuna porta a 25 Gbps dello switch.

   e. Uscire dalla modalità di configurazione: `exit`

   L'esempio seguente mostra i comandi per l'interfaccia Ethernet1/25/1 sullo switch IP_switch_A_1:

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

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

Disattivare le porte e i canali delle porte ISL non utilizzati

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

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

```
show interface brief
```

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

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

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

Configurare la crittografia MACsec sugli switch Cisco 9336C

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

Configurare la crittografia MACsec sugli switch Cisco 9336C

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

Requisiti di licenza per MACsec

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

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

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

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Abilitare MACsec e MKA sul dispositivo:

```
feature macsec
```

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

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

   `copy running-config startup-config`

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

Configurare una catena di chiavi MACsec e le chiavi

È possibile creare una o più chiavi MACsec nella configurazione.

Key Lifetime e Hitless Key Rollover

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

Fasi

1. Accedere alla modalità di configurazione globale:

   `configure terminal`

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

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

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

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

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

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

   `key chain name macsec`

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

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

   `key key-id`

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

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

5. Configurare la stringa di ottetti per la chiave:

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

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

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

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

   `send-lifetime start-time duration duration`

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

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

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

   `copy running-config startup-config`

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

8. Visualizza la configurazione del portachiavi:

```
show key chain name
```

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

Configurare un criterio MACsec

Fasi

1. Accedere alla modalità di configurazione globale:

   ```
   configure terminal
   ```

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

2. Creare un criterio MACsec:

   ```
   macsec policy name
   ```

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

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

   ```
   cipher-suite name
   ```

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

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

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

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

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

   ```
   security-policy security policy
   ```

   Scegliere una policy di sicurezza tra le seguenti opzioni:

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

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

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

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

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

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

   `sak-expiry-time time`

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

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

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

   `conf-offsetconfidentiality offset`

   Scegliere una delle seguenti opzioni:

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

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

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

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

   `copy running-config startup-config`

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

10. Visualizzare la configurazione del criterio MACsec:

```
show macsec policy
```

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

Abilitare la crittografia Cisco MACsec sulle interfacce

1. Accedere alla modalità di configurazione globale:

   ```
   configure terminal
   ```

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

2. Selezionare l'interfaccia configurata con la crittografia MACsec.

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

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

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

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

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

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

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

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

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

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

Fasi

1. Accedere alla modalità di configurazione globale:

   ```
   configure terminal
   ```

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

2. Disattivare la configurazione MACsec sul dispositivo:

   `macsec shutdown`

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

   Selezionando l'opzione "no" si ripristina la funzione MACsec.

3. Selezionare l'interfaccia già configurata con MACsec.

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

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

4. Rimuovere il portachiavi e il criterio configurati sull'interfaccia per rimuovere la configurazione MACsec:

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

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

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

   `copy running-config startup-config`

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

Verifica della configurazione MACsec

Fasi

1. Ripetere **tutte** le procedure precedenti sul secondo switch all'interno della configurazione per stabilire una sessione MACsec.
2. Eseguire i seguenti comandi per verificare che entrambi gli switch siano crittografati correttamente:

   a. Esecuzione: `show macsec mka summary`

   b. Esecuzione: `show macsec mka session`

   c. Esecuzione: `show macsec mka statistics`

È possibile verificare la configurazione MACsec utilizzando i seguenti comandi:

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

Configurare lo switch NVIDIA IP SN2100

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

Ripristina le impostazioni predefinite dello switch NVIDIA IP SN2100

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

- Ripristinare lo switch utilizzando l'opzione del file RCF
- Ripristinare lo switch utilizzando l'opzione di installazione di Cumulus

ripristinare lo switch utilizzando l'opzione del file RCF

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

A proposito di questa attività

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

I seguenti dettagli di configurazione non vengono ripristinati:

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

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

Prima di iniziare

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

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

Fasi

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

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

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

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

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

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

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

reimpostare lo switch utilizzando l'opzione di installazione di Cumulus

A proposito di questa attività

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

Prima di iniziare

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

> Per ulteriori informazioni sull'installazione di Cumulus Linux, vedere "Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100"

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

Fasi

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

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

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

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

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

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

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

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

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

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

```
Debian GNU/Linux 10 cumulus ttyS0

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

Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configurare l'interfaccia di rete di gestione.

> L'esempio seguente mostra come configurare il nome host (IP_switch_A_1), l'indirizzo IP (10.10.10.10), la netmask (255.255.255.0 (24)) e il gateway (10.10.10.1) utilizzando i comandi: `net add hostname <hostname>`, `net add interface eth0 ip address <IPAddress/mask>`, e. `net add interface eth0 ip gateway <Gateway>`.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


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


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

6. Riavviare lo switch utilizzando `sudo reboot` comando.

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

Al riavvio dello switch, è possibile applicare una nuova configurazione seguendo la procedura descritta in Scaricare e installare il file NVIDIA RCF.

Scarica e installa i file NVIDIA RCF

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

Prima di iniziare

- È necessario disporre della password root per `sudo` accesso ai comandi.
- Il software dello switch è installato e la rete di gestione è configurata.

- È stata eseguita la procedura per installare inizialmente lo switch utilizzando il metodo 1 o il metodo 2.
- Non è stata applicata alcuna configurazione aggiuntiva dopo l'installazione iniziale.

> Se si esegue un'ulteriore configurazione dopo aver reimpostato lo switch e prima di applicare il file RCF, non è possibile utilizzare questa procedura.

A proposito di questa attività

Ripetere questa procedura su ciascuno switch IP nella configurazione MetroCluster IP (nuova installazione) o sullo switch sostitutivo (sostituzione dello switch).

Fasi

1. Generare i file NVIDIA RCF per MetroCluster IP.
   a. Scaricare il "RcfFileGenerator per MetroCluster IP".
   b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.
   c. Accedere alla home directory. Se si è registrati come 'cumulo', il percorso del file è `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

   d. Scaricare il file RCF in questa directory. L'esempio seguente mostra che si utilizza SCP per scaricare il file `MSN2100_v1.0_IP_switch_A_1.txt` dal server '50.50.50.50' alla home directory e salvarlo con nome `MSN2100_v1.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/MSN2100_v1.0_IP_switch_A_1.txt
./MSN2100_v1.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*******************************************************************
**
Banner of the SCP server
*******************************************************************
**
username@50.50.50.50's password:
MSN2100_v1.0-X2_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Eseguire il file RCF. Il file RCF richiede un'opzione per applicare uno o più passaggi. Se non richiesto dal supporto tecnico, eseguire il file RCF senza l'opzione della riga di comando. Per verificare lo stato di completamento delle varie fasi del file RCF, utilizzare l'opzione '-1' o 'all' per applicare tutte le fasi (in sospeso).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

Disattivare le porte e i canali delle porte ISL non utilizzati

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

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

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

```
net show interface
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati utilizzando il file RCF.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

Il seguente comando di esempio disattiva la porta "swp14":

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Ripetere questo passaggio per ogni porta o canale di porta non utilizzato identificato.

Configurare gli switch IP MetroCluster per il monitoraggio dello stato

Nelle configurazioni IP di MetroCluster, è possibile configurare SNMPv3 per monitorare lo stato degli switch IP.

Passaggio 1: Configurare l’utente SNMPv3 sugli switch IP MetroCluster

Per configurare l’utente SNMPv3 sugli switch IP MetroCluster, procedere come segue.

> Nei comandi è necessario utilizzare sia i protocolli di autenticazione che quelli di privacy. L’utilizzo dell’autenticazione senza privacy non è supportato.

Per gli switch IP Broadcom

Fasi

1. Se il gruppo utenti 'network-admin' non esiste già, crearlo:

   ```
   (IP_switch_1) (Config)# snmp-server group network-admin v3 auth read
   "Default"
   ```

2. Confermare che il gruppo "network-admin" è stato creato:

   ```
   (IP_switch_1) (Config)# show snmp group
   ```

3. Configurare l'utente SNMPv3 sugli switch IP Broadcom:

   ```
   (IP_switch_1)# config
   (IP_switch_1) (Config)# snmp-server user <user_name> network-admin
   [auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]
   "<priv_password>"
   ```

   È necessario utilizzare le virgolette intorno alle password di autenticazione e privacy, come illustrato nell'esempio seguente:

   ```
   snmp-server user admin1 network-admin auth-md5 "password" priv-des
   "password"
   ```

Per gli switch IP Cisco

Fasi

1. Eseguire i seguenti comandi per configurare l'utente SNMPv3 su uno switch IP Cisco:

   ```
   IP_switch_A_1 # configure terminal
   IP_switch_A_1 (config) # snmp-server user <user_name>  auth
   [md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
   ```

2. Verificare che l'utente SNMPv3 sia configurato sullo switch:

   ```
   IP_switch_A_1(config) # show snmp user <user_name>
   ```

   L'output di esempio riportato di seguito mostra che l'utente `admin` È configurato per SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User                Auth      Priv(enforce) Groups
acl_filter

____                ____      _____________ ______
__________

admin               md5       aes-128(no)   network-admin
```

Passaggio 2: Configurare l'utente SNMPv3 in ONTAP

Per configurare l'utente SNMPv3 in ONTAP, procedere come segue.

1. Configurare l'utente SNMPv3 in ONTAP:

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

2. Configurare il monitoraggio dello stato dello switch per monitorare lo switch utilizzando il nuovo utente SNMPv3:

   ```
   system switch ethernet modify -device <device_id> -snmp-version SNMPv3
   -community-or-username <user_name>
   ```

3. Verificare che il numero di serie della periferica che verrà monitorato con l'utente SNMPv3 appena creato sia corretto:
   a. Visualizzare il periodo di tempo di polling del monitoraggio dello stato dello switch:

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

   b. Eseguire il comando seguente dopo aver esaurito il tempo di polling:

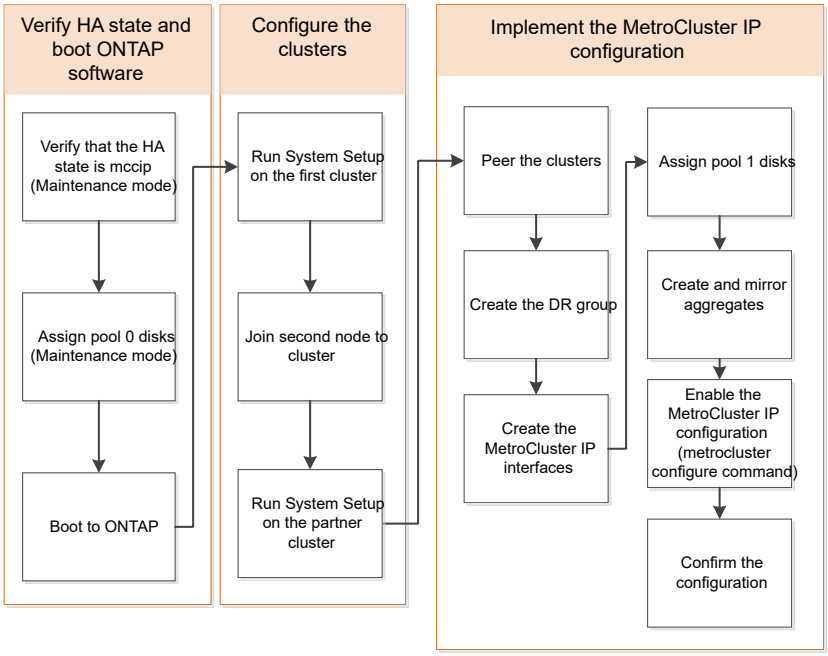
      ```
      system switch ethernet show-all -instance -device <device_serial_number>
      ```

Configurare il software MetroCluster in ONTAP

Configurazione del software MetroCluster in ONTAP

È necessario impostare ciascun nodo nella configurazione MetroCluster in ONTAP, incluse le configurazioni a livello di nodo e la configurazione dei nodi in due siti. È inoltre necessario implementare la relazione MetroCluster tra i due siti.

Se un modulo controller si guasta durante la configurazione, fare riferimento a. "Scenari di guasto del modulo controller durante l'installazione di MetroCluster".



Gestione delle configurazioni a otto nodi

Una configurazione a otto nodi è costituita da due gruppi di DR. Configurare il primo gruppo DR utilizzando le attività descritte in questa sezione.

Quindi, eseguire le attività in "Espansione di una configurazione IP MetroCluster a quattro nodi in una configurazione a otto nodi"

Raccolta delle informazioni richieste

Prima di iniziare il processo di configurazione, è necessario raccogliere gli indirizzi IP richiesti per i moduli controller.

È possibile utilizzare questi collegamenti per scaricare i file csv e compilare le tabelle con le informazioni specifiche del sito.

"Foglio di lavoro per la configurazione dell'IP MetroCluster, Site_A."

"Foglio di lavoro per la configurazione dell'IP MetroCluster, Site_B."

Analogie e differenze tra cluster standard e configurazioni MetroCluster

La configurazione dei nodi in ciascun cluster in una configurazione MetroCluster è simile a quella dei nodi in un cluster standard.

La configurazione di MetroCluster si basa su due cluster standard. Fisicamente, la configurazione deve essere simmetrica, con ciascun nodo con la stessa configurazione hardware e tutti i componenti MetroCluster devono essere cablati e configurati. Tuttavia, la configurazione software di base per i nodi in una configurazione MetroCluster è uguale a quella per i nodi in un cluster standard.

Fase di configurazione	Configurazione standard del cluster	Configurazione di MetroCluster
Configurare le LIF di gestione, cluster e dati su ciascun nodo.	Lo stesso vale per entrambi i tipi di cluster	
Configurare l'aggregato root.	Lo stesso vale per entrambi i tipi di cluster	
Impostare il cluster su un nodo del cluster.	Lo stesso vale per entrambi i tipi di cluster	
Unire l'altro nodo al cluster.	Lo stesso vale per entrambi i tipi di cluster	
Creare un aggregato root mirrorato.	Opzionale	Obbligatorio
Peer dei cluster.	Opzionale	Obbligatorio
Abilitare la configurazione MetroCluster.	Non applicabile	Obbligatorio

Verifica dello stato ha-config dei componenti

In una configurazione IP MetroCluster non preconfigurata in fabbrica, verificare che lo stato ha-config dei componenti del controller e del telaio sia impostato su "mcip" in modo che si avviino correttamente. Per i sistemi ricevuti dalla fabbrica, questo valore è preconfigurato e non è necessario verificarlo.

Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

Fasi

1. Visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Il modulo controller e lo chassis devono visualizzare il valore "mcip".

2. Se lo stato di sistema visualizzato del controller non è "mccip", impostare lo stato ha per il controller:

   ```
   ha-config modify controller mccip
   ```

3. Se lo stato di sistema visualizzato dello chassis non è "mccip", impostare lo stato ha per lo chassis:

   ```
   ha-config modify chassis mccip
   ```

4. Ripetere questi passaggi su ciascun nodo della configurazione MetroCluster.

Ripristino delle impostazioni predefinite di sistema su un modulo controller

Ripristinare le impostazioni predefinite dei moduli controller.

1. Al prompt DEL CARICATORE, riportare le variabili ambientali alle impostazioni predefinite: `set-defaults`
2. Avviare il nodo dal menu di boot: `boot_ontap menu`

   Dopo aver eseguito questo comando, attendere che venga visualizzato il menu di avvio.

3. Cancellare la configurazione del nodo:

   - Se si utilizzano sistemi configurati per ADP, selezionare l'opzione `9a` dal menu di avvio e rispondere `no` quando richiesto.

     Questo processo è disgregativo.

     La seguente schermata mostra il prompt del menu di avvio:

```
Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a
...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

- Se il sistema non è configurato per ADP, digitare `wipeconfig` Al prompt del menu di avvio, quindi premere Invio.

  La seguente schermata mostra il prompt del menu di avvio:

```
Please choose one of the following:

    (1) Normal Boot.
    (2) Boot without /etc/rc.
    (3) Change password.
    (4) Clean configuration and initialize all disks.
    (5) Maintenance mode boot.
    (6) Update flash from backup config.
    (7) Install new software first.
    (8) Reboot node.
    (9) Configure Advanced Drive Partitioning.
    Selection (1-9)?  wipeconfig
This option deletes critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken over.
Are you sure you want to continue?: yes
Rebooting to finish wipeconfig request.
```

Assegnazione manuale delle unità al pool 0

Se i sistemi preconfigurati non sono stati ricevuti dalla fabbrica, potrebbe essere necessario assegnare manualmente il pool 0 dischi. A seconda del modello di piattaforma e se il sistema utilizza ADP, è necessario assegnare manualmente le unità al pool 0 per ciascun nodo nella configurazione IP di MetroCluster. La procedura da seguire dipende dalla versione di ONTAP in uso.

Assegnazione manuale dei dischi per il pool 0 (ONTAP 9.4 e versioni successive)

Se il sistema non è stato preconfigurato in fabbrica e non soddisfa i requisiti per l'assegnazione automatica del disco, è necessario assegnare manualmente il pool 0 dischi.

A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.4 o versioni successive.

Per determinare se il sistema richiede l'assegnazione manuale del disco, è necessario esaminare "Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive".

Questa procedura viene eseguita in modalità manutenzione. La procedura deve essere eseguita su ciascun nodo della configurazione.

Gli esempi di questa sezione si basano sui seguenti presupposti:

- Node_A_1 e Node_A_2 su:
  - Site_A-shelf_1 (locale)
  - Sito_B-shelf_2 (remoto)
- Node_B_1 e Node_B_2 su:
  - Sito_B-shelf_1 (locale)
  - Site_A-shelf_2 (remoto)

Fasi

1. Visualizzare il menu di avvio:

   ```
   boot_ontap menu
   ```

2. Selezionare l'opzione 9a e rispondere `no` quando richiesto.

   La seguente schermata mostra il prompt del menu di avvio:

```
Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a

...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

3. Al riavvio del nodo, premere Ctrl-C quando richiesto per visualizzare il menu di avvio, quindi selezionare l'opzione **Maintenance mode boot** (Avvio in modalità manutenzione).
4. In modalità Maintenance (manutenzione), assegnare manualmente i dischi per gli aggregati locali sul nodo:

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   I dischi devono essere assegnati simmetricamente, in modo che ogni nodo abbia un numero uguale di dischi. La procedura seguente riguarda una configurazione con due shelf di storage in ogni sito.

   a. Durante la configurazione di Node_A_1, assegnare manualmente le unità dallo slot 0 a 11 al pool 0 del nodo A1 da Site_A-shelf_1.
   b. Durante la configurazione di Node_A_2, assegnare manualmente le unità dallo slot 12 a 23 al pool 0 del nodo A2 da Site_A-shelf_1.

c. Durante la configurazione di Node_B_1, assegnare manualmente le unità dallo slot 0 a 11 al pool 0 del nodo B1 da Site_B-shelf_1.

d. Durante la configurazione di Node_B_2, assegnare manualmente le unità dallo slot 12 a 23 al pool 0 del nodo B2 dal sito_B-shelf_1.

5. Uscire dalla modalità di manutenzione:

```
halt
```

6. Visualizzare il menu di avvio:

```
boot_ontap menu
```

7. Ripetere questa procedura sugli altri nodi nella configurazione IP MetroCluster.
8. Selezionare l'opzione **4** dal menu di boot su entrambi i nodi e lasciare che il sistema si avvii.
9. Passare a. "Configurazione di ONTAP".

Assegnazione manuale delle unità per il pool 0 (ONTAP 9.3)

Se si dispone di almeno due shelf di dischi per ciascun nodo, si utilizza la funzionalità di assegnazione automatica di ONTAP per assegnare automaticamente i dischi locali (pool 0).

A proposito di questa attività

Mentre il nodo è in modalità manutenzione, è necessario assegnare un singolo disco sugli shelf appropriati al pool 0. ONTAP assegna quindi automaticamente il resto dei dischi sullo shelf allo stesso pool. Questa attività non è richiesta sui sistemi ricevuti dalla fabbrica, che hanno il pool 0 per contenere l'aggregato root preconfigurato.

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.3.

Questa procedura non è necessaria se si riceve la configurazione MetroCluster dalla fabbrica. I nodi della fabbrica sono configurati con pool 0 dischi e aggregati root.

Questa procedura può essere utilizzata solo se si dispone di almeno due shelf di dischi per ciascun nodo, che consente l'assegnazione automatica a livello di shelf dei dischi. Se non è possibile utilizzare l'assegnazione automatica a livello di shelf, è necessario assegnare manualmente i dischi locali in modo che ogni nodo disponga di un pool locale di dischi (pool 0).

Questi passaggi devono essere eseguiti in modalità manutenzione.

Gli esempi di questa sezione presuppongono i seguenti shelf di dischi:

- Node_A_1 possiede i dischi su:
  - Site_A-shelf_1 (locale)
  - Sito_B-shelf_2 (remoto)
- Node_A_2 è connesso a:
  - Site_A-shelf_3 (locale)
  - Sito_B-shelf_4 (remoto)
- Node_B_1 è connesso a:
  - Sito_B-shelf_1 (locale)

    - Site_A-shelf_2 (remoto)
- Node_B_2 è connesso a:
    - Sito_B-shelf_3 (locale)
    - Site_A-shelf_4 (remoto)

Fasi

1. Assegnare manualmente un singolo disco per l'aggregato root su ciascun nodo:

   ```
   disk assign disk-id -p 0 -s local-node-sysid
   ```

   L'assegnazione manuale di questi dischi consente alla funzione di assegnazione automatica ONTAP di assegnare il resto dei dischi su ogni shelf.

   a. Sul nodo_A_1, assegnare manualmente un disco dal sito locale_A-shelf_1 al pool 0.
   b. Sul nodo_A_2, assegnare manualmente un disco dal sito locale_A-shelf_3 al pool 0.
   c. Sul nodo_B_1, assegnare manualmente un disco dal sito locale_B-shelf_1 al pool 0.
   d. Sul nodo_B_2, assegnare manualmente un disco dal sito locale_B-shelf_3 al pool 0.
2. Avviare ciascun nodo nel sito A, utilizzando l'opzione 4 del menu di boot:

   Completare questo passaggio su un nodo prima di passare al nodo successivo.

   a. Uscire dalla modalità di manutenzione:

      ```
      halt
      ```

   b. Visualizzare il menu di avvio:

      ```
      boot_ontap menu
      ```

   c. Selezionare l'opzione 4 dal menu di avvio e procedere.
3. Avviare ciascun nodo nel sito B, utilizzando l'opzione 4 del menu di boot:

   Completare questo passaggio su un nodo prima di passare al nodo successivo.

   a. Uscire dalla modalità di manutenzione:

      ```
      halt
      ```

   b. Visualizzare il menu di avvio:

      ```
      boot_ontap menu
      ```

   c. Selezionare l'opzione 4 dal menu di avvio e procedere.

Configurazione di ONTAP

Dopo aver avviato ciascun nodo, viene richiesto di eseguire la configurazione di base del nodo e del cluster. Dopo aver configurato il cluster, tornare alla CLI ONTAP per creare aggregati e creare la configurazione MetroCluster.

Prima di iniziare

- La configurazione MetroCluster deve essere cablata.

Se è necessario eseguire il netboot dei nuovi controller, vedere "Avvio in rete dei nuovi moduli controller".

A proposito di questa attività

Questa attività deve essere eseguita su entrambi i cluster nella configurazione MetroCluster.

Fasi

1. Accendere ciascun nodo nel sito locale, se non è già stato fatto, e lasciare che tutti i nodi si avviino completamente.

   Se il sistema si trova in modalità manutenzione, è necessario eseguire il comando halt per uscire dalla modalità manutenzione, quindi eseguire il comando `boot_ontap` per avviare il sistema e accedere alla configurazione del cluster.

2. Sul primo nodo di ciascun cluster, seguire le istruzioni per configurare il cluster.

   a. Attivare lo strumento AutoSupport seguendo le istruzioni fornite dal sistema.

      L'output dovrebbe essere simile a quanto segue:

```
Welcome to the cluster setup wizard.

    You can enter the following commands at any time:
    "help" or "?" - if you want to have a question clarified,
    "back" - if you want to change previously answered questions, and
    "exit" or "quit" - if you want to quit the cluster setup wizard.
    Any changes you made before quitting will be saved.

    You can return to cluster setup at any time by typing "cluster
setup".
    To accept a default or omit a question, do not enter a value.

    This system will send event messages and periodic reports to
NetApp Technical
    Support. To disable this feature, enter
    autosupport modify -support disable
    within 24 hours.

    Enabling AutoSupport can significantly speed problem
determination and
    resolution should a problem occur on your system.
    For further information on AutoSupport, see:
    http://support.netapp.com/autosupport/

    Type yes to confirm and continue {yes}: yes
.
.
.
```

b. Configurare l’interfaccia di gestione dei nodi rispondendo alle richieste.

   I prompt sono simili ai seguenti:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Creare il cluster rispondendo alle richieste.

   I prompt sono simili ai seguenti:

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
create


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Aggiungere licenze, configurare una SVM di amministrazione cluster e immettere le informazioni DNS rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Abilitare il failover dello storage e configurare il nodo rispondendo alle richieste.

I prompt sono simili ai seguenti:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Completare la configurazione del nodo, ma non creare aggregati di dati.

   Puoi utilizzare ONTAP System Manager puntando il browser web all'indirizzo IP di gestione del cluster (https://172.17.12.153)., Cluster Management)

   "Gestione del cluster con Gestore di sistema (ONTAP 9.7 e versioni precedenti)"

   "Gestore di sistema ONTAP (versione 9.7 e successive)"

g. Configurare il Service Processor (SP):

   "Configurare la rete SP/BMC"

"Utilizza un Service Processor con Gestione di sistema - ONTAP 9.7 e versioni precedenti"

3. Avviare il controller successivo e unirsi al cluster, seguendo le istruzioni.
4. Verificare che i nodi siano configurati in modalità ad alta disponibilità:

   ```
   storage failover show -fields mode
   ```

   In caso contrario, è necessario configurare la modalità ha su ciascun nodo, quindi riavviare i nodi:

   ```
   storage failover modify -mode ha -node localhost
   ```

   Lo stato di configurazione previsto di ha e failover dello storage è il seguente:

   - La modalità HA è configurata ma il failover dello storage non è abilitato.
   - La funzionalità HA Takeover è disattivata.
   - Le interfacce HA sono offline.
   - La modalità HA, il failover dello storage e le interfacce vengono configurati più avanti nel processo.

5. Verificare che siano configurate quattro porte come interconnessioni cluster:

   ```
   network port show
   ```

Le interfacce IP di MetroCluster non sono attualmente configurate e non vengono visualizzate nell'output del comando.

L'esempio seguente mostra due porte del cluster su Node_A_1:

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



Node: node_A_1


Ignore

                                                     Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                     Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false
```

```
e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Ripetere questi passaggi sul cluster partner.

Cosa fare in seguito

Tornare all'interfaccia della riga di comando di ONTAP e completare la configurazione di MetroCluster eseguendo le seguenti operazioni.

Configurazione dei cluster in una configurazione MetroCluster

È necessario eseguire il peer dei cluster, eseguire il mirroring degli aggregati root, creare un aggregato di dati mirrorati e quindi eseguire il comando per implementare le operazioni MetroCluster.

A proposito di questa attività

Prima di correre `metrocluster configure`, La modalità ha e il mirroring DR non sono abilitati e potrebbe essere visualizzato un messaggio di errore relativo a questo comportamento previsto. La modalità ha e il mirroring del DR vengono successivamente attivate quando si esegue il comando `metrocluster configure` per implementare la configurazione.

Disattivazione dell'assegnazione automatica del disco (se si esegue l'assegnazione manuale in ONTAP 9.4)

In ONTAP 9.4, se la configurazione MetroCluster IP ha meno di quattro shelf di storage esterni per sito, è necessario disattivare l'assegnazione automatica dei dischi su tutti i nodi e assegnarli manualmente.

A proposito di questa attività

Questa attività non è richiesta in ONTAP 9.5 e versioni successive.

Questa attività non si applica a un sistema AFF A800 con uno shelf interno e senza shelf esterni.

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

Fasi

1. Disattivare l'assegnazione automatica dei dischi:

   ```
   storage disk option modify -node node_name -autoassign off
   ```

2. È necessario eseguire questo comando su tutti i nodi della configurazione IP MetroCluster.

Verifica dell'assegnazione dei dischi del pool 0

È necessario verificare che i dischi remoti siano visibili ai nodi e che siano stati assegnati correttamente.

A proposito di questa attività

L'assegnazione automatica dipende dal modello di piattaforma del sistema storage e dalla disposizione degli

shelf di dischi.

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

Fasi

1. Verificare che i dischi del pool 0 siano assegnati automaticamente:

   ```
   disk show
   ```

   L'esempio seguente mostra l'output "cluster_A" per un sistema AFF A800 senza shelf esterni.

   Un quarto (8 dischi) è stato assegnato automaticamente a "Node_A_1" e un quarto è stato assegnato automaticamente a "Node_A_2". I dischi rimanenti saranno unità remote (pool 1) per "Node_B_1" e "Node_B_2".

   ```
   cluster_A::*> disk show
                   Usable     Disk      Container           Container
   Disk            Size       Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   ```

```
node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

L’esempio seguente mostra l’output "cluster_B":

```
cluster_B::> disk show
                 Usable     Disk              Container   Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
```

```
node_B_1
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_B_2
node_B_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_B_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_B_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_B_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_B_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_B_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_B_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_B_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_B_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_B_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_B_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_B_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_B_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_B_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_B_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_B_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.

cluster_B::>
```

Peering dei cluster

I cluster nella configurazione di MetroCluster devono essere in una relazione peer in modo da poter comunicare tra loro ed eseguire il mirroring dei dati essenziale per il disaster recovery di MetroCluster.

Informazioni correlate

"Configurazione rapida del peering di cluster e SVM"

"Considerazioni sull'utilizzo di porte dedicate"

"Considerazioni sulla condivisione delle porte dati"

Configurazione delle LIF di intercluster per il peering dei cluster

È necessario creare LIF intercluster sulle porte utilizzate per la comunicazione tra i cluster di partner MetroCluster. È possibile utilizzare porte o porte dedicate che dispongono anche di traffico dati.

Configurazione di LIF intercluster su porte dedicate

È possibile configurare le LIF tra cluster su porte dedicate. In genere, aumenta la larghezza di banda disponibile per il traffico di replica.

Fasi

1. Elencare le porte nel cluster:

   ```
   network port show
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in "cluster01":

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

   `network interface show -fields home-port,curr-port`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra che alle porte "e0e" e "e0f" non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Creare un gruppo di failover per le porte dedicate:

```
network interface failover-groups create -vserver system_SVM -failover-group
failover_group -targets physical_or_logical_ports
```

Nell'esempio seguente vengono assegnate le porte "e0e" e" e0f" al gruppo di failover "cluster01" sul sistema "SVMcluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verificare che il gruppo di failover sia stato creato:

```
network interface failover-groups show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Versione di ONTAP	Comando
9.6 e versioni successive	`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`*

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:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verificare che le LIF dell'intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta "SVMe0e" effettueranno il failover sulla porta "e0f".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         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"

Configurazione delle LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Fasi

1. Elencare le porte nel cluster:

   ```
   network port show
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in "cluster01":

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Creazione di LIF intercluster sulla SVM di sistema:

In 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`*
In 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`*

   Per la sintassi completa dei comandi, vedere la pagina man.

Nell’esempio seguente vengono create le LIF dell’intercluster "cluster01_icl01" e "cluster01_icl02":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell’intercluster siano state create:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell’intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:

`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che i LIF di intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta "e0c" effettueranno il failover sulla porta "e0d".

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         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 possibile utilizzare il comando cluster peer create per creare una relazione peer tra un cluster locale e un cluster remoto. Una volta creata la relazione peer, è possibile eseguire cluster peer create sul cluster remoto per autenticarla nel cluster locale.

A proposito di questa attività

- È necessario aver creato le LIF di intercluster su ogni nodo dei cluster che vengono sottoposti a peering.
- I cluster devono eseguire ONTAP 9.3 o versione successiva.

Fasi

1. Sul cluster di destinazione, creare una relazione peer con il cluster di origine:

   `cluster peer create -generate-passphrase -offer-expiration` *`MM/DD/YYYY HH:MM:SS|1…7days|1…168hours`* `-peer-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Se si specificano entrambi `-generate-passphrase` e. `-peer-addrs`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addrs` 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-addrs` *`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-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters.
        To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

   Inserire la passphrase per la relazione peer quando richiesto.

3. Verificare che la relazione peer del cluster sia stata creata:

   `cluster peer show -instance`

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                  Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Verificare la connettività e lo stato dei nodi nella relazione peer:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                         cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

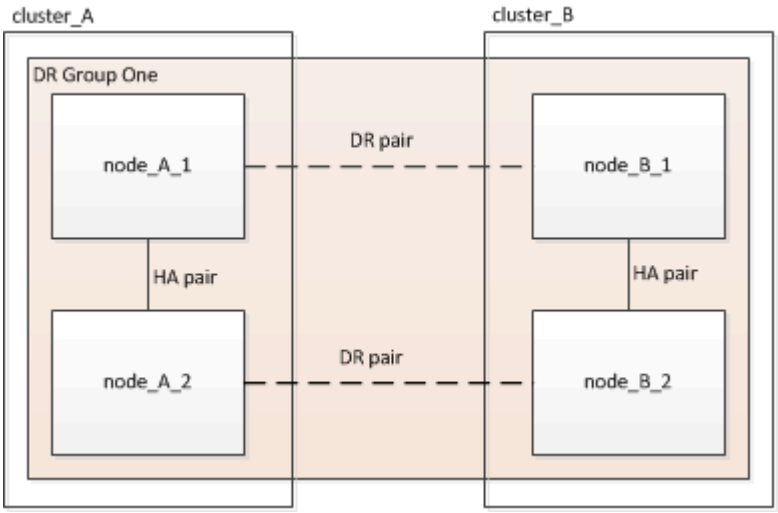
Creazione del gruppo DR

È necessario creare le relazioni del gruppo di disaster recovery (DR) tra i cluster.

A proposito di questa attività

Eseguire questa procedura su uno dei cluster nella configurazione MetroCluster per creare le relazioni di DR tra i nodi di entrambi i cluster.

> Una volta creati i gruppi DR, non è possibile modificare le relazioni di DR.



Fasi

1. Verificare che i nodi siano pronti per la creazione del gruppo DR immettendo il seguente comando su ciascun nodo:

   ```
   metrocluster configuration-settings show-status
   ```

   L'output del comando dovrebbe indicare che i nodi sono pronti:

   ```
   cluster_A::> metrocluster configuration-settings show-status
   Cluster                    Node          Configuration Settings Status
   -------------------------- -------------
   --------------------------------
   cluster_A                  node_A_1      ready for DR group create
                              node_A_2      ready for DR group create
   2 entries were displayed.
   ```

   ```
   cluster_B::> metrocluster configuration-settings show-status
   Cluster                    Node          Configuration Settings Status
   -------------------------- -------------
   --------------------------------
   cluster_B                  node_B_1      ready for DR group create
                              node_B_2      ready for DR group create
   2 entries were displayed.
   ```

2. Creare il gruppo DR:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster partner-
   ```

cluster-name -local-node *local-node-name* -remote-node *remote-node-name*

Questo comando viene emesso una sola volta. Non è necessario ripeterlo sul cluster del partner. Nel comando, specificare il nome del cluster remoto e il nome di un nodo locale e di un nodo del cluster partner.

I due nodi specificati vengono configurati come partner DR e gli altri due nodi (non specificati nel comando) vengono configurati come seconda coppia DR nel gruppo DR. Queste relazioni non possono essere modificate dopo aver immesso questo comando.

Il seguente comando crea queste coppie di DR:

- Node_A_1 e Node_B_1
- Node_A_2 e Node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Configurazione e connessione delle interfacce IP di MetroCluster

È necessario configurare le interfacce IP MetroCluster utilizzate per la replica dello storage e della cache non volatile di ciascun nodo. Le connessioni vengono quindi stabilite utilizzando le interfacce IP di MetroCluster. In questo modo si creano connessioni iSCSI per la replica dello storage.

A proposito di questa attività

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

- È necessario creare due interfacce per ciascun nodo. Le interfacce devono essere associate alle VLAN definite nel file RCF di MetroCluster.
- È necessario creare tutte le porte "A" dell'interfaccia IP MetroCluster nella stessa VLAN e tutte le porte "B" dell'interfaccia IP MetroCluster nell'altra VLAN. Fare riferimento a. "Considerazioni sulla configurazione IP di MetroCluster".

  - Alcune piattaforme utilizzano una VLAN per l'interfaccia IP di MetroCluster. Per impostazione predefinita, ciascuna delle due porte utilizza una VLAN diversa: 10 e 20. È inoltre possibile specificare una VLAN diversa (non predefinita) superiore a 100 (tra 101 e 4095) utilizzando `-vlan-id parameter` in `metrocluster configuration-settings interface create` comando.
  - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".

I seguenti modelli di piattaforma possono essere aggiunti alla configurazione MetroCluster esistente se le VLAN utilizzate sono 10/20 o superiori a 100. Se si utilizzano altre VLAN, queste piattaforme non possono essere aggiunte alla configurazione esistente, in quanto l'interfaccia MetroCluster non può essere configurata. Se si utilizza un'altra piattaforma, la configurazione della VLAN non è rilevante in quanto non è richiesta in ONTAP.

Piattaforme AFF	Piattaforme FAS
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

Negli esempi vengono utilizzati i seguenti indirizzi IP e subnet:

Nodo	Interfaccia	Indirizzo IP	Subnet
Node_A_1	Interfaccia IP MetroCluster 1	10.1.1.1	10.1.1/24
Interfaccia IP MetroCluster 2	10.1.2.1	10.1.2/24	Node_A_2
Interfaccia IP MetroCluster 1	10.1.1.2	10.1.1/24	Interfaccia IP MetroCluster 2
10.1.2.2	10.1.2/24	Node_B_1	Interfaccia IP MetroCluster 1
10.1.1.3	10.1.1/24	Interfaccia IP MetroCluster 2	10.1.2.3
10.1.2/24	Node_B_2	Interfaccia IP MetroCluster 1	10.1.1.4
10.1.1/24	Interfaccia IP MetroCluster 2	10.1.2.4	10.1.2/24

Le porte fisiche utilizzate dalle interfacce IP di MetroCluster dipendono dal modello di piattaforma, come mostrato nella tabella seguente.

Modello di piattaforma	**Porta IP MetroCluster**	**Nota**
AFF A900 e FAS9500	e5b	
e7b	AFF A800	e0b
	e1b	AFF A700 e FAS9000
e5a		e5b
AFF A400	e1a	

Modello di piattaforma	Porta IP MetroCluster	Nota
e1b	AFF A320	ad esempio
	e0h	AFF A300 e FAS8200
e1a		e1b
AFF A220 e FAS2750	e0a	Su questi sistemi, queste porte fisiche vengono utilizzate anche come interfacce cluster.
e0b	AFF A250 e FAS500f	e0c
	e0d	FAS8300 e FAS8700
e1a		e1b

L'utilizzo delle porte nei seguenti esempi riguarda un sistema AFF A700 o FAS9000.

Fasi

1. Verificare che ogni nodo abbia attivato l'assegnazione automatica del disco:

   ```
   storage disk option show
   ```

   L'assegnazione automatica del disco assegnerà i dischi del pool 0 e del pool 1 in base a shelf-by-shelf.

   La colonna Auto Assign (assegnazione automatica) indica se l'assegnazione automatica del disco è attivata.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

2. Verificare che sia possibile creare interfacce IP MetroCluster sui nodi:

   ```
   metrocluster configuration-settings show-status
   ```

   Tutti i nodi devono essere pronti:

```
Cluster       Node          Configuration Settings Status
----------    -----------   ---------------------------------
cluster_A
              node_A_1      ready for interface create
              node_A_2      ready for interface create
cluster_B
              node_B_1      ready for interface create
              node_B_2      ready for interface create
4 entries were displayed.
```

3. Creare le interfacce su Node_A_1.

> - L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
> - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".
> - Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

a. Configurare l'interfaccia sulla porta "e5a" su "Node_A_1":

   `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

   L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "node_A_1" con indirizzo IP "10.1.1.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node_A_1":

   `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

   L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "node_A_1" con indirizzo IP "10.1.2.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

È possibile verificare che queste interfacce siano presenti utilizzando `metrocluster configuration-settings interface show` comando.

4. Creare le interfacce su Node_A_2.

   - L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
   - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".
   - Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

   a. Configurare l'interfaccia sulla porta "e5a" su "Node_A_2":

      `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

      L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "node_A_2" con indirizzo IP "10.1.1.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
10.1.1.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

      Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti. L'esempio seguente mostra il comando per un sistema AFF A220 con un ID VLAN 120:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node_A_2":

   `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

   L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "node_A_2" con indirizzo IP "10.1.2.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
10.1.2.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

   Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti. L'esempio seguente mostra il comando per un sistema AFF A220 con un ID VLAN 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Creare le interfacce su "Node_B_1".

   - L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
   - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".
   - Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

a. Configurare l'interfaccia sulla porta "e5a" su "Node_B_1":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "Node_B_1" con indirizzo IP "10.1.1.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5a -address
10.1.1.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node_B_1":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "Node_B_1" con indirizzo IP "10.1.2.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Creare le interfacce su "Node_B_2".

> - L'utilizzo delle porte negli esempi seguenti riguarda un sistema AFF A700 o FAS9000 (e5a e e5b). È necessario configurare le interfacce sulle porte corrette per il modello di piattaforma, come indicato sopra.
> - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".
> - Sui modelli di piattaforma che supportano le VLAN per l'interfaccia IP di MetroCluster, è possibile includere `-vlan-id` Parametro se non si desidera utilizzare gli ID VLAN predefiniti.

a. Configurare l'interfaccia sulla porta e5a sul nodo_B_2:

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5a" su "Node_B_2" con indirizzo IP "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configurare l'interfaccia sulla porta "e5b" su "Node_B_2":

   `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

   L'esempio seguente mostra la creazione dell'interfaccia sulla porta "e5b" su "Node_B_2" con indirizzo IP "10.1.2.4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Verificare che le interfacce siano state configurate:

   `metrocluster configuration-settings interface show`

   L'esempio seguente mostra che lo stato di configurazione di ciascuna interfaccia è stato completato.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- ---------
----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Verificare che i nodi siano pronti per la connessione alle interfacce MetroCluster:

   `metrocluster configuration-settings show-status`

   L'esempio seguente mostra tutti i nodi nello stato "pronto per la connessione":

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Stabilire le connessioni: `metrocluster configuration-settings connection connect`

   Gli indirizzi IP non possono essere modificati dopo aver eseguito questo comando.

   L'esempio seguente mostra che il cluster_A è connesso correttamente:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Verificare che le connessioni siano state stabilite:

    `metrocluster configuration-settings show-status`

    Lo stato delle impostazioni di configurazione per tutti i nodi deve essere completato:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     completed
              node_A_2     completed
cluster_B
              node_B_1     completed
              node_B_2     completed
4 entries were displayed.
```

11. Verificare che le connessioni iSCSI siano state stabilite:

    a. Passare al livello di privilegio avanzato:

       `set -privilege advanced`

       Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (`*>`).

    b. Visualizzare le connessioni:

       `storage iscsi-initiator show`

       Nei sistemi che eseguono ONTAP 9.5, sono presenti otto iniziatori IP MetroCluster su ciascun cluster che dovrebbero essere visualizzati nell'output.

       Nei sistemi che eseguono ONTAP 9.4 e versioni precedenti, sono presenti quattro iniziatori IP MetroCluster su ciascun cluster che dovrebbero essere visualizzati nell'output.

       L'esempio seguente mostra gli otto iniziatori IP MetroCluster in un cluster che esegue ONTAP 9.5:

```
cluster_A::*> storage iscsi-initiator show
```

```
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
-------------------------------- --------

cluster_A-01
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-aux-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-aux-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-aux-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-pri-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-aux-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
```

```
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-pri-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-pri-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-pri-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

12. Verificare che i nodi siano pronti per l'implementazione finale della configurazione MetroCluster:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_A
              node_A_1           ready to configure -     -
              node_A_2           ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_B
              node_B_1           ready to configure -     -
              node_B_2           ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Verifica o esecuzione manuale dell'assegnazione dei dischi del pool 1

A seconda della configurazione dello storage, è necessario verificare l'assegnazione delle unità del pool 1 o assegnare manualmente le unità al pool 1 per ciascun nodo nella configurazione IP di MetroCluster. La procedura da seguire dipende dalla versione di ONTAP in uso.

Tipo di configurazione	Procedura
I sistemi soddisfano i requisiti per l'assegnazione automatica del disco o, se è in esecuzione ONTAP 9.3, sono stati ricevuti dalla fabbrica.	Verifica dell'assegnazione dei dischi per il pool 1
La configurazione include tre shelf oppure, se contiene più di quattro shelf, presenta un multiplo non uniforme di quattro shelf (ad esempio, sette shelf) e utilizza ONTAP 9.5.	Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)
La configurazione non include quattro shelf di storage per sito e utilizza ONTAP 9.4	Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)
I sistemi non sono stati ricevuti dalla fabbrica e utilizzano ONTAP 9.3i sistemi ricevuti dalla fabbrica sono preconfigurati con i dischi assegnati.	Assegnazione manuale dei dischi per il pool 1 (ONTAP 9.3)

Verifica dell'assegnazione dei dischi per il pool 1

Verificare che i dischi remoti siano visibili ai nodi e che siano stati assegnati correttamente.

Prima di iniziare

Una volta create le interfacce IP MetroCluster e le connessioni con, è necessario attendere almeno dieci minuti per il completamento dell'assegnazione automatica del disco `metrocluster configuration-settings connection connect` comando.

L'output del comando mostra i nomi dei dischi nel formato: Nome-nodo:0m.i1.0L1

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

Fasi

1. Verificare che i dischi del pool 1 siano assegnati automaticamente:

   ```
   disk show
   ```

   Il seguente output mostra l'output di un sistema AFF A800 senza shelf esterni.

   L'assegnazione automatica dei dischi ha assegnato un quarto (8 dischi) a "node_A_1" e un quarto a "node_A_2". I dischi rimanenti saranno dischi remoti (pool 1) per "Node_B_1" e "Node_B_2".

   ```
   cluster_B::> disk show -host-adapter 0m -owner node_B_2
                       Usable     Disk              Container   Container
   Disk                Size       Shelf Bay Type    Type        Name
   ```

```
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_2:0m.i0.2L4  894.0GB    0     29  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L3  894.0GB    0     28  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L9  894.0GB    0     24  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
node_B_2
8 entries were displayed.

cluster_B::> disk show -host-adapter 0m -owner node_B_1
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
node_B_1
node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
```

```
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
```

```
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
```

```
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
```

```
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Assegnazione manuale delle unità per il pool 1 (ONTAP 9.4 o versione successiva)

Se il sistema non è stato preconfigurato in fabbrica e non soddisfa i requisiti per l'assegnazione automatica del disco, è necessario assegnare manualmente i dischi del pool remoto 1.

A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.4 o versioni successive.

I dettagli per determinare se il sistema richiede l'assegnazione manuale del disco sono inclusi nella "Considerazioni sull'assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive".

Quando la configurazione include solo due shelf esterni per sito, il pool di 1 unità per ogni sito deve essere condiviso dallo stesso shelf, come mostrato negli esempi seguenti:

- Node_A_1 è assegnato ai dischi negli alloggiamenti 0-11 del sito_B-shelf_2 (remoto)
- Node_A_2 è assegnato ai dischi negli alloggiamenti 12-23 del sito_B-shelf_2 (remoto)

Fasi

1. Da ciascun nodo della configurazione IP di MetroCluster, assegnare le unità remote al pool 1.

   a. Visualizzare l'elenco delle unità non assegnate:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Assegnare la proprietà dei dischi remoti (0 m) al pool 1 del primo nodo (ad esempio, node_A_1):

   `disk assign -disk` *`disk-id`* `-pool 1 -owner` *`owner-node-name`*

   `disk-id` deve identificare un disco su uno shelf remoto di `owner-node-name`.

c. Verificare che le unità siano state assegnate al pool 1:

   `disk show -host-adapter 0m -container-type unassigned`

   > La connessione iSCSI utilizzata per accedere ai dischi remoti viene visualizzata come dispositivo 0m.

   Il seguente output mostra che i dischi sullo shelf 23 sono stati assegnati perché non compaiono più nell'elenco dei dischi non assegnati:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Ripetere questa procedura per assegnare le unità del pool 1 al secondo nodo sul sito A (ad esempio, "node_A_2").
b. Ripetere questi passaggi sul sito B.

Assegnazione manuale dei dischi per il pool 1 (ONTAP 9.3)

Se si dispone di almeno due shelf di dischi per ciascun nodo, si utilizza la funzionalità di assegnazione automatica di ONTAP per assegnare automaticamente i dischi remoti (pool1).

Prima di iniziare

È necessario assegnare un disco sullo shelf al pool 1. ONTAP assegna quindi automaticamente il resto dei dischi sullo shelf allo stesso pool.

A proposito di questa attività

Questa procedura si applica alle configurazioni che eseguono ONTAP 9.3.

Questa procedura può essere utilizzata solo se si dispone di almeno due shelf di dischi per ciascun nodo, che consente l'assegnazione automatica dei dischi a livello di shelf.

Se non è possibile utilizzare l'assegnazione automatica a livello di shelf, è necessario assegnare manualmente i dischi remoti in modo che ogni nodo disponga di un pool remoto di dischi (pool 1).

La funzione di assegnazione automatica dei dischi di ONTAP assegna i dischi in base allo shelf-by-shelf. Ad esempio:

- Tutti i dischi sul sito_B-shelf_2 vengono assegnati automaticamente al pool 1 del nodo_A_1
- Tutti i dischi sul sito_B-shelf_4 vengono assegnati automaticamente al pool 1 del nodo_A_2
- Tutti i dischi sul sito_A-shelf_2 vengono assegnati automaticamente al pool 1 del nodo_B_1
- Tutti i dischi sul sito_A-shelf_4 vengono assegnati automaticamente al pool 1 del nodo_B_2

È necessario "eseguire il seeding" dell'assegnazione automatica specificando un singolo disco su ogni shelf.

Fasi

1. Da ciascun nodo della configurazione IP MetroCluster, assegnare un disco remoto al pool 1.

   a. Visualizzare l'elenco dei dischi non assegnati:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   ```
   cluster_A::> disk show -host-adapter 0m -container-type unassigned
                        Usable           Disk    Container   Container
   Disk                   Size Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   6.23.0                    -    23   0 SSD     unassigned  -         -
   6.23.1                    -    23   1 SSD     unassigned  -         -
   .
   .
   .
   node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
   node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
   .
   .
   .
   48 entries were displayed.

   cluster_A::>
   ```

   b. Selezionare un disco remoto (0 m) e assegnare la proprietà del disco al pool 1 del primo nodo (ad esempio, "node_A_1"):

   ```
   disk assign -disk disk-id -pool 1 -owner owner-node-name
   ```

   Il `disk-id` deve identificare un disco su uno shelf remoto di `owner-node-name`.

   La funzione di assegnazione automatica dei dischi ONTAP assegna tutti i dischi sullo shelf remoto che contengono il disco specificato.

   c. Dopo aver atteso almeno 60 secondi per l'assegnazione automatica del disco, verificare che i dischi remoti sullo shelf siano stati assegnati automaticamente al pool 1:

   ```
   disk show -host-adapter 0m -container-type unassigned
   ```

   > La connessione iSCSI utilizzata per accedere ai dischi remoti viene visualizzata come periferica 0m.

   Il seguente output mostra che i dischi sullo shelf 23 sono stati assegnati e non vengono più visualizzati:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                      Usable           Disk    Container   Container
Disk                    Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Ripetere questa procedura per assegnare i dischi del pool 1 al secondo nodo del sito A (ad esempio, "node_A_2").

b. Ripetere questi passaggi sul sito B.

Abilitazione dell’assegnazione automatica del disco in ONTAP 9.4

A proposito di questa attività

In ONTAP 9.4, se l’assegnazione automatica del disco è stata disattivata come indicato in precedenza in questa procedura, è necessario riattivarla su tutti i nodi.

"Considerazioni sull’assegnazione automatica dei dischi e sui sistemi ADP in ONTAP 9.4 e versioni successive"

Fasi

1. Abilitare l'assegnazione automatica del disco:

   `storage disk option modify -node node_name -autoassign on`

   Questo comando deve essere inviato a tutti i nodi della configurazione IP MetroCluster.

Mirroring degli aggregati root

È necessario eseguire il mirroring degli aggregati root per garantire la protezione dei dati.

A proposito di questa attività

Per impostazione predefinita, l'aggregato root viene creato come aggregato di tipo RAID-DP. È possibile modificare l'aggregato root da RAID-DP a aggregato di tipo RAID4. Il seguente comando modifica l'aggregato root per l'aggregato di tipo RAID4:

`storage aggregate modify –aggregate aggr_name -raidtype raid4`

> Nei sistemi non ADP, il tipo RAID dell'aggregato può essere modificato dal RAID-DP predefinito a RAID4 prima o dopo il mirroring dell'aggregato.

Fasi

1. Eseguire il mirroring dell'aggregato root:

   `storage aggregate mirror aggr_name`

   Il seguente comando esegue il mirroring dell'aggregato root per "controller_A_1":

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Questo esegue il mirroring dell'aggregato, quindi è costituito da un plex locale e da un plex remoto situati nel sito MetroCluster remoto.

2. Ripetere il passaggio precedente per ciascun nodo della configurazione MetroCluster.

Informazioni correlate

"Gestione dello storage logico"

Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

A proposito di questa attività

- Devi sapere quali dischi verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come assicurarsi di selezionare il tipo di disco corretto.
- I dischi sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi in tale aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale per quell'aggregato.

  Nei sistemi che utilizzano ADP, gli aggregati vengono creati utilizzando partizioni in cui ciascun disco viene

partizionato nelle partizioni P1, P2 e P3.

- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.

  "Gestione di dischi e aggregati"

Fasi

1. Visualizzare un elenco delle parti di ricambio disponibili:

   ```
   storage disk show -spare -owner node_name
   ```

2. Creare l'aggregato:

   ```
   storage aggregate create -mirror true
   ```

   Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su qualsiasi nodo del cluster. Per assicurarsi che l'aggregato venga creato su un nodo specifico, utilizzare `-node` o specificare i dischi di proprietà di quel nodo.

   È possibile specificare le seguenti opzioni:

   - Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
   - Elenco dei dischi specifici da aggiungere all'aggregato
   - Numero di dischi da includere

     > Nella configurazione minima supportata, in cui è disponibile un numero limitato di dischi, è necessario utilizzare l'opzione force-Small-aggregate per consentire la creazione di un aggregato RAID-DP a tre dischi.

   - Stile checksum da utilizzare per l'aggregato
   - Tipo di dischi da utilizzare
   - Dimensioni delle unità da utilizzare
   - Velocità del disco da utilizzare
   - Tipo RAID per i gruppi RAID sull'aggregato
   - Numero massimo di dischi che possono essere inclusi in un gruppo RAID
   - Se sono consentiti dischi con diversi RPM per ulteriori informazioni su queste opzioni, consulta la pagina man di creazione degli aggregati di storage.

     Il seguente comando crea un aggregato mirrorato con 10 dischi:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verificare il gruppo RAID e i dischi del nuovo aggregato:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

Implementazione della configurazione MetroCluster

È necessario eseguire `metrocluster configure` Comando per avviare la protezione dei dati in una configurazione MetroCluster.

A proposito di questa attività

- Su ciascun cluster devono essere presenti almeno due aggregati di dati mirrorati non root.

  È possibile verificarlo con `storage aggregate show` comando.

  > Se si desidera utilizzare un singolo aggregato di dati mirrorato, vedere Fase 1 per istruzioni.

- Lo stato ha-config dei controller e dello chassis deve essere "mccip".

Si emette il `metrocluster configure` Eseguire un comando una volta su uno dei nodi per abilitare la configurazione MetroCluster. Non è necessario eseguire il comando su ciascuno dei siti o nodi e non è importante il nodo o il sito su cui si sceglie di eseguire il comando.

Il `metrocluster configure` Command associa automaticamente i due nodi con gli ID di sistema più bassi in ciascuno dei due cluster come partner di disaster recovery (DR). In una configurazione MetroCluster a quattro nodi, esistono due coppie di partner DR. La seconda coppia di DR viene creata dai due nodi con ID di sistema superiori.

> È necessario **non** configurare Onboard Key Manager (OKM) o la gestione delle chiavi esterne prima di eseguire il comando `metrocluster configure`.

Fasi

1. configurare MetroCluster nel seguente formato:

Se la configurazione di MetroCluster dispone di…	Quindi…
Aggregati di dati multipli	Dal prompt di qualsiasi nodo, configurare MetroCluster: `metrocluster configure` *`node-name`*

Un singolo aggregato di dati mirrorato	a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
	
	`set -privilege advanced`
	
	Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (*).
	
	b. Configurare MetroCluster con `-allow-with -one-aggregate true` parametro:
	
	`metrocluster configure -allow-with -one-aggregate true` *`node-name`*
	
	c. Tornare al livello di privilegio admin:
	
	`set -privilege admin`

La Best practice consiste nell'avere più aggregati di dati. Se il primo gruppo DR dispone di un solo aggregato e si desidera aggiungere un gruppo DR con un aggregato, è necessario spostare il volume di metadati dal singolo aggregato di dati. Per ulteriori informazioni su questa procedura, vedere "Spostamento di un volume di metadati nelle configurazioni MetroCluster".

Il seguente comando abilita la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene "controller_A_1":

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verificare lo stato della rete sul sito A:

   `network port show`

   L'esempio seguente mostra l'utilizzo della porta di rete in una configurazione MetroCluster a quattro nodi:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster.

   a. Verificare la configurazione dal sito A:

   `metrocluster show`

   ```
   cluster_A::> metrocluster show

   Configuration: IP fabric

   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
   Remote: cluster_B         Configuration state configured
                             Mode                normal
   ```

   b. Verificare la configurazione dal sito B:

   `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

4. Per evitare possibili problemi con il mirroring della memoria non volatile, riavviare ciascuno dei quattro nodi:

   `node reboot -node node-name -inhibit-takeover true`

5. Eseguire il `metrocluster show` su entrambi i cluster per verificare nuovamente la configurazione.

Configurazione del secondo gruppo DR in una configurazione a otto nodi

Ripetere le operazioni precedenti per configurare i nodi nel secondo gruppo di DR.

Creazione di aggregati di dati senza mirror

È possibile creare aggregati di dati senza mirroring per i dati che non richiedono il mirroring ridondante fornito dalle configurazioni MetroCluster.

A proposito di questa attività

- È necessario sapere quali dischi o LUN di array verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come verificare che sia selezionato il tipo di disco corretto.

> Nelle configurazioni MetroCluster IP, gli aggregati remoti senza mirror non sono accessibili dopo uno switchover

> Gli aggregati senza mirror devono essere locali rispetto al nodo che li possiede.

- I dischi e le LUN degli array sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi dell'aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale dell'aggregato.
- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.
- *Gestione di dischi e aggregati* contiene ulteriori informazioni sugli aggregati di mirroring.

Fasi

1. Implementazione aggregata senza mirror:

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

2. Verificare che l'assegnazione automatica del disco sia disattivata:

   ```
   disk option show
   ```

3. Installare e cablare gli shelf di dischi che conterranno gli aggregati senza mirror.

   È possibile utilizzare le procedure descritte nella documentazione di installazione e configurazione per la piattaforma e gli shelf di dischi.

   "Documentazione dei sistemi hardware ONTAP"

4. Assegnare manualmente tutti i dischi sul nuovo shelf al nodo appropriato:

   ```
   disk assign -disk disk-id -owner owner-node-name
   ```

5. Creare l'aggregato:

   ```
   storage aggregate create
   ```

   Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su qualsiasi nodo del cluster. Per verificare che l'aggregato sia creato su un nodo specifico, è necessario utilizzare il parametro -node o specificare i dischi di proprietà di quel nodo.

   È inoltre necessario assicurarsi di includere nell'aggregato solo i dischi sullo shelf senza mirror.

   È possibile specificare le seguenti opzioni:

   - Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
   - Elenco di unità o LUN di array specifici da aggiungere all'aggregato
   - Numero di dischi da includere
   - Stile checksum da utilizzare per l'aggregato
   - Tipo di dischi da utilizzare
   - Dimensioni delle unità da utilizzare
   - Velocità del disco da utilizzare
   - Tipo RAID per i gruppi RAID sull'aggregato
   - Numero massimo di unità o LUN di array che possono essere inclusi in un gruppo RAID
   - Se sono consentiti dischi con diversi RPM

     Per ulteriori informazioni su queste opzioni, consulta la pagina man di creazione dell'aggregato di storage.

     Il seguente comando crea un aggregato senza mirror con 10 dischi:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. Verificare il gruppo RAID e i dischi del nuovo aggregato:

   `storage aggregate show-status -aggregate` *`aggregate-name`*

7. Disattiva implementazione aggregata senza mirror:

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

8. Verificare che l'assegnazione automatica del disco sia abilitata:

   `disk option show`

Informazioni correlate

"Gestione di dischi e aggregati"

Verifica della configurazione MetroCluster

È possibile verificare che i componenti e le relazioni nella configurazione di MetroCluster funzionino correttamente.

A proposito di questa attività

Dopo la configurazione iniziale e dopo aver apportato eventuali modifiche alla configurazione MetroCluster, è necessario eseguire un controllo.

È inoltre necessario eseguire un controllo prima di un'operazione di switchover negoziata (pianificata) o di switchback.

Se il `metrocluster check run` il comando viene emesso due volte in un breve periodo di tempo su uno o entrambi i cluster, può verificarsi un conflitto e il comando potrebbe non raccogliere tutti i dati. Successivo `metrocluster check show` i comandi non mostrano l'output previsto.

Fasi

1. Controllare la configurazione:

   `metrocluster check run`

   Il comando viene eseguito come processo in background e potrebbe non essere completato immediatamente.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Visualizzare risultati più dettagliati dal comando di esecuzione del controllo MetroCluster più recente:

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`

   `metrocluster check node show`

   > Il `metrocluster check show` i comandi mostrano i risultati dei più recenti `metrocluster check run` comando. Eseguire sempre il `metrocluster check run` prima di utilizzare `metrocluster check show` i comandi in modo che le informazioni visualizzate siano aggiornate.

   Nell'esempio riportato di seguito viene illustrato il `metrocluster check aggregate show` Output di comando per una configurazione MetroCluster a quattro nodi sana:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58
```

```
Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr2
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_2_aggr1
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_2_aggr2
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
```

```
                                                        ownership-state
ok

18 entries were displayed.
```

L'esempio seguente mostra l'output del comando show del cluster di controllo MetroCluster per una configurazione MetroCluster a quattro nodi sana. Indica che i cluster sono pronti per eseguire uno switchover negoziato, se necessario.

```
Last Checked On: 9/13/2017 20:47:04

Cluster                 Check                            Result
--------------------- -------------------------------- ---------
mccint-fas9000-0102
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
mccint-fas9000-0304
                        negotiated-switchover-ready     not-applicable
                        switchback-ready                not-applicable
                        job-schedules                   ok
                        licenses                        ok
                        periodic-check-enabled          ok
10 entries were displayed.
```

Informazioni correlate

"Gestione di dischi e aggregati"

"Gestione di rete e LIF"

Completamento della configurazione ONTAP

Dopo aver configurato, attivato e verificato la configurazione MetroCluster, è possibile completare la configurazione del cluster aggiungendo ulteriori SVM, interfacce di rete e altre funzionalità ONTAP in base alle necessità.

Verifica dello switchover, della riparazione e dello switchback

Fase

1. Utilizzare le procedure per lo switchover negoziato, la riparazione e lo switchback menzionate nella *Guida alla gestione e al disaster recovery di MetroCluster*.

   "Gestione MetroCluster e disaster recovery"

Configurazione del software MetroCluster Tiebreaker o ONTAP Mediator

È possibile scaricare e installare su un terzo sito il software MetroCluster Tiebreaker o, a partire da ONTAP 9.7, il ONTAP Mediator.

Prima di iniziare

È necessario disporre di un host Linux dotato di connettività di rete per entrambi i cluster nella configurazione MetroCluster. I requisiti specifici sono contenuti nella documentazione di MetroCluster Tiebreaker o ONTAP Mediator.

Se si effettua la connessione a un'istanza di Tiebreaker o ONTAP Mediator esistente, è necessario disporre del nome utente, della password e dell'indirizzo IP del servizio di spareggio o mediatore.

Se è necessario installare una nuova istanza di ONTAP Mediator, seguire le istruzioni per installare e configurare il software.

"Configurazione del servizio ONTAP Mediator per lo switchover automatico non pianificato"

Se è necessario installare una nuova istanza del software Tiebreaker, seguire la "istruzioni per installare e configurare il software".

A proposito di questa attività

Non è possibile utilizzare sia il software MetroCluster Tiebreaker che il mediatore ONTAP con la stessa configurazione MetroCluster.

"Considerazioni sull'utilizzo di ONTAP Mediator o MetroCluster Tiebreaker"

Fase

1. Configurare il servizio ONTAP Mediator o il software Tiebreaker:
   - Se si utilizza un'istanza esistente del mediatore ONTAP, aggiungere il servizio del mediatore ONTAP a ONTAP:

     ```
     metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
     ```

   - Se si utilizza il software Tiebreaker, fare riferimento a. "Documentazione di Tiebreaker".

Protezione dei file di backup della configurazione

È possibile fornire una protezione aggiuntiva per i file di backup della configurazione del cluster specificando un URL remoto (HTTP o FTP) in cui verranno caricati i file di backup della configurazione oltre alle posizioni predefinite nel cluster locale.

Fase

1. Impostare l'URL della destinazione remota per i file di backup della configurazione:

   ```
   system configuration backup settings modify URL-of-destination
   ```

Il "Gestione dei cluster con la CLI" Contiene ulteriori informazioni nella sezione *Gestione dei backup di configurazione*.

Configurare il servizio ONTAP Mediator per lo switchover automatico non pianificato

Preparare l'installazione del servizio ONTAP Mediator

L'ambiente deve soddisfare determinati requisiti.

I seguenti requisiti si applicano a un gruppo di disaster recovery (gruppo di DR). Scopri di più "Gruppi DR".

- Se si prevede di aggiornare la versione di Linux, eseguire questa operazione prima di installare il servizio ONTAP Mediator più recente.
- Il servizio ONTAP Mediator e il software MetroCluster Tiebreaker non devono essere utilizzati con la stessa configurazione MetroCluster.
- Il supporto ONTAP deve essere installato su un host LINUX in una posizione separata dai siti MetroCluster.

  La connettività tra il mediatore ONTAP e ciascun sito deve essere composta da due domini di guasto separati.

- Il servizio ONTAP può supportare fino a cinque configurazioni MetroCluster contemporaneamente.
- Lo switchover automatico non pianificato è supportato in ONTAP 9.7 e versioni successive.

Requisiti di rete per l'utilizzo di Mediator in una configurazione MetroCluster

Per installare il servizio ONTAP Mediator in una configurazione MetroCluster, è necessario assicurarsi che la configurazione soddisfi diversi requisiti di rete.

- Latenza

  Latenza massima inferiore a 75 ms (RTT).

  Il jitter non deve superare i 5 ms.

- MTU

  La dimensione MTU deve essere di almeno 1400.

- Perdita di pacchetti

  Per il traffico ICMP (Internet Control message Protocol) e TCP, la perdita di pacchetti deve essere inferiore al 0.01%.

- Larghezza di banda

  Il collegamento tra il servizio Mediator e un gruppo DR deve avere almeno 20 Mbps di larghezza di banda.

- Connettività indipendente

  È necessaria una connettività indipendente tra ciascun sito e il mediatore ONTAP. Un guasto in un sito non deve interrompere la connettività IP tra gli altri due siti non interessati.

Requisiti dell'host per il mediatore ONTAP in una configurazione MetroCluster

È necessario assicurarsi che la configurazione soddisfi diversi requisiti dell'host.

- ONTAP Mediator deve essere installato in un sito esterno fisicamente separato dai due cluster ONTAP.
- Il mediatore ONTAP supporta un numero massimo di cinque configurazioni MetroCluster.
- Il mediatore ONTAP non richiede requisiti superiori a quelli minimi del sistema operativo host per CPU e memoria (RAM).
- Oltre ai requisiti minimi del sistema operativo host, devono essere disponibili almeno 30 GB di spazio su disco utilizzabile aggiuntivo.
  - Ogni gruppo di DR richiede fino a 200 MB di spazio su disco.

Requisiti del firewall per ONTAP Mediator

Il mediatore ONTAP utilizza una serie di porte per comunicare con servizi specifici.

Se si utilizza un firewall di terze parti:

- L'accesso HTTPS deve essere attivato.
- Deve essere configurato per consentire l'accesso alle porte 31784 e 3260.

  Quando si utilizza il firewall predefinito Red Hat o CentOS, il firewall viene configurato automaticamente durante l'installazione di Mediator.

La tabella seguente elenca le porte che è necessario consentire nel firewall:

> La porta iSCSI è richiesta solo in una configurazione IP MetroCluster.

Porta/servizi	Origine	Destinazione	Scopo
31784/tcp	Interfacce di gestione del cluster ONTAP	Server web di ONTAP Mediator	API REST (HTTPS)
3260/tcp	Cluster ONTAP (LIF per la gestione dei dati o LIF per la gestione dei dati)	Target iSCSI del mediatore ONTAP	Connessione dati iSCSI per caselle postali

Linee guida per l'aggiornamento del mediatore ONTAP in una configurazione MetroCluster

Se si sta aggiornando il mediatore ONTAP, è necessario soddisfare i requisiti della versione Linux e seguire le linee guida per l'aggiornamento.

- Il servizio Mediator può essere aggiornato da una versione immediatamente precedente alla versione corrente.
- Tutte le versioni di Mediator sono supportate nelle configurazioni MetroCluster IP con ONTAP 9.7 o versioni successive.

"Installare o aggiornare il servizio di supporto ONTAP"

Dopo l'aggiornamento

Una volta completato l'aggiornamento di Mediator e del sistema operativo, eseguire il `storage iscsi-initiator show` Per confermare che le connessioni del Mediator sono attive.

Configurare il servizio ONTAP Mediator da una configurazione IP MetroCluster

Il servizio ONTAP Mediator deve essere configurato sul nodo ONTAP per essere utilizzato in una configurazione IP MetroCluster.

Prima di iniziare

- Il mediatore ONTAP deve essere stato installato correttamente in una posizione di rete raggiungibile da entrambi i siti MetroCluster.

  "Installare o aggiornare il servizio di supporto ONTAP"

- È necessario disporre dell'indirizzo IP dell'host che esegue il servizio ONTAP Mediator.
- È necessario disporre del nome utente e della password per il servizio di supporto ONTAP.
- Tutti i nodi della configurazione IP di MetroCluster devono essere in linea.

> A partire da ONTAP 9.12.1, è possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster. Questa funzione è un'estensione dello switchover non pianificato assistito dal mediatore. Prima di attivare questa funzione, consultare la "Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster".

A proposito di questa attività

- Questa attività attiva lo switchover automatico non pianificato per impostazione predefinita.
- Questa attività può essere eseguita sull'interfaccia ONTAP di qualsiasi nodo della configurazione IP di MetroCluster.
- Una singola installazione del servizio ONTAP può essere configurata con un massimo di cinque configurazioni IP MetroCluster.

Fasi

1. Aggiungere il servizio ONTAP Mediator a ONTAP:

   `metrocluster configuration-settings mediator add -mediator-address` *`ip-address-of-mediator-host`*

   > Verranno richiesti nome utente e password per l'account utente amministratore di Mediator.

2. Verificare che la funzione di switchover automatico sia attivata:

   `metrocluster show`

3. Verificare che Mediator sia in esecuzione.

   a. Mostra i dischi virtuali di Mediator:

      `storage disk show -container-type mediator`

```
 cluster_A::> storage disk show -container-type mediator
                        Usable           Disk    Container
Container
 Disk                   Size Shelf Bay Type    Type        Name
Owner
 ---------------- ---------- ----- --- ------- ----------- ---------
--------
 NET-1.5                   -     -   - VMDISK  mediator    -
node_A_2
 NET-1.6                   -     -   - VMDISK  mediator    -
node_B_1
 NET-1.7                   -     -   - VMDISK  mediator    -
node_B_2
 NET-1.8                   -     -   - VMDISK  mediator    -
node_A_1
```

b. Impostare la modalità dei privilegi su Advanced (avanzata):

```
set advanced
```

```
 cluster_A::> set advanced
```

c. Visualizzare gli iniziatori etichettati come mediatore:

```
storage iscsi-initiator show -label mediator
```

```
 cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
--------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

d. Verificare lo stato del dominio dell'errore di switchover non pianificato automatico (AURO):

```
metrocluster show
```

> L'output di esempio riportato di seguito è valido per ONTAP 9.13.1 e versioni successive. Per ONTAP 9.12.1 e versioni precedenti, lo stato del dominio di errore AUSO dovrebbe essere `auso-on-cluster-disaster`.

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

4. In alternativa, configurare lo switchover forzato automatico MetroCluster.

È possibile utilizzare il seguente comando solo a livello di privilegi avanzati.

> Prima di utilizzare questo comando, rivedere la "Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster".

```
metrocluster modify -allow-auto-forced-switchover true
```

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

Disconfigurare il servizio ONTAP Mediator dalla configurazione IP di MetroCluster

È possibile annullare la configurazione del servizio ONTAP Mediator dalla configurazione IP di MetroCluster.

Prima di iniziare

È necessario aver installato e configurato correttamente il mediatore ONTAP in una posizione di rete raggiungibile da entrambi i siti MetroCluster.

Fasi

1. Per annullare la configurazione del servizio ONTAP Mediator, utilizzare il seguente comando:

   `metrocluster configuration-settings mediator remove`

   Vengono richiesti il nome utente e la password per l'account utente admin di ONTAP Mediator.

   > Se il mediatore ONTAP non è attivo, il `metrocluster configuration-settings mediator remove` Il comando richiede comunque di inserire il nome utente e la password per l'account utente amministratore di ONTAP Mediator e rimuove il servizio ONTAP Mediator dalla configurazione MetroCluster.

   a. Controllare se sono presenti dischi rotti utilizzando il seguente comando:

      `disk show -broken`

      Esempio

```
There are no entries matching your query.
```

2. Verificare che il servizio ONTAP Mediator sia stato rimosso dalla configurazione MetroCluster eseguendo i seguenti comandi su entrambi i cluster:

   a. `metrocluster configuration-settings mediator show`

      Esempio

```
This table is currently empty.
```

   b. `storage iscsi-initiator show -label mediator`

      Esempio

```
There are no entries matching your query.
```

Connessione di una configurazione MetroCluster a un'istanza diversa di ONTAP Mediator

Se si desidera connettere i nodi MetroCluster a un'altra istanza di ONTAP Mediator, è necessario disconfigurare e riconfigurare la connessione nel software ONTAP.

Prima di iniziare

Sono necessari il nome utente, la password e l'indirizzo IP della nuova istanza di ONTAP Mediator.

A proposito di questa attività

Questi comandi possono essere emessi da qualsiasi nodo della configurazione MetroCluster.

Fasi

1. Rimuovere il mediatore ONTAP corrente dalla configurazione MetroCluster:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Stabilire la nuova connessione del mediatore ONTAP alla configurazione MetroCluster:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

In che modo il mediatore ONTAP supporta lo switchover automatico non pianificato

ONTAP Mediator fornisce i LUN delle cassette postali per memorizzare le informazioni sullo stato dei nodi IP di MetroCluster. Queste LUN sono in co-location con il mediatore ONTAP, che viene eseguito su un host Linux fisicamente separato dai siti MetroCluster. I nodi IP di MetroCluster possono utilizzare le informazioni della cassetta postale per monitorare lo stato dei partner di disaster recovery (DR) e implementare uno switchover non pianificato assistito da Mediator (MAUSO) in caso di emergenza.

> MAUSO non è supportato nelle configurazioni MetroCluster FC.

Quando un nodo rileva un guasto di un sito che richiede uno switchover, prende le misure necessarie per confermare che lo switchover è appropriato e, in tal caso, esegue lo switchover. Per impostazione predefinita, viene avviato un MAUSO per i seguenti scenari:

- Il mirroring SyncMirror e il mirroring DR della cache non volatile di ciascun nodo sono in funzione e le cache e i mirror vengono sincronizzati al momento dell'errore.
- Nessuno dei nodi nel sito sopravvissuto è in stato di Takeover.
- In caso di disastro del sito. Un disastro del sito è un errore di *tutti* nodi nello stesso sito.

Un MAUSO viene *non* avviato nei seguenti scenari di arresto:

- Si avvia un arresto. Ad esempio, quando:
  - Arrestare i nodi
  - Riavviare i nodi

Informazioni sulle funzioni MAUSO disponibili in ogni versione di ONTAP 9.

A partire da…	Descrizione
ONTAP 9.13.1	• Un MAUSO viene avviato se un scenario predefinito si verifica e un guasto della ventola o dell'hardware avvia un arresto ambientale. Esempi di guasti hardware includono una temperatura alta o bassa, o un'unità di alimentazione, una batteria NVRAM o un guasto heartbeat del Service Processor. • Il valore predefinito per il dominio di errore è impostato su "auso-on-dr-group" in una configurazione IP di MetroCluster. Per ONTAP 9.12.1 e versioni precedenti, il valore predefinito è impostato su "auso-on-cluster-disaster". In una configurazione IP MetroCluster a otto nodi, "auso-on-dr-group" attiva un MAUSO in caso di errore del cluster o di coppia ha in un gruppo di DR. Per una coppia ha, entrambi i nodi devono guastarsi allo stesso tempo. In alternativa, è possibile modificare l'impostazione del dominio di errore nel dominio "auso-on-cluster-disaster" utilizzando `metrocluster modify -auto-switchover -failure-domain auso-on-cluster-disaster` Comando che attiva un MAUSO solo in presenza di errori nella coppia di nodi ha in entrambi i gruppi di DR. • È possibile modificare il comportamento per forzare un MAUSO anche se la NVRAM non è sincronizzata al momento dell'errore.
ONTAP 9.12.1	È possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster utilizzando il `metrocluster modify -allow-auto -forced-switchover true` comando. Lo switchover al rilevamento di un guasto di un sito avviene automaticamente quando si attiva la funzione di switchover forzato automatico di MetroCluster. È possibile utilizzare questa funzione per integrare la funzionalità di switchover automatico di MetroCluster IP. **Rischi e limitazioni dell'utilizzo dello switchover forzato automatico di MetroCluster** Quando si consente a una configurazione IP di MetroCluster di funzionare in modalità di switchover forzato automatico, il seguente problema noto potrebbe causare la perdita di dati: • La memoria non volatile negli storage controller non viene mirrorati sul partner di DR remoto sul sito partner, **Attenzione**: Si potrebbero incontrare scenari non menzionati. NetApp non è responsabile di eventuali danneggiamenti dei dati, perdite di dati o altri danni che potrebbero derivare dall'attivazione della funzione di switchover automatico forzato di MetroCluster. Non utilizzare la funzione di switchover forzato automatico di MetroCluster se i rischi e le limitazioni non sono accettabili per l'utente.

Test della configurazione MetroCluster

È possibile verificare gli scenari di errore per confermare il corretto funzionamento della configurazione MetroCluster.

Verifica dello switchover negoziato

È possibile testare l'operazione di switchover negoziata (pianificata) per confermare la disponibilità ininterrotta dei dati.

A proposito di questa attività

Questo test verifica che la disponibilità dei dati non sia interessata (ad eccezione dei protocolli SMB (Server message Block) di Microsoft e Fibre Channel di Solaris) passando il cluster al secondo data center.

Questo test dovrebbe richiedere circa 30 minuti.

Questa procedura ha i seguenti risultati attesi:

- Il `metrocluster switchover` viene visualizzato un messaggio di avviso.

  Se rispondi `yes` al prompt, il sito da cui viene inviato il comando passerà al sito del partner.

Per le configurazioni MetroCluster IP:

- Per ONTAP 9.4 e versioni precedenti:
  - Gli aggregati mirrorati diventeranno degradati dopo lo switchover negoziato.
- Per ONTAP 9.5 e versioni successive:
  - Gli aggregati mirrorati rimarranno in stato normale se lo storage remoto è accessibile.
  - In caso di perdita dell'accesso allo storage remoto, gli aggregati mirrorati diventeranno degradati dopo lo switchover negoziato.
- Per ONTAP 9.8 e versioni successive:
  - Gli aggregati senza mirror che si trovano nel sito di disastro non saranno più disponibili in caso di perdita dell'accesso allo storage remoto. Questo potrebbe causare un'interruzione del controller.

Fasi

1. Verificare che tutti i nodi si trovino nello stato configurato e nella modalità normale:

   `metrocluster node show`

   ```
   cluster_A::>  metrocluster node show

   Cluster                         Configuration State    Mode
   ------------------------------- ----------------------
   ------------------------
    Local: cluster_A                configured             normal
   Remote: cluster_B                configured             normal
   ```

2. Avviare l'operazione di switchover:

   `metrocluster switchover`

```
cluster_A::> metrocluster switchover
Warning: negotiated switchover is about to start. It will stop all the
data Vservers on cluster "cluster_B" and
automatically re-start them on cluster "cluster_A". It will finally
gracefully shutdown cluster "cluster_B".
```

3. Verificare che il cluster locale si trovi nello stato configurato e nella modalità di switchover:

   `metrocluster node show`

```
cluster_A::>  metrocluster node show

Cluster                         Configuration State    Mode
------------------------------- ----------------------
------------------------
Local: cluster_A                 configured             switchover
Remote: cluster_B                not-reachable          -
              configured             normal
```

4. Verificare che l'operazione di switchover sia stata eseguita correttamente:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Utilizzare `vserver show` e. `network interface show` Comandi per verificare che le SVM DR e le LIF siano online.

Verifica della riparazione e dello switchback manuale

È possibile testare le operazioni di riparazione e switchback manuale per verificare che la disponibilità dei dati non sia compromessa (ad eccezione delle configurazioni SMB e Solaris FC), ripristinando il cluster al data center originale dopo uno switchover negoziato.

A proposito di questa attività

Questo test dovrebbe richiedere circa 30 minuti.

Il risultato previsto di questa procedura è che i servizi devono essere ripristinati nei nodi domestici.

I passaggi di riparazione non sono richiesti nei sistemi che eseguono ONTAP 9.5 o versioni successive, sui quali la riparazione viene eseguita automaticamente dopo uno switchover negoziato. Nei sistemi che eseguono ONTAP 9.6 e versioni successive, la riparazione viene eseguita automaticamente anche dopo uno switchover non pianificato.

Fasi

1. Se sul sistema è in esecuzione ONTAP 9.4 o versioni precedenti, riparare l'aggregato di dati:

   `metrocluster heal aggregates`

   L'esempio seguente mostra il completamento corretto del comando:

   ```
   cluster_A::> metrocluster heal aggregates
   [Job 936] Job succeeded: Heal Aggregates is successful.
   ```

2. Se sul sistema è in esecuzione ONTAP 9.4 o versioni precedenti, riparare l'aggregato root:

   `metrocluster heal root-aggregates`

   Questo passaggio è necessario per le seguenti configurazioni:

   - Configurazioni MetroCluster FC.
   - Configurazioni IP di MetroCluster con ONTAP 9.4 o versioni precedenti. L'esempio seguente mostra il completamento corretto del comando:

   ```
   cluster_A::> metrocluster heal root-aggregates
   [Job 937] Job succeeded: Heal Root Aggregates is successful.
   ```

3. Verificare che la riparazione sia completata:

   `metrocluster node show`

   L'esempio seguente mostra il completamento corretto del comando:

   ```
   cluster_A::> metrocluster node show
   DR                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   heal roots
   completed
         cluster_B
                 node_B_2         unreachable    -         switched over
   42 entries were displayed.metrocluster operation show
   ```

   Se l'operazione di riparazione automatica non riesce per qualsiasi motivo, è necessario eseguire il

`metrocluster heal` Comandi manuali come nelle versioni di ONTAP precedenti a ONTAP 9.5. È possibile utilizzare `metrocluster operation show` e. `metrocluster operation history show -instance` comandi per monitorare lo stato di riparazione e determinare la causa di un errore.

4. Verificare che tutti gli aggregati siano mirrorati:

   `storage aggregate show`

   L'esempio seguente mostra che tutti gli aggregati hanno uno stato RAID di mirrored:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

5. Controllare lo stato del ripristino dello switchback:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              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.
```

6. Eseguire lo switchback:

   `metrocluster switchback`

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

7. Confermare lo stato dei nodi:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
             node_A_1         configured     enabled   normal
      cluster_B
             node_B_2         configured     enabled   normal

2 entries were displayed.
```

8. Confermare lo stato dell'operazione MetroCluster:

   `metrocluster operation show`

   L'output dovrebbe mostrare uno stato di successo.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Verifica del funzionamento in seguito a interruzione della linea di alimentazione

È possibile verificare la risposta della configurazione MetroCluster in caso di errore di una PDU.

A proposito di questa attività

La procedura consigliata consiste nel collegare ciascun alimentatore di un componente a alimentatori separati. Se entrambe le PSU sono collegate alla stessa unità di distribuzione dell'alimentazione (PDU) e si verifica un'interruzione dell'alimentazione elettrica, il sito potrebbe non essere operativo o uno shelf completo potrebbe non essere disponibile. Il guasto di una linea di alimentazione viene testato per verificare che non vi siano incongruenze nel cablaggio che potrebbero causare un'interruzione del servizio.

Questo test dovrebbe richiedere circa 15 minuti.

Questo test richiede lo spegnimento di tutte le PDU di sinistra e quindi di tutte le PDU di destra su tutti i rack contenenti i componenti MetroCluster.

Questa procedura ha i seguenti risultati attesi:

- Gli errori devono essere generati quando le PDU sono disconnesse.
- Non devono verificarsi failover o perdita di servizio.

Fasi

1. Spegnere le PDU sul lato sinistro del rack contenente i componenti MetroCluster.
2. Monitorare il risultato sulla console:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Riaccendere le PDU di sinistra.
4. Assicurarsi che ONTAP cancella la condizione di errore.
5. Ripetere i passaggi precedenti con le PDU di destra.

Verifica del funzionamento dopo la perdita di un singolo shelf di storage

È possibile verificare il guasto di un singolo shelf di storage per verificare che non vi sia un singolo punto di errore.

A proposito di questa attività

Questa procedura ha i seguenti risultati attesi:

- Il software di monitoraggio dovrebbe segnalare un messaggio di errore.
- Non devono verificarsi failover o perdita di servizio.
- La risincronizzazione del mirror viene avviata automaticamente dopo il ripristino dell'errore hardware.

Fasi

1. Controllare lo stato di failover dello storage:

   ```
   storage failover show
   ```

   ```
   cluster_A::> storage failover show

   Node           Partner        Possible State Description
   -------------- -------------- --------
   ------------------------------------
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Controllare lo stato dell'aggregato:

   ```
   storage aggregate show
   ```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Verificare che tutti gli SVM e i volumi di dati siano online e che servano i dati:

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identificare uno shelf nel Pool 1 per il nodo "node_A_2" da spegnere per simulare un guasto hardware improvviso:

`storage aggregate show -r -node node-name !*root`

Lo shelf selezionato deve contenere dischi che fanno parte di un aggregato di dati mirrorati.

Nell'esempio seguente, l'ID dello shelf "31" è stato selezionato per non riuscire.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                       0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                       0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                       1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                       1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.3                       1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                       1   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     1.31.5                       1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                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. Spegnere fisicamente lo shelf selezionato.
6. Controllare di nuovo lo stato dell'aggregato:

   ```
   storage aggregate show

   storage aggregate show -r -node node_A_2 !*root
   ```

   L'aggregato con i dischi sullo shelf spento dovrebbe avere uno stato RAID "degradato" e i dischi sul plex interessato dovrebbero avere uno stato "guasto", come mostrato nell'esempio seguente:

   ```
   cluster_A::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1data01_mirrored
               4.15TB    3.40TB   18% online       3 node_A_1
   raid_dp,
   ```

```
mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                       0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                       0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.6                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                       0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                       -   -          -  827.7GB
-  (failed)
     parity   FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)
     data     FAILED                       -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Verificare che i dati siano stati forniti e che tutti i volumi siano ancora online:

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Accendere fisicamente lo shelf.

   La risincronizzazione viene avviata automaticamente.

9. Verificare che la risincronizzazione sia stata avviata:

   ```
   storage aggregate show
   ```

   L'aggregato interessato deve avere uno stato RAID di "risyncing", come mostrato nell'esempio seguente:

   ```
   cluster_A::> storage aggregate show
   cluster Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1_data01_mirrored
              4.15TB    3.40TB   18% online       3 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_1_root
             707.7GB   34.29GB   95% online       1 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_2_data01_mirrored
              4.15TB    4.12TB    1% online       2 node_A_2
   raid_dp,

   resyncing
   node_A_2_data02_unmirrored
              2.18TB    2.18TB    0% online       1 node_A_2
   raid_dp,

   normal
   node_A_2_root
             707.7GB   34.27GB   95% online       1 node_A_2
   raid_dp,

   resyncing
   ```

10. Monitorare l'aggregato per confermare che la risincronizzazione è completa:

    ```
    storage aggregate show
    ```

    L'aggregato interessato deve avere uno stato RAID "normale", come mostrato nell'esempio seguente:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

Considerazioni sulla rimozione delle configurazioni MetroCluster

Dopo aver rimosso la configurazione MetroCluster, tutte le interconnessioni e la connettività dei dischi devono essere regolate in modo da essere supportate. Per rimuovere la configurazione MetroCluster, contattare il supporto tecnico.

Non è possibile annullare la configurazione di MetroCluster. Questo processo deve essere eseguito solo con l'assistenza del supporto tecnico. Contattare il supporto tecnico NetApp e consultare la guida appropriata per la configurazione dal "Come rimuovere i nodi da una configurazione MetroCluster - Guida alla risoluzione."

Considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster

Quando si utilizza ONTAP in una configurazione MetroCluster, è necessario tenere presente alcune considerazioni relative a licenze, peering ai cluster al di fuori della configurazione MetroCluster, esecuzione di operazioni sui volumi, operazioni NVFAIL e altre operazioni ONTAP.

La configurazione ONTAP dei due cluster, inclusa la rete, deve essere identica, perché la funzionalità MetroCluster si basa sulla capacità di un cluster di fornire dati perfettamente al partner in caso di switchover.

Considerazioni sulle licenze

- Entrambi i siti devono essere concessi in licenza per le stesse funzionalità concesse in licenza al sito.
- Tutti i nodi devono essere concessi in licenza per le stesse funzioni bloccate dal nodo.

Considerazione di SnapMirror

- Il disaster recovery di SnapMirror SVM è supportato solo nelle configurazioni MetroCluster con versioni di ONTAP 9.5 o successive.

Operazioni MetroCluster in Gestore di sistema ONTAP

A seconda della versione di ONTAP in uso, è possibile eseguire alcune operazioni specifiche di MetroCluster utilizzando Gestione di sistema di ONTAP.

Per ulteriori informazioni, fare riferimento alla "Gestire i siti MetroCluster con Gestione di sistema" documentazione.

Supporto di FlexCache in una configurazione MetroCluster

A partire da ONTAP 9.7, i volumi FlexCache sono supportati nelle configurazioni MetroCluster. È necessario conoscere i requisiti per l'abrogazione manuale dopo le operazioni di switchover o switchback.

Annullamento della SVM dopo lo switchover quando l'origine e la cache di FlexCache si trovano all'interno dello stesso sito MetroCluster

Dopo uno switchover negoziato o non pianificato, qualsiasi relazione di peering SVM FlexCache all'interno del cluster deve essere configurata manualmente.

Ad esempio, le SVM vs1 (cache) e vs2 (origine) si trovano sul sito_A. Questi SVM sono in peering.

Dopo lo switchover, le SVM vs1-mc e vs2-mc vengono attivate presso il sito del partner (Site_B). Devono essere revocati manualmente perché FlexCache funzioni utilizzando il comando di annullamento peer vserver.

Annullamento della SVM dopo lo switchover o lo switchback quando una destinazione FlexCache si trova su un terzo cluster e in modalità disconnessa

Per le relazioni FlexCache con un cluster al di fuori della configurazione MetroCluster, il peering deve sempre essere riconfigurato manualmente dopo uno switchover se i cluster coinvolti sono in modalità disconnessa durante lo switchover.

Ad esempio:

- Un'estremità del FlexCache (cache_1 su vs1) risiede nel sito MetroCluster_A ha un'estremità del FlexCache
- L'altra estremità del FlexCache (origin_1 su vs2) risiede sul sito_C (non nella configurazione MetroCluster)

Quando viene attivato lo switchover e se Site_A e Site_C non sono connessi, è necessario revocare manualmente le SVM sul sito_B (il cluster di switchover) e sul sito_C utilizzando il comando di peer repeer del vserver dopo lo switchover.

Quando viene eseguito lo switchback, è necessario revocare nuovamente le SVM sul sito_A (il cluster originale) e sul sito_C.

Informazioni correlate

"Gestione dei volumi FlexCache con l'interfaccia CLI"

Supporto FabricPool nelle configurazioni MetroCluster

A partire da ONTAP 9.7, le configurazioni MetroCluster supportano i Tier di storage FabricPool.

Per informazioni generali sull'utilizzo di FabricPools, vedere "Gestione di dischi e Tier (aggregato)".

Considerazioni sull'utilizzo di FabricPools

- I cluster devono disporre di licenze FabricPool con limiti di capacità corrispondenti.
- I cluster devono avere IPspaces con nomi corrispondenti.

  Può trattarsi dell'IPSpace predefinito o di uno spazio IP creato da un amministratore. Questo IPSpace verrà utilizzato per le impostazioni di configurazione dell'archivio di oggetti FabricPool.

- Per l'IPSpace selezionato, ciascun cluster deve avere una LIF intercluster definita che possa raggiungere l'archivio di oggetti esterno

Configurazione di un aggregato per l'utilizzo in un FabricPool mirrorato

> Prima di configurare l'aggregato, è necessario configurare gli archivi di oggetti come descritto in "impostazione degli archivi di oggetti per FabricPool in una configurazione MetroCluster" in "Gestione di dischi e aggregati".

Fasi

Per configurare un aggregato per l'utilizzo in un FabricPool:

1. Creare l'aggregato o selezionare un aggregato esistente.
2. Eseguire il mirroring dell'aggregato come tipico aggregato mirrorato all'interno della configurazione MetroCluster.

3. Creare il mirror FabricPool con l'aggregato, come descritto in "Gestione di dischi e aggregati"
   a. Allegare un archivio di oggetti primario.

      Questo archivio di oggetti è fisicamente più vicino al cluster.

   b. Aggiungere un archivio di oggetti mirror.

      Questo archivio di oggetti è fisicamente più lontano dal cluster rispetto all'archivio di oggetti primario.

Supporto FlexGroup nelle configurazioni MetroCluster

A partire da ONTAP 9.6, le configurazioni MetroCluster supportano i volumi FlexGroup.

Pianificazioni dei lavori in una configurazione MetroCluster

In ONTAP 9.3 e versioni successive, le pianificazioni dei processi create dall'utente vengono replicate automaticamente tra i cluster in una configurazione MetroCluster. Se si crea, modifica o elimina una pianificazione di processo su un cluster, la stessa pianificazione viene creata automaticamente sul cluster partner, utilizzando il servizio di replica configurazione (CRS).

> Le pianificazioni create dal sistema non vengono replicate ed è necessario eseguire manualmente la stessa operazione sul cluster partner in modo che le pianificazioni dei processi su entrambi i cluster siano identiche.

Peering dei cluster dal sito MetroCluster a un terzo cluster

Poiché la configurazione di peering non viene replicata, se si esegue il peer di uno dei cluster della configurazione MetroCluster in un terzo cluster esterno a tale configurazione, è necessario configurare anche il peering sul cluster MetroCluster del partner. In questo modo, è possibile mantenere il peering in caso di commutazione.

Il cluster non MetroCluster deve eseguire ONTAP 8.3 o versione successiva. In caso contrario, il peering viene perso se si verifica uno switchover anche se il peering è stato configurato su entrambi i partner MetroCluster.

Replica della configurazione del client LDAP in una configurazione MetroCluster

Una configurazione del client LDAP creata su una macchina virtuale di storage (SVM) su un cluster locale viene replicata nella SVM dei dati del partner sul cluster remoto. Ad esempio, se la configurazione del client LDAP viene creata sulla SVM amministrativa sul cluster locale, viene replicata su tutti gli SVM dei dati di amministrazione sul cluster remoto. Questa funzione MetroCluster è intenzionale in modo che la configurazione del client LDAP sia attiva su tutte le SVM partner sul cluster remoto.

Linee guida per il networking e la creazione di LIF per le configurazioni MetroCluster

È necessario conoscere le modalità di creazione e replica delle LIF in una configurazione MetroCluster. È inoltre necessario conoscere i requisiti di coerenza per poter prendere decisioni appropriate durante la configurazione della rete.

Informazioni correlate

"Gestione di rete e LIF"

"Replica di oggetti IPSpace e requisiti di configurazione della subnet"

"Requisiti per la creazione di LIF in una configurazione MetroCluster"

"Requisiti e problemi di posizionamento e replica LIF"

Replica di oggetti IPSpace e requisiti di configurazione della subnet

È necessario conoscere i requisiti per la replica degli oggetti IPSpace nel cluster partner e per la configurazione di subnet e IPv6 in una configurazione MetroCluster.

Replica di IPSpace

Durante la replica degli oggetti IPSpace nel cluster partner, è necessario prendere in considerazione le seguenti linee guida:

- I nomi IPSpace dei due siti devono corrispondere.
- Gli oggetti IPSpace devono essere replicati manualmente nel cluster partner.

  Tutte le macchine virtuali di storage (SVM) create e assegnate a un IPSpace prima della replica di IPSpace non verranno replicate nel cluster partner.

Configurazione della subnet

Durante la configurazione delle subnet in una configurazione MetroCluster, è necessario prendere in considerazione le seguenti linee guida:

- Entrambi i cluster della configurazione MetroCluster devono avere una subnet nello stesso IPSpace con lo stesso nome di subnet, subnet, dominio di trasmissione e gateway.
- Gli intervalli IP dei due cluster devono essere diversi.

  Nell’esempio seguente, gli intervalli IP sono diversi:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                   Avail/
Name      Subnet            Domain    Gateway           Total    Ranges
--------- ---------------- --------- ------------      -------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                   Avail/
Name      Subnet            Domain    Gateway           Total    Ranges
--------- ---------------- --------- ------------     --------
---------------
subnet1   192.168.2.0/24   Default   192.168.2.1       10/10
192.168.2.21-192.168.2.30
```

Configurazione IPv6

Se IPv6 è configurato su un sito, IPv6 deve essere configurato anche sull'altro sito.

Informazioni correlate

"Requisiti per la creazione di LIF in una configurazione MetroCluster"

"Requisiti e problemi di posizionamento e replica LIF"

Requisiti per la creazione di LIF in una configurazione MetroCluster

Quando si configura la rete in una configurazione MetroCluster, è necessario conoscere i requisiti per la creazione di LIF.

Durante la creazione di LIF, è necessario prendere in considerazione le seguenti linee guida:

- Fibre Channel (canale fibra): È necessario utilizzare fabric allungati VSAN o allungati
- IP/iSCSI: È necessario utilizzare la rete con estensione Layer 2
- ARP Broadcasts (trasmissioni ARP): È necessario attivare le trasmissioni ARP tra i due cluster
- LIF duplicati: Non è necessario creare più LIF con lo stesso indirizzo IP (LIF duplicati) in un IPSpace
- Configurazioni NFS e SAN: È necessario utilizzare diverse macchine virtuali di storage (SVM) per gli aggregati senza mirror e con mirroring

Verificare la creazione di LIF

È possibile confermare la creazione di una LIF in una configurazione MetroCluster eseguendo il comando MetroCluster check lif show. In caso di problemi durante la creazione del file LIF, è possibile utilizzare il comando MetroCluster check lif repair-placement per risolvere i problemi.

Informazioni correlate

"Replica di oggetti IPSpace e requisiti di configurazione della subnet"

"Requisiti e problemi di posizionamento e replica LIF"

Requisiti e problemi di posizionamento e replica LIF

È necessario conoscere i requisiti di replica LIF in una configurazione MetroCluster. È inoltre necessario conoscere il modo in cui un LIF replicato viene collocato in un cluster di partner e tenere presenti i problemi che si verificano quando la replica LIF o il posizionamento LIF non riesce.

Replica di LIF nel cluster del partner

Quando si crea una LIF su un cluster in una configurazione MetroCluster, la LIF viene replicata sul cluster partner. I LIF non vengono posizionati in base al nome uno a uno. Per verificare la disponibilità di LIF dopo un'operazione di switchover, il processo di posizionamento LIF verifica che le porte siano in grado di ospitare LIF in base ai controlli di raggiungibilità e attributo delle porte.

Il sistema deve soddisfare le seguenti condizioni per inserire i file LIF replicati nel cluster del partner:

Condizione	Tipo LIF: FC	Tipo LIF: IP/iSCSI
Identificazione del nodo	ONTAP tenta di collocare il LIF replicato nel partner di disaster recovery (DR) del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.	ONTAP tenta di posizionare il LIF replicato sul partner DR del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.
Identificazione della porta	ONTAP identifica le porte di destinazione FC collegate sul cluster DR.	Le porte del cluster DR che si trovano nello stesso IPSpace del LIF di origine vengono selezionate per un controllo di raggiungibilità.se non vi sono porte nel cluster DR nello stesso IPSpace, il LIF non può essere posizionato. Tutte le porte del cluster di DR che ospitano già una LIF nello stesso IPSpace e nella stessa subnet vengono automaticamente contrassegnate come raggiungibili e possono essere utilizzate per il posizionamento. Queste porte non sono incluse nel controllo di raggiungibilità.
Controllo della raggiungibilità	La raggiungibilità viene determinata verificando la connettività del WWN del fabric di origine sulle porte del cluster DR.se lo stesso fabric non è presente nel sito DR, il LIF viene posizionato su una porta casuale del partner DR.	La raggiungibilità è determinata dalla risposta a una trasmissione ARP (Address Resolution Protocol) da ciascuna porta precedentemente identificata sul cluster DR all'indirizzo IP di origine della LIF da posizionare.per il successo dei controlli di raggiungibilità, è necessario consentire le trasmissioni ARP tra i due cluster. Ogni porta che riceve una risposta dalla LIF di origine verrà contrassegnata come possibile per il posizionamento.

Selezione della porta	ONTAP classifica le porte in base ad attributi quali tipo di adattatore e velocità, quindi seleziona le porte con attributi corrispondenti.se non viene trovata alcuna porta con attributi corrispondenti, la LIF viene posizionata su una porta connessa in modo casuale sul partner DR.	Dalle porte contrassegnate come raggiungibili durante il controllo di raggiungibilità, ONTAP preferisce le porte che si trovano nel dominio di trasmissione associato alla subnet della LIF.se non sono disponibili porte di rete sul cluster di DR che si trovano nel dominio di trasmissione associato alla subnet della LIF, Quindi, ONTAP seleziona le porte che hanno la raggiungibilità alla LIF di origine. 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. ONTAP classifica le porte in base ad attributi quali tipo di adattatore, tipo di interfaccia e velocità, quindi seleziona le porte con attributi corrispondenti.
Posizionamento LIF	Dalle porte raggiungibili, ONTAP seleziona la porta meno caricata per il posizionamento.	Dalle porte selezionate, ONTAP seleziona la porta meno caricata per il posizionamento.

Posizionamento di LIF replicati quando il nodo partner DR non è attivo

Quando viene creato un LIF iSCSI o FC su un nodo il cui partner DR è stato sostituito, il LIF replicato viene posizionato sul nodo del partner ausiliario DR. Dopo una successiva operazione di giveback, i LIF non vengono spostati automaticamente nel partner DR. Ciò può portare alla concentrazione di LIF su un singolo nodo nel cluster del partner. Durante un'operazione di switchover MetroCluster, i tentativi successivi di mappare le LUN appartenenti alla macchina virtuale di storage (SVM) non riescono.

Eseguire il `metrocluster check lif show` Comando dopo un'operazione di Takeover o giveback per verificare che il posizionamento LIF sia corretto. In caso di errori, è possibile eseguire `metrocluster check lif repair-placement` comando per risolvere i problemi.

Errori di posizionamento LIF

Errori di posizionamento LIF visualizzati da `metrocluster check lif show` i comandi vengono conservati dopo un'operazione di switchover. Se il `network interface modify`, `network interface rename`, o. `network interface delete` Viene inviato un comando per un LIF con un errore di posizionamento, l'errore viene rimosso e non viene visualizzato nell'output di `metrocluster check lif show` comando.

Errore di replica LIF

È inoltre possibile verificare se la replica LIF ha avuto esito positivo utilizzando `metrocluster check lif show` comando. Se la replica LIF non riesce, viene visualizzato un messaggio EMS.

È possibile correggere un errore di replica eseguendo `metrocluster check lif repair-placement` Comando per qualsiasi LIF che non riesce a trovare una porta corretta. È necessario risolvere al più presto eventuali errori di replica LIF per verificare la disponibilità di LIF durante un'operazione di switchover MetroCluster.

Anche se la SVM di origine non è disponibile, il posizionamento LIF potrebbe procedere normalmente se esiste una LIF appartenente a una SVM diversa in una porta con lo stesso IPSpace e la stessa rete nella SVM di destinazione.

Informazioni correlate

"Replica di oggetti IPSpace e requisiti di configurazione della subnet"

"Requisiti per la creazione di LIF in una configurazione MetroCluster"

Creazione di un volume su un aggregato root

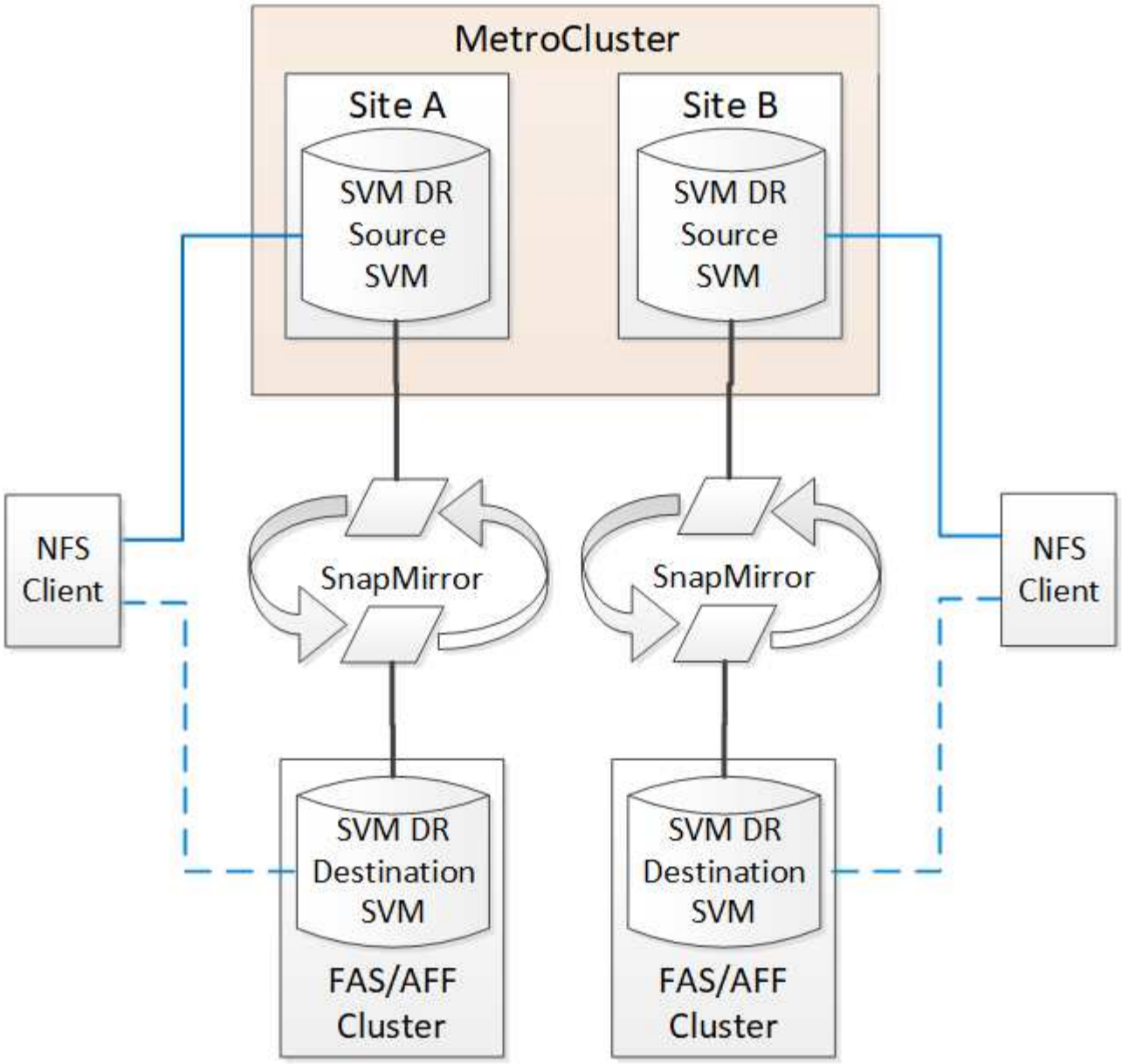
Il sistema non consente la creazione di nuovi volumi nell'aggregato root (un aggregato con un criterio ha di CFO) di un nodo in una configurazione MetroCluster.

A causa di questa restrizione, non è possibile aggiungere aggregati root a una SVM utilizzando `vserver add-aggregates` comando.

Disaster recovery SVM in una configurazione MetroCluster

A partire da ONTAP 9.5, le macchine virtuali con storage attivo (SVM) in una configurazione MetroCluster possono essere utilizzate come origini con la funzione di disaster recovery di SnapMirror SVM. La SVM di destinazione deve trovarsi sul terzo cluster al di fuori della configurazione MetroCluster.

A partire da ONTAP 9.11.1, entrambi i siti all'interno di una configurazione MetroCluster possono essere l'origine di una relazione DR SVM con un cluster di destinazione FAS o AFF, come mostrato nell'immagine seguente.



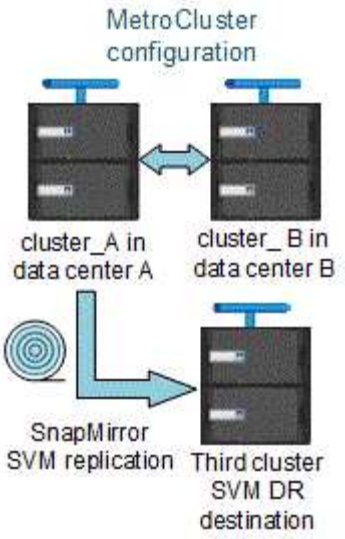
È necessario conoscere i seguenti requisiti e limitazioni dell'utilizzo di SVM con il disaster recovery SnapMirror:

- Solo una SVM attiva all'interno di una configurazione MetroCluster può essere l'origine di una relazione di disaster recovery SVM.

  Un'origine può essere una SVM di origine della sincronizzazione prima dello switchover o una SVM di destinazione della sincronizzazione dopo lo switchover.

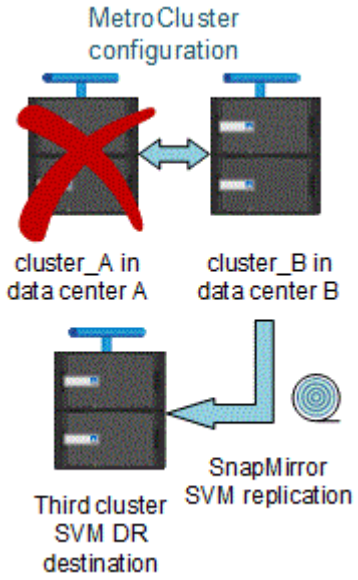
- Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.

  La seguente immagine mostra il comportamento del disaster recovery SVM in uno stato stabile:



- Quando la SVM di origine della sincronizzazione è l'origine di una relazione DR con SVM, le informazioni di relazione DR con SVM di origine vengono replicate nel partner MetroCluster.

  In questo modo, gli aggiornamenti DR di SVM possono continuare dopo uno switchover, come mostrato nell'immagine seguente:



- Durante i processi di switchover e switchback, la replica alla destinazione DR SVM potrebbe non riuscire.

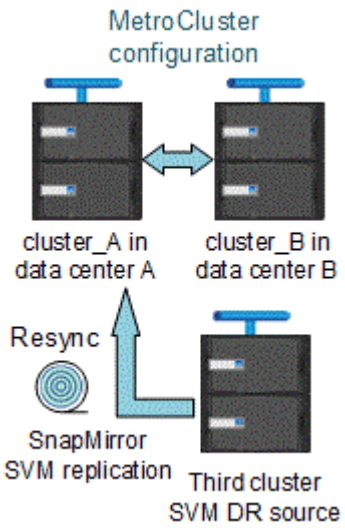
  Tuttavia, una volta completato il processo di switchover o switchback, gli aggiornamenti pianificati per il DR SVM successivi avranno esito positivo.

Vedere "Replica della configurazione SVM" in "Protezione dei dati" Per informazioni dettagliate sulla configurazione di una relazione DR SVM.

Risincronizzazione SVM in un sito di disaster recovery

Durante la risincronizzazione, l'origine del disaster recovery (DR) delle macchine virtuali dello storage sulla configurazione MetroCluster viene ripristinata dalla SVM di destinazione sul sito non MetroCluster.

Durante la risincronizzazione, la SVM di origine (cluster_A) agisce temporaneamente come SVM di destinazione, come mostrato nell'immagine seguente:



Se durante la risincronizzazione si verifica uno switchover non pianificato

Gli switchover non pianificati che si verificano durante la risincronizzazione arrestano il trasferimento di risincronizzazione. Se si verifica uno switchover non pianificato, sono soddisfatte le seguenti condizioni:

- La SVM di destinazione sul sito MetroCluster (che era una SVM di origine prima della risincronizzazione) rimane come SVM di destinazione. La SVM del cluster partner continuerà a conservare il sottotipo e rimarrà inattiva.
- La relazione SnapMirror deve essere ricreata manualmente con la SVM di destinazione della sincronizzazione come destinazione.
- La relazione di SnapMirror non viene visualizzata nell'output di SnapMirror dopo uno switchover nel sito superstite, a meno che non venga eseguita un'operazione di creazione di SnapMirror.

Esecuzione dello switchback dopo uno switchover non pianificato durante la risincronizzazione

Per eseguire correttamente il processo di switchback, la relazione di risincronizzazione deve essere interrotta ed eliminata. Lo switchback non è consentito se sono presenti SVM di destinazione DR SnapMirror nella configurazione MetroCluster o se il cluster dispone di una SVM di sottotipo "dp-destination".

L'output per il comando di visualizzazione plesso dell'aggregato di storage è indeterminato dopo uno switchover MetroCluster

Quando si esegue il comando show dell'aggregato di storage dopo uno switchover MetroCluster, lo stato di plex0 dell'aggregato root commutato è indeterminato e viene visualizzato come failed (non riuscito). Durante questo periodo, la root commutata non viene aggiornata. Lo stato effettivo di questo plex può essere determinato solo dopo la fase di riparazione MetroCluster.

Modifica dei volumi per impostare il flag NVFAIL in caso di switchover

È possibile modificare un volume in modo che il flag NVFAIL venga impostato sul volume in caso di switchover MetroCluster. Il flag NVFAIL disattiva il volume da qualsiasi modifica. Ciò è necessario per i volumi che devono essere gestiti come se le scritture assegnate al volume fossero perse dopo il passaggio.

Nelle versioni di ONTAP precedenti alla 9.0, il flag NVFAIL viene utilizzato per ogni switchover. In ONTAP 9.0 e versioni successive, viene utilizzato lo switchover non pianificato (USO).

Fase

1. Abilitare la configurazione MetroCluster per attivare NVFAIL allo switchover impostando `vol -dr-force -nvfail` parametro su on:

   ```
   vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
   ```

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto
"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Gestione di MetroCluster"	• Informazioni sulla configurazione di MetroCluster • Switchover, healing e switchback
"Disaster recovery"	• Disaster recovery • Switchover forzato • Ripristino da un errore di storage o multi-controller

"Manutenzione MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster FC • Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch • Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch • Sostituzione dell'hardware in un sito di emergenza in una configurazione FC MetroCluster Fabric-Attached o Stretch • Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.
"Upgrade ed espansione di MetroCluster"	• Aggiornamento o aggiornamento di una configurazione MetroCluster • Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi
"Transizione MetroCluster"	• Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP
"Upgrade, transizione ed espansione di MetroCluster"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
"Documentazione dei sistemi hardware ONTAP" **Nota:** le procedure standard di manutenzione dello shelf storage possono essere utilizzate con le configurazioni MetroCluster IP.	• Aggiunta a caldo di uno shelf di dischi • Rimozione a caldo di uno shelf di dischi
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster
"Concetti di ONTAP"	• Come funzionano gli aggregati mirrorati

Installare una configurazione stretch MetroCluster

Panoramica

Per installare la configurazione di Stretch 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
  - "Configurazione SAS a due nodi"
  - "Configurazione con collegamento a ponte a due nodi"
- "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 Tutti gli array SAN	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 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

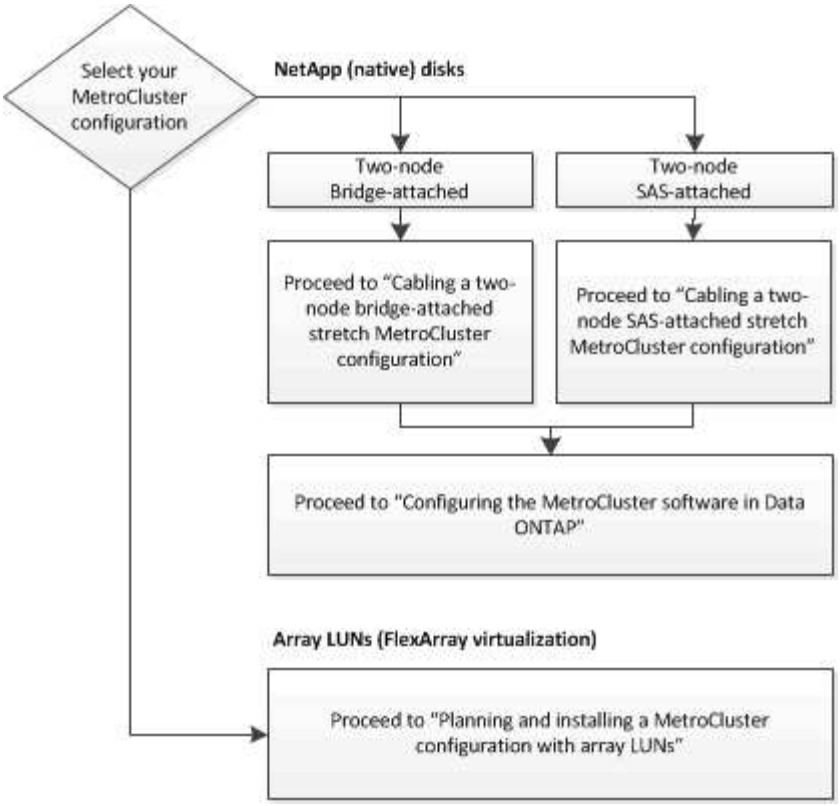
Se si utilizza un firewall in un sito MetroCluster, è necessario garantire l'accesso per le porte richieste.

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 delle LUN FlexArray e alla modalità di connessione dei controller di storage agli shelf di storage.



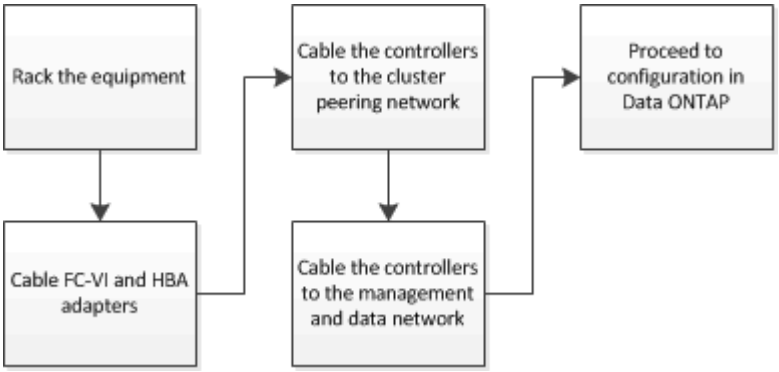
Per questo tipo di installazione…	Utilizzare queste procedure…
Configurazione stretch a due nodi con bridge FC-SAS	1. "Cablaggio di una configurazione Stretch MetroCluster con collegamento a ponte a due nodi" 2. "Configurazione del software MetroCluster in ONTAP"
Configurazione stretch a due nodi con cablaggio SAS a collegamento diretto	1. "Collegamento di una configurazione MetroCluster stretch con collegamento SAS a due nodi" 2. "Configurazione del software MetroCluster in ONTAP"
Installazione con LUN array	"Connessioni in configurazioni MetroCluster stretch con LUN array"

Collegare una configurazione MetroCluster stretch con collegamento SAS a due nodi

Collegamento di una configurazione MetroCluster stretch con collegamento SAS a due nodi

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 di Stretch MetroCluster con collegamento SAS a due nodi

La configurazione con collegamento SAS a due nodi MetroCluster richiede diverse parti, tra cui due cluster a nodo singolo in cui i controller di storage sono collegati direttamente allo storage mediante cavi SAS.

La configurazione MetroCluster include i seguenti elementi hardware principali:

- Controller di storage

  I controller di storage si collegano direttamente allo storage utilizzando cavi SAS.

  Ogni controller di storage è configurato come partner di DR per uno storage controller sul sito del partner.

  - I cavi SAS in rame possono essere utilizzati per distanze più brevi.
  - I cavi SAS ottici possono essere utilizzati per lunghe distanze.

  > Nei sistemi che utilizzano LUN array e-Series, i controller storage possono essere collegati direttamente agli array storage e-Series. Per gli altri LUN di array, sono necessarie connessioni tramite 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.

- Rete di peering del cluster

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

Componenti hardware MetroCluster richiesti e linee guida di denominazione per le configurazioni con collegamento SAS a due nodi

La configurazione MetroCluster richiede una vasta gamma di componenti hardware. Per comodità e chiarezza, i nomi standard dei componenti vengono utilizzati nella documentazione di MetroCluster. 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.

Ridondanza dell'hardware nella configurazione MetroCluster

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

Due cluster ONTAP a nodo singolo

La configurazione di Stretch MetroCluster SAS-attached richiede due cluster ONTAP a nodo singolo.

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

Nomi di esempio:

- Sito A: Cluster_A
- Sito B: Cluster_B

Due moduli controller storage

La configurazione di Stretch MetroCluster SAS-attached richiede due moduli controller storage.

- 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.
- 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 altro 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

Almeno quattro shelf di dischi SAS (consigliato)

La configurazione Smagliature MetroCluster con connessione SAS richiede almeno due shelf di dischi SAS. Si consigliano quattro shelf di dischi SAS.

Si consiglia di utilizzare due shelf in ogni sito per consentire la proprietà dei dischi in base allo shelf. È supportato un minimo di uno shelf in ogni sito.

Nomi di esempio:

- Sito A:
  - Shelf_A_1_1
  - Shelf_A_1_2
- Sito B:
  - Shelf_B_1_1
  - Shelf_B_1_2

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"

Installare e cablare i componenti MetroCluster per le configurazioni smaglianti collegate da SAS a due nodi

Installazione e cablaggio dei componenti MetroCluster per configurazioni smaglianti collegate con SAS a due nodi

I controller di storage devono essere cablati tra loro e sui supporti di storage. I controller di storage devono anche essere cablati alla rete di gestione e dati.

Prima di iniziare qualsiasi procedura descritta in questo documento

Prima di completare questa attività, è necessario soddisfare i seguenti requisiti generali:

- Prima dell'installazione, è necessario acquisire familiarità con le considerazioni e le Best practice per l'installazione e il cablaggio degli shelf di dischi per il modello di shelf di dischi.
- Tutti i componenti MetroCluster devono essere supportati.

  "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.

A proposito di questa attività

- I termini nodo e controller sono utilizzati in modo intercambiabile.

Scaffalatura dei componenti hardware

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

Questa attività deve essere eseguita su entrambi i siti MetroCluster.

Fasi

1. Pianificare il posizionamento dei componenti di MetroCluster.

   La quantità di spazio rack necessaria 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. Utilizzando le procedure di officina standard per lavorare con le apparecchiature elettriche, assicurati di essere messo a terra correttamente.
3. Installare i controller di storage nel rack o nell'armadietto.

   "Documentazione dei sistemi hardware ONTAP"

4. Installare gli shelf di dischi, collegare a margherita gli shelf di dischi in ogni stack, accenderli e impostare gli ID dello shelf.

   Consultare la guida appropriata per il modello di shelf di dischi per informazioni sugli shelf di dischi a margherita e sull'impostazione degli shelf ID.

   > Gli shelf ID devono essere univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster (inclusi entrambi i siti). Quando si impostano manualmente gli shelf ID, è necessario spegnere e riaccendere lo shelf di dischi.

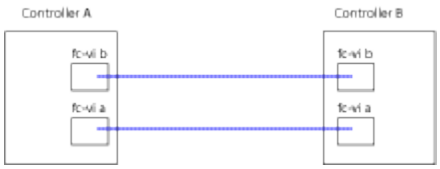
Collegamento dei controller tra loro e degli shelf di storage

Gli adattatori FC-VI del controller devono essere collegati direttamente tra loro. Le porte SAS del controller devono essere cablate agli stack di storage remoto e locale.

Questa attività deve essere eseguita in entrambi i siti MetroCluster.

Fasi

1. Collegare le porte FC-VI.

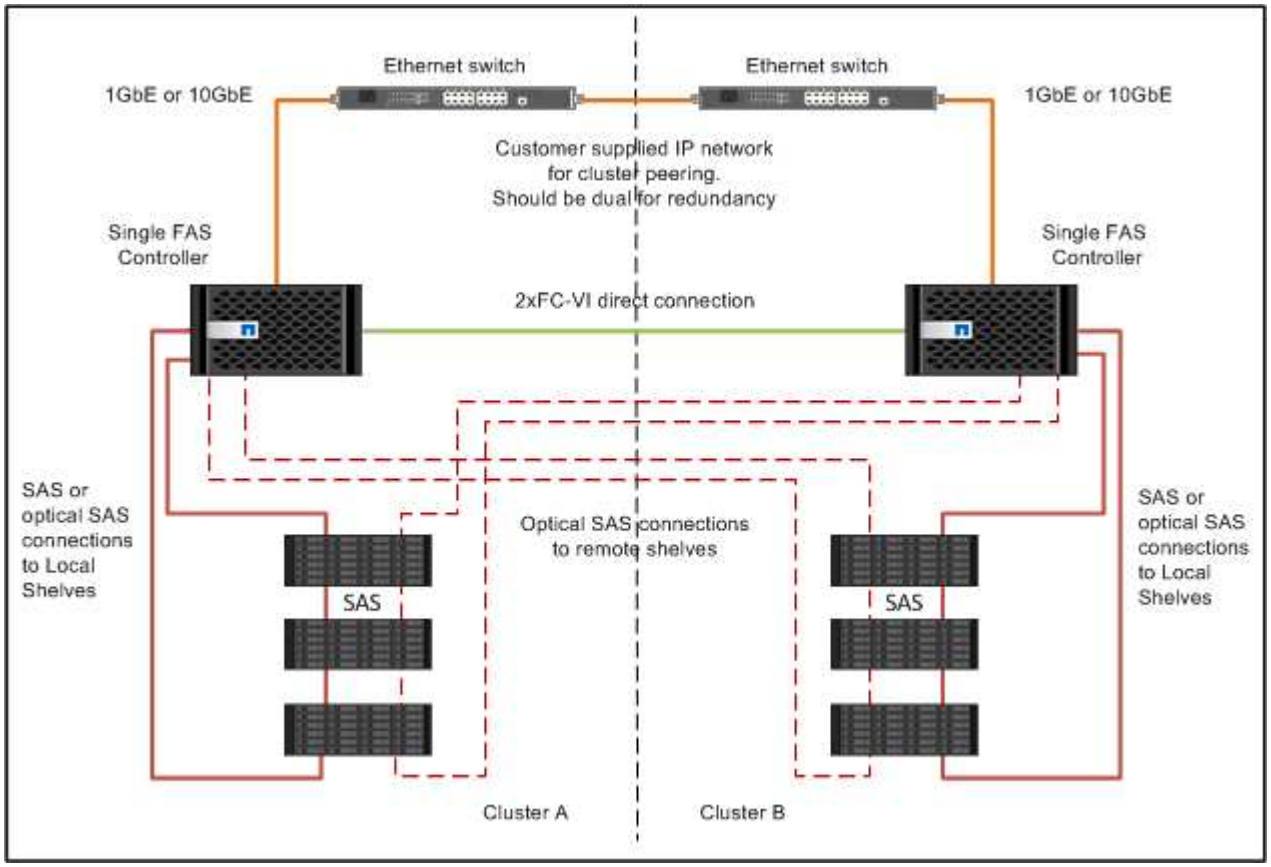


La figura precedente mostra una tipica connessione via cavo rappresentativa. Le porte FC-VI specifiche variano in base al modulo controller.

- I moduli controller FAS8200 e AFF A300 possono essere ordinati con una delle due opzioni per la connettività FC-VI:
  - Le porte onboard 0e e 0f sono configurate in modalità FC-VI.
  - Le porte 1a e 1b di una scheda FC-VI vanno inserite nello slot 1.
- I moduli controller dei sistemi storage AFF A700 e FAS9000 utilizzano quattro porte FC-VI ciascuna.
- I moduli controller del sistema storage AFF A400 e FAS8300 utilizzano le porte FC-VI 2a e 2b.

2. Collegare le porte SAS.

   La figura seguente mostra i collegamenti. L'utilizzo delle porte potrebbe variare a seconda delle porte SAS e FC-VI disponibili sul modulo controller.



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.

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.

Fasi

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

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

   "Configurazione rapida del peering di cluster e SVM"

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.

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. Inoltre, è possibile collegare il controller a nuovi switch di rete dedicati, come gli switch di gestione dei cluster NetApp CN1601.

Fasi

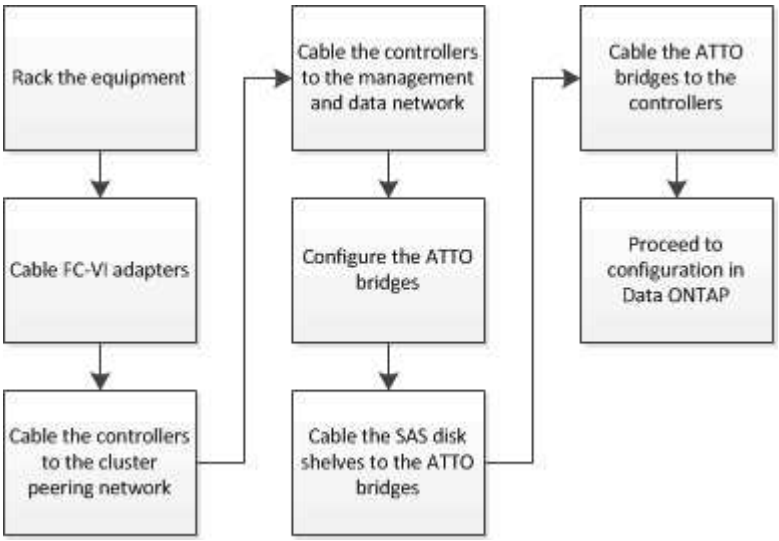
1. Collegare le porte dati e di gestione del controller alle reti dati e di gestione del sito locale.

   "Documentazione dei sistemi hardware ONTAP"

Configurazione Stretch MetroCluster con collegamento a ponte a due nodi

Cablaggio di una configurazione Stretch MetroCluster con collegamento a ponte a due nodi

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 Stretch MetroCluster con collegamento a ponte a due nodi

Durante la pianificazione della configurazione MetroCluster, è necessario comprendere le parti della configurazione e il modo in cui funzionano insieme.

La configurazione MetroCluster include i seguenti elementi hardware principali:

- Controller di storage

  I controller di storage non sono collegati direttamente allo storage ma a bridge FC-SAS. I controller storage sono collegati tra loro tramite cavi FC tra gli adattatori FC-VI di ciascun controller.

  Ogni controller di storage è configurato come partner di DR per uno storage controller sul sito del partner.

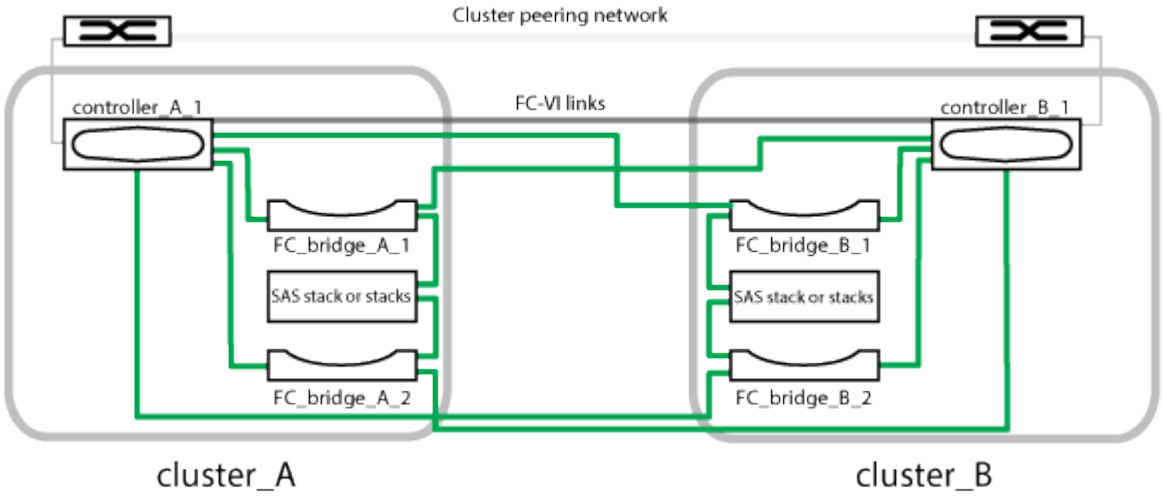
- Bridge FC-SAS

  I bridge FC-SAS collegano gli stack di storage SAS alle porte initiator FC dei controller, fornendo un bridging tra i due protocolli.

- Rete di peering del cluster

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

La figura seguente mostra una vista semplificata della configurazione MetroCluster. 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 configurazione è costituita da due cluster a nodo singolo.
- Ogni sito dispone di uno o più stack di storage SAS.

  > Gli shelf SAS nelle configurazioni MetroCluster non sono supportati con il cablaggio ACP.

  Sono supportati ulteriori stack di storage, ma ne viene mostrato solo uno per ciascun sito.

Componenti hardware MetroCluster richiesti e convenzioni di denominazione per le configurazioni di stretch a due nodi collegate tramite bridge

Durante la pianificazione della configurazione MetroCluster, è necessario comprendere 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.

Ridondanza dell'hardware nella configurazione MetroCluster

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

Requisito per due cluster ONTAP a nodo singolo

La configurazione Stretch MetroCluster con collegamento a ponte richiede due cluster ONTAP a nodo singolo.

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

Nomi di esempio:

- Sito A: Cluster_A
- Sito B: Cluster_B

Requisito per due moduli controller storage

La configurazione Stretch MetroCluster con collegamento a ponte richiede due moduli controller storage.

I 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.
- 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 altro 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

Requisiti per i bridge FC-SAS

La configurazione Stretch MetroCluster con collegamento a ponte richiede due o più bridge FC-SAS in ciascun sito.

Questi bridge collegano gli shelf di dischi SAS ai moduli controller.

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

- I bridge FibreBridge 7600N e 7500N supportano fino a quattro stack SAS.
- Ogni stack può utilizzare diversi modelli di IOM, ma tutti gli shelf all'interno di uno stack devono utilizzare lo stesso modello.

  I modelli di 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 procedura identificano il modulo controller a cui il bridge si collega e la porta.

Nomi di esempio:

- Sito A:
  - bridge_A_1_*port-number*
  - bridge_A_2_*port-number*
- Sito B:
  - bridge_B_1_*port-number*
  - bridge_B_2_*port-number*

Requisito per almeno quattro shelf SAS (consigliato)

La configurazione Stretch MetroCluster con collegamento a ponte richiede almeno due shelf SAS. Tuttavia, si consiglia di utilizzare due shelf per ciascun sito per consentire la proprietà dei dischi per shelf, per un totale di quattro shelf SAS.

È supportato un minimo di uno shelf in ogni sito.

Nomi di esempio:

- Sito A:

    - Shelf_A_1_1
    - Shelf_A_1_2
- Sito B:
    - Shelf_B_1_1
    - Shelf_B_1_2

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"

Foglio di lavoro per la raccolta di informazioni per bridge FC-SAS

Prima di iniziare a configurare i siti MetroCluster, è necessario raccogliere le informazioni di configurazione richieste.

Sito A, bridge FC-SAS 1 (FC_bridge_A_1a)

Ogni stack SAS richiede almeno due bridge FC-SAS.

Ciascun bridge si connette a Controller_A_1_*port-number* E Controller_B_1_*port-number*.

Sito A	Il tuo valore
Indirizzo IP Bridge_A_1a	
Nome utente Bridge_A_1a	
Password Bridge_A_1a	

Sito A, bridge FC-SAS 2 (FC_bridge_A_1b)

Ogni stack SAS richiede almeno due bridge FC-SAS.

Ciascun bridge si connette a Controller_A_1_*port-number* E Controller_B_1_*port-number*.

Sito A	Il tuo valore
Indirizzo IP Bridge_A_1b	
Nome utente Bridge_A_1b	
Password Bridge_A_1b	

Sito B, bridge FC-SAS 1 (FC_bridge_B_1a)

Ogni stack SAS richiede almeno due bridge FC-SAS.

Ciascun bridge si connette a Controller_A_1_`*Port-Number*` e Controller_B_1_`*Port-Number*`.

Sito B	Il tuo valore
Indirizzo IP Bridge_B_1a	
Nome utente Bridge_B_1a	
Password Bridge_B_1a	

Sito B, bridge FC-SAS 2 (FC_bridge_B_1b)

Ogni stack SAS richiede almeno due bridge FC-SAS.

Ciascun bridge si connette a Controller_A_1_`*Port-Number*` e Controller_B_1_`*Port-Number*`.

Sito B	Il tuo valore
Indirizzo IP Bridge_B_1b	
Nome utente Bridge_B_1b	
Password Bridge_B_1b	

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.

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 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.

   "Documentazione dei sistemi hardware ONTAP"

4. Installare gli shelf di dischi, accenderli e 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).

5. 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).

      Per ulteriori informazioni e un'illustrazione dell'installazione, consultare il *Manuale d'installazione e funzionamento di FibreBridge atto relativo al modello di bridge in uso*.

   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.

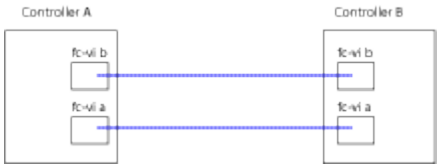
   Il LED Bridge Ready potrebbe impiegare fino a 30 secondi per accendersi, a indicare che il bridge ha completato la sequenza di test automatico all'accensione.

Collegamento dei controller tra loro

Gli adattatori FC-VI di ciascun controller devono essere cablati direttamente al partner.

Fasi

1. Collegare le porte FC-VI.



   La figura sopra riportata è una tipica rappresentazione del cablaggio richiesto. Le porte FC-VI specifiche variano in base al modulo controller.

   - I moduli controller 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 moduli controller dei sistemi storage AFF A700 e FAS9000 utilizzano quattro porte FC-VI ciascuna.

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.

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.

Fasi

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

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

   "Configurazione rapida del peering di cluster e SVM"

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.

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. Inoltre, è possibile collegare il controller a nuovi switch di rete dedicati, come gli switch di gestione dei cluster NetApp CN1601.

Fasi

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

   "Documentazione dei sistemi hardware ONTAP"

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.

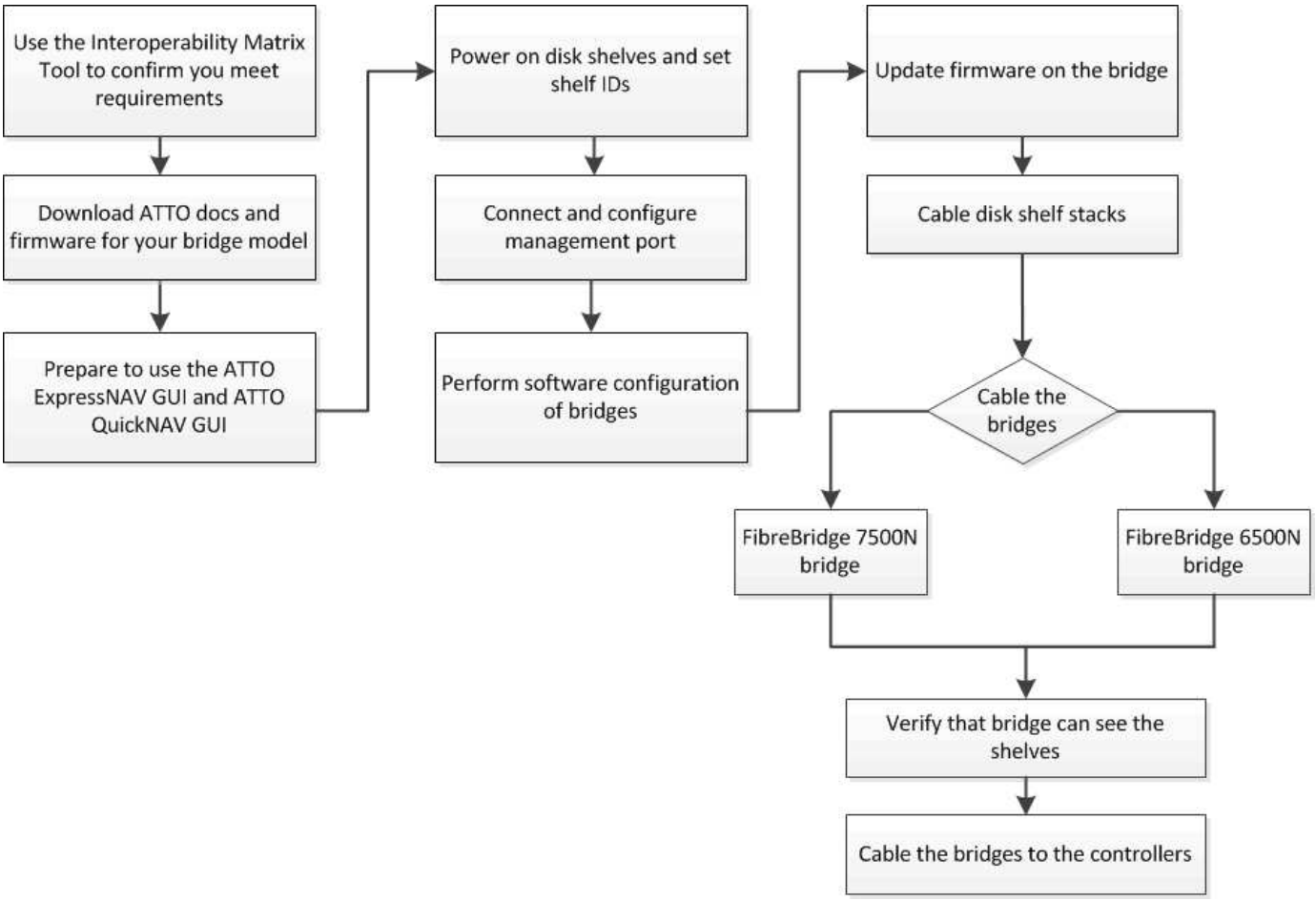
Per i sistemi ricevuti in fabbrica, i bridge FC-SAS sono preconfigurati e non richiedono alcuna configurazione aggiuntiva.

Questa procedura presuppone che si stiano utilizzando le interfacce di gestione del bridge consigliate: La GUI ExpressNAV atto e l'utility barra di navigazione atto.

Utilizzare l'interfaccia grafica di ATTO ExpressNAV per configurare e gestire un bridge e per aggiornare il firmware del bridge. Utilizzare l'utility barra di navigazione atto per configurare la porta di gestione Ethernet del bridge 1.

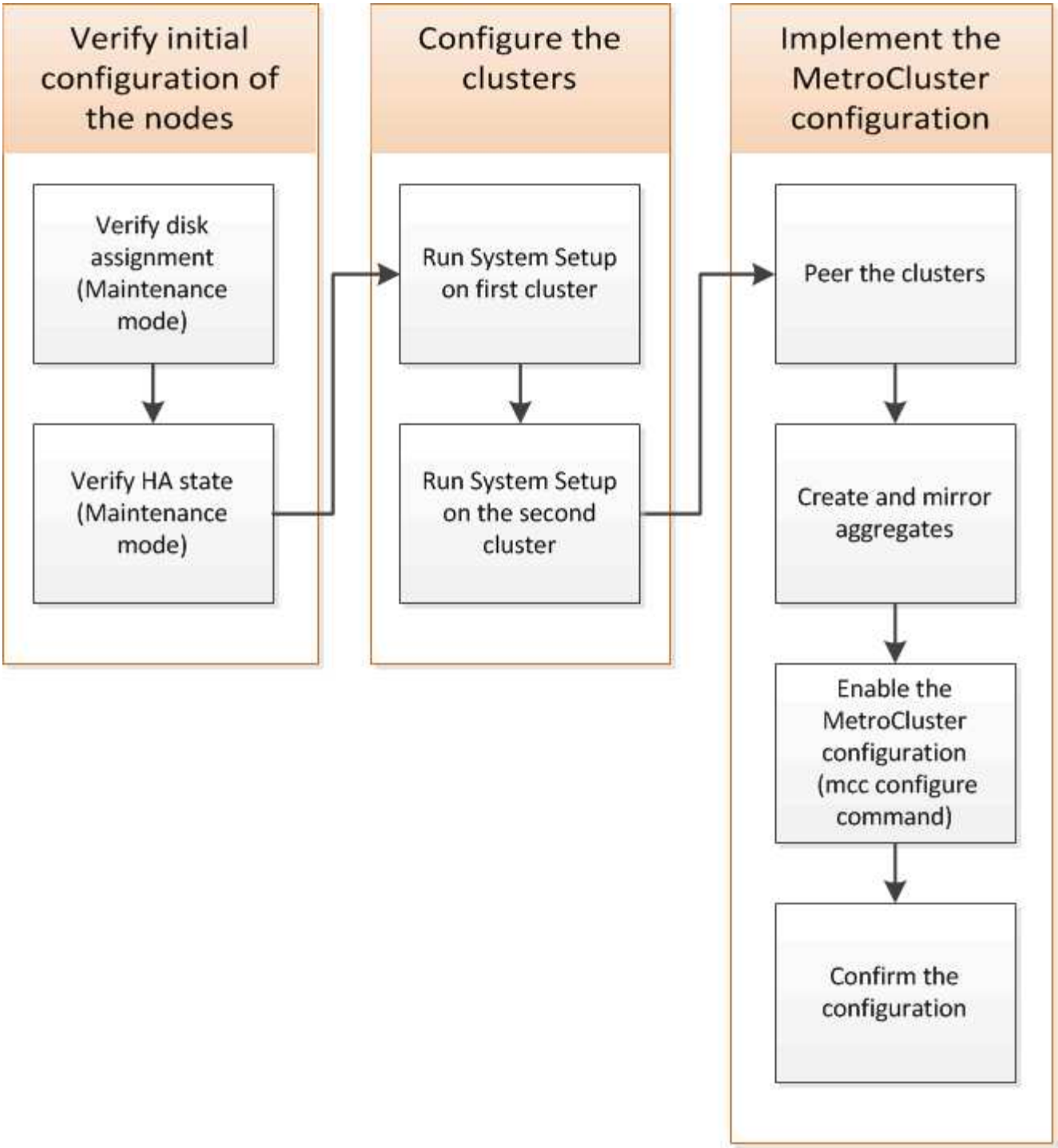
Se necessario, è possibile utilizzare altre interfacce di gestione, ad esempio una porta seriale o Telnet, per configurare e gestire un bridge e per configurare la porta di gestione Ethernet 1 e FTP per aggiornare il firmware del bridge.

Questa procedura utilizza il seguente flusso di lavoro:



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.



Fasi

1. Prima di iniziare il processo di configurazione, raccogliere gli indirizzi IP richiesti per i moduli controller.
2. Completare il foglio di lavoro con le informazioni sulla rete IP per il sito A.

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 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 queste informazioni: 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 queste informazioni: Controller_A_1				
Nodo 2. Non richiesto se si utilizza una configurazione MetroCluster a due nodi (un nodo per ogni sito). Esempio utilizzato in queste informazioni: Controller_A_2				

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				

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 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	

Informazioni SP del sito A.

È necessario abilitare l'accesso al Service Processor (SP) di ciascun nodo per la risoluzione dei problemi e la manutenzione. Ciò richiede le seguenti informazioni di rete per ciascun nodo:

Nodo	Indirizzo IP	Maschera di rete	Gateway predefinito
Nodo 1			

Foglio di lavoro con le informazioni sulla 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 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 queste informazioni: 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 queste informazioni: Controller_B_1				
Nodo 2. Non richiesto per configurazioni MetroCluster a due nodi (un nodo per sito). Esempio utilizzato in queste informazioni: 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				

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	

Sito B nbsp; 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)			

Analogie e differenze tra cluster standard e configurazioni MetroCluster

La configurazione dei nodi in ciascun cluster in una configurazione MetroCluster è simile a quella dei nodi in un cluster standard.

La configurazione di MetroCluster si basa su due cluster standard. Fisicamente, la configurazione deve essere simmetrica, con ciascun nodo con la stessa configurazione hardware e tutti i componenti MetroCluster devono essere cablati e configurati. Tuttavia, la configurazione software di base per i nodi in una configurazione MetroCluster è uguale a quella per i nodi in un cluster standard.

Fase di configurazione	Configurazione standard del cluster	Configurazione di MetroCluster

Configurare le LIF di gestione, cluster e dati su ciascun nodo.	Lo stesso vale per entrambi i tipi di cluster	Configurare l'aggregato root.
Lo stesso vale per entrambi i tipi di cluster	Impostare il cluster su un nodo del cluster.	Lo stesso vale per entrambi i tipi di cluster
Unire l'altro nodo al cluster.	Lo stesso vale per entrambi i tipi di cluster	Creare un aggregato root mirrorato.
Opzionale	Obbligatorio	Peer dei cluster.
Opzionale	Obbligatorio	Abilitare la configurazione MetroCluster.

Ripristino delle impostazioni predefinite del sistema e configurazione del tipo di HBA su un modulo controller

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	`ucadmin modify -m fc -t initiator` *`adapter_name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter_name`*
Destinazione FC	`fcadmin config -t target` *`adapter_name`*

Iniziatore FC	`fcadmin config -t initiator` *`adapter_name`*

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	`ucadmin show`
FC	`fcadmin show`

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
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       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
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Spegnere 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 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 le assegnazioni 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

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

   ```
   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. Mostra gli ID e gli alloggiamenti degli shelf di dischi per ciascun disco:
`disk show –v`

Verifica dello stato ha dei componenti

In una configurazione stretch MetroCluster non preconfigurata in fabbrica, è necessario verificare che lo stato ha del controller e del componente dello chassis sia impostato su “mcc-2n” in modo che si avvii correttamente. Per i sistemi ricevuti dalla fabbrica, questo valore è preconfigurato e non è necessario verificarlo.

Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Il modulo controller e lo chassis devono visualizzare il valore “mcc-2n”.

2. Se lo stato di sistema visualizzato del controller non è “mcc-2n”, impostare lo stato ha per il controller:

   ```
   ha-config modify controller mcc-2n
   ```

3. Se lo stato di sistema visualizzato dello chassis non è “mcc-2n”, impostare lo stato ha per lo chassis:

   ```
   ha-config modify chassis mcc-2n
   ```

   Arrestare il nodo.

   Attendere che il nodo sia tornato al prompt DEL CARICATORE.

4. Ripetere questi passaggi su ciascun nodo della configurazione MetroCluster.

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 dall'installazione guidata cluster e utilizzare `cluster setup` 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, consultare "Setup ONTAP (Configurazione guidata)"

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 per informare 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 l'impostazione predefinita del sistema "yes" premendo Invio oppure immettere i propri valori

digitando “no” e premendo 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 averlo 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 **Cluster Setup** utilizzando `cluster setup` comando.

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.

Peering dei cluster

I cluster nella configurazione di MetroCluster devono essere in una relazione peer in modo da poter comunicare tra loro ed eseguire il mirroring dei dati essenziale per il disaster recovery di MetroCluster.

Informazioni correlate

"Configurazione rapida del peering di cluster e SVM"

"Considerazioni sull’utilizzo di porte dedicate"

"Considerazioni sulla condivisione delle porte dati"

Configurazione delle LIF 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.

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 le porte "e0e" e "e0f" non sono state assegnate a LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port

Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Creare un gruppo di failover per le porte dedicate:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Nell'esempio seguente vengono assegnate le porte "e0e" e "e0f" al gruppo di failover "intercluster01" sulla SVM di sistema "cluster01":

```
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
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Versione di ONTAP	Comando
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 dell'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:

Versione di ONTAP	Comando
ONTAP 9.6 e versioni successive	`network interface show -service-policy default-intercluster`
ONTAP 9.5 e versioni precedenti	`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verificare che le LIF dell'intercluster siano ridondanti:

Versione di ONTAP	Comando

ONTAP 9.6 e versioni successive	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti	`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta 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"

Configurazione delle LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Fasi

1. Elencare le porte nel cluster:

   `network port show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in "cluster01":

```
cluster01::> network port show
                                                            Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Creazione di LIF intercluster sulla SVM di sistema:

Versione di ONTAP	Comando
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`*
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`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono creati i LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02":

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

Versione di ONTAP	Comando
ONTAP 9.6 e versioni successive	`network interface show -service-policy default-intercluster`
ONTAP 9.5 e versioni precedenti	`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

Versione di ONTAP	Comando
ONTAP 9.6 e versioni successive	`network interface show –service-policy default-intercluster -failover`
ONTAP 9.5 e versioni precedenti	`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta "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.

Creazione di una relazione peer del cluster

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-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   Se si specificano entrambi `-generate-passphrase` e. `-peer-addrs`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addrs` 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-addrs` *`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-addrs
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-addrs` *`peer_LIF_IPs`* `-ipspace` *`ipspace`*

   È possibile ignorare `-ipspace` Se non si utilizza un IPSpace personalizzato. Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene creata una relazione di 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-addrs 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-addrs` *`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-addrs 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
             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
```

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"

"Concetti di ONTAP"

Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

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 assicurarsi di selezionare il tipo di disco corretto.

A proposito di questa attività

- I dischi e le LUN degli array sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi dell'aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale dell'aggregato.
- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.

  "Gestione di dischi e aggregati"

Fasi

1. Visualizzare un elenco delle parti di ricambio disponibili:

   `storage disk show -spare -owner node_name`

2. Creare l'aggregato:

   `storage aggregate create -mirror true`

   Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su

qualsiasi nodo del cluster. Per assicurarsi che l'aggregato venga creato su un nodo specifico, utilizzare `-node` o specificare i dischi di proprietà di quel nodo.

È possibile specificare le seguenti opzioni:

- Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
- Elenco 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 l'opzione force-Small-aggregate per consentire la creazione di un aggregato RAID-DP a tre dischi.

- Stile checksum da utilizzare per l'aggregato
- Tipo di dischi da utilizzare
- Dimensioni delle unità da utilizzare
- Velocità del disco da utilizzare
- Tipo RAID per i gruppi RAID sull'aggregato
- Numero massimo di 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 la `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.

Esempio 1. A proposito di questa attività

ATTENZIONE: 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.

Gli aggregati senza mirror devono essere locali rispetto al nodo che li possiede.

- I dischi e le LUN degli array sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi dell'aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale dell'aggregato.
- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.
- Il "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, consultare la `storage aggregate create` pagina man.

     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`*

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.

  Verificare i tipi di aggregato:

  `storage aggregate show`

  > Se si desidera utilizzare un singolo aggregato di dati mirrorato, vedere "Configurare il software MCC in ONTAP" per istruzioni.

- Lo stato ha-config dei controller e dello chassis deve essere “mcc-2n”.

A proposito di questa attività

È possibile eseguire 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.

Fasi

1. Configurare MetroCluster nel seguente formato:

Se la configurazione di MetroCluster dispone di…	Quindi…
Aggregati di dati multipli	Dal prompt di qualsiasi nodo, configurare MetroCluster: `metrocluster configure` *`node-name`*

Un singolo aggregato di dati mirrorato	a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
	
	`set -privilege advanced`
	
	Rispondere con “y” quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (*).
	
	b. Configurare MetroCluster con `-allow-with-one-aggregate true` parametro:
	
	`metrocluster configure -allow-with-one-aggregate true` *`node-name`*
	
	c. Tornare al livello di privilegio admin:
	`set -privilege admin`

> La Best practice consiste nell’avere più aggregati di dati. Se il primo gruppo DR dispone di un solo aggregato e si desidera aggiungere un gruppo DR con un aggregato, è necessario spostare il volume di metadati dal singolo aggregato di dati. Per ulteriori informazioni su questa procedura, vedere "Spostamento di un volume di metadati nelle configurazioni MetroCluster".

Il seguente comando abilita la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene “controller_A_1”:

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Verificare lo stato della rete sul sito A:

   `network port show`

   L’esempio seguente mostra l’utilizzo della porta di rete:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    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

7 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 di bridge FC-SAS per il monitoraggio dello stato di salute

Nei sistemi con versioni di ONTAP precedenti alla 9.8, se la configurazione include bridge FC-SAS, è necessario eseguire alcune procedure di configurazione speciali per monitorare i bridge FC-SAS nella configurazione MetroCluster.

- 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
ONTAP 9.5 e versioni successive	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
ONTAP 9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   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 "Satus" è "ok" e se vengono visualizzate altre informazioni, come il nome globale (WWN).

L'esempio seguente mostra che i bridge FC-SAS sono configurati:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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.

Se il `metrocluster check run` il comando viene emesso due volte in un breve periodo di tempo su uno o entrambi i cluster, può verificarsi un conflitto e il comando potrebbe non raccogliere tutti i dati. Successivo `metrocluster check show` i comandi non mostrano l'output previsto.

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. Visualizzazione di risultati più dettagliati:

   `metrocluster check run`

   `metrocluster check aggregate show`

   `metrocluster check cluster show`

   `metrocluster check config-replication show`

   `metrocluster check lif show`

   `metrocluster check node show`

   Il `metrocluster check show` i comandi mostrano i risultati dei più recenti `metrocluster check run` comando. Eseguire sempre il `metrocluster check run` prima di utilizzare `metrocluster check show` i comandi in modo che le informazioni visualizzate siano aggiornate.

   Nell'esempio riportato di seguito viene illustrato il `metrocluster check aggregate show` Output di comando per una configurazione MetroCluster a quattro nodi sana:

```
cluster_A::> metrocluster check aggregate show

Last Checked On: 8/5/2014 00:42:58

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
```

```
                                                    ownership-state
ok
                     controller_A_1_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2       controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    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.

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.

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 dello switchover, della riparazione e dello switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

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.

1. Impostare l'URL della destinazione remota per i file di backup della configurazione:

   ```
   system configuration backup settings modify URL-of-destination
   ```

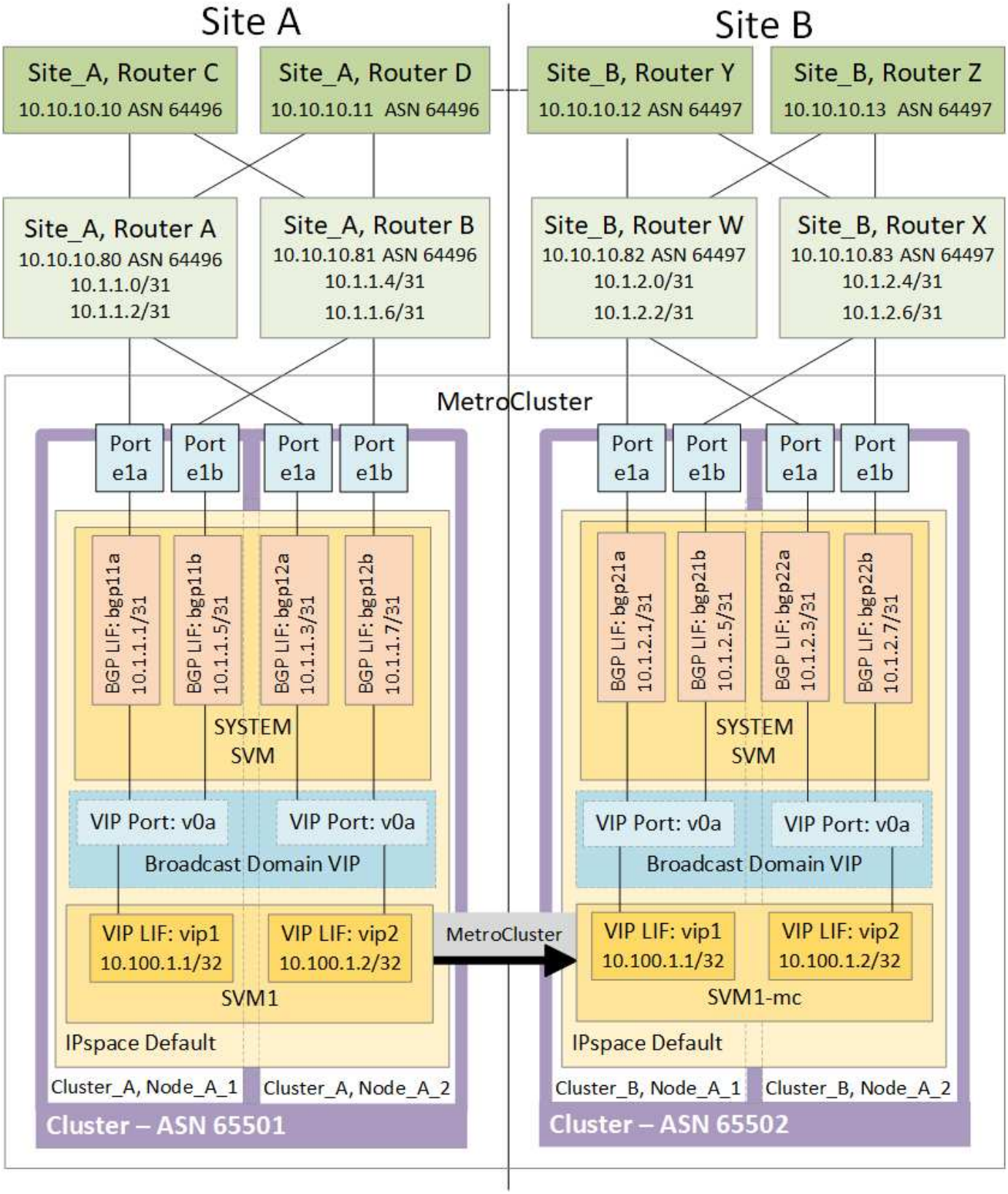
   Il "Gestione dei cluster con la CLI" Contiene ulteriori informazioni nella sezione *Gestione dei backup di configurazione*.

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 alla seguente sezione:

"Configurazione di LIF IP virtuali (VIP)"



Limitazioni ONTAP

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

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

in qualsiasi momento.

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

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

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

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

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

A seconda della versione di ONTAP in uso, è necessario configurare le LIF di peering BGP nel nodo SVM, non nel sistema o nei dati SVM. 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.

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

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

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

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

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

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

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

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 un'operazione di switchover negoziata (pianificata) per confermare la disponibilità ininterrotta dei dati.

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.

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                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1         configured     enabled   heal roots
   completed
         cluster_B
                 node_B_2         unreachable    -         switched over
   42 entries were displayed.metrocluster operation show
   ```

2. Verificare che tutti gli aggregati siano `mirrored`:

   ```
   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. Nodi di boot dal sito di disastro.
4. Controllare lo stato del ripristino dello switchback:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
            node_A_1            configured     enabled   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                              Configuration  DR
   Group Cluster Node              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.

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. Spegnere gli alimentatori del bridge.
2. Verificare che il monitoraggio del bridge indichi un errore:

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                                  Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
   Status
   ---------- ------------- ------- --------- ---------------- ---------
   -------
   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.

La procedura migliore consiste nel collegare ciascun alimentatore di un componente a un alimentatore separato. 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 e uno shelf completo potrebbe non essere disponibile. Il guasto di una linea di alimentazione viene testato per verificare che non vi siano incongruenze nel cablaggio che potrebbero causare un'interruzione del servizio.

Questo test dovrebbe richiedere circa 15 minuti.

Questo test richiede lo spegnimento di tutte le PDU di sinistra e quindi di tutte le PDU di destra su tutti i rack contenenti i componenti MetroCluster.

Questa procedura ha i seguenti risultati attesi:

- Gli errori devono essere generati quando le PDU sono disconnesse.
- Non devono verificarsi failover o perdita di servizio.

Fasi

1. Spegnere le PDU sul lato sinistro del rack contenente i componenti MetroCluster.
2. Monitorare il risultato sulla console utilizzando `system environment sensors show -state fault` e. `storage shelf show -errors` comandi.

```
cluster_A::> system environment sensors show -state fault

Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
4 entries were displayed.

cluster_A::> storage shelf show -errors
    Shelf Name: 1.1
     Shelf UID: 50:0a:09:80:03:6c:44:d5
 Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf
power supply unit "1". The unit might fail.Reconnect PSU1
```

3. Riaccendere le PDU di sinistra.
4. Assicurarsi che ONTAP cancella la condizione di errore.
5. Ripetere i passaggi precedenti con le PDU di destra.

Verifica del funzionamento dopo la perdita di un singolo shelf di storage

È possibile verificare il guasto di un singolo shelf di storage per verificare che non vi sia un singolo punto di errore.

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::> vserver show -type data

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       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. Spegnere fisicamente lo shelf selezionato.
6. Controllare di nuovo lo stato dell'aggregato:

   ```
   storage aggregate

   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::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       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
```

Connessioni in configurazioni MetroCluster stretch con LUN array

Connessioni in configurazioni MetroCluster stretch con LUN array

In una configurazione stretch MetroCluster, con LUN array, è necessario collegare le porte FC-VI tra i controller. È supportata la connettività diretta tra i controller e gli array di storage e-Series. Per tutti gli altri array di configurazioni LUN, è necessario utilizzare

switch FC nella configurazione.

È inoltre possibile impostare una configurazione stretch MetroCluster con dischi e LUN di array. In tale configurazione, è necessario utilizzare bridge FC-SAS o cavi ottici SAS per collegare i controller ai dischi.

Esempio di configurazione stretch MetroCluster con LUN array

In una configurazione stretch MetroCluster con LUN array, è necessario collegare le porte FC-VI per la connettività diretta tra i controller. Inoltre, è necessario collegare ciascuna porta HBA del controller alle porte dello switch degli switch FC corrispondenti. Il cablaggio ai LUN degli array è lo stesso di quello di un MetroCluster collegato a fabric, ad eccezione dei LUN degli array e-Series, che possono essere collegati direttamente.

La figura seguente mostra le porte FC-VI cablate tra i controller A e B in una configurazione stretch MetroCluster:

I moduli controller dei sistemi storage FAS9000 utilizzano quattro porte FC-VI ciascuna.

Per le configurazioni con LUN array e-Series, è possibile collegare direttamente i LUN e-Series.

"Supporto di collegamento diretto per la configurazione Stretch MetroCluster con array NetApp e-Series"

Ad eccezione del collegamento delle porte FC-VI, il resto di questa procedura serve per configurare una configurazione MetroCluster con LUN di array, che non utilizzano LUN di array e-Series. Ciò richiede switch FC che siano gli stessi dell'utilizzo di LUN array nelle configurazioni fabric-attached.

"Installazione e configurazione di Fabric-Attached MetroCluster"

Esempi di configurazioni MetroCluster stretch a due nodi con dischi e LUN di array

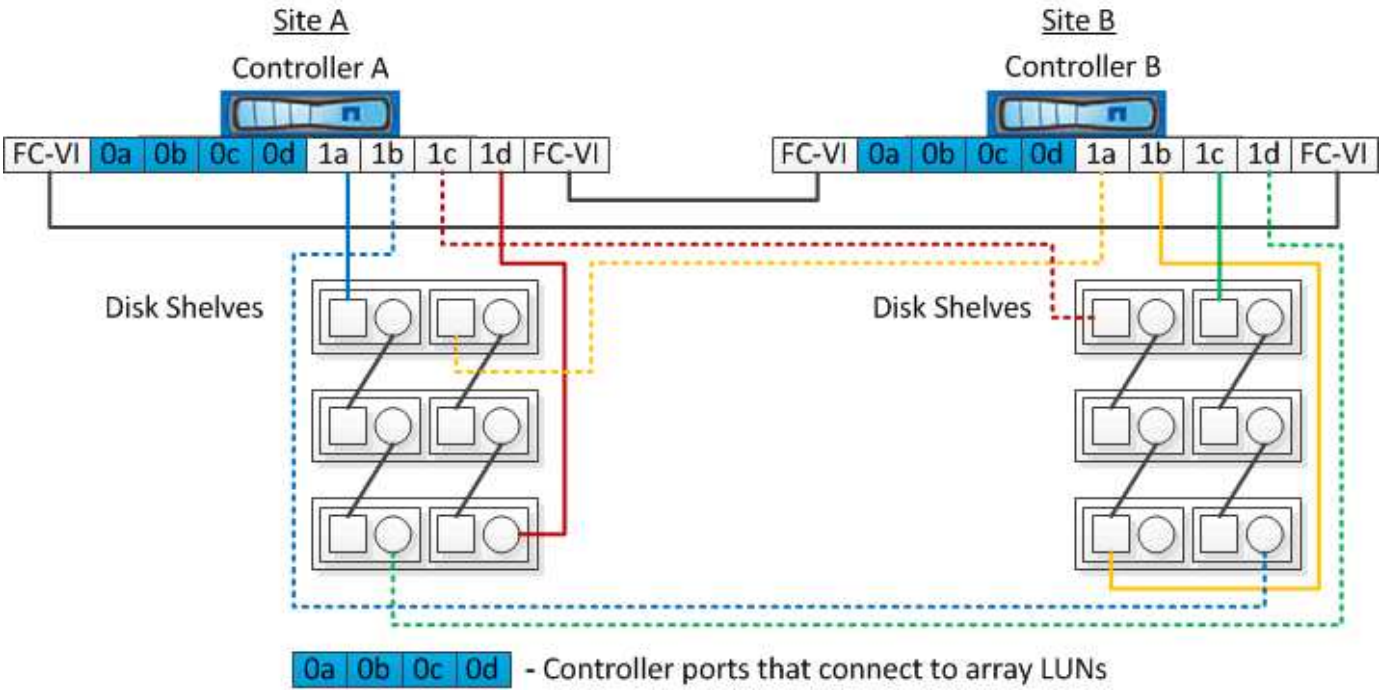
Per configurare una configurazione stretch MetroCluster con dischi nativi e LUN di array, è necessario utilizzare bridge FC-SAS o cavi ottici SAS per collegare i sistemi ONTAP agli shelf di dischi. Inoltre, è necessario utilizzare gli switch FC per collegare i LUN degli array ai sistemi ONTAP.

Sono necessarie almeno otto porte HBA per il collegamento di un sistema ONTAP a dischi nativi e LUN di array.

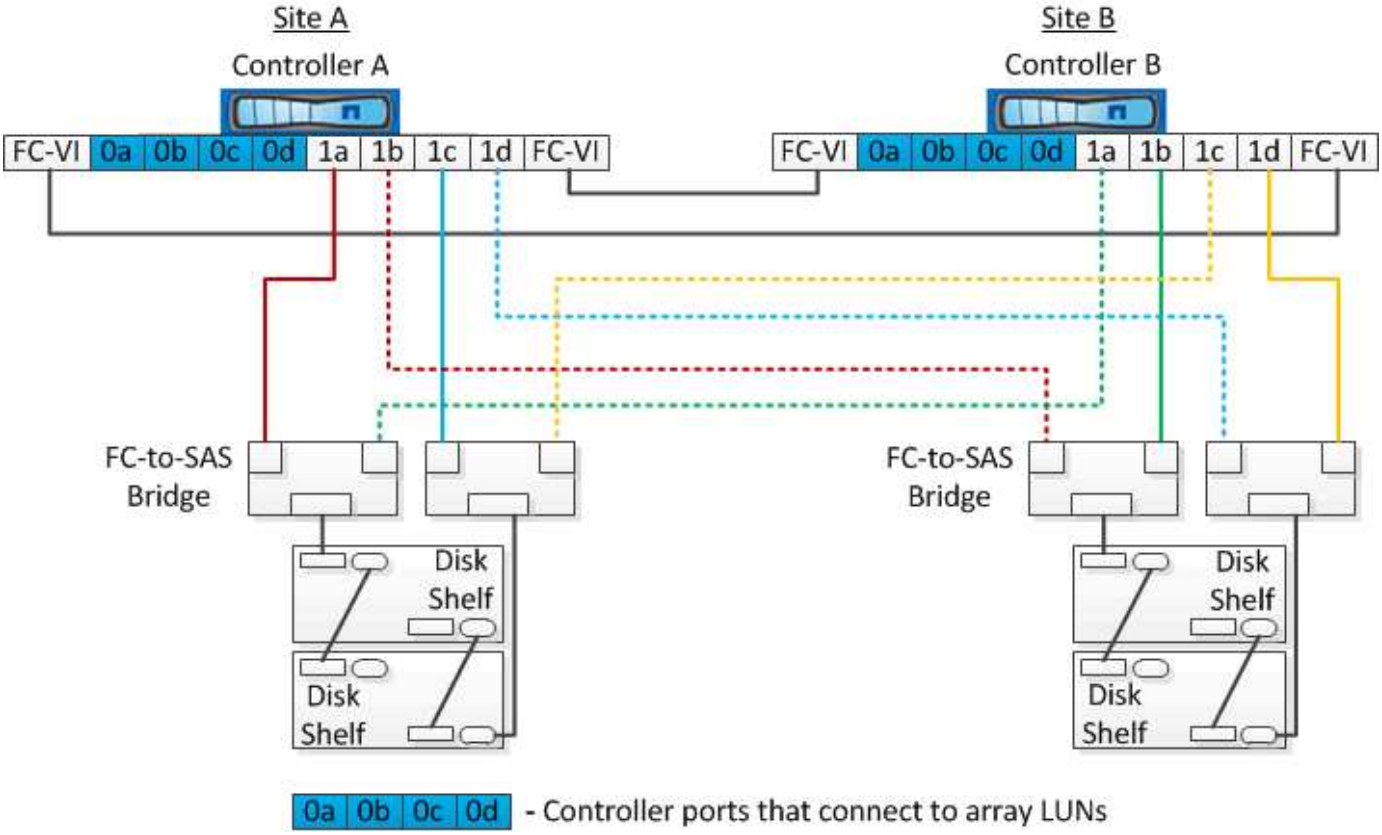
Nei seguenti esempi che rappresentano configurazioni stretch MetroCluster a due nodi con dischi e LUN di array, le porte HBA da 0a a 0d vengono utilizzate per il collegamento con LUN di array. Le porte HBA da 1a a

1d vengono utilizzate per le connessioni con dischi nativi.

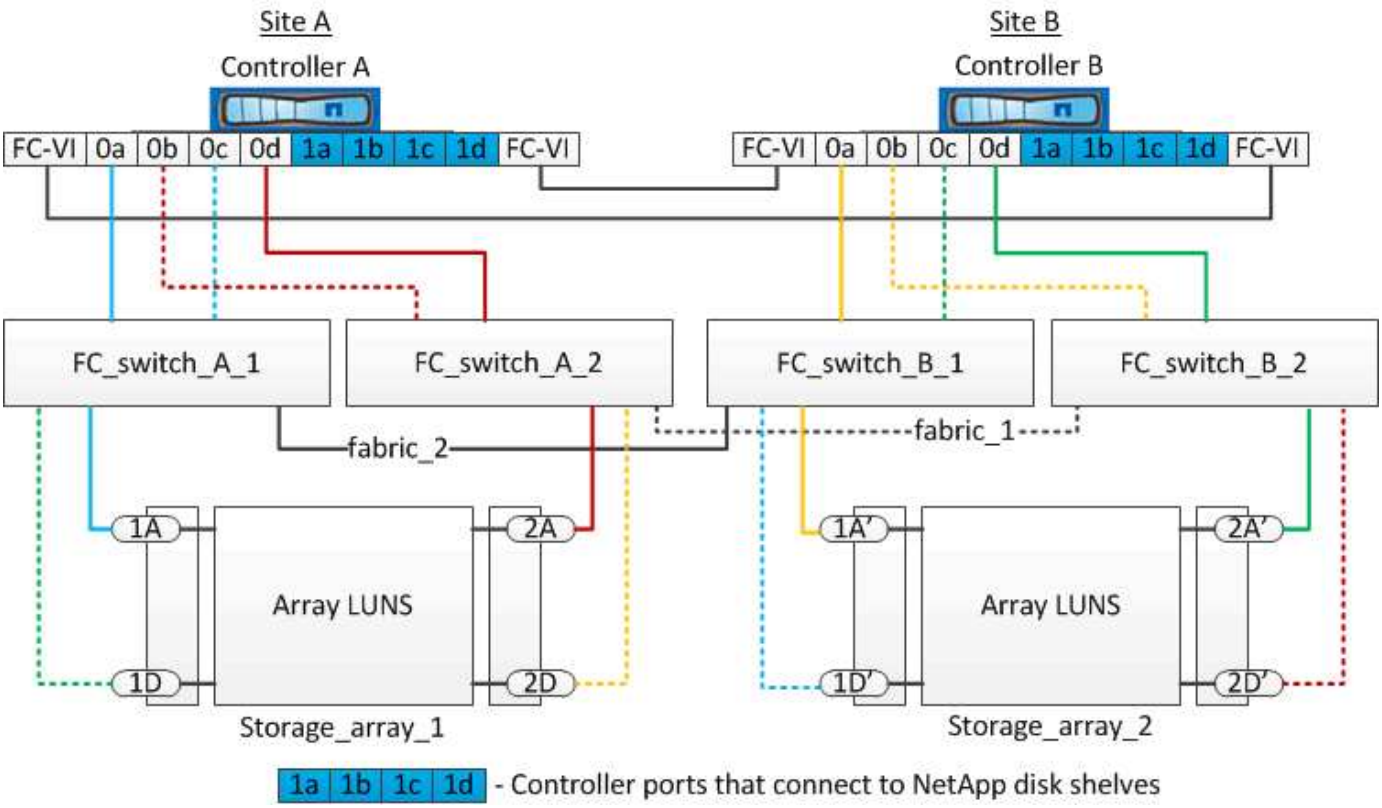
La figura seguente mostra una configurazione Stretch MetroCluster a due nodi in cui i dischi nativi sono collegati ai sistemi ONTAP utilizzando cavi ottici SAS:



La figura seguente mostra una configurazione Stretch MetroCluster a due nodi in cui i dischi nativi sono connessi ai sistemi ONTAP utilizzando bridge FC-SAS:



La figura seguente mostra una configurazione Stretch MetroCluster a due nodi con le connessioni LUN dell'array:



Se necessario, è anche possibile utilizzare gli stessi switch FC per collegare i dischi nativi e le LUN degli array ai controller nella configurazione MetroCluster.

"Installazione e configurazione di Fabric-Attached MetroCluster"

Esempio di configurazione stretch MetroCluster con storage array e-Series

In una configurazione stretch MetroCluster con un array di storage e-Series, è possibile collegare direttamente i controller di storage e gli array di storage. A differenza di altri LUN di array, non sono richiesti switch FC.

Il "Supporto di collegamento diretto per la configurazione Stretch MetroCluster con array NetApp e-Series" L'articolo della Knowledge base fornisce esempi di configurazioni con LUN array e-Series.

Considerazioni sulla rimozione delle configurazioni MetroCluster

È possibile rimuovere la configurazione MetroCluster 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."

Come utilizzare Active IQ Unified Manager e Gestore di sistema di ONTAP per ulteriori configurazioni e monitoraggi

Utilizzo di Active IQ Unified Manager e Gestore di sistema di ONTAP per ulteriori configurazioni e monitoraggi

Active IQ Unified Manager e Gestore di sistema ONTAP possono essere utilizzati per la gestione GUI dei cluster e il monitoraggio della configurazione.

Ogni nodo dispone di Gestione di sistema ONTAP preinstallato. Per caricare System Manager, inserire l'indirizzo LIF di gestione del cluster come URL in un browser Web che dispone di connettività al nodo.

È inoltre possibile utilizzare Active IQ Unified Manager per monitorare la configurazione di MetroCluster.

Informazioni correlate

"Documentazione di Active IQ Unified Manager e Gestore di sistema di ONTAP"

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.

Verificare di aver scaricato e installato System Manager. System Manager è disponibile sul sito di supporto NetApp.

- Non è possibile modificare le impostazioni del fuso orario per un nodo guasto o per il nodo partner dopo l'acquisizione.
- Ogni cluster nella configurazione MetroCluster FC deve disporre di uno o più server NTP separati utilizzati dai nodi e (se presenti) 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 quando i cluster coinvolti si trovano in una modalità disconnessa durante lo switchover.

Ad esempio:

- Un'estremità del FlexCache (cache_1 su vs1) risiede nel sito MetroCluster_A ha un'estremità del FlexCache
- L'altra estremità del FlexCache (origin_1 su vs2) risiede sul sito_C (non nella configurazione MetroCluster)

Quando viene attivato lo switchover e se Site_A e Site_C non sono connessi, è necessario revocare

manualmente le SVM sul sito_B (il cluster di switchover) e sul sito_C utilizzando `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.

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, consultare "Gestione di dischi e aggregati".

Considerazioni sull'utilizzo di FabricPools

- I cluster devono disporre di licenze FabricPool con limiti di capacità corrispondenti.
- I cluster devono avere IPspaces con nomi corrispondenti.

  Può trattarsi dell'IPSpace predefinito o di uno spazio IP creato da un amministratore. Questo IPSpace verrà utilizzato per le impostazioni di configurazione dell'archivio di oggetti FabricPool.

- Per l'IPSpace selezionato, ciascun cluster deve avere una LIF intercluster definita che possa raggiungere l'archivio di oggetti esterno

Configurazione di un aggregato per l'utilizzo in un FabricPool mirrorato

> Prima di configurare l'aggregato, è necessario impostare gli archivi di oggetti come descritto in "impostazione degli archivi di oggetti per FabricPool in una configurazione MetroCluster" in "Gestione di dischi e aggregati".

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 si trova fisicamente più lontano dal cluster rispetto all'archivio di oggetti primario.

Supporto FlexGroup nelle configurazioni MetroCluster

A partire da ONTAP 9.6, le configurazioni MetroCluster supportano i volumi FlexGroup.

Pianificazioni dei lavori in una configurazione MetroCluster

In ONTAP 9.3 e versioni successive, le pianificazioni dei processi create dall'utente vengono replicate

automaticamente tra i cluster in una configurazione MetroCluster. Se si crea, modifica o elimina una pianificazione di processo su un cluster, la stessa pianificazione viene creata automaticamente sul cluster partner, utilizzando il servizio di replica configurazione (CRS).

> Le pianificazioni create dal sistema non vengono replicate ed è necessario eseguire manualmente la stessa operazione sul cluster partner in modo che le pianificazioni dei processi su entrambi i cluster siano identiche.

Peering dei cluster dal sito MetroCluster a un terzo cluster

Poiché la configurazione di peering non viene replicata, se si esegue il peer di uno dei cluster della configurazione MetroCluster in un terzo cluster esterno a tale configurazione, è necessario configurare anche il peering sul cluster MetroCluster del partner. In questo modo, è possibile mantenere il peering in caso di commutazione.

Il cluster non MetroCluster deve eseguire ONTAP 8.3 o versione successiva. In caso contrario, il peering viene perso se si verifica uno switchover anche se il peering è stato configurato su entrambi i partner MetroCluster.

Replica della configurazione del client LDAP in una configurazione MetroCluster

Una configurazione del client LDAP creata su una macchina virtuale di storage (SVM) su un cluster locale viene replicata nella SVM dei dati del partner sul cluster remoto. Ad esempio, se la configurazione del client LDAP viene creata sulla SVM amministrativa sul cluster locale, viene replicata su tutti gli SVM dei dati di amministrazione sul cluster remoto. Questa funzione MetroCluster è intenzionale in modo che la configurazione del client LDAP sia attiva su tutte le SVM partner sul cluster remoto.

Linee guida per il networking e la creazione di LIF per le configurazioni MetroCluster

È necessario conoscere le modalità di creazione e replica delle LIF in una configurazione MetroCluster. È inoltre necessario conoscere i requisiti di coerenza per poter prendere decisioni appropriate durante la configurazione della rete.

Informazioni correlate

"Concetti di ONTAP"

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.

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.

Requisiti e problemi di posizionamento e replica LIF

È necessario conoscere i requisiti di replica LIF in una configurazione MetroCluster. È inoltre necessario conoscere il modo in cui un LIF replicato viene collocato in un cluster di partner e tenere presenti i problemi che si verificano quando la replica LIF o il posizionamento LIF non riesce.

Replica di LIF nel cluster del partner

Quando si crea una LIF su un cluster in una configurazione MetroCluster, la LIF viene replicata sul cluster partner. I LIF non vengono posizionati in base al nome uno a uno. Per verificare la disponibilità di LIF dopo un'operazione di switchover, il processo di posizionamento LIF verifica che le porte siano in grado di ospitare LIF in base ai controlli di raggiungibilità e attributo delle porte.

Il sistema deve soddisfare le seguenti condizioni per inserire i file LIF replicati nel cluster del partner:

Condizione	Tipo LIF: FC	Tipo LIF: IP/iSCSI
Identificazione del nodo	ONTAP tenta di collocare il LIF replicato nel partner di disaster recovery (DR) del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.	ONTAP tenta di posizionare il LIF replicato sul partner DR del nodo in cui è stato creato. Se il partner DR non è disponibile, il partner ausiliario DR viene utilizzato per il posizionamento.
Identificazione della porta	ONTAP identifica le porte di destinazione FC collegate sul cluster DR.	Le porte del cluster DR che si trovano nello stesso IPSpace del LIF di origine vengono selezionate per un controllo di raggiungibilità. Se non sono presenti porte nel cluster DR nello stesso IPSpace, non è possibile posizionare la LIF. Tutte le porte del cluster di DR che ospitano già una LIF nello stesso IPSpace e nella stessa subnet vengono automaticamente contrassegnate come raggiungibili e possono essere utilizzate per il posizionamento. Queste porte non sono incluse nel controllo di raggiungibilità.

Controllo della raggiungibilità	La raggiungibilità viene determinata verificando la connettività del WWN del fabric di origine sulle porte del cluster DR. Se lo stesso fabric non è presente nel sito di DR, il LIF viene posizionato su una porta casuale del partner di DR.	La raggiungibilità è determinata dalla risposta a una trasmissione ARP (Address Resolution Protocol) da ciascuna porta precedentemente identificata sul cluster DR all'indirizzo IP di origine della LIF da posizionare. Per il successo dei controlli di raggiungibilità, le trasmissioni ARP devono essere consentite tra i due cluster. Ogni porta che riceve una risposta dalla LIF di origine verrà contrassegnata come possibile per il posizionamento.
Selezione della porta	ONTAP classifica le porte in base ad attributi quali tipo di adattatore e velocità, quindi seleziona le porte con attributi corrispondenti. Se non vengono trovate porte con attributi corrispondenti, la LIF viene posizionata su una porta connessa in modo casuale del partner DR.	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. 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. 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. ONTAP classifica le porte in base ad attributi quali tipo di adattatore, tipo di interfaccia e velocità, quindi seleziona le porte con attributi corrispondenti.
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.

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.

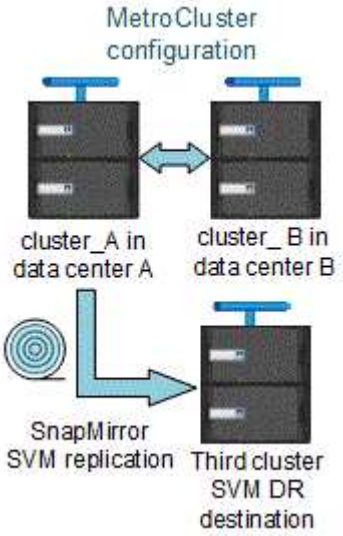
È necessario conoscere i seguenti requisiti e limitazioni dell'utilizzo di SVM con il disaster recovery SnapMirror:

- 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.

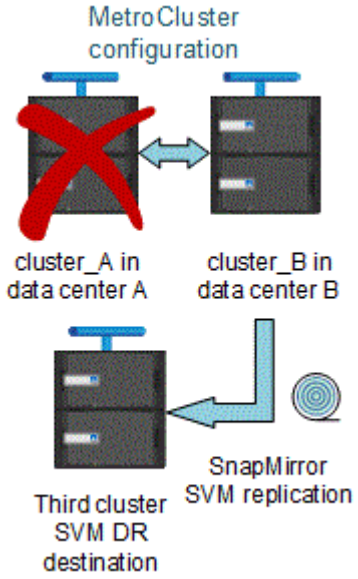
- Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.

  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.

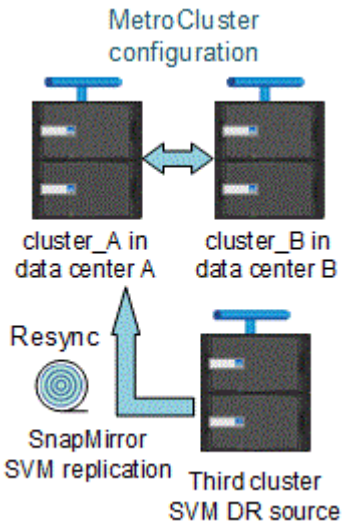
  Tuttavia, una volta completato il processo di switchover o switchback, gli aggiornamenti pianificati per il DR SVM successivi avranno esito positivo.

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 dello shelf di storage e del disco di storage mostra i comandi in una configurazione stretch MetroCluster a due nodi

In una configurazione Stretch MetroCluster a due nodi, il `is-local-attach` campo di `storage disk show` e. `storage shelf show` i comandi mostrano tutti i dischi e gli shelf di storage come locali, indipendentemente dal nodo a cui sono collegati.

L'output per il comando di visualizzazione plesso dell'aggregato di storage 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.

> 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).

Fasi

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
   ```

Passaggio da una configurazione MetroCluster con collegamento a fabric a una configurazione stretch

In una configurazione Fabric-Attached MetroCluster, i nodi si trovano in posizioni diverse. Questa differenza geografica aumenta la protezione dai disastri. Per passare da una configurazione MetroCluster stretch a una fabric-attached, è necessario aggiungere alla configurazione switch FC e, se necessario, bridge FC-SAS.

- È necessario disattivare lo switchover automatico su entrambi i cluster eseguendo `metrocluster modify -auto-switchover-failure-domain auto-disabled` comando.
- È necessario arrestare i nodi.

  Questa procedura ha un'interruzione.

La configurazione MetroCluster deve essere eseguita su entrambi i siti. Dopo aver aggiornato la configurazione MetroCluster, è necessario attivare lo switchover automatico su entrambi i cluster. È inoltre necessario convalidare la configurazione eseguendo `metrocluster check run` comando.

Questa procedura fornisce una panoramica delle fasi richieste. Per informazioni dettagliate, fare riferimento alle sezioni specifiche di "Installazione e configurazione di Fabric-Attached MetroCluster". Non è necessario eseguire un'installazione e una configurazione complete.

Fasi

1. Preparare l'aggiornamento consultando attentamente la sezione "preparazione dell'installazione di MetroCluster" di "Installazione e configurazione di Fabric-Attached MetroCluster".

2. Installare, collegare e configurare gli switch e i bridge FC-SAS richiesti.

> Attenersi alle procedure descritte nella sezione "collegamento di una configurazione MetroCluster collegata al fabric" di "Installazione e configurazione di Fabric-Attached MetroCluster".

3. Aggiornare la configurazione MetroCluster seguendo la procedura riportata di seguito.

   Non utilizzare le procedure descritte nella sezione "Configurazione del software MetroCluster in ONTAP" della "Installazione e configurazione di Fabric-Attached MetroCluster".

   a. Accedere alla modalità avanzata dei privilegi:
      `set -privilege advanced`

   b. Aggiornare la configurazione MetroCluster:
      `metrocluster configure -refresh true`

      Il seguente comando aggiorna la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true
[Job 009] Job succeeded: Configure is successful.
```

   a. Tornare alla modalità privilegi di amministratore:
      `set -privilege admin`

4. Verificare la presenza di errori nella configurazione MetroCluster e verificare che sia operativa.

   Attenersi alle procedure descritte nelle seguenti sezioni di "Installazione e configurazione di Fabric-Attached MetroCluster":

   - Verifica degli errori di configurazione di MetroCluster con Config Advisor
   - Verifica del funzionamento locale di ha
   - Verifica dello switchover, della riparazione e dello switchback

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione e sul funzionamento di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto
"Documentazione di ONTAP 9"	• Tutte le guide MetroCluster
	• Panoramica tecnica della configurazione e del funzionamento del MetroCluster FC. • Best practice per la configurazione MetroCluster FC.

"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Installazione e configurazione di MetroCluster IP: Differenze tra le configurazioni di ONTAP MetroCluster"	• Architettura IP di MetroCluster • Cablaggio della configurazione • Configurazione di MetroCluster in ONTAP
"Gestione MetroCluster e disaster recovery"	• Informazioni sulla configurazione di MetroCluster • Switchover, healing e switchback • Disaster recovery (DR)
"Gestire i componenti di MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster FC • Sostituzione o aggiornamento dell'hardware. Procedure di aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch • Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch • Sostituzione dell'hardware in un sito di disaster recovery in una configurazione MetroCluster FC con connessione fabric o stretch • Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.
"Transizione da MetroCluster FC a MetroCluster IP" "Guida all'upgrade e all'espansione di MetroCluster"	• Aggiornamento o aggiornamento di una configurazione MetroCluster • Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP • Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi

"Installazione e configurazione del software MetroCluster Tiebreaker"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
Documentazione Active IQ Unified Manager "Documentazione NetApp: Guide e risorse sui prodotti"	• Monitoraggio della configurazione e delle prestazioni di MetroCluster
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster
"Concetti di ONTAP"	• Come funzionano gli aggregati mirrorati

Installare e configurare MetroCluster Tiebreaker

Novità

Ogni versione include miglioramenti al software MetroCluster Tiebreaker. Ecco le novità delle ultime versioni di MetroCluster Tiebreaker.

Miglioramenti

Versione Tiebreaker ONTAP	Miglioramenti
1.6	• Maggiore facilità di installazione • Aggiornamento delle librerie di supporto • Miglioramenti della sicurezza
1.5	• Aggiornamento delle librerie di supporto • Miglioramenti della sicurezza
1,4	• Aggiornamento delle librerie di supporto

Matrice di supporto del sistema operativo

Versione Tiebreaker	CentOS 7 - 7,9	Red Hat 7 - 7,9	Red Hat 8,1 - 8,7	Red Hat 8,8 -9,2	Rocky Linux 9.0
1.6	No	No	Sì	Sì	Sì
1.5	No	No	Sì	No	No
1,4	Sì	Sì	Sì	No	No

Panoramica del software Tiebreaker

È utile comprendere che cos'è il software NetApp MetroCluster Tiebreaker e come si distingue tra i tipi di guasti in modo da poter monitorare le configurazioni MetroCluster in modo efficiente. La CLI di tiebreaker consente di gestire le impostazioni e monitorare lo stato e le operazioni delle configurazioni MetroCluster.

Rilevamento degli errori con il software NetApp MetroCluster Tiebreaker

Il software Tiebreaker è necessario solo se si desidera monitorare due cluster e lo stato di connettività tra di essi da un terzo sito. Il software Tiebreaker si trova su un host Linux nel terzo sito e consente a ciascun partner in un cluster di distinguere tra un errore ISL, quando i collegamenti tra siti sono inattivi, da un errore del sito.

Dopo aver installato il software Tiebreaker su un host Linux, è possibile configurare i cluster in una configurazione MetroCluster per monitorare le condizioni di emergenza.

Il software Tiebreaker è in grado di monitorare fino a 15 configurazioni MetroCluster contemporaneamente. Supporta una combinazione di configurazioni MetroCluster IP, MetroCluster FC e Stretch MetroCluster.

Il modo in cui il software Tiebreaker rileva i guasti del sito

Il software NetApp MetroCluster Tiebreaker verifica la raggiungibilità dei nodi in una configurazione MetroCluster e del cluster per determinare se si è verificato un guasto al sito. Il software di spareggio attiva anche un avviso in determinate condizioni.

Componenti monitorati dal software Tiebreaker

Il software Tiebreaker monitora ciascun controller nella configurazione MetroCluster stabilendo connessioni ridondanti attraverso percorsi multipli a una LIF di gestione dei nodi e alla LIF di gestione dei cluster, entrambi ospitati sulla rete IP.

Il software Tiebreaker monitora i seguenti componenti nella configurazione MetroCluster:

- Nodi attraverso interfacce di nodi locali
- Attraverso le interfacce designate dal cluster
- Sopravvivenza del cluster per valutare se dispone di connettività al sito di disastro (interconnessione NV, storage e peering intercluster)

In caso di perdita di connessione tra il software Tiebreaker e tutti i nodi del cluster e del cluster stesso, il cluster viene dichiarato “non raggiungibile” dal software Tiebreaker. Il rilevamento di un errore di connessione richiede da tre a cinque secondi. Se un cluster non è raggiungibile dal software di spareggio, il cluster che rimane (il cluster che è ancora raggiungibile) deve indicare che tutti i collegamenti al cluster partner sono interrotti prima che il software di spareggio attivi un avviso.

> Tutti i collegamenti vengono interrotti se il cluster sopravvissuto non riesce più a comunicare con il cluster nel sito di disastro tramite FC (interconnessione e storage NV) e peering tra cluster.

Scenari di guasto durante i quali il software di spareggio attiva un avviso

Il software di spareggio attiva un avviso quando il cluster (tutti i nodi) nel sito di disastro è inattivo o irraggiungibile e il cluster nel sito sopravvissuto indica lo stato “AllLinksSevered”.

Il software di spareggio non attiva un avviso (o l’avviso viene vetoato) nei seguenti scenari:

- In una configurazione MetroCluster a otto nodi, se una coppia ha nel sito di emergenza non è attiva
- In un cluster con tutti i nodi nel sito di disastro non attivi, una coppia ha nel sito di sopravvivenza è inattiva e il cluster nel sito di sopravvivenza indica lo stato “AllLinksSevered”

  Il software di spareggio attiva un avviso, ma ONTAP veto tale avviso. In questa situazione, viene veto anche lo switchover manuale

- Qualsiasi scenario in cui il software di spareggio può raggiungere almeno un nodo o l’interfaccia del cluster nel sito di disastro, oppure il sito sopravvissuto può ancora raggiungere uno dei due nodi nel sito di disastro tramite FC (interconnessione e storage NV) o peering intercluster

Informazioni correlate

"Rischi e limitazioni dell'utilizzo di MetroCluster Tiebreaker in modalità attiva"

Il modo in cui il software Tiebreaker rileva gli errori di connettività tra siti

Il software MetroCluster Tiebreaker avvisa l'utente in caso di perdita di tutte le connessioni tra i siti.

Tipi di percorsi di rete

A seconda della configurazione, esistono tre tipi di percorsi di rete tra i due cluster in una configurazione MetroCluster:

- **Rete FC (presente nelle configurazioni Fabric-Attached MetroCluster)**

  Questo tipo di rete è composto da due fabric switch FC ridondanti. Ogni fabric di switch dispone di due switch FC, con uno switch di ciascun fabric di switch co-allocato con un cluster. Ogni cluster dispone di due switch FC, uno per ciascun fabric di switch. Tutti i nodi sono dotati di connettività FC (interconnessione NV e iniziatore FCP) a ciascuno degli switch FC co-localizzati. I dati vengono replicati dal cluster al cluster tramite l'ISL.

- **Rete di peering intercluster**

  Questo tipo di rete è composto da un percorso di rete IP ridondante tra i due cluster. La rete di peering del cluster fornisce la connettività necessaria per eseguire il mirroring della configurazione della macchina virtuale di storage (SVM). La configurazione di tutte le SVM su un cluster viene sottoposta a mirroring dal cluster partner.

- **Rete IP (presente nelle configurazioni MetroCluster IP)**

  Questo tipo di rete è composto da due reti di switch IP ridondanti. Ogni rete dispone di due switch IP, con uno switch per ciascun fabric switch co-allocato con un cluster. Ogni cluster dispone di due switch IP, uno per ciascun fabric di switch. Tutti i nodi sono connessi a ciascuno switch FC co-localizzati. I dati vengono replicati dal cluster al cluster tramite l'ISL.

Monitoraggio della connettività tra siti

Il software Tiebreaker recupera regolarmente lo stato della connettività tra siti dai nodi. Se la connettività di interconnessione NV viene persa e il peering dell'intercluster non risponde ai ping, i cluster presumono che i siti siano isolati e il software di spareggio attiva un avviso come "AllLinksSevered". Se un cluster identifica lo stato "AllLinksSevered" e l'altro cluster non è raggiungibile attraverso la rete, il software di spareggio attiva un avviso come "disaster".

In che modo i diversi tipi di disastro influiscono sul tempo di rilevamento del software Tiebreaker

Per una migliore pianificazione del disaster recovery, il software MetroCluster Tiebreaker richiede un po' di tempo per rilevare un disastro. Questo tempo impiegato è il "dtempo di rilevamento dell'isaster". Il software MetroCluster Tiebreaker rileva il disastro del sito entro 30 secondi dal verificarsi del disastro e attiva l'operazione di disaster recovery per avvisare l'utente in merito.

Il tempo di rilevamento dipende anche dal tipo di disastro e potrebbe superare i 30 secondi in alcuni scenari, noti soprattutto come "disastri in corso". I principali tipi di disastro in corso sono i seguenti:

- Perdita di alimentazione
- Panico
- Arrestare o riavviare
- Perdita di switch FC nel sito di emergenza

Perdita di alimentazione

Il software Tiebreaker attiva immediatamente un avviso quando il nodo smette di funzionare. In caso di interruzione dell'alimentazione, tutte le connessioni e gli aggiornamenti, ad esempio peering tra cluster, interconnessione NV e disco della mailbox, si interrompono. Il tempo necessario tra l'irraggiungibile del cluster, il rilevamento del disastro e il trigger, compreso il tempo di inattività predefinito di 5 secondi, non deve superare i 30 secondi.

Panico

Nelle configurazioni MetroCluster FC, il software di spareggio attiva un avviso quando la connessione di interconnessione NV tra i siti è inattiva e il sito sopravvissuto indica lo stato "AllLinksSevered". Questo avviene solo dopo il completamento del processo di coredump. In questo scenario, il tempo impiegato tra il passaggio da un cluster all'altro e il rilevamento di un disastro potrebbe essere più lungo o approssimativamente uguale al tempo impiegato per il processo di coredump. In molti casi, il tempo di rilevamento è superiore a 30 secondi.

Se un nodo smette di funzionare ma non genera un file per il processo di coredump, il tempo di rilevamento non deve superare i 30 secondi. Nelle configurazioni MetroCluster IP, il sistema NV smette di comunicare e il sito sopravvissuto non è a conoscenza del processo di coredump.

Arrestare o riavviare

Il software di spareggio attiva un avviso solo quando il nodo è inattivo e il sito sopravvissuto indica lo stato "AllLinksSevered". Il tempo impiegato tra l'inraggiungibile del cluster e il rilevamento di un disastro potrebbe essere superiore a 30 secondi. In questo scenario, il tempo necessario per rilevare un disastro dipende dal tempo necessario per l'arresto dei nodi nel sito di disastro.

Perdita di switch FC nel sito di emergenza (configurazione Fabric-Attached MetroCluster)

Il software di spareggio attiva un avviso quando un nodo smette di funzionare. In caso di perdita degli switch FC, il nodo tenta di ripristinare il percorso di un disco per circa 30 secondi. Durante questo periodo di tempo, il nodo è attivo e risponde sulla rete di peering. Quando entrambi gli switch FC sono disattivi e non è possibile ripristinare il percorso di un disco, il nodo genera un errore MultiDiskFailure e si arresta. Il tempo impiegato tra il guasto dello switch FC e il numero di volte in cui i nodi hanno generato errori MultiDiskFailure è di circa 30 secondi più lungo. Questi 30 secondi aggiuntivi devono essere aggiunti al tempo di rilevamento dei disastri.

Informazioni sulle pagine di manuale e CLI di spareggio

La CLI di Tiebreaker fornisce comandi che consentono di configurare in remoto il software di Tiebreaker e monitorare le configurazioni MetroCluster.

Il prompt dei comandi CLI è rappresentato come NetApp MetroCluster tiebreaker::.

Le pagine man sono disponibili nella CLI inserendo il nome del comando appropriato al prompt.

Installare il software Tiebreaker

Flusso di lavoro di installazione di Tiebreaker

Il software Tiebreaker offre funzionalità di monitoraggio per un ambiente di storage in cluster. Inoltre, invia notifiche SNMP in caso di problemi di connettività del nodo e di disastri del sito.

Questo flusso di lavoro

È possibile utilizzare questo flusso di lavoro per installare o aggiornare il software Tiebreaker.

1. **"Preparare l'installazione del software Tiebreaker"**

Prima di installare e configurare il software Tiebreaker, verificare che il sistema soddisfi determinati requisiti.

2. **"Fissare l'installazione"**

Per le configurazioni che eseguono MetroCluster Tiebreaker 1.5 e versioni successive, è possibile proteggere e rafforzare il sistema operativo host e il database.

3. **"Installare il pacchetto software Tiebreaker"**

Eseguire una nuova installazione o aggiornamento del software Tiebreaker. La procedura di installazione che segui dipende dalla versione di Tiebreaker che desideri installare.

Preparare l'installazione del software Tiebreaker

Prima di installare e configurare il software Tiebreaker, è necessario verificare che il sistema soddisfi determinati requisiti.

Requisiti software

È necessario soddisfare i seguenti requisiti software a seconda della versione di Tiebreaker che si sta installando.

Versione Tiebreaker ONTAP	Versioni di ONTAP supportate	Versioni Linux supportate	Requisiti Java/MariaDB
1.6	ONTAP 9.12.1 e versioni successive	Fare riferimento a. "Matrice di supporto del sistema operativo" per ulteriori informazioni.	Nessuno. Le dipendenze vengono fornite in bundle con l'installazione.

1.5	Da ONTAP 9,8 a ONTAP 9.14.1	• Red Hat Enterprise Linux dal 8.1 al 8.7	Con Red Hat Enterprise Linux da 8,1 a 8,7: • MariaDB 10.x (utilizzare la versione predefinita installata utilizzando "yum install mariadb-server.x86_64") • OpenJDK 17, 18 o 19
1,4	Da ONTAP 9,1 a ONTAP 9.9.1	• Red Hat Enterprise Linux dal 8.1 al 8.7 • Red Hat Enterprise Linux da 7 a 7,9 • CentOS da 7 a 7,9 64 bit	Con CentOS: • MariaDB 5.5.52.x/MySQL Server 5.6x • 4 GB DI RAM • Aprire JRE 8 Con Red Hat Enterprise Linux da 8,1 a 8,7: • MariaDB 10.x (utilizzare la versione predefinita installata utilizzando "yum install mariadb-server.x86_64") • JRE 8

Requisiti aggiuntivi

È necessario essere a conoscenza dei seguenti requisiti aggiuntivi:

- Il software Tiebreaker viene installato su un terzo sito, consentendo al software di distinguere tra un errore di collegamento interswitch (ISL) (quando i collegamenti tra siti sono inattivi) e un guasto del sito. Il sistema host deve soddisfare determinati requisiti prima di poter installare o aggiornare il software Tiebreaker per monitorare la configurazione MetroCluster.
- Per installare il software MetroCluster Tiebreaker e i pacchetti dipendenti, è necessario disporre dei privilegi "root".
- È possibile utilizzare un solo monitor MetroCluster Tiebreaker per ogni configurazione MetroCluster per evitare qualsiasi conflitto con più monitor Tiebreaker.
- Quando si seleziona l'origine NTP (Network Time Protocol) per il software Tiebreaker, è necessario utilizzare un'origine NTP locale. Il software Tiebreaker non deve utilizzare la stessa fonte dei siti MetroCluster monitorati dal software Tiebreaker.
- Capacità del disco: 8 GB
- Firewall:
  - Accesso diretto per la configurazione dei messaggi AutoSupport
  - SSH (porta 22/TCP), HTTPS (porta 443/TCP) e ping (ICMP)

Proteggere l'installazione dell'host tiebreaker e del database

Per le configurazioni che eseguono MetroCluster Tiebreaker 1.5 e versioni successive, è possibile proteggere e rafforzare il sistema operativo host e il database.

Proteggere l'host

Le seguenti linee guida mostrano come proteggere l'host in cui è installato il software Tiebreaker.

Consigli per la gestione degli utenti

- Limitare l'accesso dell'utente "root".
  - È possibile utilizzare utenti in grado di elevare l'accesso root per installare e amministrare il software Tiebreaker.
  - È possibile utilizzare utenti che non sono in grado di elevare l'accesso root per amministrare il software Tiebreaker.
  - Durante l'installazione, è necessario creare un gruppo denominato "mctbgrp". L'utente root dell'host e l'utente creato durante l'installazione devono essere entrambi membri. Solo i membri di questo gruppo possono amministrare completamente il software di spareggio.

    > Gli utenti che non sono membri di questo gruppo non possono accedere al software Tiebreaker o alla CLI. È possibile creare utenti aggiuntivi sull'host e renderli membri del gruppo. Questi membri aggiuntivi non possono amministrare completamente il software Tiebreaker. Hanno accesso a ReadOnly e non possono aggiungere, modificare o eliminare i monitor.

  - Non eseguire tiebreaker come utente root. Utilizzare un account di servizio dedicato e senza privilegi per eseguire Tiebreaker.
- Modificare la stringa di comunità predefinita nel file "/etc/snmp/snmpd.conf".
- Consentire privilegi di scrittura minimi. L'account di servizio tiebreaker senza privilegi non deve avere accesso per sovrascrivere il binario eseguibile o qualsiasi file di configurazione. Solo le directory e i file per lo storage tiebreaker locale (ad esempio, per lo storage backend integrato) o i log di audit devono essere scrivibili dall'utente di tiebreaker.
- Non consentire utenti anonimi.
  - Impostare AllowTcpForwarding su "no" o utilizzare la direttiva Match per limitare gli utenti anonimi.

Informazioni correlate

- "Documentazione del prodotto Red Hat Enterprise Linux 8"
- "Documentazione del prodotto Red Hat Enterprise Linux 9"

Raccomandazioni sulla protezione dell'host di base

- Utilizzare la crittografia del disco
  - È possibile attivare la crittografia del disco. Può essere FullDiskEncryption (hardware) o la crittografia fornita dall'host (software) o dall'host SVM.
- Disattiva i servizi inutilizzati che consentono le connessioni in entrata. È possibile disattivare qualsiasi servizio non in uso. Il software Tiebreaker non richiede un servizio per le connessioni in entrata perché tutte le connessioni dall'installazione di Tiebreaker sono in uscita. I servizi che potrebbero essere attivati per impostazione predefinita e che possono essere disattivati sono:
  - Server HTTP/HTTPS
  - Server FTP
  - Telnet, RSH, rlogin

- Accesso a NFS, CIFS e altri protocolli
- RDP (RemoteDesktopProtocol), X11 Server, VNC o altri provider di servizi "desktop" remoti.

> Per amministrare l'host in remoto, è necessario lasciare attivato l'accesso alla console seriale (se supportato) o almeno un protocollo. Se si disattivano tutti i protocolli, è necessario disporre dell'accesso fisico all'host per l'amministrazione.

- Proteggere l'host utilizzando FIPS
  - È possibile installare il sistema operativo host in modalità conforme a FIPS, quindi installare Tiebreaker.

> OpenJDK 19 verifica all'avvio se l'host è installato in modalità FIPS. Non devono essere richieste modifiche manuali.

  - Se si protegge l'host, è necessario assicurarsi che sia in grado di avviarsi senza l'intervento dell'utente. Se è necessario l'intervento dell'utente, la funzionalità Tiebreaker potrebbe non essere disponibile se l'host si riavvia inaspettatamente. In questo caso, la funzionalità Tiebreaker è disponibile solo dopo l'intervento manuale e quando l'host è completamente avviato.
- Disattiva Cronologia comandi shell.
- Eseguire l'aggiornamento frequentemente. Tiebreaker è sviluppato attivamente e l'aggiornamento frequente è importante per incorporare correzioni di sicurezza e qualsiasi modifica nelle impostazioni predefinite, come la lunghezza delle chiavi o le suite di crittografia.
- Iscriviti alla mailing list di HashiCorp Announcement per ricevere gli annunci delle nuove release e visita il sito di Tiebreaker CHANGELOG per maggiori dettagli sugli aggiornamenti più recenti delle nuove release.
- Utilizzare le autorizzazioni file corrette. Prima di avviare il software Tiebreaker, assicurarsi sempre che vengano applicate autorizzazioni appropriate ai file, in particolare a quelli contenenti informazioni sensibili.
- L'autenticazione multifattore (MFA) migliora la sicurezza della tua organizzazione richiedendo agli amministratori di identificarsi utilizzando più di un nome utente e una password. Anche se importante, i nomi utente e le password sono vulnerabili agli attacchi di forza bruta e possono essere rubati da terze parti.
  - Red Hat Enterprise Linux 8 fornisce MFA che richiede agli utenti di fornire più di un'informazione per eseguire correttamente l'autenticazione su un account o un host Linux. Le informazioni aggiuntive potrebbero essere una password monouso inviata al telefono cellulare tramite SMS o credenziali da un'applicazione come Google Authenticator, Twilio Authy o FreeOTP.

Informazioni correlate

- "Documentazione del prodotto Red Hat Enterprise Linux 8"
- "Documentazione del prodotto Red Hat Enterprise Linux 9"

Proteggere l'installazione del database

Le seguenti linee guida mostrano come proteggere e rafforzare l'installazione del database MariaDB 10.x.

- Limitare l'accesso dell'utente "root".
  - Tiebreaker utilizza un account dedicato. L'account e le tabelle per la memorizzazione dei dati (di configurazione) vengono creati durante l'installazione di Tiebreaker. L'unica volta che è necessario un accesso elevato al database è durante l'installazione.
- Durante l'installazione sono necessari i seguenti privilegi e accesso:

- La possibilità di creare un database e tabelle
- La possibilità di creare opzioni globali
- La possibilità di creare un utente del database e di impostare la password
- Possibilità di associare l'utente del database al database e alle tabelle e assegnare i diritti di accesso

> L'account utente specificato durante l'installazione di Tiebreaker deve disporre di tutti questi privilegi. L'utilizzo di più account utente per le diverse attività non è supportato.

- Utilizzare la crittografia del database
  - È supportata la crittografia dei dati inattivi. "Scopri di più sulla crittografia dei dati a riposo"
  - I dati in volo non sono crittografati. I dati in volo utilizzano una connessione di file locale "SOCKS".
  - Conformità FIPS per MariaDB: Non è necessario attivare la conformità FIPS nel database. È sufficiente installare l'host in modalità conforme a FIPS.

    "Ulteriori informazioni su MySQL Enterprise transparent Data Encryption (TDE)"

> Le impostazioni di crittografia devono essere attivate prima dell'installazione del software Tiebreaker.

Informazioni correlate

- Gestione degli utenti del database

  "Controllo degli accessi e gestione degli account"

- Proteggere il database

  "Rendere MySQL sicuro dagli attacchi"

  "Protezione di MariaDB"

- Installazione sicura del vault

  "Protezione avanzata della produzione"

Installare il pacchetto software Tiebreaker

Scegliere la procedura di installazione

La procedura di installazione di Tiebreaker che segue dipende dalla versione di Tiebreaker che si sta installando.

Versione Tiebreaker	Vai a…
Tiebreaker 1,6	"Installare il Tiebreaker 1,6"
Tiebreaker 1,5	"Installare il Tiebreaker 1,5"

Tiebreaker 1,4	"Installare il Tiebreaker 1,4"

Installare il Tiebreaker 1,6

Eseguire una nuova installazione o un aggiornamento a tiebreaker 1,6 sul sistema operativo Linux host per monitorare le configurazioni MetroCluster.

A proposito di questa attività

- Il sistema storage deve eseguire ONTAP 9.12.1 o versione successiva.
- È possibile installare MetroCluster Tiebreaker come utente non root con privilegi amministrativi sufficienti per eseguire l'installazione di tiebreaker, creare tabelle e utenti e impostare la password utente.

Fasi

1. Scaricare il software MetroCluster Tiebreaker 1,6.

   "MetroCluster Tiebreaker (Download) - Sito di supporto NetApp"

2. Accedere all'host come utente root.
3. Se si sta eseguendo un aggiornamento, verificare la versione di tiebreaker in esecuzione:

   L'esempio seguente mostra il tiebreaker 1,5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Installare o aggiornare il software Tiebreaker.

Installare il Tiebreaker 1,6

Per una nuova installazione di Tiebreaker 1,6, procedere come segue.

Fasi

a. Eseguire il seguente comando nella `[root@mcctb ~] #` prompt per iniziare l'installazione:

```
sh MetroClusterTiebreakerInstall-1.6
```

Il sistema visualizza i seguenti output per una corretta installazione:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish to
create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
```

```
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing version
history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
```

```
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping rollback
manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully mounted:
```

```
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities restored
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6.
```

Aggiornamento da tiebreaker 1,5 a 1,6

Per aggiornare la versione software di Tiebreaker 1,5 a Tiebreaker 1,6, procedere come segue.

Fasi

a. Eseguire il seguente comando nella `[root@mcctb ~] #` richiesta di aggiornamento del software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Il sistema visualizza il seguente output per un aggiornamento riuscito:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
```

```
Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping rollback
manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener: rpc
listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
```

```
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing version
history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier not
initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier not
initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping token
key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting rollback
manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
```

```
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge collection
is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping rollback
manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping token
key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting rollback
manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge collection
```

```
is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
```

```
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
```

```
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Aggiornamento da tiebreaker 1,4 a 1,6

Per aggiornare la versione software di Tiebreaker 1,4 a Tiebreaker 1,6, procedere come segue.

Fasi

a. Eseguire il seguente comando nella `[root@mcctb ~] #` richiesta di aggiornamento del software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Il sistema visualizza il seguente output per un aggiornamento riuscito:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish to
create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.
```

```
MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing version
history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier not
initialized
```

```
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping rollback
manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
```

```
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
```

```
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
```

```
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
```

```
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

Installare il Tiebreaker 1,5

Configurare l'accesso amministratore all'API e all'SSH ONTAP

È possibile configurare l'accesso admin alle API e SSH ONTAP.

Fasi

1. Creare un utente amministratore con accesso API ONTAP: `security login create -user-or -group-name mcctb -application ontapi -authentication-method password`
2. Creare un utente amministratore con accesso SSH: `security login create -user-or-group -name mcctb -application ssh -authentication-method password`
3. Verificare che siano stati creati i nuovi utenti admin: `security login show`
4. Ripetere questi passaggi sul cluster partner.

> "Autenticazione amministratore e RBAC" è implementato.

Installare le dipendenze di MetroCluster tiebreaker 1,5

A seconda del sistema operativo Linux host, è necessario installare un server MySQL o MariaDB prima di installare o aggiornare il software tiebreaker.

Fasi

1. Installare JDK
2. Installare e configurare il vault
3. Installare il server MySQL o MariaDB:

Se l'host Linux è	Quindi…
Red Hat Enterprise Linux 7/CentOS 7	Installare MySQL Server 5.5.30 o versioni successive e 5,6.x su Red Hat Enterprise Linux 7 o CentOS 7
Red Hat Enterprise Linux 8	Installare il server MariaDB su Red Hat Enterprise Linux 8

Installare JDK

È necessario installare JDK sul sistema host prima di installare o aggiornare il software tiebreaker. Tiebreaker 1,5 e versioni successive supporta OpenJDK 17, 18 o 19.

Fasi

1. Accedere come utente "root" o come utente sudo che può passare alla modalità avanzata dei privilegi.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Controllare le versioni JDK disponibili:

```
yum search openjdk
```

3. Installare JDK 17,18 o 19.

   Il seguente comando installa JDK 17:

   ```
   yum install java-17-openjdk
   ```

4. Verificare l'installazione:

   ```
   java -version
   ```

   Una corretta installazione visualizza il seguente output:

   ```
   openjdk version "17.0.2" 2022-01-18 LTS
   OpenJDK Runtime Environment 21.9 (build 17.0.2+8-LTS)
   OpenJDK 64-Bit Server VM 21.9 (build 17.0.2+8-LTS, mixed mode, sharing)
   ```

Installare e configurare il vault

Se non si dispone o si desidera utilizzare il server del vault locale, è necessario installare Vault. Si può fare riferimento a questa procedura standard per l'installazione del vault o fare riferimento alle istruzioni di installazione di Hashicorp per linee guida alternative.

> Se si dispone di un server vault nella rete, è possibile configurare l'host MetroCluster Tiebreaker per l'utilizzo dell'installazione del vault. In questo caso, non è necessario installare Vault sull'host.

Fasi

1. Passare a. `/bin` directory:

   ```
   [root@mcctb] cd /bin
   ```

2. Scaricare il file zip del vault.

   ```
   [root@mcctb /bin]#  curl -sO
   https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
   ```

3. Decomprimere il file del vault.

   ```
   [root@mcctb /bin]# unzip vault_1.12.2_linux_amd64.zip
   Archive:  vault_1.12.2_linux_amd64.zip
     inflating: vault
   ```

4. Verificare l'installazione.

```
[root@mcctb /bin]# vault -version
Vault v1.12.2 (415e1fe3118eebd5df6cb60d13defdc01aa17b03), built 2022-11-
23T12:53:46Z
```

5. Passare a. `/root` directory:

```
[root@mcctb /bin] cd /root
```

6. Creare un file di configurazione del vault in `/root` directory.

   Su `[root@mcctb ~]` prompt, copiare ed eseguire il comando seguente per creare `config.hcl` file:

```
# cat > config.hcl << EOF
 storage "file" {
  address = "127.0.0.1:8500"
  path    = "/mcctb_vdata/data"
 }
 listener "tcp" {
   address     = "127.0.0.1:8200"
   tls_disable = 1
 }
EOF
```

7. Avviare il server del vault:

```
[root@mcctb ~] vault server -config config.hcl &
```

8. Esportare l'indirizzo del vault.

```
[root@mcctb ~]# export VAULT_ADDR="http://127.0.0.1:8200"
```

9. Inizializzare il vault.

```
[root@mcctb ~]# vault operator init
2022-12-15T14:57:22.113+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.113+0530 [INFO]  core: seal configuration missing,
not initialized
2022-12-15T14:57:22.114+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.116+0530 [INFO]  core: security barrier initialized:
```

```
stored=1 shares=5 threshold=3
2022-12-15T14:57:22.118+0530 [INFO]  core: post-unseal setup starting
2022-12-15T14:57:22.137+0530 [INFO]  core: loaded wrapping token key
2022-12-15T14:57:22.137+0530 [INFO]  core: Recorded vault version: vault
version=1.12.2 upgrade time="2022-12-15 09:27:22.137200412 +0000 UTC"
build date=2022-11-23T12:53:46Z
2022-12-15T14:57:22.137+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T14:57:22.137+0530 [INFO]  core: no mounts; adding default
mount table
2022-12-15T14:57:22.143+0530 [INFO]  core: successfully mounted backend:
type=cubbyhole version="" path=cubbyhole/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=system version="" path=sys/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=identity version="" path=identity/
2022-12-15T14:57:22.148+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T14:57:22.149+0530 [INFO]  rollback: starting rollback manager
2022-12-15T14:57:22.149+0530 [INFO]  core: restoring leases
2022-12-15T14:57:22.150+0530 [INFO]  expiration: lease restore complete
2022-12-15T14:57:22.150+0530 [INFO]  identity: entities restored
2022-12-15T14:57:22.150+0530 [INFO]  identity: groups restored
2022-12-15T14:57:22.151+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T14:57:23.385+0530 [INFO]  core: post-unseal setup complete
2022-12-15T14:57:23.387+0530 [INFO]  core: root token generated
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown starting
2022-12-15T14:57:23.387+0530 [INFO]  rollback: stopping rollback manager
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown complete
Unseal Key 1: <unseal_key_1_id>
Unseal Key 2: <unseal_key_2_id>
Unseal Key 3: <unseal_key_3_id>
Unseal Key 4: <unseal_key_4_id>
Unseal Key 5: <unseal_key_5_id>

Initial Root Token: <initial_root_token_id>


Vault initialized with 5 key shares and a key threshold of 3. Please
securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to
unseal it
before it can start servicing requests.
```

```
Vault does not store the generated root key. Without at least 3 keys to
reconstruct the root key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum
of
existing unseal keys shares. See "vault operator rekey" for more
information.
```

È necessario registrare e memorizzare gli ID della chiave e il token principale iniziale in una posizione sicura per poterli utilizzare successivamente nella procedura.

10. Esportare il token root del vault.

```
[root@mcctb ~]#  export VAULT_TOKEN="<initial_root_token_id>"
```

11. Rimuovere il sigillo del vault usando tre delle cinque chiavi create.

È necessario eseguire `vault operator unseal` comando per ciascuna delle tre chiavi:

a. Rimuovere il sigillo del vault usando la prima chiave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    1/3
Unseal Nonce       <unseal_key_1_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

b. Rimuovere il sigillo del vault usando la seconda chiave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
Key                Value
---                -----
Seal Type          shamir
Initialized        true
Sealed             true
Total Shares       5
Threshold          3
Unseal Progress    2/3
Unseal Nonce       <unseal_key_2_id>
Version            1.12.2
Build Date         2022-11-23T12:53:46Z
Storage Type       file
HA Enabled         false
```

c. Rimuovere il sigillo del vault usando la terza chiave:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=127.0.0.1:8201
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener: serving
cluster requests: cluster_listen_address=127.0.0.1:8201
2022-12-15T15:15:00.981+0530 [INFO]  core: post-unseal setup starting
2022-12-15T15:15:00.981+0530 [INFO]  core: loaded wrapping token key
2022-12-15T15:15:00.982+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T15:15:00.983+0530 [INFO]  core: successfully mounted
backend: type=system version="" path=sys/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=identity version="" path=identity/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=cubbyhole version="" path=cubbyhole/
2022-12-15T15:15:00.986+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T15:15:00.986+0530 [INFO]  rollback: starting rollback
manager
2022-12-15T15:15:00.987+0530 [INFO]  core: restoring leases
2022-12-15T15:15:00.987+0530 [INFO]  expiration: lease restore
complete
2022-12-15T15:15:00.987+0530 [INFO]  identity: entities restored
2022-12-15T15:15:00.987+0530 [INFO]  identity: groups restored
2022-12-15T15:15:00.988+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T15:15:00.989+0530 [INFO]  core: post-unseal setup complete
2022-12-15T15:15:00.989+0530 [INFO]  core: vault is unsealed
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

12. Verificare che lo stato del Vault Sealed sia falso.

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

13. Configurare il servizio Vault per avviarlo all'avvio.
    a. Eseguire il seguente comando: `cd /etc/systemd/system`

    ```
    [root@mcctb ~]#  cd /etc/systemd/system
    ```

    b. Su `[root@mcctb system]` Richiedere, copiare ed eseguire il comando seguente per creare il file di servizio del vault.

    ```
    # cat > vault.service << EOF
    [Unit]
    Description=Vault Service
    After=mariadb.service

    [Service]
    Type=forking
    ExecStart=/usr/bin/vault server -config /root/config.hcl &
    Restart=on-failure

    [Install]
    WantedBy=multi-user.target
    EOF
    ```

    c. Eseguire il seguente comando: `systemctl daemon-reload`

    ```
    [root@mcctb system]#  systemctl daemon-reload
    ```

    d. Eseguire il seguente comando: `systemctl enable vault.service`

```
[root@mcctb system]#  systemctl enable vault.service
Created symlink /etc/systemd/system/multi-
user.target.wants/vault.service → /etc/systemd/system/vault.service.
```

Viene richiesto di utilizzare questa funzione durante l'installazione di MetroCluster Tiebreaker. Se si desidera modificare il metodo per dissigillare il vault, è necessario disinstallare e reinstallare il software MetroCluster Tiebreaker.

Installare MySQL Server 5.5.30 o versioni successive e 5,6.x su Red Hat Enterprise Linux 7 o CentOS 7

È necessario installare MySQL Server 5.5.30 o versione successiva e la versione 5.6.x sul sistema host prima di installare o aggiornare il software Tiebreaker. Per Red Hat Enterprise Linux 8, Installare il server MariaDB.

Fasi

1. Accedere come utente root o sudo che può passare alla modalità avanzata dei privilegi.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Aggiungi il repository MySQL al tuo sistema host:

```
[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
========
Package               Arch   Version
                                     Repository
Size
=============================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
=============================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Disattivare il repository MySQL 57:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Abilitare il repository MySQL 56:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Abilitare il repository:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Installare il server della community MySQL:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
======
Package                          Arch   Version       Repository
Size
=============================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
=================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ---------------------------------------------------------------------------
--------
Total                                               289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. Avviare il server MySQL:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Verificare che MySQL Server sia in esecuzione:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Configurare le impostazioni di sicurezza e password:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                          hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Verificare che l'accesso MySQL funzioni:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Se il login MySQL funziona, l'output terminerà con `mysql>` prompt.

Abilitare l'impostazione di avvio automatico di MySQL

Verificare che la funzionalità di autostart sia attivata per il daemon MySQL. L'attivazione del daemon MySQL riavvia automaticamente MySQL se il sistema su cui risiede il software MetroCluster Tiebreaker si riavvia. Se il daemon MySQL non è in esecuzione, il software Tiebreaker continua a funzionare, ma non può essere riavviato e non è possibile apportare modifiche alla configurazione.

Fase

1. Verificare che MySQL sia abilitato all'avvio automatico all'avvio:

   ```
   [root@mcctb ~]# systemctl list-unit-files mysqld.service
   ```

   ```
   UNIT FILE          State
   ------------------ ----------
   mysqld.service     enabled
   ```

   Se MySQL non è abilitato all'avvio automatico all'avvio, consultare la documentazione di MySQL per abilitare la funzione di avvio automatico per l'installazione.

Installare il server MariaDB su Red Hat Enterprise Linux 8

È necessario installare il server MariaDB sul sistema host prima di installare o aggiornare il software Tiebreaker. Per Red Hat Enterprise Linux 7 o CentOS 7, Installare MySQL Server.

Prima di iniziare

Il sistema host deve essere in esecuzione su Red Hat Enterprise Linux (RHEL) 8.

Fasi

1. Accedere come a. `root` utente o utente che può passare alla modalità avanzata dei privilegi.

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
   ```

2. Installare il server MariaDB:

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   ```

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
    ...
    ...

   ==========================================================================
   ===
    Package                      Arch   Version         Repository
   Size
   ==========================================================================
   ===
   Installing:
   mariadb-server               x86_64   1:5.5.56-2.el7   base
   11 M
   ```

```
Installing for dependencies:

Transaction Summary
=========================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
-------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. Avviare il server MariaDB:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Verificare che il server MariaDB sia stato avviato:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Configurare le impostazioni di sicurezza e password:

> Quando viene richiesta la password di root, lasciarla vuota e premere Invio per continuare a configurare le impostazioni di sicurezza e password.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
```

```
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Attivare l’impostazione di avvio automatico per il server MariaDB

Verificare che la funzione di avvio automatico sia attivata per il server MariaDB. Se non si attiva la funzione di avvio automatico e il sistema su cui risiede il software MetroCluster Tiebreaker deve essere riavviato, il software Tiebreaker continua a funzionare, ma il servizio MariaDB non può essere riavviato e non è possibile apportare modifiche alla configurazione.

Fasi

1. Attivare il servizio di avvio automatico:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Verificare che MariaDB sia abilitato all'avvio automatico all'avvio:

   `[root@mcctb ~]# systemctl list-unit-files mariadb.service`

   ```
   UNIT FILE          State
   ------------------ ----------
   mariadb.service    enabled
   ```

Installare o aggiornare a tiebreaker 1,5

Eseguire una nuova installazione o un aggiornamento a tiebreaker 1,5 sul sistema operativo Linux host per monitorare le configurazioni MetroCluster.

A proposito di questa attività

- Nel tuo sistema storage deve essere in esecuzione una versione supportata di ONTAP. Vedere "Requisiti software" tabella per ulteriori dettagli.
- OpenJDK deve essere installato utilizzando `yum install java-x.x.x-openjdk` comando. Tiebreaker 1,5 e versioni successive supporta OpenJDK 17, 18 o 19.
- È possibile installare MetroCluster Tiebreaker come utente non root con privilegi amministrativi sufficienti per eseguire l'installazione di tiebreaker, creare tabelle e utenti e impostare la password utente.

Fasi

1. Scaricare il software MetroCluster Tiebreaker e la chiave MetroCluster_tiebreaker_RPM_GPG.

   > La chiave MetroCluster_tiebreaker_RPM_GPG è disponibile per il download dalla stessa pagina in cui è stato scaricato il pacchetto software per tiebreaker 1,5 sul sito di supporto NetApp.

   "MetroCluster Tiebreaker (Download) - Sito di supporto NetApp"

2. Accedere all'host come utente root.
3. Creare un utente non root e. `mcctbgrp` gruppo.

   a. Creare un utente non root e impostare la password.

      I seguenti comandi di esempio creano un utente non root denominato `mcctbuser1`:

      ```
      [root@mcctb ~]# useradd mcctbuser1
      [root@mcctb ~]# passwd mcctbuser1
      Changing password for user mcctbuser1.
      New password:
      Retype new password:
      passwd: all authentication tokens updated successfully.
      ```

   b. Creare un gruppo denominato `mcctbgrp`:

```
[root@mcctb ~~]# groupadd mcctbgrp
```

c. Aggiungere l'utente non root creato al `mcctbgrp` gruppo.

Viene aggiunto il seguente comando `mcctbuser1` al `mcctbgrp` gruppo:

```
[root@mcctb ~]# usermod -a -G mcctbgrp mcctbuser1
```

4. Verificare il file RPM.

Eseguire i seguenti passaggi secondari dalla directory che contiene la chiave RPM.

a. Scaricare e importare il file della chiave RPM:

```
[root@mcctb ~]# rpm --import MetroCluster_Tiebreaker_RPM_GPG.key
```

b. Verificare che sia stata importata la chiave corretta controllando l'impronta digitale.

L'esempio seguente mostra un'impronta digitale della chiave corretta:

```
root@mcctb:~/signing/mcctb-rpms# gpg --show-keys --with-fingerprint
MetroCluster_Tiebreaker_RPM_GPG.key
pub   rsa3072 2022-11-17 [SCEA] [expires: 2025-11-16]
      65AC 1562 E28A 1497 7BBD  7251 2855 EB02 3E77 FAE5
uid                      MCCTB-RPM (mcctb RPM production signing)
<mcctb-rpm@netapp.com>
```

a. Verificare la firma: `rpm --checksig NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

```
NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm: digests OK
```

> È necessario procedere con l'installazione solo dopo aver verificato la firma.

5. Installa o aggiorna il software tiebreaker:

> È possibile eseguire l'aggiornamento alla versione 1.5 di Tiebreaker solo quando si esegue l'aggiornamento dalla versione 1.4 di Tiebreaker. L'aggiornamento da versioni precedenti a tiebreaker 1.5 non è supportato.

Selezionare la procedura corretta a seconda che si stia eseguendo una nuova installazione o aggiornando un'installazione esistente.

Eseguire una nuova installazione

a. Recuperare e registrare il percorso assoluto per Java:

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Eseguire il seguente comando: `rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

   Il sistema visualizza i seguenti output per una corretta installazione:

   > Quando richiesto durante l'installazione, fornire l'utente non root precedentemente creato e assegnato al `mcctbgrp` gruppo.

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Enter database user name:
root
Please enter database password for root
Enter password:
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.5.
```

Aggiornamento di un'installazione esistente

a. Verificare che sia installata una versione supportata di OpenJDK e che sia la versione corrente di Java presente sull'host.

> Per gli aggiornamenti a tiebreaker 1.5, è necessario installare OpenJDK versione 17, 18 o 19.

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Verificare che il servizio Vault sia dissigillato e in esecuzione: `vault status`

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault
Cluster ID      <cluster_id>
HA Enabled      false
```

c. Aggiornare il software Tiebreaker.

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.5-1.x86_64.rpm
```

Il sistema visualizza il seguente output per un aggiornamento riuscito:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]

Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Enter database user name : root
Please enter database password for root
Enter password:
Password updated successfully in the database.
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.5.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

> Se si immette la password root MySQL errata, il software Tiebreaker indica che è stato installato correttamente, ma visualizza i messaggi "Access denied" (accesso negato). Per risolvere il problema, è necessario disinstallare il software Tiebreaker utilizzando `rpm -e` E quindi reinstallare il software utilizzando la password root corretta di MySQL.

6. Verificare la connettività di Tiebreaker al software MetroCluster aprendo una connessione SSH dall'host di Tiebreaker a ciascuna delle LIF di gestione dei nodi e delle LIF di gestione dei cluster.

Informazioni correlate

"Supporto NetApp"

Installare il Tiebreaker 1,4

Installare le dipendenze di MetroCluster tiebreaker 1,4

A seconda del sistema operativo Linux host, installare un server MySQL o MariaDB prima di installare o aggiornare il software tiebreaker.

Fasi

1. Installare JDK.
2. Installare il server MySQL o MariaDB:

Se l'host Linux è	Quindi…
Red Hat Enterprise Linux 7/CentOS 7	Installare MySQL Server 5.5.30 o versioni successive e 5,6.x su Red Hat Enterprise Linux 7 o CentOS 7
Red Hat Enterprise Linux 8	Installare il server MariaDB su Red Hat Enterprise Linux 8

Installare JDK

È necessario installare JDK sul sistema host prima di installare o aggiornare il software tiebreaker. Tiebreaker 1,4 e versioni precedenti supporta JDK 1,8.0. (JRE 8).

Fasi

1. Accedere come utente "root".

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Installare JDK 1,8.0:

```
yum install java-1.8.0-openjdk.x86_64
```

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

=================================================================================
Package                Arch   Version                  Repository    Size
=================================================================================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4 updates      238 k
 ..
 ..
Transaction Summary
=================================================================================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Installare MySQL Server 5.5.30 o versioni successive e 5,6.x su Red Hat Enterprise Linux 7 o CentOS 7

È necessario installare MySQL Server 5.5.30 o versione successiva e la versione 5.6.x sul sistema host prima di installare o aggiornare il software Tiebreaker. Per Red Hat Enterprise Linux 8, Installare il server MariaDB.

Fasi

1. Accedere come utente root.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Aggiungi il repository MySQL al tuo sistema host:

```
[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
release-el6-11.noarch.rpm
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
========
Package               Arch   Version
                                     Repository
Size
=============================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
=============================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Disattivare il repository MySQL 57:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Abilitare il repository MySQL 56:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Abilitare il repository:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Installare il server della community MySQL:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
======
Package                          Arch   Version       Repository
Size
=============================================================================
======
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
=================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ---------------------------------------------------------------------------
--------
Total                                               289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. Avviare il server MySQL:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Verificare che MySQL Server sia in esecuzione:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Configurare le impostazioni di sicurezza e password:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                          hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Verificare che l'accesso MySQL funzioni:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Quando il login MySQL funziona come previsto, l'output termina al `mysql>` prompt.

Abilitare l'impostazione di avvio automatico di MySQL

Verificare che la funzionalità di autostart sia attivata per il daemon MySQL. L'attivazione del daemon MySQL riavvia automaticamente MySQL se il sistema su cui risiede il software MetroCluster Tiebreaker si riavvia. Se il daemon MySQL non è in esecuzione, il software Tiebreaker continua a funzionare, ma non può essere riavviato e non è possibile apportare modifiche alla configurazione.

Fase

1. Verificare che MySQL sia abilitato all'avvio automatico all'avvio:

   ```
   [root@mcctb ~]# systemctl list-unit-files mysqld.service
   ```

   ```
   UNIT FILE          State
   ------------------ ----------
   mysqld.service     enabled
   ```

   Se MySQL non è abilitato all'avvio automatico all'avvio, consultare la documentazione di MySQL per abilitare la funzione di avvio automatico per l'installazione.

Installare il server MariaDB su Red Hat Enterprise Linux 8

È necessario installare il server MariaDB sul sistema host prima di installare o aggiornare il software Tiebreaker. Per Red Hat Enterprise Linux 7 o CentOS 7, Installare MySQL Server.

Prima di iniziare

Il sistema host deve essere in esecuzione su Red Hat Enterprise Linux (RHEL) 8.

Fasi

1. Accedere come a. `root` utente.

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
   ```

2. Installare il server MariaDB:

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   ```

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
    ...
    ...

   ==========================================================================
   ===
    Package                      Arch   Version         Repository
   Size
   ==========================================================================
   ===
   Installing:
   mariadb-server               x86_64   1:5.5.56-2.el7   base
   11 M
   ```

```
Installing for dependencies:

Transaction Summary
================================================================================
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
--------------------------------------------------------------------------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. Avviare il server MariaDB:

```
[root@mcctb ~]# systemctl start mariadb
```

4. Verificare che il server MariaDB sia stato avviato:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

5. Configurare le impostazioni di sicurezza e password:

> Quando viene richiesta la password di root, lasciarla vuota e premere Invio per continuare a configurare le impostazioni di sicurezza e password.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
```

```
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

  ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Attivare l’impostazione di avvio automatico per il server MariaDB

Verificare che la funzione di avvio automatico sia attivata per il server MariaDB. Se non si attiva la funzione di avvio automatico e il sistema su cui risiede il software MetroCluster Tiebreaker deve essere riavviato, il software Tiebreaker continua a funzionare, ma il servizio MariaDB non può essere riavviato e non è possibile apportare modifiche alla configurazione.

Fasi

1. Attivare il servizio di avvio automatico:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Verificare che MariaDB sia abilitato all'avvio automatico all'avvio:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Installare o aggiornare a tiebreaker 1,4

Eseguire una nuova installazione o un aggiornamento a tiebreaker 1,4 sul sistema operativo Linux host per monitorare le configurazioni MetroCluster.

A proposito di questa attività

- Nel tuo sistema storage deve essere in esecuzione una versione supportata di ONTAP. Vedere "Requisiti software" tabella per ulteriori dettagli.
- OpenJDK deve essere installato utilizzando `yum install java-x.x.x-openjdk` comando. Tiebreaker 1,4 e versioni precedenti supporta JDK 1.8.0 (JRE 8).

Fasi

1. Scaricare il software MetroCluster Tiebreaker.

   "MetroCluster Tiebreaker (Download) - Sito di supporto NetApp"

2. Accedere all'host come utente root.
3. Installa o aggiorna il software tiebreaker:

   Selezionare la procedura corretta a seconda che si stia eseguendo una nuova installazione o aggiornando un'installazione esistente.

Eseguire una nuova installazione

a. Installare il software Tiebreaker eseguendo :

```
rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.4-1.x86_64.rpm
```

Il sistema visualizza i seguenti output per una corretta installazione:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Post installation start Fri Apr  5 02:28:09 EDT 2024
Enter MetroCluster Tiebreaker user password:

Please enter mysql root password when prompted
Enter password:
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post installation end Fri Apr  5 02:28:22 EDT 2024
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.4.
```

Aggiornare un’installazione esistente

a. Aggiornare il software Tiebreaker.

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.4-1.x86_64.rpm
```

Il sistema visualizza il seguente output per un aggiornamento riuscito:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Upgrading NetApp MetroCluster Tiebreaker software....
Stopping NetApp MetroCluster Tiebreaker software services before
upgrade.
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################## [ 50%]
Post installation start Mon Apr  8 06:29:51 EDT 2024
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Enabled autostart of NetApp MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp MetroCluster Tiebreaker software
CLI
Post upgrade end Mon Apr  8 06:29:51 EDT 2024
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.4.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################## [100%]
```

Se si immette la password root MySQL errata, il software Tiebreaker indica che è stato installato correttamente, ma visualizza i messaggi "Access denied" (accesso negato). Per risolvere il problema, è necessario disinstallare il software Tiebreaker utilizzando `rpm -e` E quindi reinstallare il software utilizzando la password root corretta di MySQL.

4. Verificare la connettività di Tiebreaker al software MetroCluster aprendo una connessione SSH dall'host di Tiebreaker a ciascuna delle LIF di gestione dei nodi e delle LIF di gestione dei cluster.

Informazioni correlate

"Supporto NetApp"

Aggiornare l'host in cui è in esecuzione il monitor Tiebreaker

Potrebbe essere necessario aggiornare l'host su cui è in esecuzione il monitor Tiebreaker.

Fasi

1. Disinstallare il software Tiebreaker:

   ```
   rpm -e NetApp-MetroCluster-Tiebreaker-Software
   ```

2. Aggiornare l'host. Per ulteriori informazioni, fare riferimento alla documentazione del sistema operativo host.
3. Reinstallare il software Tiebreaker.

   Eseguire una nuova installazione di Tiebreaker seguendo i passaggi descritti nella "Installare il software Tiebreaker".

Configurazione del software Tiebreaker

Dopo l'installazione del software Tiebreaker, è possibile aggiungere o modificare le configurazioni MetroCluster o rimuoverle dal software Tiebreaker.

Avvio della CLI del software Tiebreaker

Dopo aver installato il software Tiebreaker, è necessario avviarne la CLI per configurare il software.

1. Avviare la CLI dal prompt dell'host su cui è stato installato il software:

   ```
   netapp-metrocluster-tiebreaker-software-cli
   ```

2. Dopo l'installazione e durante il primo avvio, immettere la password per l'utente di Tiebreaker per accedere al database. Si tratta della password specificata per l'utente del database durante l'installazione.

Aggiunta di configurazioni MetroCluster

Dopo aver installato il software NetApp MetroCluster Tiebreaker, è possibile aggiungere altre configurazioni MetroCluster, una alla volta.

È necessario aver installato la configurazione MetroCluster in un ambiente ONTAP e aver attivato le impostazioni nel software.

1. Utilizzare il comando add dell'interfaccia a riga di comando (CLI) di tiebreaker per aggiungere configurazioni MetroCluster.

   Se si utilizza il nome host, questo deve essere il nome di dominio completo (FQDN).

   L'esempio seguente mostra la configurazione di cluster_A:

```
NetApp MetroCluster Tiebreaker :> monitor add wizard
Enter monitor Name: cluster_A
Enter Cluster IP Address: 10.222.196.130
Enter Cluster Username: admin
Enter Cluster Password:
Enter Peer Cluster IP Address: 10.222.196.40
Enter Peer Cluster Username: admin
Enter Peer Cluster Password:
Successfully added monitor to NetApp MetroCluster Tiebreaker software.
```

2. Verificare che la configurazione MetroCluster sia stata aggiunta correttamente utilizzando l'interfaccia CLI di tiebreaker `monitor show -status` comando.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

3. Disattivare la modalità osservatore affinché il software di spareggio avvii automaticamente uno switchover dopo aver rilevato un guasto del sito:

   `monitor modify -monitor-name monitor_name -observer-mode false`

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
-observer-mode false
Warning: If you are turning observer-mode to false, make sure to review
the 'risks and limitations'
as described in the MetroCluster Tiebreaker installation and
configuration.
Are you sure you want to enable automatic switchover capability for
monitor "8pack"? [Y/N]: y
```

Informazioni correlate

"Rischi e limitazioni dell'utilizzo di MetroCluster Tiebreaker in modalità attiva"

Comandi per la modifica delle configurazioni di MetroCluster Tiebreaker

È possibile modificare la configurazione MetroCluster ogni volta che si desidera modificare le impostazioni.

Il comando tiebreaker CLI monitor modify può essere utilizzato con una delle seguenti opzioni. È possibile confermare le modifiche con il comando monitor show -status.

Opzione	Descrizione
-nome-monitor	Nome della configurazione MetroCluster
-enable-monitor	Attiva e disattiva il monitoraggio della configurazione MetroCluster

-silent-period	Periodo in secondi per il quale il software MetroCluster Tiebreaker attende la conferma di un errore del sito dopo il rilevamento
-observer-mode	La modalità osservatore (true) fornisce solo il monitoraggio e non attiva uno switchover in caso di disastro del sito. La modalità online (false) attiva uno switchover in caso di disastro del sito. • "Il modo in cui il software Tiebreaker rileva i guasti del sito" • "Rischi e limitazioni dell'utilizzo di MetroCluster Tiebreaker in modalità attiva"

Nell'esempio seguente viene modificato il periodo di silenzio per la configurazione.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

La CLI di spareggio `debug` il comando può essere utilizzato per modificare la modalità di registrazione.

Comando	Descrizione
stato di debug	Visualizza lo stato della modalità di debug
abilitazione debug	Attiva la modalità di debug per la registrazione
disattivazione del debug	Disattiva la modalità di debug per la registrazione

Nei sistemi che eseguono tiebreaker 1.4 e versioni precedenti, la CLI di tiebreaker `update-mcctb-password` è possibile utilizzare il comando per aggiornare la password utente. Questo comando è obsoleto in tiebreaker 1.5 e versioni successive.

Comando	Descrizione
update-mctb-password	La password utente è stata aggiornata correttamente

Rimozione delle configurazioni MetroCluster

È possibile rimuovere la configurazione MetroCluster monitorata dal software Tiebreaker quando non si desidera più monitorare una configurazione MetroCluster.

1. Utilizzare l'interfaccia CLI di tiebreaker `monitor remove` Comando per rimuovere la configurazione MetroCluster.

   Nell'esempio seguente, "cluster_A" viene rimosso dal software:

```
NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
Successfully removed monitor from NetApp MetroCluster Tiebreaker
software.
```

2. Verificare che la configurazione MetroCluster sia stata rimossa correttamente utilizzando l'interfaccia CLI di Tiebreaker `monitor show -status` comando.

```
NetApp MetroCluster Tiebreaker :> monitor show -status
```

Configurazione delle impostazioni SNMP per il software Tiebreaker

Per utilizzare SNMP con il software Tiebreaker, è necessario configurare le impostazioni SNMP.

1. Utilizzare l'interfaccia CLI di tiebreaker `snmp config wizard` Comando per aggiungere configurazioni MetroCluster.

   Al momento è supportato un solo host trap SNMP.

   L'esempio seguente mostra la configurazione di un ricevitore SNMP che supporta SNMP V3 con un indirizzo IP 10.240.45.66 e il numero di porta 162 per i messaggi trap. Il software Tiebreaker è pronto per inviare trap al ricevitore SNMP specificato.

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Version[V1/V3]: v3
Enter SNMP Host: 10.240.45.66
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
Enter SNMP V3 Privacy password:
Engine ID : 8000031504932eff571825192a6f1193b265e24593
Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
software.
```

   È necessario configurare SNMPv3 perché SNMPv1 non è sicuro. Assicurarsi che la stringa di comunità predefinita sia **NOT** impostata su public.

2. Verificare che le impostazioni SNMP siano configurate:

```
snmp config test
```

   L'esempio seguente mostra che il software di spareggio può inviare una trap SNMP per l'evento TEST_SNMP_CONFIG:

```
NetApp MetroCluster Tiebreaker :> snmp config test
Sending SNMP trap to localhost. Version : V1.
Successfully sent SNMP trap for event TEST_SNMP_CONFIG
NetApp MetroCluster Tiebreaker :>
```

Monitoraggio della configurazione di MetroCluster

Il software MetroCluster Tiebreaker automatizza il processo di recovery consentendo di monitorare lo stato della configurazione MetroCluster, valutare gli eventi SNMP e le trap inviati al supporto clienti NetApp e visualizzare lo stato delle operazioni di monitoraggio.

Configurazione di AutoSupport

Per impostazione predefinita, i messaggi AutoSupport vengono inviati a NetApp una settimana dopo l'installazione del software Tiebreaker. Gli eventi che attivano la notifica AutoSupport includono la panoramica del software Tiebreaker, il rilevamento di condizioni di emergenza nelle configurazioni MetroCluster o uno stato di configurazione MetroCluster sconosciuto.

Prima di iniziare

Per configurare i messaggi AutoSupport, è necessario disporre di un accesso diretto.

Fasi

1. Utilizzare il comando tiebreaker CLI AutoSupport con una delle seguenti opzioni:

Opzione	Descrizione
-invoke	Invia un messaggio AutoSupport all'assistenza clienti
-configure wizard	Procedura guidata per configurare le credenziali del server proxy
-elimina configurazione	Elimina le credenziali del server proxy
--enable (attiva)	Attiva la notifica AutoSupport (impostazione predefinita).
-disable	Disattiva la notifica AutoSupport
-show	Visualizza lo stato del AutoSupport

L'esempio seguente mostra che AutoSupport è attivato o disattivato e la destinazione in cui viene inviato il contenuto AutoSupport:

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status            : disabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status            : enabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission      : success
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

L'esempio seguente mostra AutoSupport configurato per mezzo di un server proxy autenticato, utilizzando un indirizzo IP e un numero di porta:

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

L'esempio seguente mostra l'eliminazione di una configurazione AutoSupport:

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

Eventi e trap SNMP

Il software NetApp MetroCluster Tiebreaker utilizza trap SNMP per notificare eventi significativi. Questi trap fanno parte del file NetApp MIB. Ogni trap contiene le seguenti informazioni: Nome, severità, livello di impatto, data e ora e messaggio.

Nome dell'evento	Dettaglio dell'evento	Numero trap
L'interruttore automatico MetroCluster non è in grado di raggiungere la configurazione MetroCluster	Avvisa l'amministratore che il software non è in grado di rilevare un disastro. Questo evento si verifica quando entrambi i cluster non sono raggiungibili.	25000
Impossibile raggiungere il cluster con l'interruttore automatico MetroCluster	Avvisa l'amministratore che il software non riesce a raggiungere uno dei cluster.	25001
MetroCluster Tie-Breaker ha rilevato un disastro nel cluster	Notifica all'amministratore che il software rileva un errore del sito. Verrà inviata una notifica.	25002
Tutti i collegamenti tra cluster di partner vengono interrotti.	Il software rileva che entrambi i cluster sono raggiungibili, ma tutti i percorsi di rete tra i due cluster non sono disponibili e i cluster non possono comunicare tra loro.	25005
Trap di test SNMP	La configurazione SNMP può ora essere testata eseguendo il comando di test di configurazione snmp.	25006

Visualizzazione dello stato delle operazioni di monitoraggio

È possibile visualizzare lo stato generale delle operazioni di monitoraggio per una configurazione MetroCluster.

Fase

1. Utilizzare il comando tiebreaker CLI monitor show per visualizzare lo stato di un'operazione MetroCluster con una delle seguenti opzioni:

Opzione	Descrizione
-nome-monitor	Visualizza lo stato del nome del monitor specificato
-cronologia delle operazioni	Visualizza fino a 10 operazioni di monitoraggio eseguite per ultime su un cluster
-stats (statistiche)	Visualizza le statistiche relative al cluster specificato
-status	Visualizza lo stato del cluster specificato **Nota:** il software MetroCluster Tiebreaker potrebbe impiegare fino a 10 minuti per riflettere lo stato di completamento di operazioni come aggregati di heal, radici di heal o switchback.

Il seguente esempio mostra che i cluster cluster cluster cluster_A e cluster_B sono connessi e funzionanti:

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

Nell’esempio seguente vengono visualizzate le ultime sette operazioni eseguite su cluster_B:

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

Visualizzazione delle informazioni di configurazione di MetroCluster

È possibile visualizzare il nome del monitor e l'indirizzo IP di tutte le istanze di configurazioni MetroCluster nel software Tiebreaker.

Fase

1. Utilizzare il comando tiebreaker CLI Configuration show per visualizzare le informazioni di configurazione MetroCluster.

   L'esempio seguente mostra le informazioni per i cluster cluster cluster cluster_A e cluster_B:

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

Creazione di file dump

Si salva lo stato generale del software Tiebreaker in un file dump a scopo di debug.

Fase

1. Utilizzare il comando tilebreaker CLI monitor dump -status per creare un file dump dello stato generale di tutte le configurazioni MetroCluster.

   Nell'esempio seguente viene illustrata la corretta creazione del file dump /var/log/netapp/mctb/metrocluster-tiebreaker-status.xml:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

Rischi e limitazioni dell'utilizzo di MetroCluster Tiebreaker in modalità attiva

Lo switchover al rilevamento di un guasto di un sito avviene automaticamente, con MetroCluster Tiebreaker in modalità attiva. Questa modalità può essere utilizzata per integrare la funzionalità di switchover automatico di ONTAP/FAS.

Quando si implementa MetroCluster Tiebreaker in modalità attiva, i seguenti problemi noti possono causare la perdita di dati:

- In caso di errore del collegamento tra siti, i controller di ciascun sito continuano a servire i client. Tuttavia, i controller non verranno sottoposti a mirroring. Il guasto di un controller in un sito viene identificato come un guasto del sito e il Tiebreaker MetroCluster avvia uno switchover. I dati che non vengono mirrorati dopo un errore di collegamento tra siti con il sito remoto andranno persi.
- Si verifica uno switchover quando gli aggregati nel sito remoto sono in stato degradato. I dati non verranno replicati se lo switchover si è verificato prima della risincronizzazione dell'aggregato.
- Si verifica un errore dello storage remoto durante lo switchover.
- La memoria non volatile (NVRAM o NVMEM, a seconda del modello di piattaforma) nei controller di storage non viene sottoposta a mirroring con il partner di disaster recovery remoto (DR) sul sito del partner.
- I metadati vengono persi se la rete di peering del cluster rimane inattiva per un periodo prolungato e i volumi di metadati non sono online dopo uno switchover.

Potrebbero verificarsi scenari non menzionati. NetApp non è responsabile per eventuali danni derivanti dall'utilizzo di MetroCluster Tiebreaker in modalità attiva. Non utilizzare MetroCluster Tiebreaker in modalità attiva se i rischi e le limitazioni non sono accettabili per l'utente.

Requisiti del firewall per MetroCluster Tiebreaker

MetroCluster Tiebreaker utilizza una serie di porte per comunicare con servizi specifici.

La tabella seguente elenca le porte che è necessario consentire nel firewall:

Porta/servizi	Origine	Destinazione	Scopo
443 / TCP	Spareggio	Internet	Invio di messaggi AutoSupport a NetApp
22 / TCP	Host di gestione	Spareggio	Gestione di spareggio

443 / TCP	Spareggio	LIF di gestione del cluster	Comunicazioni sicure al cluster tramite HTTP (SSL)
22 / TCP	Spareggio	LIF di gestione del cluster	Comunicazioni sicure al cluster tramite SSH
443 / TCP	Spareggio	LIF di gestione dei nodi	Comunicazioni sicure al nodo tramite HTTP (SSL)
22 / TCP	Spareggio	LIF di gestione dei nodi	Comunicazioni sicure al nodo tramite SSH
162/UDP	Spareggio	Host trap SNMP	Utilizzato per inviare messaggi trap SNMP di notifica degli avvisi
ICMP (ping)	Spareggio	LIF di gestione del cluster	Controllare se l'IP del cluster è raggiungibile
ICMP (ping)	Spareggio	LIF di gestione dei nodi	Verificare che l'IP del nodo sia raggiungibile

File di log degli eventi per MetroCluster Tiebreaker

Il file di registro eventi contiene un registro di tutte le azioni eseguite dal software MetroCluster Tiebreaker.

Il software Tiebreaker esegue le seguenti operazioni:

- Rileva i disastri del sito
- Rileva le modifiche di configurazione relative al database, ad altri monitor di spareggio o al software di spareggio MetroCluster
- Rileva le connessioni SSH e le disconnessioni
- Rileva le configurazioni MetroCluster

Queste azioni vengono registrate nel file di registro eventi nel seguente formato:

modulo id thread livello di registro/severità timestamp

```
2022-09-07 06:14:30,797 INFO  [MCCTBCommandServer-16] [SslSupport]
Successfully initiated SSL context. Protocol used is TLSv1.3.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16] [DataBase]
Successfully read MCCTB database.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16]
[ConfigurationMonitor] Debug mode disabled.
```

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione e sul funzionamento di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto
"Documentazione MetroCluster"	• Tutte le informazioni MetroCluster
"Report tecnico NetApp 4375: NetApp MetroCluster per ONTAP 9.3"	• Panoramica tecnica della configurazione e del funzionamento di MetroCluster. • Best practice per la configurazione di MetroCluster.
"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Installazione e configurazione di MetroCluster IP"	• Architettura IP di MetroCluster • Collegamento della configurazione IP di MetroCluster • Configurazione di MetroCluster in ONTAP

"Gestire i componenti di MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster • Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione Fabric-Attached o Stretch MetroCluster • Rimozione a caldo di uno shelf di dischi in una configurazione Fabric-Attached o Stretch MetroCluster • Sostituzione dell'hardware in un sito di emergenza in una configurazione MetroCluster con connessione fabric o stretch • Espansione di una configurazione MetroCluster a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione fabric-attached o stretch MetroCluster a quattro nodi in una configurazione MetroCluster a otto nodi.
Documentazione Active IQ Unified Manager "Documentazione NetApp: Guide e risorse sui prodotti"	• Monitoraggio della configurazione e delle prestazioni di MetroCluster
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster

Comprendere la protezione dei dati e il disaster recovery di MetroCluster

Comprensione della protezione dei dati e del disaster recovery di MetroCluster

È utile comprendere in che modo MetroCluster protegge i dati e fornisce un ripristino trasparente dai guasti, in modo da poter gestire le attività di switchover e switchback in modo semplice ed efficiente.

MetroCluster utilizza il mirroring per proteggere i dati in un cluster. Fornisce il disaster recovery attraverso un singolo comando MetroCluster che attiva un secondario sul sito di sopravvivenza per fornire i dati mirrorati originariamente di proprietà di un sito primario colpito da un disastro.

In che modo le configurazioni MetroCluster a otto e quattro nodi offrono failover e switchover locali

Le configurazioni MetroCluster a otto e quattro nodi proteggono i dati sia a livello locale che a livello di cluster. Se si sta configurando una configurazione MetroCluster, è necessario conoscere il modo in cui le configurazioni MetroCluster proteggono i dati.

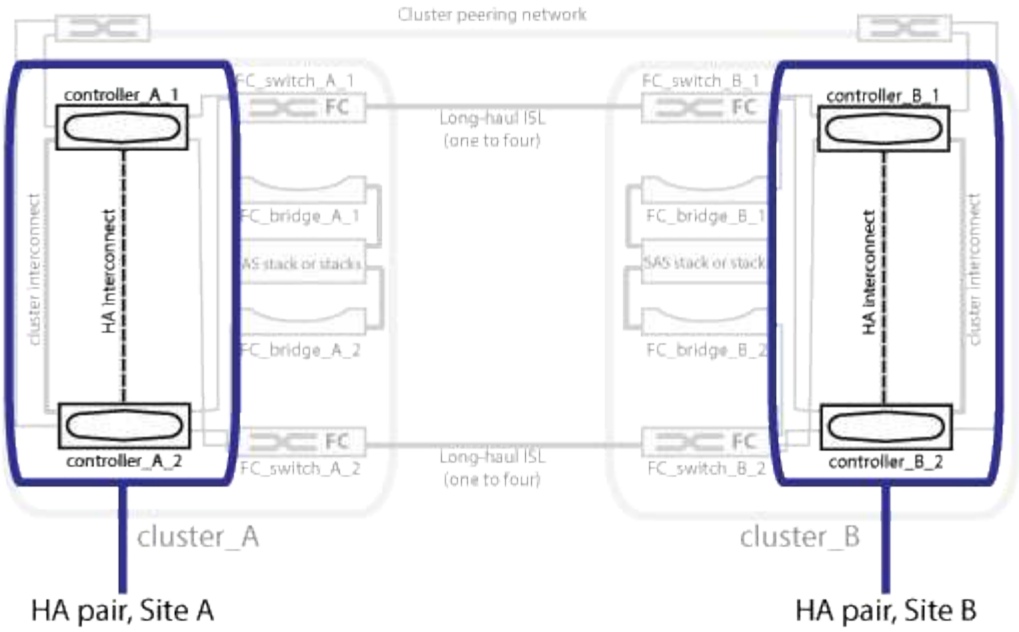
Le configurazioni MetroCluster proteggono i dati utilizzando due cluster con mirroring fisicamente separati. Ogni cluster esegue il mirroring sincrono della configurazione SVM (Data and Storage Virtual Machine) dell'altro. Quando si verifica un disastro in un sito, un amministratore può attivare la SVM mirrorata e iniziare a fornire i dati mirrorati dal sito sopravvissuto. Inoltre, i nodi di ciascun cluster sono configurati come coppia ha, fornendo un livello di failover locale.

Come funziona la protezione locale dei dati ha in una configurazione MetroCluster

È necessario comprendere il funzionamento delle coppie ha nella configurazione MetroCluster.

I due cluster della rete peered forniscono il disaster recovery bidirezionale, in cui ciascun cluster può essere l'origine e il backup dell'altro cluster. Ciascun cluster include due nodi configurati come coppia ha. In caso di guasto o manutenzione richiesta all'interno della configurazione di un singolo nodo, il failover dello storage può trasferire le operazioni del nodo al partner ha locale.

La figura seguente mostra una configurazione MetroCluster FC. La funzionalità ha è la stessa nelle configurazioni IP di MetroCluster, tranne per il fatto che l'interconnessione ha è fornita dagli switch del cluster.



Informazioni correlate

"Configurazione ad alta disponibilità"

In che modo le configurazioni MetroCluster forniscono la replica di dati e configurazione

Le configurazioni MetroCluster utilizzano una vasta gamma di funzionalità ONTAP per fornire replica sincrona dei dati e configurazione tra i due siti MetroCluster.

Protezione della configurazione con il servizio di replica della configurazione

Il servizio di replica della configurazione ONTAP (CRS) protegge la configurazione MetroCluster replicando automaticamente le informazioni al partner di DR.

Il CRS replica in modo sincrono la configurazione del nodo locale al partner di DR nel cluster del partner. Questa replica viene eseguita sulla rete di peering del cluster.

Le informazioni replicate includono la configurazione del cluster e la configurazione SVM.

Replica di SVM durante le operazioni MetroCluster

Il servizio di replica della configurazione di ONTAP (CRS) fornisce la configurazione del server dati ridondante e il mirroring dei volumi di dati che appartengono alla SVM. Se si verifica uno switchover, la SVM di origine viene portata in basso e la SVM di destinazione, situata nel cluster in uso, diventa attiva.

> Le SVM di destinazione nella configurazione MetroCluster hanno il suffisso “-mc” aggiunto automaticamente al loro nome per facilitarne l’identificazione. Una configurazione MetroCluster aggiunge il suffisso “-mc” al nome delle SVM di destinazione; se il nome SVM contiene un punto, il suffisso “-mc” viene applicato prima del primo punto. Ad esempio, se il nome SVM è SVM.DNS.NAME, il suffisso “-mc” viene aggiunto come SVM-MC.DNS.NAME.

Nell’esempio riportato di seguito vengono illustrate le SVM per una configurazione MetroCluster, dove “SVM_cluster_A” è una SVM sul sito di origine e “SVM_cluster_A-mc” è un aggregato di destinazione di sincronizzazione sul sito di disaster recovery.

- SVM_cluster_A fornisce i dati sul cluster A.

  Si tratta di una SVM Sync-source che rappresenta la configurazione SVM (LIF, protocolli e servizi) e i dati nei volumi appartenenti alla SVM. La configurazione e i dati vengono replicati in SVM_cluster_A-mc, una SVM di destinazione della sincronizzazione situata sul cluster B.

- SVM_cluster_B fornisce i dati sul cluster B.

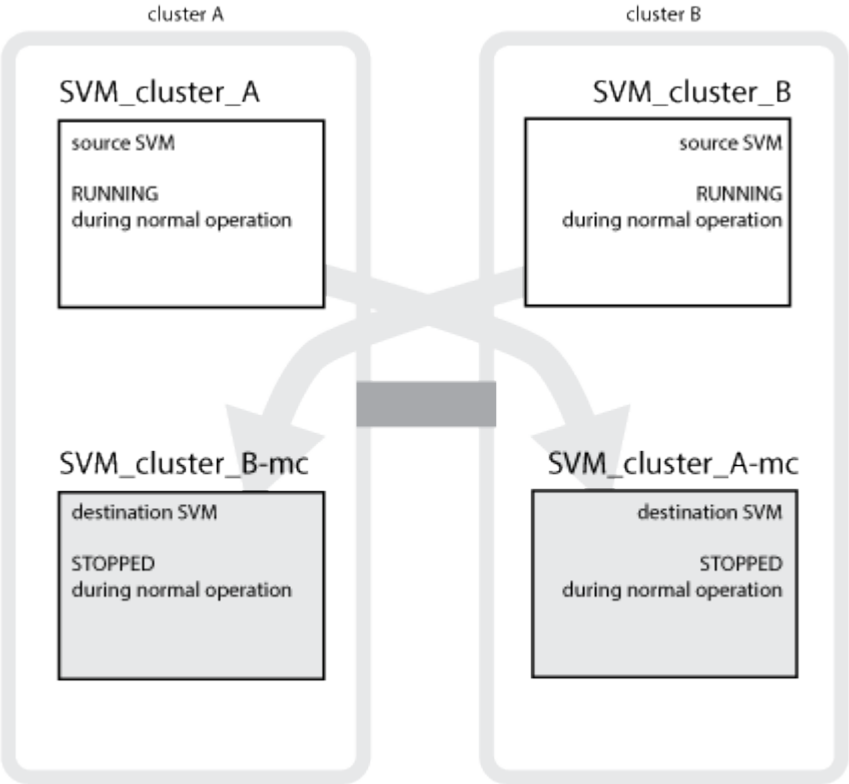
  Si tratta di una SVM di origine sincrona che rappresenta la configurazione e i dati a SVM_cluster_B-mc situata sul cluster A.

- SVM_cluster_B-mc è una SVM di destinazione della sincronizzazione che viene interrotta durante il normale funzionamento della configurazione MetroCluster.

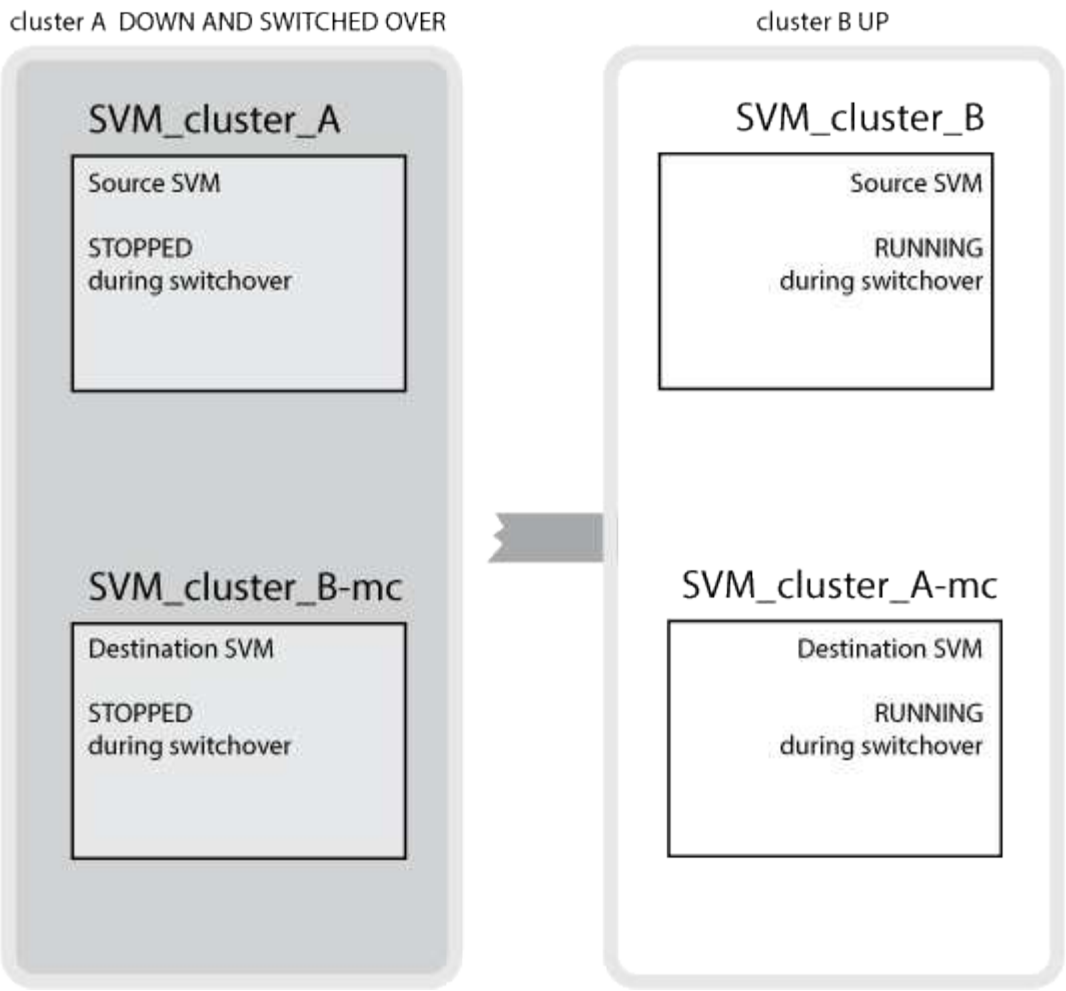
  In caso di passaggio riuscito dal cluster B al cluster A, SVM_cluster_B viene arrestato e SVM_cluster_B-mc viene attivato e inizia a fornire i dati dal cluster A.

- SVM_cluster_A-mc è una SVM di destinazione della sincronizzazione che viene interrotta durante il normale funzionamento della configurazione MetroCluster.

  In caso di passaggio riuscito dal cluster A al cluster B, SVM_cluster_A viene arrestato e SVM_cluster_A-mc viene attivato e inizia a fornire i dati dal cluster B.



Se si verifica uno switchover, il plex remoto sul cluster in uso viene online e la SVM secondaria inizia a fornire i dati.



La disponibilità di plessi remoti dopo lo switchover dipende dal tipo di configurazione MetroCluster:

- Per le configurazioni MetroCluster FC, dopo lo switchover, i plex locali e remoti rimangono online se lo storage del sito di disastro è accessibile tramite gli ISL.

  Se gli ISL si sono guastati e lo storage del sito di emergenza non è disponibile, la SVM di destinazione della sincronizzazione inizia a fornire i dati dal sito sopravvissuto.

- Per le configurazioni MetroCluster IP, la disponibilità dei plessi remoti dipende dalla versione di ONTAP:
  - A partire da ONTAP 9.5, i plex locali e remoti rimangono online se i nodi del sito di emergenza rimangono avviati.
  - Prima di ONTAP 9.5, lo storage è disponibile solo dal plesso locale sul sito sopravvissuto.

    La SVM di destinazione della sincronizzazione inizia a fornire i dati dal sito sopravvissuto.

Informazioni correlate

"Amministrazione del sistema"

In che modo le configurazioni MetroCluster utilizzano SyncMirror per fornire ridondanza dei dati

Gli aggregati mirrorati che utilizzano la funzionalità SyncMirror forniscono la ridondanza dei dati e contengono i volumi di proprietà della macchina virtuale di storage di origine e di destinazione (SVM). I dati vengono replicati in pool di dischi sul cluster partner. Sono supportati anche gli aggregati senza mirror.

La seguente tabella mostra lo stato (online o offline) di un aggregato senza mirror dopo uno switchover:

Tipo di switchover	Stato di configurazione di MetroCluster FC	Stato di configurazione dell'IP MetroCluster
Switchover negoziato (NSO)	Online	Offline (Nota 1)
Switchover automatico non pianificato (AUSO)	Online	Offline (Nota 1)
Switchover non pianificato (USO)	• Se lo storage non è disponibile: Offline • Se lo storage è disponibile: Online	Offline (Nota 1)

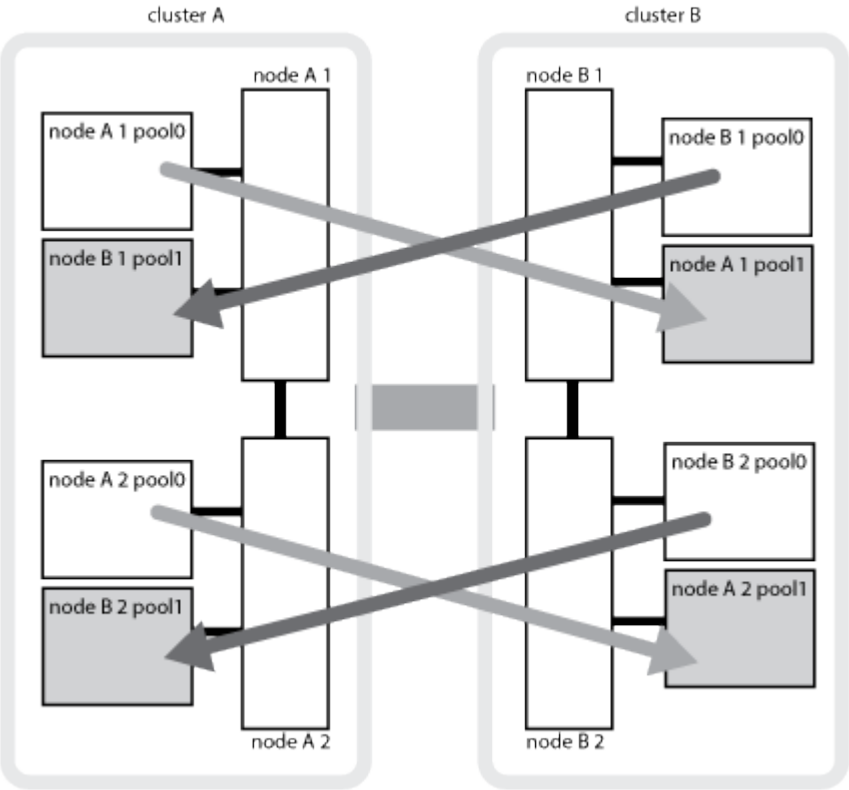
Nota 1: Nelle configurazioni IP di MetroCluster, una volta completato lo switchover, è possibile portare online manualmente gli aggregati senza mirror.

Scopri di più Differenze nello switchover tra le configurazioni MetroCluster FC e IP.

> Dopo uno switchover, se l'aggregato senza mirror si trova nel nodo partner DR e si verifica un errore di collegamento interswitch (ISL), il nodo locale potrebbe non funzionare.

La seguente illustrazione mostra come vengono mirrorati i pool di dischi tra i cluster partner. I dati nei plessi locali (in pool0) vengono replicati in plessi remoti (in pool1).

> Se si utilizzano aggregati ibridi, le performance possono peggiorare dopo un guasto di un SyncMirror plex a causa del riempimento dello strato del disco a stato solido (SSD).

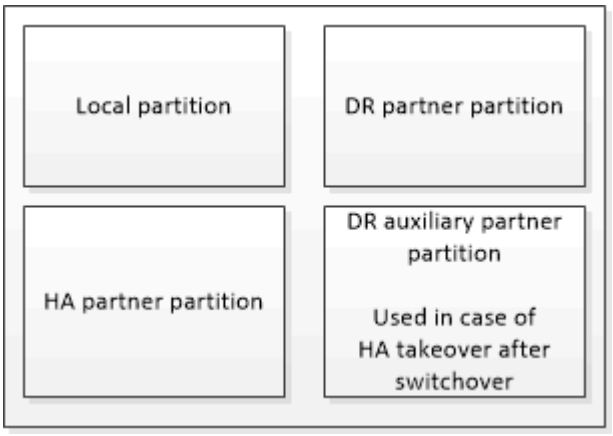
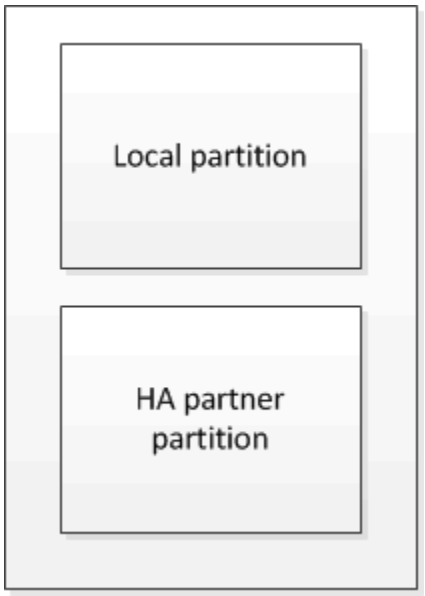


Funzionamento del mirroring della cache NVRAM o NVMEM e del mirroring dinamico nelle configurazioni MetroCluster

La memoria non volatile (NVRAM o NVMEM, a seconda del modello di piattaforma) nei controller di storage viene sottoposta a mirroring sia localmente su un partner ha locale che in remoto su un partner di disaster recovery remoto (DR) sul sito del partner. In caso di failover o switchover locale, questa configurazione consente di conservare i dati nella cache non volatile.

In una coppia ha che non fa parte di una configurazione MetroCluster, ogni controller di storage mantiene due partizioni della cache non volatile: Una per sé e una per il partner ha.

In una configurazione MetroCluster a quattro nodi, la cache non volatile di ciascun controller di storage è divisa in quattro partizioni. In una configurazione MetroCluster a due nodi, la partizione partner ha e la partizione ausiliaria DR non vengono utilizzate, perché i controller di storage non sono configurati come coppia ha.

Cache non volatili per un controller di storage	
In una configurazione MetroCluster	In una coppia ha non MetroCluster
	

Le cache non volatili memorizzano i seguenti contenuti:

- La partizione locale contiene i dati che il controller di storage non ha ancora scritto su disco.
- La partizione partner ha contiene una copia della cache locale del partner ha del controller di storage.

  In una configurazione MetroCluster a due nodi, non esiste alcuna partizione partner ha perché i controller di storage non sono configurati come coppia ha.

- La partizione partner di DR contiene una copia della cache locale del partner DR del controller di storage.

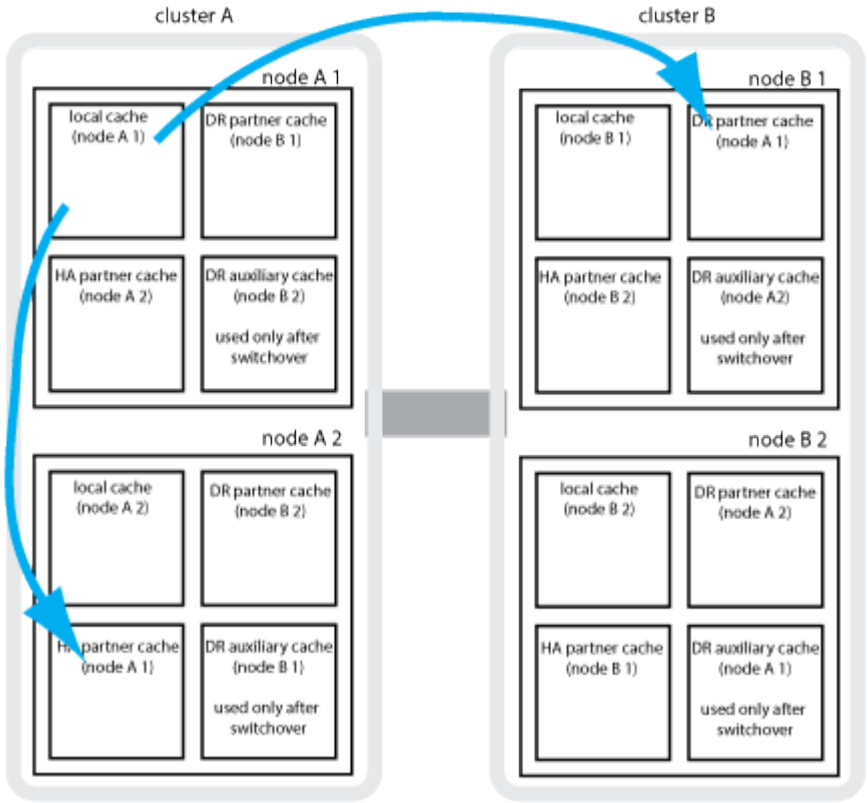
  Il partner DR è un nodo del cluster partner associato al nodo locale.

- La partizione partner ausiliaria DR contiene una copia della cache locale del partner ausiliario DR del controller di storage.

  Il partner ausiliario DR è il partner ha del partner DR del nodo locale. Questa cache è necessaria in caso di un takeover ha (quando la configurazione è in funzione normale o dopo uno switchover MetroCluster).

In una configurazione MetroCluster a due nodi, non esiste alcuna partizione partner ausiliaria DR perché i controller di storage non sono configurati come coppia ha.

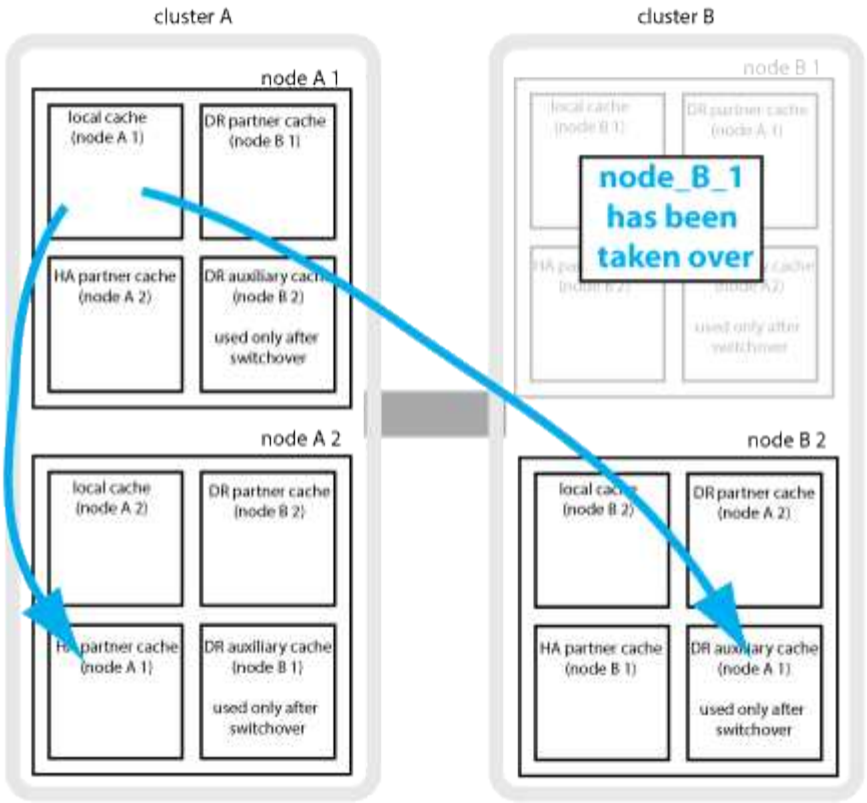
Ad esempio, la cache locale di un nodo (Node_A_1) viene sottoposta a mirroring sia localmente che in remoto nei siti MetroCluster. L'illustrazione seguente mostra che la cache locale di Node_A_1 viene mirrorata al partner ha (Node_A_2) e al partner DR (Node_B_1):



Mirroring dinamico in caso di takeover ha locale

Se si verifica un Takeover ha locale in una configurazione MetroCluster a quattro nodi, il nodo preso in consegna non può più fungere da mirror per il partner di DR. Per consentire il mirroring del DR, il mirroring passa automaticamente al partner ausiliario del DR. Dopo un giveback riuscito, il mirroring ritorna automaticamente al partner DR.

Ad esempio, Node_B_1 non riesce e viene sostituito da Node_B_2. Non è più possibile eseguire il mirroring della cache locale di Node_A_1 su Node_B_1. Il mirroring passa al partner ausiliario DR, Node_B_2.



Tipi di disastri e metodi di ripristino

È necessario conoscere i diversi tipi di guasti e disastri in modo da poter utilizzare la configurazione MetroCluster per rispondere in modo appropriato.

- Guasto a nodo singolo

  Un singolo componente della coppia ha locale si guasta.

  In una configurazione MetroCluster a quattro nodi, questo errore potrebbe portare a un Takeover automatico o negoziato del nodo danneggiato, a seconda del componente che ha avuto esito negativo. Il ripristino dei dati è descritto in "Gestione delle coppie ad alta disponibilità" .

  In una configurazione MetroCluster a due nodi, questo guasto porta a uno switchover automatico non pianificato (USO).

- Guasto del controller a livello di sito

  Tutti i moduli controller si guastano in un sito a causa di perdita di alimentazione, sostituzione dell'apparecchiatura o disastro. In genere, le configurazioni MetroCluster non sono in grado di distinguere tra guasti e disastri. Tuttavia, il software Witness, come il software MetroCluster Tiebreaker, può differenziarsi tra di loro. Una condizione di guasto del controller a livello di sito può portare a uno switchover automatico se i collegamenti e gli switch InterSwitch link (ISL) sono attivati e lo storage è accessibile.

  "Gestione delle coppie ad alta disponibilità" contiene ulteriori informazioni su come eseguire il ripristino da guasti dei controller a livello di sito che non includono guasti dei controller, oltre a guasti che includono uno o più controller.

- Errore ISL

I collegamenti tra i siti non funzionano. La configurazione di MetroCluster non esegue alcuna operazione. Ogni nodo continua a servire i dati normalmente, ma i mirror non vengono scritti nei rispettivi siti di disaster recovery perché l'accesso ad essi viene perso.

- Guasti sequenziali multipli

  Più componenti si guastano in una sequenza. Ad esempio, un modulo controller, un fabric di switch e uno shelf si guastano in una sequenza e si traducono in un failover dello storage, ridondanza del fabric e SyncMirror che proteggono in sequenza da downtime e perdita di dati.

La tabella seguente mostra i tipi di errore, il meccanismo di disaster recovery (DR) e il metodo di recovery corrispondenti:

> AUSO (switchover automatico non pianificato) non è supportato nelle configurazioni IP MetroCluster.

Tipo di guasto	Meccanismo DR		Riepilogo del metodo di ripristino	
	Configurazione a quattro nodi	Configurazione a due nodi	Configurazione a quattro nodi	Configurazione a due nodi
Guasto a nodo singolo	Failover ha locale	AUSNO	Non necessario se sono attivati failover e giveback automatici.	Una volta ripristinato il nodo, eseguire la riparazione manuale e lo switchback utilizzando `metrocluster heal -phase aggregates`, `metrocluster heal -phase root-aggregates`, e. `metrocluster switchback` i comandi sono obbligatori. NOTA: Il `metrocluster heal` I comandi non sono richiesti nelle configurazioni MetroCluster IP con ONTAP 9.5 o versioni successive.

Guasto del sito	Switchover MetroCluster		Una volta ripristinato il nodo, eseguire la riparazione manuale e lo switchback utilizzando `metrocluster healing` e. `metrocluster switchback` i comandi sono obbligatori. Il `metrocluster heal` I comandi non sono richiesti nelle configurazioni MetroCluster IP con ONTAP 9.5.
Guasto del controller a livello di sito	AUSO solo se lo storage nel sito di disastro è accessibile.	AUSO (come un guasto a nodo singolo)	
Guasti sequenziali multipli	Failover ha locale seguito da switchover forzato MetroCluster utilizzando il comando MetroCluster switchover -forced -on-disaster. NOTA: A seconda del componente guasto, potrebbe non essere necessario uno switchover forzato.	MetroCluster ha forzato lo switchover utilizzando `metrocluster switchover -forced-on -disaster` comando.	
Errore ISL	Nessun switchover MetroCluster; i due cluster servono i propri dati in modo indipendente		Non richiesto per questo tipo di guasto. Una volta ripristinata la connettività, lo storage viene risincronizzato automaticamente.

In che modo una configurazione MetroCluster a otto o quattro nodi offre operazioni senza interruzioni

In caso di problemi limitati a un singolo nodo, un failover e un giveback all'interno della coppia ha locale garantiscono un funzionamento continuo e senza interruzioni. In questo caso, la configurazione MetroCluster non richiede uno switchover al sito remoto.

Poiché la configurazione MetroCluster a otto o quattro nodi è costituita da una o più coppie ha in ogni sito, ciascun sito può resistere a guasti locali ed eseguire operazioni senza interruzioni senza dover passare al sito del partner. Il funzionamento della coppia ha è lo stesso delle coppie ha nelle configurazioni non MetroCluster.

Per le configurazioni MetroCluster a quattro e otto nodi, i guasti dei nodi dovuti a panico o perdita di alimentazione possono causare uno switchover automatico.

"Gestione delle coppie ad alta disponibilità"

Se si verifica un secondo guasto dopo un failover locale, l'evento di switchover MetroCluster offre operazioni senza interruzioni. Analogamente, dopo un'operazione di switchover, in caso di un secondo guasto in uno dei nodi sopravvissuti, un evento di failover locale offre operazioni senza interruzioni. In questo caso, il singolo nodo sopravvissuto serve i dati per gli altri tre nodi del gruppo DR.

Switchover e switchback durante la transizione MetroCluster

La transizione FC-IP di MetroCluster implica l'aggiunta di nodi IP MetroCluster e switch IP a una configurazione FC MetroCluster esistente, quindi il ritiro dei nodi FC MetroCluster. A seconda della fase del processo di transizione, le operazioni di switchover, riparazione e switchback di MetroCluster utilizzano flussi di lavoro diversi.

Vedere "Operazioni di switchover, riparazione e switchback durante la transizione".

Conseguenze del failover locale dopo lo switchover

Se si verifica uno switchover MetroCluster e si verifica un problema nel sito sopravvissuto, un failover locale può garantire un funzionamento continuo e senza interruzioni. Tuttavia, il sistema è a rischio perché non si trova più in una configurazione ridondante.

Se si verifica un failover locale dopo uno switchover, un singolo controller serve i dati per tutti i sistemi storage nella configurazione MetroCluster, causando possibili problemi di risorse ed è vulnerabile a ulteriori guasti.

In che modo una configurazione MetroCluster a due nodi offre operazioni senza interruzioni

Se uno dei due siti presenta un problema dovuto al panico, lo switchover MetroCluster garantisce un funzionamento continuo e senza interruzioni. Se la perdita di alimentazione influisce sia sul nodo che sullo storage, lo switchover non è automatico e si verifica un'interruzione fino al `metrocluster switchover` viene emesso il comando.

Poiché tutto lo storage viene mirrorato, è possibile utilizzare un'operazione di switchover per fornire una resilienza senza interruzioni in caso di guasto di un sito simile a quello riscontrato in un failover dello storage in una coppia ha per un guasto di un nodo.

Per le configurazioni a due nodi, gli stessi eventi che attivano un failover automatico dello storage in una coppia ha attivano uno switchover automatico non pianificato (AUSO). Ciò significa che una configurazione MetroCluster a due nodi ha lo stesso livello di protezione di una coppia ha.

Informazioni correlate

"Switchover automatico non pianificato nelle configurazioni MetroCluster FC"

Panoramica del processo di switchover

L'operazione di switchover MetroCluster consente la ripresa immediata dei servizi in seguito a un disastro spostando lo storage e l'accesso client dal cluster di origine al sito remoto. Devi essere consapevole delle modifiche da prevedere e delle azioni da eseguire in caso di passaggio.

Durante un'operazione di switchover, il sistema esegue le seguenti operazioni:

- La proprietà dei dischi appartenenti al sito di disaster recovery viene modificata in partner di disaster recovery (DR).

  Questo è simile al caso di un failover locale in una coppia ad alta disponibilità (ha), in cui la proprietà dei dischi appartenenti al partner che non è in funzione viene modificata in un partner sano.

- I plex sopravvissuti che si trovano nel sito sopravvissuto ma appartengono ai nodi del cluster di disastro vengono portati online nel cluster nel sito sopravvissuto.
- La SVM (Storage Virtual Machine) di origine di sincronizzazione che appartiene al sito di disastro viene interrotta solo durante uno switchover negoziato.

  Ciò è applicabile solo a uno switchover negoziato.

- Viene creata la SVM di destinazione della sincronizzazione appartenente al sito di emergenza.

Durante il passaggio, gli aggregati root del partner DR non vengono portati online.

Il `metrocluster switchover` Command consente di passare dai nodi di tutti i gruppi di DR nella configurazione MetroCluster. Ad esempio, in una configurazione MetroCluster a otto nodi, viene eseguita la commutazione dei nodi in entrambi i gruppi di DR.

Se si passa solo ai servizi del sito remoto, è necessario eseguire uno switchover negoziato senza scherma del sito. Se lo storage o le apparecchiature non sono affidabili, è necessario individuare il sito di emergenza ed eseguire uno switchover non pianificato. La funzione di scherma impedisce le ricostruzioni RAID quando i dischi si accendano in modo sfalsato.

> Questa procedura deve essere utilizzata solo se l'altro sito è stabile e non deve essere portato offline.

Disponibilità dei comandi durante lo switchover

La seguente tabella mostra la disponibilità dei comandi durante lo switchover:

Comando	Disponibilità
`storage aggregate create`	È possibile creare un aggregato: • Se è di proprietà di un nodo che fa parte del cluster esistente Impossibile creare un aggregato: • Per un nodo nel sito di disastro • Per un nodo che fa parte del cluster esistente
`storage aggregate delete`	È possibile eliminare un aggregato di dati.
`storage aggregate mirror`	È possibile creare un plesso per un aggregato non mirrorato.
`storage aggregate plex delete`	È possibile eliminare un plex per un aggregato mirrorato.
`vserver create`	È possibile creare una SVM: • Se il volume root risiede in un aggregato di dati di proprietà del cluster esistente Impossibile creare una SVM: • Se il volume root risiede in un aggregato di dati di proprietà del cluster del sito di emergenza
`vserver delete`	È possibile eliminare le SVM di origine e di destinazione della sincronizzazione.

`network interface create -lif`	È possibile creare una LIF SVM di dati per le SVM di origine e di destinazione della sincronizzazione.
`network interface delete -lif`	È possibile eliminare una LIF SVM di dati sia per le SVM di origine sincronizzazione che di destinazione sincronizzazione.
`volume create`	È possibile creare un volume per le SVM di origine e di destinazione della sincronizzazione. • Per una SVM di origine della sincronizzazione, il volume deve risiedere in un aggregato di dati di proprietà del cluster esistente • Per una SVM di destinazione della sincronizzazione, il volume deve risiedere in un aggregato di dati di proprietà del cluster del sito di emergenza
`volume delete`	È possibile eliminare un volume per le SVM di origine e di destinazione della sincronizzazione.
`volume move`	È possibile spostare un volume per le SVM di origine e di destinazione della sincronizzazione. • Per una SVM di origine della sincronizzazione, il cluster sopravvissuto deve possedere l'aggregato di destinazione • Per una SVM di destinazione della sincronizzazione, il cluster del sito di emergenza deve possedere l'aggregato di destinazione
`snapmirror break`	È possibile interrompere una relazione SnapMirror tra un endpoint di origine e di destinazione di un mirror per la protezione dei dati.

Differenze nello switchover tra le configurazioni MetroCluster FC e IP

Nelle configurazioni MetroCluster IP, poiché l'accesso ai dischi remoti avviene attraverso i nodi partner di DR remoti che fungono da destinazioni iSCSI, i dischi remoti non sono accessibili quando i nodi remoti vengono interrati in un'operazione di switchover. Ciò comporta differenze con le configurazioni MetroCluster FC:

- Gli aggregati mirrorati di proprietà del cluster locale diventano degradati.
- Gli aggregati mirrorati che sono stati commutati dal cluster remoto diventano degradati.

> Quando gli aggregati senza mirror sono supportati su una configurazione IP MetroCluster, gli aggregati senza mirror che non vengono commutati dal cluster remoto non sono accessibili.

La proprietà del disco cambia durante il takeover ha e lo switchover MetroCluster in una configurazione MetroCluster a quattro nodi

La proprietà dei dischi viene temporaneamente modificata automaticamente durante le operazioni MetroCluster e ad alta disponibilità. È utile sapere in che modo il sistema tiene traccia del nodo proprietario dei dischi.

In ONTAP, l'ID di sistema univoco di un modulo controller (ottenuto dalla scheda NVRAM o dalla scheda NVMEM di un nodo) viene utilizzato per identificare quale nodo possiede un disco specifico. A seconda dello stato ha o DR del sistema, la proprietà del disco potrebbe cambiare temporaneamente. Se la proprietà cambia a causa di un takeover ha o di uno switchover DR, il sistema registra quale nodo è il proprietario originale (chiamato "home") del disco, in modo che possa restituire la proprietà dopo il giveback ha o lo switchback DR. Il sistema utilizza i seguenti campi per tenere traccia della proprietà del disco:

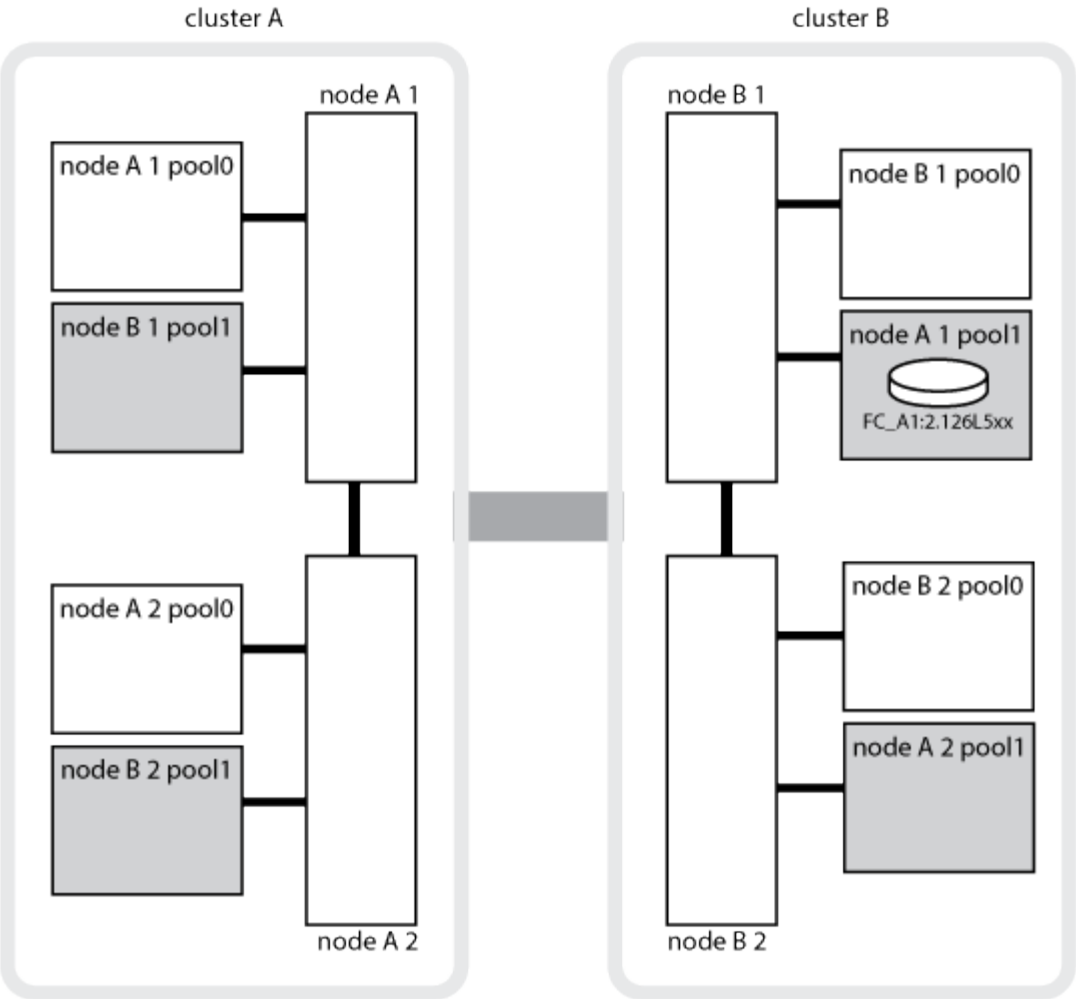
- Proprietario
- Proprietario di casa
- Proprietario di DR Home

Nella configurazione MetroCluster, in caso di switchover, un nodo può assumere la proprietà di un aggregato originariamente di proprietà dei nodi nel cluster partner. Tali aggregati sono indicati come aggregati cluster-estranei. La caratteristica distintiva di un aggregato esterno al cluster è che si tratta di un aggregato non attualmente noto al cluster, pertanto il campo DR Home Owner viene utilizzato per dimostrare che è di proprietà di un nodo del cluster partner. Un aggregato estraneo tradizionale all'interno di una coppia ha è identificato da valori proprietari e proprietari domestici diversi, ma i valori proprietari e proprietari domestici sono gli stessi per un aggregato estraneo al cluster; pertanto, è possibile identificare un aggregato estraneo al cluster in base al valore proprietario DR.

Man mano che lo stato del sistema cambia, i valori dei campi cambiano, come mostrato nella seguente tabella:

Campo	Valore durante…			
	Funzionamento normale	Takeover ha locale	Switchover MetroCluster	Takeover durante lo switchover
Proprietario	ID del nodo che ha accesso al disco.	ID del partner ha, che ha temporaneamente accesso al disco.	ID del partner DR, che ha temporaneamente accesso al disco.	ID del partner ausiliario DR, che ha temporaneamente accesso al disco.
Proprietario di casa	ID del proprietario originale del disco all'interno della coppia ha.	ID del proprietario originale del disco all'interno della coppia ha.	ID del partner DR, che è il proprietario di casa nella coppia ha durante lo switchover.	ID del partner DR, che è il proprietario di casa nella coppia ha durante lo switchover.
Proprietario di DR Home	Vuoto	Vuoto	ID del proprietario originale del disco all'interno della configurazione MetroCluster.	ID del proprietario originale del disco all'interno della configurazione MetroCluster.

L'illustrazione e la tabella seguenti forniscono un esempio di come cambia la proprietà, per un disco nel pool di dischi di Node_A_1, fisicamente ubicato in cluster_B.



Stato MetroCluster	Proprietario	Proprietario di casa	Proprietario di DR Home	Note
Normale con tutti i nodi completamente operativi.	Node_A_1	Node_A_1	non applicabile	
Local ha Takeover, node_A_2 ha preso il controllo dei dischi appartenenti al suo nodo partner ha_A_1.	Node_A_2	Node_A_1	non applicabile	

Switchover DR, Node_B_1 ha preso il controllo dei dischi appartenenti al proprio partner DR, Node_A_1.	Node_B_1	Node_B_1	Node_A_1	L'ID del nodo principale originale viene spostato nel campo DR Home Owner. Dopo lo switchback o la riparazione dell'aggregato, la proprietà ritorna al nodo_A_1.
Nello switchover DR e nel Takeover ha locale (doppio guasto), il nodo_B_2 ha sostituito i dischi appartenenti al nodo ha_B_1.	Node_B_2	Node_B_1	Node_A_1	Dopo il giveback, la proprietà torna al nodo_B_1. Dopo lo switchback o la riparazione, la proprietà ritorna al nodo_A_1.
Dopo il giveback ha e lo switchback DR, tutti i nodi sono pienamente operativi.	Node_A_1	Node_A_1	non applicabile	

Considerazioni sull'utilizzo di aggregati senza mirror

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

Considerazioni per gli aggregati senza mirror 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 offline qualsiasi aggregato senza mirror di proprietà del sito di disastro.

In caso contrario, i nodi del sito sopravvissuto potrebbero andare in stato di inattività a causa della panica su più dischi. Questo potrebbe verificarsi se gli aggregati senza mirror con switch-over non sono in linea o mancano a causa della perdita di connettività allo storage nel sito di emergenza a causa dell'interruzione 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 aggregato senza mirror. Se si

trovano su aggregato senza mirror, le operazioni di switchover e switchback negoziate vengono vetoed. Il `metrocluster check` in questo caso, il comando 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

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

Switchover automatico non pianificato nelle configurazioni MetroCluster FC

Nelle configurazioni MetroCluster FC, alcuni scenari possono attivare uno switchover automatico non pianificato (USO) in caso di guasto di un controller a livello di sito per fornire operazioni senza interruzioni. SE lo si desidera, È possibile disattivare AUSO.

> Lo switchover automatico non pianificato non è supportato nelle configurazioni MetroCluster IP.

In una configurazione MetroCluster FC, è possibile attivare UNA FUNZIONE AUSO se tutti i nodi di un sito sono guasti per i seguenti motivi:

- Spegnere
- Perdita di alimentazione
- Panico

> In una configurazione MetroCluster FC a otto nodi, è possibile impostare un'opzione per attivare UN AUSO se entrambi i nodi in una coppia ha falliscono.

Poiché non è disponibile un failover ha locale in una configurazione MetroCluster a due nodi, il sistema esegue UN'ALTRA FUNZIONE per garantire un funzionamento continuo dopo un guasto del controller. Questa funzionalità è simile alla funzionalità ha Takeover in una coppia ha. In una configurazione MetroCluster a due nodi, è possibile attivare AUSO nei seguenti scenari:

- Disattivazione del nodo
- Perdita di alimentazione del nodo
- Nodo panico
- Riavvio del nodo

Se si verifica un'INTERRUZIONE, la proprietà del disco per i dischi pool0 e pool1 del nodo compromesso viene modificata in partner di disaster recovery (DR). Questo cambiamento di proprietà impedisce agli aggregati di passare a uno stato degradato dopo lo switchover.

Dopo lo switchover automatico, è necessario eseguire manualmente le operazioni di riparazione e switchback per ripristinare il normale funzionamento del controller.

AUSO con supporto hardware in configurazioni MetroCluster a due nodi

In una configurazione MetroCluster a due nodi, il Service Processor (SP) del modulo controller monitora la configurazione. In alcuni scenari, l'SP è in grado di rilevare un guasto più rapidamente rispetto al software ONTAP. In questo caso, l'SP attiva AUSO. Questa funzione viene attivata automaticamente.

L'SP invia e riceve il traffico SNMP da e verso il proprio partner DR per monitorarne lo stato di salute.

Modifica dell'impostazione AUSO nelle configurazioni MetroCluster FC

AUSO è impostato su "auso-on-cluster-disaster" per impostazione predefinita. Il relativo stato può essere visualizzato in `metrocluster show` comando.

> L'impostazione AUSO non si applica alle configurazioni IP MetroCluster.

È possibile disattivare AUSO con `metrocluster modify -auto-switchover-failure-domain auto-disabled` comando. Questo comando impedisce L'attivazione DI AUSO in un guasto del controller DR a livello di sito. Dovrebbe essere eseguito su entrambi i siti se si desidera disattivare AUSO su entrambi i siti.

AUSO può essere riabilitato con `metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster` comando.

AUSO può anche essere impostato su "auso-on-dr-group-disaster". Questo comando di livello avanzato attiva AUSO su failover ha in un sito. Deve essere eseguito su entrambi i siti con `metrocluster modify -auto -switchover-failure-domain auso-on-dr-group-disaster` comando.

L'impostazione AUSO durante lo switchover

Quando si verifica lo switchover, l'impostazione AUSO viene disattivata internamente perché, se un sito è in switchover, non può passare automaticamente.

Ripristino da AUSO

Per eseguire il ripristino da AUSO, eseguire le stesse operazioni di uno switchover pianificato.

"Esecuzione di uno switchover per test o manutenzione"

Switchover automatico non pianificato assistito dal mediatore nelle configurazioni MetroCluster IP

"Scoprite in che modo ONTAP Mediator supporta lo switchover automatico non pianificato nelle configurazioni IP di MetroCluster".

Cosa succede durante la riparazione (configurazioni MetroCluster FC)

Durante la riparazione nelle configurazioni MetroCluster FC, la risincronizzazione degli aggregati mirrorati avviene in un processo in fasi che prepara i nodi nel sito di emergenza riparato per lo switchback. Si tratta di un evento pianificato, che ti offre il pieno controllo di ogni fase per ridurre al minimo i downtime. La riparazione è un processo in due fasi che si verifica sui componenti dello storage e del controller.

Riparazione degli aggregati di dati

Una volta risolto il problema nel sito di emergenza, si avvia la fase di riparazione dello storage:

1. Verifica che tutti i nodi siano attivi e in esecuzione nel sito sopravvissuto.

2. Modifica la proprietà di tutti i dischi del pool 0 nel sito di disastro, compresi gli aggregati root.

Durante questa fase di riparazione, il sottosistema RAID risincronizza gli aggregati mirrorati e il sottosistema WAFL riproduce i file nvsaved degli aggregati mirrorati con un pool 1 plex guasto al momento dello switchover.

Se alcuni componenti dello storage di origine si sono guastati, il comando riporta gli errori ai livelli applicabili: Storage, Sanown o RAID.

Se non vengono segnalati errori, gli aggregati vengono risincronizzati correttamente. A volte il completamento di questo processo può richiedere ore.

"Riparazione della configurazione"

Healing dell'aggregato root

Una volta sincronizzati gli aggregati, si avvia la fase di healing del controller restituendo gli aggregati CFO e gli aggregati root ai rispettivi partner DR.

"Riparazione della configurazione"

Cosa succede durante la riparazione (configurazioni MetroCluster IP)

Durante la riparazione nelle configurazioni MetroCluster IP, la risincronizzazione degli aggregati mirrorati avviene in un processo in fasi che prepara i nodi nel sito di emergenza riparato per lo switchback. Si tratta di un evento pianificato, che ti offre il pieno controllo di ogni fase per ridurre al minimo i downtime. La riparazione è un processo in due fasi che si verifica sui componenti dello storage e del controller.

Differenze con le configurazioni MetroCluster FC

Nelle configurazioni MetroCluster IP, è necessario avviare i nodi nel cluster del sito di emergenza prima di eseguire l'operazione di riparazione.

I nodi nel cluster del sito di emergenza devono essere in esecuzione in modo che sia possibile accedere ai dischi iSCSI remoti quando gli aggregati vengono risincronizzati.

Se i nodi del sito di emergenza non sono in esecuzione, l'operazione di riparazione non riesce perché il nodo di emergenza non può eseguire le modifiche necessarie alla proprietà del disco.

Riparazione degli aggregati di dati

Una volta risolto il problema nel sito di emergenza, si avvia la fase di riparazione dello storage:

1. Verifica che tutti i nodi siano attivi e in esecuzione nel sito sopravvissuto.
2. Modifica la proprietà di tutti i dischi del pool 0 nel sito di disastro, compresi gli aggregati root.

Durante questa fase di riparazione, il sottosistema RAID risincronizza gli aggregati mirrorati e il sottosistema WAFL riproduce i file nvsaved degli aggregati mirrorati con un pool 1 plex guasto al momento dello switchover.

Se alcuni componenti dello storage di origine si sono guastati, il comando riporta gli errori ai livelli applicabili: Storage, Sanown o RAID.

Se non vengono segnalati errori, gli aggregati vengono risincronizzati correttamente. A volte il completamento di questo processo può richiedere ore.

"Riparazione della configurazione"

Healing dell'aggregato root

Una volta sincronizzati gli aggregati, viene eseguita la fase di healing dell'aggregato root. Nelle configurazioni MetroCluster IP, questa fase conferma che gli aggregati sono stati riparati.

"Riparazione della configurazione"

Riparazione automatica degli aggregati nelle configurazioni MetroCluster IP dopo lo switchover

A partire da ONTAP 9.5, la riparazione viene automatizzata durante le operazioni di switchover negoziate sulle configurazioni IP di MetroCluster. A partire da ONTAP 9.6, è supportata la riparazione automatica dopo lo switchover non pianificato. In questo modo si elimina il requisito di emissione di `metrocluster heal` comandi.

Riparazione automatica dopo lo switchover negoziato (a partire da ONTAP 9.5)

Dopo aver eseguito uno switchover negoziato (un comando di switchover emesso senza l'opzione -forced-on -disaster true), la funzionalità di riparazione automatica semplifica le operazioni necessarie per riportare il sistema al normale funzionamento. Nei sistemi con riparazione automatica, dopo lo switchover si verifica quanto segue:

- I nodi del sito di disastro rimangono attivi.

  Poiché si trovano nello stato di switchover, non stanno fornendo dati dai loro plessi locali mirrorati.

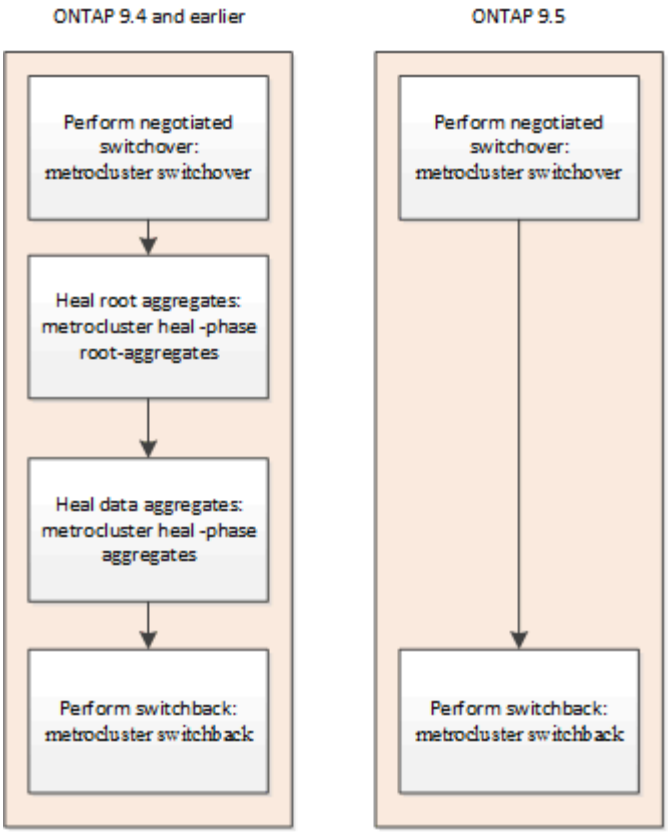
- I nodi del sito di emergenza vengono spostati nello stato "Waiting for switchback" (in attesa di switchback).

  È possibile confermare lo stato dei nodi del sito di emergenza utilizzando il comando MetroCluster Operation show.

- È possibile eseguire l'operazione di switchback senza emettere i comandi di riparazione.

Questa funzione si applica alle configurazioni IP di MetroCluster con ONTAP 9.5 e versioni successive. Non si applica alle configurazioni MetroCluster FC.

I comandi di riparazione manuale sono ancora necessari nelle configurazioni MetroCluster IP con ONTAP 9.4 e versioni precedenti.



Riparazione automatica dopo switchover non pianificato (a partire da ONTAP 9.6)

La riparazione automatica dopo uno switchover non pianificato è supportata nelle configurazioni MetroCluster IP a partire da ONTAP 9.6. Uno switchover non pianificato è quello in cui viene eseguito il `switchover` con il `-forced-on-disaster true` opzione.

La riparazione automatica dopo uno switchover non pianificato non è supportata nelle configurazioni MetroCluster FC e i comandi di riparazione manuale sono ancora necessari dopo lo switchover non pianificato nelle configurazioni MetroCluster IP con ONTAP 9.5 e versioni precedenti.

Nei sistemi che eseguono ONTAP 9.6 e versioni successive, dopo lo switchover non pianificato si verifica quanto segue:

- A seconda dell'entità del disastro, i nodi del sito di emergenza possono essere guasti.

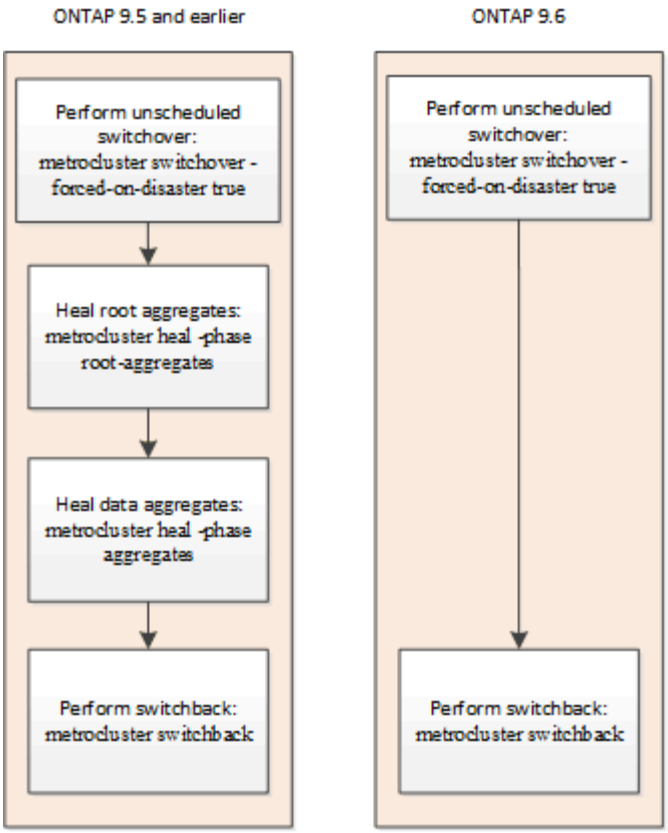
  Poiché si trovano nello stato di switchover, non stanno fornendo dati dai loro plessi locali mirrorati, anche se sono accesi.

- Se i siti di emergenza non erano attivi, all'avvio, i nodi del sito di emergenza vengono spostati nello stato "Waiting for switchback" (in attesa di switchback).

  Se i siti di disastro sono rimasti in alto, vengono immediatamente spostati nello stato "Waiting for switchback" (in attesa di switchback).

- Le operazioni di riparazione vengono eseguite automaticamente.

  È possibile confermare lo stato dei nodi del sito di emergenza e le operazioni di riparazione riuscite utilizzando `metrocluster operation show` comando.



Se la riparazione automatica non riesce

Se l'operazione di riparazione automatica non riesce per qualsiasi motivo, è necessario eseguire il `metrocluster heal` Comandi manuali come nelle versioni di ONTAP precedenti a ONTAP 9.6. È possibile utilizzare `metrocluster operation show` e. `metrocluster operation history show -instance` comandi per monitorare lo stato di riparazione e determinare la causa di un errore.

Creazione di SVM per una configurazione MetroCluster

È possibile creare SVM per una configurazione MetroCluster per fornire disaster recovery sincrono e alta disponibilità dei dati sui cluster configurati per una configurazione MetroCluster.

- I due cluster devono essere in una configurazione MetroCluster.
- Gli aggregati devono essere disponibili e online in entrambi i cluster.
- Se necessario, è necessario creare spazi IPcon gli stessi nomi su entrambi i cluster.
- Se uno dei cluster che formano la configurazione MetroCluster viene riavviato senza utilizzare uno switchover, le SVM di origine della sincronizzazione potrebbero essere online come "ssormontato" invece di "started".

Quando si crea una SVM su uno dei cluster in una configurazione MetroCluster, la SVM viene creata come SVM di origine e la SVM partner viene creata automaticamente con lo stesso nome ma con il suffisso "-mc" sul cluster partner. Se il nome SVM contiene un punto, il suffisso "-mc" viene applicato prima del primo periodo, ad esempio SVM-MC.DNS.NAME.

In una configurazione MetroCluster, è possibile creare 64 SVM su un cluster. Una configurazione MetroCluster supporta 128 SVM.

1. Utilizzare `vserver create` comando.

   Nell'esempio seguente viene illustrata la SVM con il sottotipo "sync-source" sul sito locale e la SVM con il sottotipo "sync-destination" sul sito partner:

   ```
   cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -aggregate
   aggr1
   -rootvolume-security-style mixed
   [Job 196] Job succeeded:
   Vserver creation completed
   ```

   La SVM "vs4" viene creata sul sito locale e la SVM "vs4-mc" viene creata sul sito del partner.

2. Visualizzare le SVM appena create.

   - Sul cluster locale, verificare lo stato di configurazione delle SVM:

     ```
     metrocluster vserver show
     ```

     L'esempio seguente mostra le SVM del partner e il relativo stato di configurazione:

     ```
     cluster_A::> metrocluster vserver show

                          Partner    Configuration
     Cluster     Vserver   Vserver    State
     ---------  --------  --------- -----------------
     cluster_A   vs4       vs4-mc     healthy
     cluster_B   vs1       vs1-mc     healthy
     ```

   - Dai cluster locali e partner, verificare lo stato delle SVM appena configurate:

     ```
     vserver show command
     ```

     Nell'esempio seguente vengono visualizzati gli stati amministrativi e operativi delle SVM:

```
cluster_A::> vserver show

                              Admin   Operational Root
Vserver Type  Subtype         State   State       Volume     Aggregate
------- ----- -------       ------- --------    -----------
----------
vs4     data  sync-source   running   running    vs4_root   aggr1

cluster_B::> vserver show

                                Admin   Operational  Root
Vserver Type  Subtype           State   State        Volume
Aggregate
------- ----- -------           ------  ---------    -----------
----------
vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
```

La creazione di SVM potrebbe non riuscire se le operazioni intermedie, ad esempio la creazione del volume root, non riescono e la SVM si trova nello stato “Initializing”. È necessario eliminare la SVM e ricrearla.

Le SVM per la configurazione MetroCluster vengono create con una dimensione del volume root di 1 GB. La SVM di origine della sincronizzazione si trova nello stato “in esecuzione” e la SVM di destinazione della sincronizzazione si trova nello stato “ssuperiore”.

Cosa succede durante uno switchback

Dopo il ripristino del sito di emergenza e la guarigione degli aggregati, il processo di switchback di MetroCluster restituisce lo storage e l’accesso client dal sito di disaster recovery al cluster domestico.

Il `metrocluster switchback` Il comando riporta il sito primario alla normale operazione MetroCluster completa. Le modifiche di configurazione vengono propagate alle SVM originali. Il funzionamento del server di dati viene quindi restituito alle SVM di origine della sincronizzazione sul sito di disastro e le SVM di destinazione della sincronizzazione che erano state operative sul sito di sopravvivenza vengono disattivate.

Se le SVM sono state eliminate nel sito sopravvissuto mentre la configurazione MetroCluster era in stato di switchover, il processo di switchback esegue le seguenti operazioni:

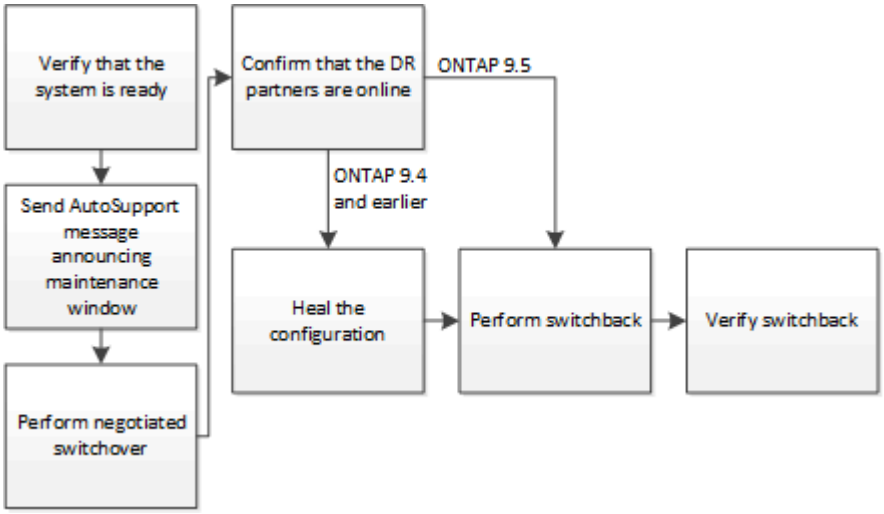
- Elimina le SVM corrispondenti sul sito del partner (il sito di disastro precedente).
- Elimina tutte le relazioni di peering delle SVM eliminate.

Eseguire lo switchover, la riparazione e lo switchback

Eseguire lo switchover per i test o la manutenzione

Esecuzione di uno switchover per test o manutenzione

Se si desidera testare la funzionalità MetroCluster o eseguire la manutenzione pianificata, è possibile eseguire uno switchover negoziato in cui un cluster viene trasferito correttamente al cluster partner. È quindi possibile riparare e ripristinare la configurazione.



A partire da ONTAP 9.6, le operazioni di switchover e switchback possono essere eseguite sulle configurazioni IP di MetroCluster con Gestore di sistema di ONTAP.

Verificare che il sistema sia pronto per lo switchover

È possibile utilizzare `-simulate` opzione per visualizzare in anteprima i risultati di un'operazione di switchover. Un controllo di verifica consente di verificare che la maggior parte delle condizioni preliminari per un'esecuzione corretta siano soddisfatte prima di iniziare l'operazione. Eseguire questi comandi dal sito che rimarranno attivi e operativi:

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Dal sito che rimarrà attivo e operativo, simulare un'operazione di switchover: `metrocluster switchover -simulate`
3. Esaminare l'output restituito.

   L'output mostra se eventuali veti impedirebbero un'operazione di switchover. Ogni volta che si esegue un'operazione MetroCluster, è necessario verificare una serie di criteri per la riuscita dell'operazione. Un "veto" è un meccanismo che impedisce l'operazione se uno o più dei criteri non sono soddisfatti. Esistono due tipi di veto: Un veto "soft" e un veto "hard". È possibile ignorare un veto morbido, ma non un veto difficile. Ad esempio, per eseguire uno switchover negoziato in una configurazione MetroCluster a quattro

nodi, un criterio è che tutti i nodi sono attivi e funzionanti. Supponiamo che un nodo sia inattivo e sia stato sostituito dal partner ha. L'operazione di switchover sarà difficile da veto perché è un criterio difficile che tutti i nodi devono essere attivi e sani. Poiché si tratta di un veto difficile, non è possibile ignorare il veto.

> Si consiglia di non ignorare alcun veto.

Esempio: Risultati della verifica

L'esempio seguente mostra gli errori riscontrati in una simulazione di un'operazione di switchover:

```
cluster4::*> metrocluster switchover -simulate

[Job 126] Preparing the cluster for the switchover operation...
[Job 126] Job failed: Failed to prepare the cluster for the switchover
operation. Use the "metrocluster operation show" command to view detailed
error
information. Resolve the errors, then try the command again.
```

> Lo switchover e lo switchback negoziati non avranno esito positivo fino a quando non verranno sostituiti tutti i dischi guasti. È possibile eseguire il disaster recovery dopo aver sostituito i dischi guasti. Se si desidera ignorare l'avviso relativo ai dischi guasti, è possibile aggiungere un veto soft per lo switchover e lo switchback negoziati.

Invio di un messaggio AutoSupport personalizzato prima dello switchover negoziato

Prima di eseguire uno switchover negoziato, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Lo switchover negoziato potrebbe causare errori operativi plex o MetroCluster che attivano i messaggi AutoSupport. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster dal sito_A.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

   intervallo di manutenzione in ore specifica la durata della finestra di manutenzione e può essere di un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile inviare un comando a per indicare che il periodo di manutenzione è terminato:`system node autosupport invoke -node * -type all -message MAINT=end`
3. Ripetere questo passaggio sul sito del partner.

Esecuzione di uno switchover negoziato

Uno switchover negoziato arresta in modo pulito i processi sul sito del partner, quindi passa alle operazioni dal sito del partner. È possibile utilizzare uno switchover negoziato per eseguire la manutenzione su un sito MetroCluster o per testare la funzionalità di switchover.

- Tutte le modifiche di configurazione precedenti devono essere completate prima di eseguire un'operazione di switchback.

  In questo modo si evita la concorrenza con lo switchover negoziato o con l'operazione di switchback.

- Tutti i nodi precedentemente non attivi devono essere avviati e in base al quorum del cluster.

  Nella sezione "informazioni sul quorum e sull'epsilon" del documento *System Administration Reference* sono disponibili ulteriori informazioni sul quorum dei cluster.

  "Amministrazione del sistema"

- La rete di peering del cluster deve essere disponibile da entrambi i siti.
- Tutti i nodi nella configurazione MetroCluster devono eseguire la stessa versione del software ONTAP.
- L'opzione Replication.create_data_Protection_rels.enable deve essere impostata SU ON su entrambi i siti in una configurazione MetroCluster prima di creare una nuova relazione SnapMirror.
- Per una configurazione MetroCluster a due nodi, non è necessario creare una nuova relazione SnapMirror durante un aggiornamento in caso di versioni di ONTAP non corrispondenti tra i siti.
- Per una configurazione MetroCluster a quattro nodi, le versioni di ONTAP non corrispondenti tra i siti non sono supportate.

Il sito di ripristino può richiedere alcune ore per poter eseguire l'operazione di switchback.

Il comando MetroCluster switchover consente di passare ai nodi di tutti i gruppi di DR nella configurazione MetroCluster. Ad esempio, in una configurazione MetroCluster a otto nodi, viene eseguita la commutazione dei nodi in entrambi i gruppi di DR.

Durante la preparazione e l'esecuzione di uno switchover negoziato, non è necessario apportare modifiche alla configurazione del cluster o eseguire operazioni di Takeover o giveback.

Per le configurazioni MetroCluster FC:

- 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.
- 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.

Per le configurazioni MetroCluster IP:

> Prima di eseguire le attività di manutenzione, è necessario rimuovere il monitoraggio se la configurazione MetroCluster viene monitorata con l'utilità Tiebreaker o Mediator."Prima di eseguire le attività di manutenzione, rimuovere il mediatore ONTAP o il monitoraggio di spareggio"

- 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.

    i. Utilizzare i comandi MetroCluster check run, MetroCluster check show e MetroCluster check config-Replication show per assicurarsi che non siano in corso aggiornamenti di configurazione o in sospeso. Eseguire questi comandi dal sito che rimarranno attivi e operativi.

    ii. Dal sito che rimarrà attivo e operativo, implementare lo switchover: `metrocluster switchover`

    Il completamento dell'operazione può richiedere alcuni minuti.

    iii. Monitorare il completamento dello switchover: `metrocluster operation show`

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

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

    iv. Ripristinare le configurazioni SnapMirror o SnapVault.

Verificare che le SVM siano in esecuzione e che gli aggregati siano online

Una volta completato lo switchover, è necessario verificare che i partner di DR abbiano acquisito la proprietà dei dischi e che le SVM del partner siano online.

Quando si esegue il comando show dell'aggregato di storage dopo uno switchover MetroCluster, lo stato di plex0 dell'aggregato root commutato è indeterminato e viene visualizzato come failed (non riuscito). Durante questo periodo, la root commutata non viene aggiornata. Lo stato effettivo di questo plex può essere determinato solo dopo la fase di riparazione MetroCluster.

Fasi

1. Controllare che gli aggregati siano stati invertiti utilizzando il comando show dell'aggregato di storage.

In questo esempio, gli aggregati sono stati invertiti. L'aggregato root (aggr0_b2) si trova in uno stato degradato. L'aggregato di dati (b2_aggr2) si trova in uno stato normale mirrorato:

```
cluster_A::*> storage aggregate show

.
.
.
mcc1-b Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b2    227.1GB   45.1GB    80% online       0 node_A_1
raid_dp,

mirror

degraded
b2_aggr1    227.1GB   200.3GB    20% online       0 node_A_1
raid_dp,

mirrored

normal
```

2. Verificare che le SVM secondarie siano online utilizzando il comando vserver show.

   In questo esempio, le SVM di destinazione di sincronizzazione precedentemente inattive sul sito secondario sono state attivate e hanno uno stato di esecuzione Admin:

```
cluster_A::*> vserver show
                                          Admin      Operational  Root
Name    Name
Vserver           Type  Subtype           State      State        Volume
Aggregate  Service Mapping
-----------       ----- ----------        ---------- -----------
--------- ---------- ------- -------
...
cluster_B-vs1b-mc data   sync-destination  running   running
vs1b_vol   aggr_b1   file    file
```

Riparare la configurazione

Correggere la configurazione in una configurazione MetroCluster FC

Riparazione della configurazione in una configurazione MetroCluster FC

Dopo uno switchover, è necessario eseguire le operazioni di riparazione in ordine specifico per ripristinare la funzionalità MetroCluster.

- Lo switchover deve essere stato eseguito e il sito sopravvissuto deve fornire i dati.
- I nodi nel sito di disastro devono essere arrestati o spenti.

  Non devono essere completamente avviati durante il processo di riparazione.

- Lo storage nel sito di disastro deve essere accessibile (gli shelf sono accesi, funzionali e accessibili).
- Nelle configurazioni Fabric-Attached MetroCluster, i collegamenti inter-switch (ISL) devono essere operativi.
- Nelle configurazioni MetroCluster a quattro nodi, i nodi nel sito sopravvissuto non devono essere in stato di failover ha (tutti i nodi devono essere attivi e in esecuzione per ogni coppia ha).

L'operazione di riparazione deve essere eseguita prima sugli aggregati di dati, quindi sugli aggregati root.

Riparazione degli aggregati di dati dopo lo switchover negoziato

È necessario riparare gli aggregati di dati dopo aver completato qualsiasi manutenzione o test. Questo processo risincronizza gli aggregati di dati e prepara il sito di emergenza per il normale funzionamento. È necessario riparare gli aggregati di dati prima di riparare gli aggregati root.

Tutti gli aggiornamenti della configurazione nel cluster remoto vengono replicati correttamente nel cluster locale. L'alimentazione dello storage nel sito di disastro viene eseguita nell'ambito di questa procedura, ma non è necessario accendere i moduli controller nel sito di disastro.

Fasi

1. Assicurarsi che lo switchover sia stato completato eseguendo il comando show di MetroCluster Operation.

   ```
   controller_A_1::> metrocluster operation show
     Operation: switchover
         State: successful
    Start Time: 7/25/2014 20:01:48
      End Time: 7/25/2014 20:02:14
        Errors: -
   ```

2. Risincronizzare gli aggregati di dati eseguendo il comando MetroCluster Heal -Phase Aggregates dal cluster esistente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Se la riparazione è vetoed, è possibile emettere nuovamente il comando MetroCluster Heal con il parametro --override-vetoes. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

3. Verificare che l'operazione sia stata completata eseguendo il comando MetroCluster Operation show.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Controllare lo stato degli aggregati eseguendo il comando show dell'aggregato di storage.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

5. Se lo storage è stato sostituito nel sito di disastro, potrebbe essere necessario eseguire il remirrore degli aggregati.

Riparazione degli aggregati root dopo lo switchover negoziato

Una volta guariti gli aggregati di dati, è necessario riparare gli aggregati root in preparazione dell'operazione di switchback.

La fase di aggregazione dei dati del processo di riparazione MetroCluster deve essere stata completata correttamente.

Fasi

1. Ripristinare gli aggregati mirrorati eseguendo il comando MetroCluster Heal -Phase root-aggregates.

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Se la riparazione è vetoed, è possibile emettere nuovamente il comando MetroCluster Heal con il parametro --override-vetoes. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

2. Verificare che l'operazione di riparazione sia completa eseguendo il comando MetroCluster Operation show sul cluster integro:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2014 20:54:41
   End Time: 7/29/2014 20:54:42
     Errors: -
```

3. Controllare e rimuovere eventuali dischi guasti appartenenti al sito di disastro eseguendo il seguente comando sul sito di integrità: `disk show -broken`
4. Accendere o avviare ciascun modulo controller nel sito di emergenza.

   Se il sistema visualizza il prompt DEL CARICATORE, eseguire `boot_ontap` comando.

5. Dopo l'avvio dei nodi, verificare che gli aggregati root siano mirrorati.

   Se entrambi i plessi sono presenti, la risincronizzazione viene eseguita automaticamente se i plessi non sono sincronizzati. In caso di errore di un plex, tale plex deve essere distrutto e il mirror deve essere ricreato utilizzando il comando storage aggregate mirror -aggregateaggregate-name per ristabilire la relazione mirror.

Riparazione della configurazione in una configurazione MetroCluster IP (ONTAP 9.4 e versioni precedenti)

È necessario riparare gli aggregati in preparazione dell'operazione di switchback.

> Nei sistemi MetroCluster IP che eseguono ONTAP 9.5, la riparazione viene eseguita automaticamente ed è possibile ignorare queste attività.

Prima di eseguire la procedura di riparazione, devono sussistere le seguenti condizioni:

- Lo switchover deve essere stato eseguito e il sito sopravvissuto deve fornire i dati.
- Gli shelf di storage nel sito di disastro devono essere alimentati, funzionali e accessibili.
- Gli ISL devono essere operativi.
- I nodi nel sito sopravvissuto non devono essere in stato di failover ha (entrambi i nodi devono essere attivi e in esecuzione).

Questa attività si applica solo alle configurazioni IP di MetroCluster con versioni di ONTAP precedenti alla 9.5.

Questa procedura differisce dalla procedura di riparazione per le configurazioni MetroCluster FC.

Fasi

1. Accendere ciascun modulo controller sul sito che è stato attivato e lasciarlo avviare completamente.

Se il sistema visualizza il prompt DEL CARICATORE, eseguire `boot_ontap` comando.

2. Eseguire la fase di healing dell'aggregato root: `metrocluster heal root-aggregates`

```
cluster_A::> metrocluster heal root-aggregates
[Job 137] Job succeeded: Heal Root-Aggregates is successful
```

Se la riparazione è vetoed, è possibile emettere nuovamente il comando MetroCluster heal root-aggregates con il parametro --override-vetoes. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

3. Risincronizzare gli aggregati: `metrocluster heal aggregates`

```
cluster_A::> metrocluster heal aggregates
[Job 137] Job succeeded: Heal Aggregates is successful
```

Se la riparazione è vetoed, è possibile emettere nuovamente il comando MetroCluster Heal con il parametro --override-vetoes. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

4. Verificare che l'operazione di riparazione sia completa eseguendo il comando MetroCluster Operation show sul cluster integro:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2017 20:54:41
   End Time: 7/29/2017 20:54:42
     Errors: -
```

Esecuzione di uno switchback

Dopo aver corretto la configurazione MetroCluster, è possibile eseguire l'operazione di switchback MetroCluster. L'operazione di switchback MetroCluster riporta la configurazione al suo normale stato operativo, con le macchine virtuali dello storage di origine di sincronizzazione (SVM) sul sito di emergenza attive e i dati provenienti dai pool di dischi locali.

- Il cluster di emergenza deve essere passato correttamente al cluster esistente.
- La riparazione deve essere stata eseguita sui dati e sugli aggregati root.
- I nodi del cluster sopravvissuti non devono trovarsi nello stato di failover ha (tutti i nodi devono essere attivi e in esecuzione per ogni coppia ha).
- I moduli controller del sito di emergenza devono essere completamente avviati e non in modalità ha Takeover.

- L'aggregato root deve essere mirrorato.
- I collegamenti Inter-Switch (ISL) devono essere online.
- Tutte le licenze richieste devono essere installate sul sistema.

a. Verificare che tutti i nodi siano nello stato abilitato: `metrocluster node show`

   Nell'esempio riportato di seguito vengono visualizzati i nodi che si trovano nello stato abilitato:

```
cluster_B::>  metrocluster node show

DR                         Configuration  DR
Group Cluster Node         State          Mirroring Mode
----- ------- ----------- -------------- ---------
--------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots
completed
              node_A_2    configured     enabled   heal roots
completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

b. Verificare che la risincronizzazione sia completa su tutte le SVM: `metrocluster vserver show`

c. Verificare che tutte le migrazioni LIF automatiche eseguite dalle operazioni di riparazione siano state completate correttamente: `metrocluster check lif show`

d. Eseguire uno switchback simulato per verificare che il sistema sia pronto: `metrocluster switchback -simulate`

e. 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
Last Checked On: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 entries were displayed.
```

f. Eseguire lo switchback eseguendo il comando MetroCluster switchback da qualsiasi nodo del cluster esistente: `metrocluster switchback`

g. Controllare l'avanzamento dell'operazione di switchback: `metrocluster show`

   L'operazione di switchback è ancora in corso quando l'output visualizza Waiting-for-switchback:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   L'operazione di switchback è completa quando l'output visualizza normale:

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

+ Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando. Questo comando si trova al livello di privilegio avanzato.

a. Ripristinare le configurazioni SnapMirror o SnapVault.

   In ONTAP 8.3, è necessario ristabilire manualmente una configurazione di SnapMirror persa dopo un'operazione di switchback MetroCluster. In ONTAP 9.0 e versioni successive, la relazione viene ristabilita automaticamente.

Verifica di uno switchback riuscito

Dopo aver eseguito lo switchback, si desidera confermare che tutti gli aggregati e le macchine virtuali di storage (SVM) siano ripristinati e in linea.

1. Verificare che gli aggregati di dati di switchover siano ripristinati:

   `storage aggregate show`

   Nell'esempio seguente, aggr_b2 sul nodo B2 è tornato:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal
```

2. Verificare che tutte le SVM di destinazione della sincronizzazione sul cluster sopravvissuto siano inattive (mostrando uno stato di amministrazione di "ssurfared") e che le SVM di origine della sincronizzazione sul cluster di emergenza siano attive e in esecuzione:

`vserver show -subtype sync-source`

```
node_B_1::> vserver show -subtype sync-source
                               Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                               running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                               Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                      stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Gli aggregati Sync-destination nella configurazione MetroCluster hanno il suffisso “-mc” aggiunto automaticamente al loro nome per facilitarne l’identificazione.

3. Verificare che le operazioni di switchback siano riuscite utilizzando `metrocluster operation show` comando.

Se l’output del comando mostra…	Quindi…
Che lo stato operativo di switchback sia riuscito.	Il processo di switchback è completo ed è possibile procedere con il funzionamento del sistema.
Che l’operazione di switchback o l’operazione switchback-continuation-Agent abbia parzialmente esito positivo.	Eseguire la correzione suggerita nell’output di `metrocluster operation show` comando.

Ripetere le sezioni precedenti per eseguire il switchback nella direzione opposta. Se Site_A ha eseguito uno

switchover di Site_B, chiedere a Site_B di eseguire uno switchover di Site_A.

Comandi per switchover, healing e switchback

Esistono comandi ONTAP specifici per l'esecuzione dei processi di disaster recovery di MetroCluster.

Se si desidera…	Utilizzare questo comando…
Verificare che lo switchover possa essere eseguito senza errori o veti.	`metrocluster switchover -simulate` + a livello di privilegi avanzati
Verificare che lo switchback possa essere eseguito senza errori o veti.	`metrocluster switchback -simulate` + a livello di privilegi avanzati
Passare ai nodi partner (switchover negoziato).	`metrocluster switchover`
Passare ai nodi partner (switchover forzato).	`metrocluster switchover -forced-on-disaster true`
Eseguire la riparazione degli aggregati di dati.	`metrocluster heal -phase aggregates`
Eseguire la riparazione dell'aggregato root.	`metrocluster heal -phase root-aggregates`
Tornare ai nodi home.	`metrocluster switchback`

Monitoraggio della configurazione di MetroCluster

È possibile utilizzare ONTAP MetroCluster Commands e Active IQ Unified Manager (precedentemente noto come Gestore unificato di OnCommand) per monitorare lo stato di salute di una vasta gamma di componenti software e lo stato delle operazioni MetroCluster.

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` i comandi non mostrano l'output previsto.

Fasi

1. Controllare la configurazione:

   `metrocluster check run`

   Il comando viene eseguito come processo in background e potrebbe non essere completato immediatamente.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

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                  Aggregate                  Check
   Result
   ---------------       --------------------       ---------------------
   ---------
   controller_A_1        controller_A_1_aggr0
                                                    mirroring-status
   ok
                                                    disk-pool-allocation
   ok
   ```

```
                                                    ownership-state
ok
                     controller_A_1_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2       controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    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.
```

Comandi per il controllo e il monitoraggio della configurazione MetroCluster

Sono disponibili comandi ONTAP specifici per il monitoraggio della configurazione MetroCluster e il controllo delle operazioni MetroCluster.

Comandi per il controllo delle operazioni MetroCluster

Se si desidera…	Utilizzare questo comando…
Eseguire un controllo delle operazioni MetroCluster. **Nota:** questo comando non deve essere utilizzato come unico comando per la convalida del sistema operativo pre-DR.	`metrocluster check run`
Visualizzare i risultati dell'ultimo controllo sulle operazioni MetroCluster.	`metrocluster show`
Visualizza i risultati del controllo sulla replica della configurazione tra i siti.	`metrocluster check config-replication show` `metrocluster check config-replication show-aggregate-eligibility`
Visualizza i risultati del controllo sulla configurazione del nodo.	`metrocluster check node show`
Visualizza i risultati del controllo sulla configurazione aggregata.	`metrocluster check aggregate show`

Visualizzare gli errori di posizionamento LIF nella configurazione MetroCluster.	`metrocluster check lif show`

Comandi per il monitoraggio dell'interconnessione MetroCluster

Se si desidera…	Utilizzare questo comando…
Visualizzare lo stato e le informazioni del mirroring ha e DR per i nodi MetroCluster nel cluster.	`metrocluster interconnect mirror show`

Comandi per il monitoraggio delle SVM MetroCluster

Se si desidera…	Utilizzare questo comando…
Visualizzare tutte le SVM in entrambi i siti nella configurazione MetroCluster.	`metrocluster vserver show`

Utilizzo di MetroCluster Tiebreaker o ONTAP Mediator per monitorare la configurazione

Vedere "Differenze tra ONTAP Mediator e MetroCluster Tiebreaker" Per comprendere le differenze tra questi due metodi di monitoraggio della configurazione di MetroCluster e di avvio di uno switchover automatico.

Utilizzare questi collegamenti per installare e configurare tiebreaker o Mediator:

- "Installare e configurare il software MetroCluster Tiebreaker"
- "Preparare l'installazione del servizio ONTAP Mediator"

Il modo in cui il software NetApp MetroCluster Tiebreaker rileva i guasti

Il software Tiebreaker risiede su un host Linux. Il software Tiebreaker è necessario solo se si desidera monitorare due cluster e lo stato di connettività tra di essi da un terzo sito. In questo modo, ciascun partner di un cluster può distinguere tra un errore ISL, quando i collegamenti tra siti sono inattivi, da un guasto di un sito.

Dopo aver installato il software Tiebreaker su un host Linux, è possibile configurare i cluster in una configurazione MetroCluster per monitorare le condizioni di emergenza.

Il modo in cui il software Tiebreaker rileva gli errori di connettività tra siti

Il software MetroCluster Tiebreaker avvisa l'utente in caso di perdita di tutte le connessioni tra i siti.

Tipi di percorsi di rete

A seconda della configurazione, esistono tre tipi di percorsi di rete tra i due cluster in una configurazione MetroCluster:

- **Rete FC (presente nelle configurazioni Fabric-Attached MetroCluster)**

  Questo tipo di rete è composto da due fabric switch FC ridondanti. Ogni fabric di switch dispone di due switch FC, con uno switch di ciascun fabric di switch co-allocato con un cluster. Ogni cluster dispone di due

switch FC, uno per ciascun fabric di switch. Tutti i nodi dispongono di connettività FC (interconnessione NV e iniziatore FCP) a ciascuno degli switch IP co-localizzati. I dati vengono replicati dal cluster al cluster tramite l'ISL.

- **Rete di peering intercluster**

  Questo tipo di rete è composto da un percorso di rete IP ridondante tra i due cluster. La rete di peering del cluster fornisce la connettività necessaria per eseguire il mirroring della configurazione della macchina virtuale di storage (SVM). La configurazione di tutte le SVM su un cluster viene sottoposta a mirroring dal cluster partner.

- **Rete IP (presente nelle configurazioni MetroCluster IP)**

  Questo tipo di rete è composto da due reti di switch IP ridondanti. Ogni rete dispone di due switch IP, con uno switch per ciascun fabric switch co-allocato con un cluster. Ogni cluster dispone di due switch IP, uno per ciascun fabric di switch. Tutti i nodi sono connessi a ciascuno switch FC co-localizzati. I dati vengono replicati dal cluster al cluster tramite l'ISL.

Monitoraggio della connettività tra siti

Il software Tiebreaker recupera regolarmente lo stato della connettività tra siti dai nodi. Se la connettività di interconnessione NV viene persa e il peering dell'intercluster non risponde ai ping, i cluster presumono che i siti siano isolati e il software di spareggio attiva un avviso come "AllLinksSevered". Se un cluster identifica lo stato "AllLinksSevered" e l'altro cluster non è raggiungibile attraverso la rete, il software di spareggio attiva un avviso come "disaster".

Il modo in cui il software Tiebreaker rileva i guasti del sito

Il software NetApp MetroCluster Tiebreaker verifica la raggiungibilità dei nodi in una configurazione MetroCluster e del cluster per determinare se si è verificato un guasto al sito. Il software di spareggio attiva anche un avviso in determinate condizioni.

Componenti monitorati dal software Tiebreaker

Il software Tiebreaker monitora ciascun controller nella configurazione MetroCluster stabilendo connessioni ridondanti attraverso percorsi multipli a una LIF di gestione dei nodi e alla LIF di gestione dei cluster, entrambi ospitati sulla rete IP.

Il software Tiebreaker monitora i seguenti componenti nella configurazione MetroCluster:

- Nodi attraverso interfacce di nodi locali
- Attraverso le interfacce designate dal cluster
- Sopravvivenza del cluster per valutare se dispone di connettività al sito di disastro (interconnessione NV, storage e peering intercluster)

In caso di perdita di connessione tra il software Tiebreaker e tutti i nodi del cluster e del cluster stesso, il cluster viene dichiarato "non raggiungibile" dal software Tiebreaker. Il rilevamento di un errore di connessione richiede da tre a cinque secondi. Se un cluster non è raggiungibile dal software di spareggio, il cluster che rimane (il cluster che è ancora raggiungibile) deve indicare che tutti i collegamenti al cluster partner sono interrotti prima che il software di spareggio attivi un avviso.

> Tutti i collegamenti vengono interrotti se il cluster sopravvissuto non riesce più a comunicare con il cluster nel sito di disastro tramite FC (interconnessione e storage NV) e peering tra cluster.

Scenari di guasto durante i quali il software di spareggio attiva un avviso

Il software di spareggio attiva un avviso quando il cluster (tutti i nodi) nel sito di disastro è inattivo o irraggiungibile e il cluster nel sito di sopravvivenza indica lo stato "AllLinksSevered".

Il software di spareggio non attiva un avviso (o l'avviso viene vetoato) nei seguenti scenari:

- In una configurazione MetroCluster a otto nodi, se una coppia ha nel sito di emergenza non è attiva
- In un cluster con tutti i nodi nel sito di disastro non attivi, una coppia ha nel sito di sopravvivenza è inattiva e il cluster nel sito di sopravvivenza indica lo stato "AllLinksSevered"

  Il software di spareggio attiva un avviso, ma ONTAP veto tale avviso. In questa situazione, viene veto anche lo switchover manuale

- Qualsiasi scenario in cui il software di spareggio può raggiungere almeno un nodo o l'interfaccia del cluster nel sito di disastro, oppure il sito sopravvissuto può ancora raggiungere uno dei due nodi nel sito di disastro tramite FC (interconnessione e storage NV) o peering intercluster

In che modo il mediatore ONTAP supporta lo switchover automatico non pianificato

"Scoprite in che modo ONTAP Mediator supporta lo switchover automatico non pianificato nelle configurazioni IP di MetroCluster".

Monitoraggio e protezione della coerenza del file system con NVFAIL

Il `-nvfail` del parametro `volume modify` Il comando consente a ONTAP di rilevare incoerenze della RAM non volatile (NVRAM) durante l'avvio del sistema o dopo un'operazione di switchover. Inoltre, avvisa e protegge il sistema dall'accesso e dalla modifica dei dati fino a quando il volume non può essere recuperato manualmente.

Se ONTAP rileva problemi, le istanze del database o del file system smettono di rispondere o si arrestano. ONTAP invia quindi messaggi di errore alla console per avvisare l'utente di controllare lo stato del database o del file system. È possibile abilitare NVFAIL per avvisare gli amministratori di database delle incoerenze NVRAM tra i nodi in cluster che possono compromettere la validità del database.

Dopo la perdita dei dati NVRAM durante il failover o il boot recovery, i client NFS non possono accedere ai dati da uno dei nodi fino a quando lo stato NVFAIL non viene cancellato. I client CIFS non sono interessati.

Impatto di NVFAIL sull'accesso ai volumi NFS o alle LUN

Lo stato NVFAIL viene impostato quando ONTAP rileva errori NVRAM durante l'avvio, quando si verifica un'operazione di switchover MetroCluster o durante un'operazione di takeover ha se l'opzione NVFAIL è impostata sul volume. Se all'avvio non vengono rilevati errori, il file service viene avviato normalmente. Tuttavia, se vengono rilevati errori NVRAM o l'elaborazione NVFAIL viene applicata in caso di disaster switchover, ONTAP impedisce alle istanze del database di rispondere.

Quando si attiva l'opzione NVFAIL, durante l'avvio viene eseguito uno dei processi descritti nella seguente tabella:

Se…	Quindi…
ONTAP non rileva errori NVRAM	Il file service si avvia normalmente.
ONTAP rileva errori NVRAM	• ONTAP restituisce un errore ESTALE (stale file handle) ai client NFS che tentano di accedere al database, causando il blocco o l'arresto dell'applicazione. ONTAP invia quindi un messaggio di errore alla console di sistema e al file di log. • Al riavvio dell'applicazione, i file sono disponibili per i client CIFS anche se non si è verificato che siano validi. Per i client NFS, i file rimangono inaccessibili fino a quando non viene reimpostato `in-nvfailed-state` sul volume interessato.
Se viene utilizzato uno dei seguenti parametri: • `dr-force-nvfail` l'opzione del volume è impostata • `force-nvfail-all` l'opzione del comando di switchover è impostata.	È possibile annullare l'impostazione di `dr-force-nvfail` Dopo lo switchover, se l'amministratore non prevede di forzare l'elaborazione NVFAIL per eventuali future operazioni di switchover in caso di disastro. Per i client NFS, i file rimangono inaccessibili fino a quando non viene reimpostato `in-nvfailed-state` sul volume interessato. Utilizzando il `force-nvfail-all` causa l'opzione `dr-force-nvfail` Opzione da impostare su tutti i volumi DR elaborati durante il disaster switchover.
ONTAP rileva gli errori NVRAM su un volume che contiene LUN	Le LUN di quel volume vengono portate offline. Il `in-nvfailed-state` L'opzione sul volume deve essere deselezionata e l'attributo NVFAIL sui LUN deve essere cancellato portando online ogni LUN nel volume interessato. È possibile eseguire la procedura per verificare l'integrità dei LUN e ripristinare il LUN da una copia Snapshot o da un backup secondo necessità. Una volta ripristinate tutte le LUN del volume, la `in-nvfailed-state` l'opzione sul volume interessato viene deselezionata.

Comandi per il monitoraggio degli eventi di perdita dei dati

Se si attiva l'opzione NVFAIL, si riceve una notifica quando si verifica un crash di sistema causato da incoerenze della NVRAM o uno switchover MetroCluster.

Per impostazione predefinita, il parametro NVFAIL non è attivato.

Se si desidera…	Utilizzare questo comando…
Creare un nuovo volume con NVFAIL attivato	`volume create -nvfail on`
Attivare NVFAIL su un volume esistente	`volume modify` **Nota:** è stato impostato il `-nvfail` Opzione su "on" per attivare NVFAIL sul volume creato.
Visualizza se NVFAIL è attualmente abilitato per un volume specificato	`volume show` **Nota:** è stato impostato il `-fields` Parametro su "nvfail" per visualizzare l'attributo NVFAIL per un volume specificato.

Informazioni correlate

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

Accesso ai volumi in stato NVFAIL dopo uno switchover

Dopo uno switchover, è necessario cancellare lo stato NVFAIL ripristinando `-in-nvfailed-state` del parametro `volume modify` comando per rimuovere la restrizione di accesso dei client ai dati.

Prima di iniziare

Il database o il file system non deve essere in esecuzione o non deve tentare di accedere al volume interessato.

A proposito di questa attività

Impostazione `-in-nvfailed-state` il parametro richiede privilegi di livello avanzato.

Fase

1. Ripristinare il volume utilizzando il comando di modifica del volume con il parametro -in-nvfailed-state impostato su false.

Al termine

Per istruzioni sull'esame della validità del file di database, consultare la documentazione relativa al software di database specifico.

Se il database utilizza LUN, rivedere la procedura per rendere le LUN accessibili all'host dopo un errore della NVRAM.

Informazioni correlate

"Monitoraggio e protezione della coerenza del file system con NVFAIL"

Ripristino delle LUN negli stati NVFAIL dopo lo switchover

Dopo uno switchover, l'host non ha più accesso ai dati sulle LUN che si trovano negli stati NVFAIL. Prima che il database abbia accesso alle LUN, è necessario eseguire diverse azioni.

Prima di iniziare

Il database non deve essere in esecuzione.

Fasi

1. Azzerare lo stato NVFAIL sul volume che ospita i LUN reimpostando `-in-nvfailed-state` del parametro `volume modify` comando.
2. Portare online le LUN interessate.
3. Esaminare le LUN per individuare eventuali incoerenze di dati e risolverle.

   Ciò potrebbe comportare il ripristino o il ripristino basato su host eseguito sul controller dello storage utilizzando SnapRestore.

4. Portare l'applicazione di database online dopo il ripristino dei LUN.

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione e sul funzionamento di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto
"Documentazione MetroCluster"	• Tutte le informazioni MetroCluster
"Report tecnico NetApp 4375: NetApp MetroCluster per ONTAP 9.3"	• Panoramica tecnica della configurazione e del funzionamento di MetroCluster. • Best practice per la configurazione di MetroCluster.
"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP

"Installazione e configurazione di MetroCluster IP"	• Architettura IP di MetroCluster • Cablaggio della configurazione • Configurazione di MetroCluster in ONTAP
"Installazione e configurazione del software MetroCluster Tiebreaker 1.21"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
Documentazione Active IQ Unified Manager "Documentazione NetApp: Guide e risorse sui prodotti"	• Monitoraggio della configurazione e delle prestazioni di MetroCluster
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster

Gestire i componenti di MetroCluster

Dove trovare le procedure per le attività di manutenzione di MetroCluster

Quando si eseguono le attività di manutenzione dell'hardware MetroCluster, assicurarsi di selezionare la procedura corretta.

> Con il rilascio di ONTAP 9.8, le procedure di aggiornamento ed espansione di MetroCluster sono state spostate in "Upgrade ed espansione di MetroCluster" e. "Transizione da MetroCluster FC a MetroCluster IP".

Componente	Tipo di MetroCluster (FC o IP)	Attività	Procedura
Software ONTAP	Entrambi	Aggiornamento del software ONTAP	"Upgrade, revert o downgrade"
Modulo controller	Entrambi	Sostituzione della FRU (inclusi moduli controller, schede PCIe, scheda FC-VI e così via) Lo spostamento di un modulo controller storage o di una scheda NVRAM tra i sistemi storage MetroCluster non è supportato.	"Documentazione dei sistemi hardware ONTAP"
Upgrade ed espansione	"Upgrade ed espansione di MetroCluster®"	Transizione dalla connettività FC a quella IP	"Transizione da MetroCluster FC a MetroCluster IP"

Shelf di dischi	FC	Aggiunta di shelf (stack con bridge o shelf singolo)	"Aggiunta a caldo di uno stack di shelf di dischi SAS a una coppia esistente di bridge FibreBridge 7500N" "Aggiunta a caldo di uno stack di shelf di dischi SAS e bridge a un sistema MetroCluster" "Aggiunta a caldo di uno shelf di dischi SAS a uno stack di shelf di dischi SAS"
FC	Rimozione dello shelf	"Rimozione a caldo dello storage da una configurazione MetroCluster FC"	FC
Tutte le altre procedure di manutenzione degli shelf. È possibile utilizzare le procedure standard.	"Manutenzione degli shelf di dischi DS460C DS224C e DS212C"	IP	Tutte le procedure di manutenzione degli shelf. È possibile utilizzare le procedure standard. Se si aggiungono shelf per un aggregato senza mirror, vedere "Considerazioni sull'utilizzo di aggregati senza mirror"
"Manutenzione degli shelf di dischi DS460C DS224C e DS212C"	Entrambi	Aggiunta a caldo di shelf IOM12 a una pila di shelf IOM6	"Shelf hot-adding con moduli IOM12 a uno stack di shelf con moduli IOM6"
Bridge FC-SAS	FC	Sostituzione del bridge	"Sostituzione di un singolo bridge FC-SAS" "Sostituzione di una coppia di bridge FibreBridge 6500N con bridge 7600N o 7500N" "Scambio a caldo di un FibreBridge 7500N con un bridge 7600N"

FC	Aggiornamento del firmware	"Aggiornamento del firmware su un bridge FibreBridge"	FC
Sostituzione di un modulo alimentatore guasto	"Sostituzione a caldo di un modulo alimentatore guasto"	Switch FC	FC
Upgrade dello switch	"Aggiornamento a nuovi switch Brocade FC"	FC	Sostituzione dello switch
"Sostituzione di uno switch FC Brocade (MetroCluster)" "Sostituzione di uno switch FC Cisco"	FC	Aggiornamento del firmware	"Aggiornamento del firmware su uno switch FC Brocade" "Aggiornamento del firmware su uno switch FC Cisco"
Switch IP	IP	Sostituzione o sostituzione dell'interruttore	"Sostituire uno switch IP o modificare l'utilizzo degli switch IP MetroCluster esistenti"
IP	Aggiornamento del firmware	"Aggiornare il firmware sugli switch IP MetroCluster"	IP
Aggiornamento del file RCF	"Aggiornare i file RCF sugli switch IP MetroCluster" "Aggiornare i file RCF sugli switch IP Cisco utilizzando CleanUpFiles"	IP	Rinominare uno switch

Scenari di guasti e recovery di MetroCluster

È necessario conoscere il modo in cui la configurazione MetroCluster risponde a diversi eventi di errore.

> Per ulteriori informazioni sul ripristino da guasti dei nodi, vedere la sezione "scelta della procedura di ripristino corretta" in "Ripristino in caso di disastro".

Evento	Impatto	Recovery (recupero)

Guasto a nodo singolo	Viene attivato un failover.	La configurazione viene ripristinata attraverso un Takeover locale. Il RAID non viene influenzato. Rivedere i messaggi di sistema e sostituire le FRU guaste secondo necessità. "Documentazione dei sistemi hardware ONTAP"
Due nodi si guastano in un sito	Due nodi si guastano solo se è abilitato lo switchover automatico nel software MetroCluster Tiebreaker.	Unplanned switchover manuale (USO) se il switchover automatico nel software MetroCluster Tiebreaker non è abilitato. "Documentazione dei sistemi hardware ONTAP"
Interfaccia IP MetroCluster - errore di una porta	Il sistema è degradato. Un errore di porta aggiuntivo influisce sul mirroring ha.	Viene utilizzata la seconda porta. Health Monitor genera un avviso in caso di interruzione del collegamento fisico alla porta. Rivedere i messaggi di sistema e sostituire le FRU guaste secondo necessità. "Documentazione dei sistemi hardware ONTAP"
Interfaccia IP MetroCluster - errore di entrambe le porte	La funzionalità HA è interessata. RAID SyncMirror del nodo interrompe la sincronizzazione.	È necessario un recupero manuale immediato in quanto non è previsto un Takeover in ha. Rivedere i messaggi di sistema e sostituire le FRU guaste secondo necessità. "Documentazione dei sistemi hardware ONTAP"
Guasto di uno switch IP MetroCluster	Nessun impatto. La ridondanza viene fornita attraverso la seconda rete.	Sostituire lo switch guasto secondo necessità. "Sostituzione di uno switch IP"
Guasto di due switch IP MetroCluster che si trovano nella stessa rete	Nessun impatto. La ridondanza viene fornita attraverso la seconda rete.	Sostituire lo switch guasto secondo necessità. "Sostituzione di uno switch IP"

Guasto di due switch IP MetroCluster presenti in un sito	RAID SyncMirror del nodo interrompe la sincronizzazione. La funzionalità HA viene influenzata e il cluster esce dal quorum.	Sostituire lo switch guasto secondo necessità. "Sostituzione di uno switch IP"
Guasto di due switch IP MetroCluster che si trovano in siti diversi e non sulla stessa rete (errore diagonale)	RAID SyncMirror del nodo interrompe la sincronizzazione.	RAID SyncMirror del nodo interrompe la sincronizzazione. Le funzionalità cluster e ha non vengono influenzate. Sostituire lo switch guasto secondo necessità. "Sostituzione di uno switch IP"

Prima di eseguire le attività di manutenzione, rimuovere il mediatore ONTAP o il monitoraggio di spareggio

Prima di eseguire le attività di manutenzione, è necessario rimuovere il monitoraggio se la configurazione MetroCluster viene monitorata con l'utilità Tiebreaker o Mediator.

Le attività di manutenzione includono l'aggiornamento della piattaforma del controller, l'aggiornamento di ONTAP e l'esecuzione di uno switchover e uno switchback negoziati.

Fasi

1. Raccogliere l'output per il seguente comando:

   ```
   storage iscsi-initiator show
   ```

2. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza…	Utilizzare questa procedura…
Spareggio	"Rimozione delle configurazioni MetroCluster" Nel *contenuto di installazione e configurazione di MetroCluster Tiebreaker*
Mediatore	Immettere il seguente comando dal prompt di ONTAP: `metrocluster configuration-settings mediator remove`
Applicazioni di terze parti	Consultare la documentazione del prodotto.

3. Una volta completata la manutenzione della configurazione MetroCluster, è possibile riprendere il monitoraggio con l'utilità Tiebreaker o Mediator.

Se si utilizza…	Utilizzare questa procedura
Spareggio	"Aggiunta di configurazioni MetroCluster" Nella sezione *Installazione e configurazione di MetroCluster Tiebreaker*.
Mediatore	"Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster" Nella sezione *Installazione e configurazione IP MetroCluster*.
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Manutenzione del bridge FC-SAS

Supporto per bridge FibreBridge 7600N in configurazioni MetroCluster

Il bridge FibreBridge 7600N è supportato su ONTAP 9.5 e versioni successive in sostituzione del bridge FibreBridge 7500N o 6500N o quando si aggiunge nuovo storage alla configurazione MetroCluster. I requisiti di zoning e le restrizioni relative all'utilizzo delle porte FC del bridge sono gli stessi del bridge FibreBridge 7500N.

"Tool di matrice di interoperabilità NetApp"

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

Caso d'utilizzo	Sono necessarie modifiche allo zoning?	Restrizioni	Procedura
Sostituzione di un singolo bridge FibreBridge 7500N con un singolo bridge FibreBridge 7600N	No	Il bridge FibreBridge 7600N deve essere configurato esattamente come il bridge FibreBridge 7500N.	"Scambio a caldo di un FibreBridge 7500N con un bridge 7600N"
Sostituzione di un singolo bridge FibreBridge 6500N con un singolo bridge FibreBridge 7600N	No	Il bridge FibreBridge 7600N deve essere configurato esattamente come il bridge FibreBridge 6500N.	"Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N"

Aggiunta di nuovo storage mediante l'aggiunta di una nuova coppia di bridge FibreBridge 7600N	Sì È necessario aggiungere zone di storage per ciascuna porta FC dei nuovi bridge.	È necessario disporre di porte disponibili sul fabric dello switch FC (in una configurazione Fabric-Attached MetroCluster) o sui controller di storage (in una configurazione Stretch MetroCluster). Ogni coppia di bridge FibreBridge 7500N o 7600N può supportare fino a quattro stack.	"Aggiunta a caldo di uno stack di shelf di dischi SAS e bridge a un sistema MetroCluster"

Supporto per bridge FibreBridge 7500N in configurazioni MetroCluster

Il bridge FibreBridge 7500N è supportato in sostituzione del bridge FibreBridge 6500N o per l'aggiunta di nuovo storage alla configurazione MetroCluster. Le configurazioni supportate prevedono requisiti di zoning e limitazioni relative all'utilizzo delle porte FC del bridge e dei limiti di shelf di storage e stack.

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

Caso d'utilizzo	Sono necessarie modifiche allo zoning?	Restrizioni	Procedura
Sostituzione di un singolo bridge FibreBridge 6500N con un singolo bridge FibreBridge 7500N	No	Il bridge FibreBridge 7500N deve essere configurato esattamente come il bridge FibreBridge 6500N, utilizzando una singola porta FC e collegandolo a un singolo stack. Non utilizzare la seconda porta FC di FibreBridge 7500N.	"Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N"

Caso d'utilizzo	Sono necessarie modifiche allo zoning?	Restrizioni	Procedura
Consolidamento di più stack sostituendo più coppie di bridge FibreBridge 6500N con una singola coppia di bridge FibreBridge 7500N	Sì	In questo caso, i bridge FibreBridge 6500N vengono disutilizzati e sostituiti con una singola coppia di bridge FibreBridge 7500N. Ogni coppia di bridge FibreBridge 7500N o 7600N può supportare fino a quattro stack. Al termine della procedura, sia la parte superiore che la parte inferiore degli stack devono essere collegate alle porte corrispondenti sui bridge FibreBridge 7500N.	"Sostituzione di una coppia di bridge FibreBridge 6500N con bridge 7600N o 7500N"
Aggiunta di nuovo storage mediante l'aggiunta di una nuova coppia di bridge FibreBridge 7500N	Sì È necessario aggiungere zone di storage per ciascuna porta FC dei nuovi bridge.	È necessario disporre di porte disponibili sul fabric dello switch FC (in una configurazione Fabric-Attached MetroCluster) o sui controller di storage (in una configurazione Stretch MetroCluster). Ogni coppia di bridge FibreBridge 7500N o 7600N può supportare fino a quattro stack.	"Aggiunta a caldo di uno stack di shelf di dischi SAS e bridge a un sistema MetroCluster"

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 differenza del 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 ripetendo 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.

   `service` può 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 eseguire anche il comando Set SNMP Enabled (Imposta SNMP attivato):

   ```
   set SNMP enabled
   ```

   SNMP è l'unico protocollo che richiede un comando di abilitazione separato.

5. Salvare la configurazione:

   ```
   saveconfiguration
   ```

Aggiornamento del firmware su un bridge FibreBridge

La procedura di aggiornamento del firmware del bridge dipende dal modello del bridge e dalla versione del ONTAP.

Aggiornamento del firmware su bridge FibreBridge 7600N o 7500N su configurazioni con ONTAP 9.4 e versioni successive

Potrebbe essere necessario aggiornare il firmware sui bridge FibreBridge per assicurarsi di disporre delle funzionalità più recenti o per risolvere eventuali problemi. Questa procedura deve essere utilizzata per i bridge FibreBridge 7600N o 7500N su configurazioni con ONTAP 9.4 e versioni successive.

- La configurazione MetroCluster deve funzionare normalmente.
- Tutti i bridge FibreBridge nella configurazione MetroCluster devono essere operativi.
- Tutti i percorsi di storage devono essere disponibili.
- È necessaria la password di amministrazione e l'accesso a un server HTTP, FTP, SFTP o TFTP (Trivial file Transfer Protocol).
- È necessario utilizzare una versione del firmware supportata.

  "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.

- È possibile utilizzare questa attività solo sui bridge FibreBridge 7600N o 7500N in configurazioni con ONTAP 9.4 o versioni successive.
- Questa attività deve essere eseguita su ciascun bridge FibreBridge nella configurazione MetroCluster, in modo che tutti i bridge eseguano la stessa versione del firmware.

Questa procedura è senza interruzioni e richiede circa 30 minuti.

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. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   "maintenance-window-in-hours" specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

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

2. Accedere alla pagina ATTO FibreBridge e selezionare il firmware appropriato per il bridge.

   "PAGINA DI download DEL firmware DI ATTO FibreBridge"

3. Leggere attentamente il documento attenzione/MustRead e il Contratto per l'utente finale, quindi fare clic sulla casella di controllo per indicare l'accettazione e procedere.
4. Posizionare il file del firmware in un percorso di rete accessibile ai moduli controller.

È possibile immettere i comandi nelle fasi rimanenti dalla console di uno dei moduli controller.

5. Passare al livello di privilegio avanzato:

   `set -privilege advanced`

   Quando richiesto, rispondere con “y” per passare alla modalità avanzata e visualizzare il prompt della modalità avanzata (*).

6. Aggiornare il firmware del bridge:

   `storage bridge firmware update -bridge name -uri URL-of-firmware-package`

   ```
   cluster_A> storage bridge firmware update -bridge bridge_A_1a -uri
   http://192.168.132.97/firmware.ZBD
   ```

7. Tornare al livello di privilegio admin:

   `set -privilege admin`

8. Verificare che l’aggiornamento del firmware sia completo:

   `job show -name "job-name"`

   Il seguente esempio mostra che il processo “saggiornamento firmware del bridge di torage” è ancora in esecuzione:

   ```
   cluster_A> job show -name "storage bridge firmware update"
   Owning

   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   2246   job-name
                               cluster_A
                                          node_A_1
                                                         Running
   Description: Storage bridge firmware update job
   ```

   Dopo circa 10 minuti, il nuovo firmware è completamente installato e lo stato del processo sarà Success (riuscito):

```
cluster_A> job show -name "storage bridge firmware update"

                             Owning
Job ID Name                  Vserver    Node           State
------ -------------------- ---------- -------------- ----------
2246   Storage bridge firmware update
                             cluster_A
                                        node_A_1
                                                       Success
Description: Storage bridge firmware update job
```

9. Completare la procedura in base all'attivazione della gestione in-band e alla versione di ONTAP in esecuzione nel sistema:

   - Se si utilizza ONTAP 9.4, la gestione in-band non è supportata e il comando deve essere emesso dalla console bridge:

     i. Eseguire `flashimages` sulla console del bridge e verificare che siano visualizzate le versioni firmware corrette.

     > L'esempio mostra che l'immagine flash principale mostra l'immagine del nuovo firmware, mentre l'immagine flash secondaria mostra l'immagine precedente.

     ```
     flashimages

      ;Type Version
     ;=====================================================
     Primary 3.16 001H
     Secondary 3.15 002S
     Ready.
     ```

     a. Riavviare il bridge eseguendo `firmwarerestart` dal bridge.

        - Se si utilizza ONTAP 9.5 o versione successiva, la gestione in-band è supportata e il comando può essere inviato dal prompt del cluster:

     b. Eseguire `storage bridge run-cli -name` *`bridge-name`* `-command FlashImages` comando.

     > L'esempio mostra che l'immagine flash principale mostra l'immagine del nuovo firmware, mentre l'immagine flash secondaria mostra l'immagine precedente.

```
cluster_A> storage bridge run-cli -name ATTO_7500N_IB_1 -command
FlashImages

[Job 2257]

;Type         Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.


[Job 2257] Job succeeded.
```

a. Se necessario, riavviare il bridge:

```
storage bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart
```

> A partire dalla versione del firmware ATTO 2.95, il bridge si riavvia automaticamente e questo passaggio non è necessario.

10. Verificare che il bridge sia stato riavviato correttamente:

```
sysconfig
```

Il sistema deve essere cablato per l'alta disponibilità multipath (entrambi i controller hanno accesso attraverso i bridge agli shelf di dischi in ogni stack).

```
cluster_A> node run -node cluster_A-01 -command sysconfig
NetApp Release 9.6P8: Sat May 23 16:20:55 EDT 2020
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-
02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

11. Verificare che il firmware di FibreBridge sia stato aggiornato:

```
storage bridge show -fields fw-version,symbolic-name
```

```
cluster_A> storage bridge show -fields fw-version,symbolic-name
name fw-version symbolic-name
----------------- ----------------- -------------
ATTO_20000010affeaffe 3.10 A06X bridge_A_1a
ATTO_20000010affeffae 3.10 A06X bridge_A_1b
ATTO_20000010affeafff 3.10 A06X bridge_A_2a
ATTO_20000010affeaffa 3.10 A06X bridge_A_2b
4 entries were displayed.
```

12. Verificare che le partizioni siano aggiornate dal prompt del bridge:

    ```
    flashimages
    ```

    L'immagine flash principale visualizza l'immagine del nuovo firmware, mentre l'immagine flash secondaria visualizza l'immagine precedente.

    ```
    Ready.
    flashimages

    ;Type         Version
    ;=====================================================
       Primary    3.16 001H
     Secondary    3.15 002S

     Ready.
    ```

13. Ripetere i passaggi da 5 a 10 per assicurarsi che entrambe le immagini flash siano aggiornate alla stessa versione.
14. Verificare che entrambe le immagini flash siano aggiornate alla stessa versione.

    ```
    flashimages
    ```

    L'output dovrebbe mostrare la stessa versione per entrambe le partizioni.

    ```
    Ready.
    flashimages

    ;Type         Version
    ;=====================================================
       Primary    3.16 001H
     Secondary    3.16 001H

     Ready.
    ```

15. Ripetere i passaggi da 5 a 13 sul bridge successivo fino a quando tutti i bridge nella configurazione MetroCluster non sono stati aggiornati.

Aggiornamento del firmware su FibreBridge 7500N nelle configurazioni che eseguono ONTAP 9,3.x e versioni precedenti

Potrebbe essere necessario aggiornare il firmware sui bridge FibreBridge per verificare di disporre delle funzioni più recenti o per risolvere eventuali problemi. Questa procedura deve essere utilizzata per FibreBridge 7500N nelle configurazioni che eseguono ONTAP 9,3.x

Prima di iniziare

- La configurazione MetroCluster deve funzionare normalmente.
- Tutti i bridge FibreBridge nella configurazione MetroCluster devono essere operativi.
- Tutti i percorsi di storage devono essere disponibili.
- È necessaria la password admin e l'accesso a un server FTP o SCP.
- È necessario utilizzare una versione del firmware supportata.

  "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.

A partire da ONTAP 9.3, è possibile utilizzare il comando di aggiornamento del firmware del bridge di storage ONTAP per aggiornare il firmware del bridge sui bridge FibreBridge 7500N.

"Aggiornamento del firmware su bridge FibreBridge 7600N o 7500N su configurazioni con ONTAP 9.4 e versioni successive"

Questa attività deve essere eseguita su ciascun bridge FibreBridge nella configurazione MetroCluster, in modo che tutti i bridge eseguano la stessa versione del firmware.

> Questa procedura è senza interruzioni e richiede circa 30 minuti.

Fasi

1. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   "_maintenance-window-in-hours_" specifica la durata della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

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

2. Accedere alla pagina ATTO FibreBridge e selezionare il firmware appropriato per il bridge.

   "PAGINA DI download DEL firmware DI ATTO FibreBridge"

3. Leggere attentamente il documento attenzione/MustRead e il Contratto per l'utente finale, quindi fare clic sulla casella di controllo per indicare l'accettazione e procedere.
4. Scaricare il file del firmware del bridge seguendo i passaggi da 1 a 3 della procedura nella pagina di download del firmware ATTO FibreBridge.
5. Fare una copia della pagina di download del firmware ATTO FibreBridge e delle note di rilascio come riferimento quando viene richiesto di aggiornare il firmware su ciascun bridge.
6. Aggiornare il bridge:

   a. Installare il firmware sul ponte FibreBridge 7500N.

      Fare riferimento alle istruzioni fornite nella sezione "`Aggiorna firmware" del *Manuale d'installazione e funzionamento atto FibreBridge 7500N*.

      ATTENZIONE: assicurarsi di spegnere e riaccendere il singolo bridge. Se si attendono e si riattiva contemporaneamente entrambi i bridge in uno stack, il controller potrebbe perdere l'accesso ai dischi, causando un guasto al plex o un panico per più dischi.

      Il bridge dovrebbe riavviarsi.

   b. Dalla console di uno dei controller, verificare che il bridge sia stato riavviato correttamente:

      ```
      sysconfig
      ```

      Il sistema deve essere cablato per l'alta disponibilità multipath (entrambi i controller hanno accesso attraverso i bridge agli shelf di dischi in ogni stack).

      ```
      cluster_A::> node run -node cluster_A-01 -command sysconfig
      NetApp Release 9.1P7: Sun Aug 13 22:33:49 PDT 2017
      System ID: 1234567890 (cluster_A-01); partner ID: 0123456789
      (cluster_A-02)
      System Serial Number: 200012345678 (cluster_A-01)
      System Rev: A4
      System Storage Configuration: Quad-Path HA
      ```

   c. Dalla console di uno dei controller, verificare che il firmware FibreBridge sia stato aggiornato:

      ```
      storage bridge show -fields fw-version,symbolic-name
      ```

      ```
      cluster_A::> storage bridge show -fields fw-version,symbolic-name
       name              fw-version        symbolic-name
       ----------------- ----------------- -------------
       ATTO_10.0.0.1     1.63 071C 51.01   bridge_A_1a
       ATTO_10.0.0.2     1.63 071C 51.01   bridge_A_1b
       ATTO_10.0.1.1     1.63 071C 51.01   bridge_B_1a
       ATTO_10.0.1.2     1.63 071C 51.01   bridge_B_1b
       4 entries were displayed.
      ```

d. Ripetere i passaggi precedenti sullo stesso bridge per aggiornare la seconda partizione.
e. Verificare che entrambe le partizioni siano aggiornate:

```
flashimages
```

L'output dovrebbe mostrare la stessa versione per entrambe le partizioni.

```
Ready.
flashimages
4
;Type         Version
;=====================================================
Primary    2.80 003T
Secondary    2.80 003T
Ready.
```

7. Ripetere il passaggio precedente sul bridge successivo, fino a quando tutti i bridge nella configurazione MetroCluster non sono stati aggiornati.

Sostituzione di un singolo bridge FC-SAS

È possibile sostituire senza interruzioni un bridge con uno stesso modello bridge o con un nuovo modello bridge.

Prima di iniziare

È necessaria la password admin e l'accesso a un server FTP o SCP.

A proposito di questa attività

Questa procedura è senza interruzioni e richiede circa 60 minuti.

Questa procedura utilizza la CLI del bridge per configurare e gestire un bridge e per aggiornare il firmware del bridge e l'utility barra di navigazione atto per configurare la porta di gestione Ethernet del bridge 1. È possibile utilizzare altre interfacce se soddisfano i requisiti.

"Requisiti per l'utilizzo di altre interfacce per configurare e gestire i bridge FibreBridge"

Informazioni correlate

"Sostituzione di una coppia di bridge FibreBridge 6500N con bridge 7600N o 7500N"

Verifica della connettività dello storage

Prima di sostituire i bridge, verificare la connettività del bridge e dello storage. Familiarizzare con l'output dei comandi consente di confermare successivamente la connettività dopo aver apportato modifiche alla configurazione.

A proposito di questa attività

È possibile eseguire questi comandi dal prompt admin di uno qualsiasi dei moduli controller nella configurazione MetroCluster del sito sottoposto a manutenzione.

Fasi

1. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:

   ```
   run local sysconfig -v
   ```

   L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
   System Serial Number: 940001025471 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   be multi-path HA**
   .
   .
   .
   slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
   Initiator port**
           Firmware rev:      7.5.0
           Flash rev:         0.0.0
           Host Port Id:      0x60130
           FC Node Name:      5:00a:098201:bae312
           FC Port Name:      5:00a:098201:bae312
           SFP Vendor:        UTILITIES CORP.
           SFP Part Number:   FTLF8529P3BCVAN1
           SFP Serial Number: URQ0Q9R
           SFP Capabilities:  4, 8 or 16 Gbit
           Link Data Rate:    16 Gbit
           Switch Port:       brcd6505-fcs40:1
     **<List of disks visible to port\>**
            ID     Vendor   Model            FW    Size
           brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
   847.5GB (1953525168 512B/sect)
           brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
   847.5GB (1953525168 512B/sect)
           .
           .
           .
           **<List of FC-to-SAS bridges visible to port\>**
           FC-to-SAS Bridge:
           brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
   FB6500N102980
           brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
   FB6500N102980
           brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
   ```

```
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Sostituzione a caldo di un bridge con un bridge sostitutivo dello stesso modello

È possibile sostituire a caldo un bridge guasto con un altro bridge dello stesso modello.

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.

> 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. Se il vecchio bridge è accessibile, è possibile recuperare le informazioni di configurazione.

Se…	Quindi…
Si utilizza la gestione IP	Connettersi al vecchio bridge con una connessione Telnet e copiare l'output della configurazione del bridge.

Si utilizza la gestione in-band	Utilizzare l'interfaccia utente di ONTAP per recuperare le informazioni di configurazione con i seguenti comandi:
	
	`storage bridge run-cli -name` *`bridge-name`* `-command "info"`
	
	`storage bridge run-cli -name` *`bridge-name`* `-command "sasportlist"`

   a. Immettere il comando:

   ```
   storage bridge run-cli -name bridge_A1 -command "info"
   ```

```
info

Device Status         = Good
Unsaved Changes       = None
Device                = "FibreBridge 7500N"
Serial Number         = FB7500N100000
Device Version        = 3.10
Board Revision        = 7
Build Number          = 007A
Build Type            = Release
Build Date            = "Aug 20 2019" 11:01:24
Flash Revision        = 0.02
Firmware Version      = 3.10
BCE Version (FPGA 1)  = 15
BAU Version (FPGA 2)  = 33
User-defined name     = "bridgeA1"
World Wide Name       = 20 00 00 10 86 A1 C7 00
MB of RAM Installed   = 512
FC1 Node Name         = 20 00 00 10 86 A1 C7 00
FC1 Port Name         = 21 00 00 10 86 A1 C7 00
FC1 Data Rate         = 16Gb
FC1 Connection Mode   = ptp
FC1 FW Revision       = 11.4.337.0
FC2 Node Name         = 20 00 00 10 86 A1 C7 00
FC2 Port Name         = 22 00 00 10 86 A1 C7 00
FC2 Data Rate         = 16Gb
FC2 Connection Mode   = ptp
FC2 FW Revision       = 11.4.337.0
SAS FW Revision       = 3.09.52
MP1 IP Address        = 10.10.10.10
MP1 IP Subnet Mask    = 255.255.255.0
MP1 IP Gateway        = 10.10.10.1
MP1 IP DHCP           = disabled
MP1 MAC Address       = 00-10-86-A1-C7-00
MP2 IP Address        = 0.0.0.0 (disabled)
MP2 IP Subnet Mask    = 0.0.0.0
MP2 IP Gateway        = 0.0.0.0
MP2 IP DHCP           = enabled
MP2 MAC Address       = 00-10-86-A1-C7-01
SNMP                  = enabled
SNMP Community String = public
PS A Status           = Up
PS B Status           = Up
Active Configuration  = NetApp

Ready.
```

b. Immettere il comando:

```
storage bridge run-cli -name bridge_A1 -command "sasportlist"
```

```
SASPortList

;Connector      PHY     Link            Speed   SAS Address
;==============================================================
Device  A       1       Up              6Gb     5001086000a1c700
Device  A       2       Up              6Gb     5001086000a1c700
Device  A       3       Up              6Gb     5001086000a1c700
Device  A       4       Up              6Gb     5001086000a1c700
Device  B       1       Disabled        12Gb    5001086000a1c704
Device  B       2       Disabled        12Gb    5001086000a1c704
Device  B       3       Disabled        12Gb    5001086000a1c704
Device  B       4       Disabled        12Gb    5001086000a1c704
Device  C       1       Disabled        12Gb    5001086000a1c708
Device  C       2       Disabled        12Gb    5001086000a1c708
Device  C       3       Disabled        12Gb    5001086000a1c708
Device  C       4       Disabled        12Gb    5001086000a1c708
Device  D       1       Disabled        12Gb    5001086000a1c70c
Device  D       2       Disabled        12Gb    5001086000a1c70c
Device  D       3       Disabled        12Gb    5001086000a1c70c
Device  D       4       Disabled        12Gb    5001086000a1c70c
```

2. Se il bridge si trova in una configurazione Fabric-Attached MetroCluster, disattivare tutte le porte dello switch che si collegano alla porta FC del bridge.
3. Dal prompt del cluster ONTAP, rimuovere il bridge sottoposto a manutenzione dal monitoraggio dello stato di salute:
   a. Rimuovere il bridge:
      `storage bridge remove -name bridge-name`
   b. Visualizzare l'elenco dei bridge monitorati e verificare che il bridge rimosso non sia presente:
      `storage bridge show`
4. Mettere a terra l'utente.
5. Spegnere il bridge atto e rimuovere i cavi di alimentazione collegati al bridge.
6. Scollegare i cavi collegati al vecchio bridge.

   Prendere nota della porta a cui ciascun cavo è stato collegato.

7. Rimuovere il vecchio bridge dal rack.
8. Installare il nuovo bridge nel rack.
9. Ricollegare il cavo di alimentazione e, se si configura l'accesso IP al bridge, un cavo Ethernet schermato.

   Non ricollegare i cavi SAS o FC in questo momento.

10. Collegare il bridge a una fonte di alimentazione, quindi accenderlo.

    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.

11. 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.

12. 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.

13. Configurare il bridge.

    Se le informazioni di configurazione sono state recuperate dal vecchio bridge, utilizzare le informazioni per configurare il nuovo bridge.

    Annotare il nome utente e la password designati.

    Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il tuo modello di bridge contiene le informazioni più aggiornate sui comandi disponibili e su come utilizzarli.

    > 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.

       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 bridgename
```

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.

14. 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 dallo switch 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 FibreBridge 7500N, configurare la modalità di connessione che la porta utilizza 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
     ```

d. 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.

15. Accesso sicuro al bridge e salvataggio della configurazione del bridge.

    a. Dal prompt del controller, controllare 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 il seguente comando:

       ```
       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.

16. Aggiornare il firmware FibreBridge su ciascun bridge.

    Se il nuovo bridge è dello stesso tipo del bridge partner, eseguire l'aggiornamento allo stesso firmware del bridge partner. Se il nuovo bridge è di tipo diverso da quello del bridge partner, eseguire l'aggiornamento al firmware più recente supportato dal bridge e dalla versione di ONTAP. Consultare la sezione "aggiornamento del firmware su un bridge FibreBridge" in *manutenzione MetroCluster*.

17. ricollegare i cavi SAS e FC alle stesse porte del nuovo bridge.

È necessario sostituire i cavi che collegano il ponte alla parte superiore o inferiore della scaffalatura. I bridge FibreBridge 7600N e 7500N richiedono cavi mini-SAS per questi collegamenti.

> Attendere almeno 10 secondi prima di collegare la porta. I connettori dei cavi SAS sono dotati di chiave; se orientati correttamente in una porta SAS, il connettore scatta in posizione e il LED LNK della porta SAS dello shelf di dischi si illumina di verde. Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore). Per i controller, l'orientamento delle porte SAS può variare a seconda del modello di piattaforma; pertanto, l'orientamento corretto del connettore del cavo SAS varia.

18. verificare che ciascun bridge sia in grado di visualizzare tutti i dischi e gli shelf di dischi a cui è collegato il bridge.

Se si utilizza…	Quindi…
GUI ExpressNAV	a. In un browser Web supportato, inserire l'indirizzo IP del bridge nella casella del browser. Viene visualizzato il link alla homepage di ATTO FibreBridge. b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge. Viene visualizzata la pagina di stato di atto FibreBridge con un menu a sinistra. c. Fare clic su **Avanzate** nel menu. d. Visualizzare i dispositivi connessi: `sastargets` e. Fare clic su **Invia**.
Connessione alla porta seriale	Visualizzare i dispositivi connessi: `sastargets`

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.

> Se la risposta di testo troncata viene visualizzata all'inizio dell'output, è possibile utilizzare Telnet per connettersi al bridge e visualizzare l'output utilizzando `sastargets` comando.

Il seguente output indica 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 3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK 3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK 3QP1FXW600009940VERQ
```

19. Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi appropriati nello stack.

Se l'output è…	Quindi…
Esatto	Ripetere Fase 18 per ogni bridge rimanente.
Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo le operazioni Fase 17. b. Ripetere Fase 18.

20. Se il bridge si trova in una configurazione Fabric-Attached MetroCluster, riattivare la porta dello switch FC disattivata all'inizio di questa procedura.

    Deve essere la porta che si connette al bridge.

21. Dalla console di sistema di entrambi i moduli controller, verificare che tutti i moduli controller abbiano accesso attraverso il nuovo bridge agli shelf di dischi (ovvero che il sistema sia cablato per ha multipath):

    ```
    run local sysconfig
    ```

    Il completamento del rilevamento potrebbe richiedere fino a un minuto.

    Se l'output non indica ha multipath, è necessario correggere il cablaggio SAS e FC poiché non tutte le unità disco sono accessibili attraverso il nuovo bridge.

    Il seguente output indica che il sistema è cablato per ha multipath:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

Quando il sistema non è cablato come ha multipath, il riavvio di un bridge potrebbe causare la perdita di accesso ai dischi e causare un panico per più dischi.

22. Se si esegue ONTAP 9.4 o versioni precedenti, verificare che il bridge sia configurato per SNMP.

    Se si utilizza la CLI bridge, eseguire il seguente comando:

    ```
    get snmp
    ```

23. 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	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    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 "Satus" è "ok" e se vengono visualizzate altre informazioni, come il nome globale (WWN).

    L'esempio seguente mostra che i bridge FC-SAS sono configurati:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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::>
```

24. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
    a. Verificare che il sistema sia multipercorso:
       `node run -node node-name sysconfig -a`
    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
       `system health alert show`
    c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
       `metrocluster show`
    d. Eseguire un controllo MetroCluster:
       `metrocluster check run`
    e. Visualizzare i risultati del controllo MetroCluster:
       `metrocluster check show`
    f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli interruttori (se presenti):
       `storage switch show`
    g. Eseguire Config Advisor.

       "Download NetApp: Config Advisor"

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

Informazioni correlate

"Gestione in-band dei bridge FC-SAS"

Scambio a caldo di un FibreBridge 7500N con un bridge 7600N

È possibile sostituire a caldo un bridge FibreBridge 7500N con un bridge 7600N.

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.

> 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. Se il bridge si trova in una configurazione Fabric-Attached MetroCluster, disattivare tutte le porte dello switch che si collegano alla porta FC del bridge.
2. Dal prompt del cluster ONTAP, rimuovere il bridge sottoposto a manutenzione dal monitoraggio dello stato di salute:
   a. Rimuovere il bridge:
      `storage bridge remove -name` *`bridge-name`*
   b. Visualizzare l'elenco dei bridge monitorati e verificare che il bridge rimosso non sia presente:
      `storage bridge show`
3. Mettere a terra l'utente.
4. Rimuovere i cavi di alimentazione collegati al bridge per spegnere il bridge.
5. Scollegare i cavi collegati al vecchio bridge.

   Prendere nota della porta a cui ciascun cavo è stato collegato.
6. Rimuovere il vecchio bridge dal rack.
7. Installare il nuovo bridge nel rack.
8. Ricollegare il cavo di alimentazione e il cavo Ethernet schermato.

   > Non ricollegare i cavi SAS o FC in questo momento.
9. Collegare il bridge a una fonte di alimentazione, quindi accenderlo.

   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.
10. 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.
11. 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.
12. 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.

13. Configurare i bridge.

    Annotare il nome utente e la password designati.

    Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il tuo modello di bridge contiene le informazioni più aggiornate sui comandi disponibili e su come utilizzarli.

    > Non configurare la sincronizzazione dell'ora su FibreBridge 7600N. La sincronizzazione dell'ora per FibreBridge 7600N 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.

       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 bridgename
```

a. 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.

14. 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 dal bridge e dalla porta FC del modulo controller o dello switch 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. 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 disattivare la porta inutilizzata:

  `FCPortDisable port-number`

  L'esempio seguente mostra la disattivazione della porta FC 2:

```
FCPortDisable 2

Fibre Channel Port 2 has been disabled.
```

c. 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.
```

15. Accesso sicuro al bridge e salvataggio della configurazione del bridge.

    a. Dal prompt del controller, controllare 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 il seguente comando:

    ```
    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.

    Eseguire i seguenti comandi:

    ```
    SaveConfiguration

    FirmwareRestart
    ```

    Viene richiesto di riavviare il bridge.

16. Aggiornare il firmware FibreBridge su ciascun bridge.

    "Aggiornamento del firmware su bridge FibreBridge 7600N o 7500N su configurazioni con ONTAP 9.4 e versioni successive"

17. ricollegare i cavi SAS e FC alle stesse porte del nuovo bridge.

    > Attendere almeno 10 secondi prima di collegare la porta. I connettori dei cavi SAS sono dotati di chiave; se orientati correttamente in una porta SAS, il connettore scatta in posizione e il LED LNK della porta SAS dello shelf di dischi si illumina di verde. Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore). Per i controller, l'orientamento delle porte SAS può variare a seconda del modello di piattaforma; pertanto, l'orientamento corretto del connettore del cavo SAS varia.

18. Verificare che ciascun bridge sia in grado di visualizzare tutti i dischi e gli shelf di dischi a cui è collegato il

bridge:

```
sastargets
```

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.

Il seguente output indica 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        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

19. Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi appropriati nello stack.

Se l'output è…	Quindi…
Esatto	Ripetere il passaggio precedente per ogni bridge rimanente.
Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo le operazioni Fase 17. b. Ripetere la fase precedente.

20. Se il bridge si trova in una configurazione Fabric-Attached MetroCluster, riabilitare la porta dello switch FC disattivata all'inizio di questa procedura.

    Deve essere la porta che si connette al bridge.

21. Dalla console di sistema di entrambi i moduli controller, verificare che tutti i moduli controller abbiano accesso attraverso il nuovo bridge agli shelf di dischi (ovvero che il sistema sia cablato per ha multipath):

    ```
    run local sysconfig
    ```

    > Il completamento del rilevamento potrebbe richiedere fino a un minuto.

    Se l'output non indica ha multipath, è necessario correggere il cablaggio SAS e FC poiché non tutte le unità disco sono accessibili attraverso il nuovo bridge.

    Il seguente output indica che il sistema è cablato per ha multipath:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

> Quando il sistema non è cablato come ha multipath, il riavvio di un bridge potrebbe causare la perdita di accesso ai dischi e causare un panico per più dischi.

22. Se si esegue ONTAP 9.4 o versioni precedenti, verificare che il bridge sia configurato per SNMP.

    Se si utilizza la CLI bridge, eseguire il seguente comando:

    ```
    get snmp
    ```

23. 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	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    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 "Satus" è "ok" e se vengono visualizzate altre informazioni, come il nome globale (WWN).

    L'esempio seguente mostra che i bridge FC-SAS sono configurati:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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::>
```

24. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
    a. Verificare che il sistema sia multipercorso:
       `node run -node node-name sysconfig -a`
    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
       `system health alert show`
    c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
       `metrocluster show`
    d. Eseguire un controllo MetroCluster:
       `metrocluster check run`
    e. Visualizzare i risultati del controllo MetroCluster:

       ```
       metrocluster check show
       ```

    f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli interruttori (se presenti):
       `storage switch show`
    g. Eseguire Config Advisor.

       "Download NetApp: Config Advisor"

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

Informazioni correlate

"Gestione in-band dei bridge FC-SAS"

Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N

È possibile sostituire a caldo un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N per sostituire un bridge guasto o aggiornare il bridge in una configurazione MetroCluster collegata a fabric o a bridge.

A proposito di questa attività

- Questa procedura consente di sostituire a caldo un singolo bridge FibreBridge 6500N con un singolo bridge FibreBridge 7600N o 7500N.
- Quando si esegue la sostituzione a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N, è necessario utilizzare solo una porta FC e una porta SAS sul bridge FibreBridge 7600N o 7500N.
- 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.

> Se si scambiano a caldo entrambi i bridge FibreBridge 6500N in coppia, è necessario utilizzare "Consolidare più stack di storage" procedura per le istruzioni di zoning. Sostituendo entrambi i bridge FibreBridge 6500N sul bridge, è possibile sfruttare le porte aggiuntive del bridge FibreBridge 7600N o 7500N.

> 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. Effettuare una delle seguenti operazioni:
   - Se il bridge guasto si trova in una configurazione Fabric-Attached MetroCluster, disattivare la porta dello switch che si connette alla porta FC del bridge.
   - Se il bridge guasto si trova in una configurazione stretch MetroCluster, utilizzare una delle porte FC disponibili.
2. Dal prompt del cluster ONTAP, rimuovere il bridge sottoposto a manutenzione dal monitoraggio dello stato di salute:
   a. Rimuovere il bridge:

      ```
      storage bridge remove -name bridge-name
      ```

   b. Visualizzare l'elenco dei bridge monitorati e verificare che il bridge rimosso non sia presente:

      ```
      storage bridge show
      ```

3. Mettere a terra l'utente.
4. Spegnere l'interruttore di alimentazione del bridge.
5. Scollegare i cavi collegati dallo shelf alle porte e ai cavi di alimentazione del bridge FibreBridge 6500N.

   Prendere nota delle porte a cui ciascun cavo è stato collegato.

6. Rimuovere dal rack il bridge FibreBridge 6500N da sostituire.
7. Installare il nuovo bridge FibreBridge 7600N o 7500N nel rack.

8. Ricollegare il cavo di alimentazione e, se necessario, il cavo Ethernet schermato.

> Non ricollegare i cavi SAS o FC in questo momento.

9. 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.

10. 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.

11. 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.

12. Configurare il bridge.

    Se le informazioni di configurazione sono state recuperate dal vecchio bridge, utilizzare le informazioni per configurare il nuovo bridge.

    Annotare il nome utente e la password designati.

    Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il tuo modello di bridge contiene le informazioni più aggiornate sui comandi disponibili e su come utilizzarli.

    > 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.

       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 bridgename
```

a. 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.

13. 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.
- Il bridge FibreBridge 6500N supporta fino a 8, 4 o 2 Gbps.

> La velocità FCDataRate selezionata è limitata alla velocità massima supportata sia dal bridge che dallo switch 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 o 6500N, configurare la modalità di connessione utilizzata dalla porta per 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
     ```

d. 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.

14. Accesso sicuro al bridge e salvataggio della configurazione del bridge.

a. Dal prompt del controller, controllare 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 il seguente comando:

```
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.

15. Attivare il monitoraggio dello stato di salute per il bridge FibreBridge 7600N o 7500N.
16. Aggiornare il firmware FibreBridge su ciascun bridge.

    Se il nuovo bridge è dello stesso tipo del bridge partner, eseguire l'aggiornamento allo stesso firmware del bridge partner. Se il nuovo bridge è di tipo diverso da quello del bridge partner, eseguire l'aggiornamento al firmware più recente supportato dal bridge e dalla versione di ONTAP. Consultare la sezione "aggiornamento del firmware su un bridge FibreBridge" nella *Guida alla manutenzione di MetroCluster*.

17. ricollegare i cavi SAS e FC alle porte SAS A e Fibre Channel 1 del nuovo bridge.

    La porta SAS deve essere collegata alla stessa porta shelf a cui era collegato il bridge FibreBridge 6500N.

    La porta FC deve essere collegata alla stessa porta dello switch o del controller a cui era collegato il bridge FibreBridge 6500N.

    > Non forzare un connettore in una porta. I cavi mini-SAS sono dotati di chiavi; se orientati correttamente in una porta SAS, il cavo SAS scatta in posizione e il LED LNK della porta SAS dello shelf di dischi si illumina di verde. Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore). Per i controller, l'orientamento delle porte SAS può variare a seconda del modello di piattaforma; pertanto, l'orientamento corretto del connettore per cavo SAS varia.

18. Verificare che il bridge sia in grado di rilevare tutte le unità disco e gli shelf di dischi a cui è collegato.

Se si utilizza…	Quindi…
GUI ExpressNAV	a. In un browser Web supportato, inserire l'indirizzo IP del bridge nella casella del browser. Viene visualizzato il link alla homepage di ATTO FibreBridge. b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge. Viene visualizzata la pagina di stato di atto FibreBridge con un menu a sinistra. c. Fare clic su **Avanzate** nel menu. d. Immettere il seguente comando, quindi fare clic su **Submit** (Invia) per visualizzare l'elenco dei dischi visibili al bridge: `sastargets`
Connessione alla porta seriale	Visualizzare l'elenco dei dischi visibili al bridge: `sastargets`

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        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

Se all'inizio dell'output viene visualizzato il testo "respesse tronced", è possibile utilizzare Telnet per accedere al bridge e immettere lo stesso comando per visualizzare tutti gli output.

19. Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi necessari nello stack.

Se l'output è…	Quindi…
Esatto	Ripetere il passaggio precedente per ogni bridge rimanente.
Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo le operazioni Fase 17. b. Ripetere il passaggio precedente per ogni bridge rimanente.

20. Riabilitare la porta dello switch FC che si collega al bridge.
21. Verificare che tutti i controller abbiano accesso attraverso il nuovo bridge agli shelf di dischi (che il sistema sia cablato per ha multipath), sulla console di sistema di entrambi i controller:

```
run local sysconfig
```

Il completamento del rilevamento potrebbe richiedere fino a un minuto.

Ad esempio, il seguente output mostra che il sistema è cablato per ha multipath:

```
NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

Se l'output del comando indica che la configurazione è ha a percorso misto o a percorso singolo, è necessario correggere il cablaggio SAS e FC poiché non tutti i dischi sono accessibili attraverso il nuovo bridge.

> Quando il sistema non è cablato come ha multipath, il riavvio di un bridge potrebbe causare la perdita di accesso ai dischi e causare un panico per più dischi.

22. 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	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

    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 "Satus" è "ok" e se vengono visualizzate altre informazioni, come il nome globale (WWN).

    L'esempio seguente mostra che i bridge FC-SAS sono configurati:

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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::>
```

23. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
    a. Verificare che il sistema sia multipercorso:

       `node run -node node-name sysconfig -a`

    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
       `system health alert show`
    c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

       `metrocluster show`

    d. Eseguire un controllo MetroCluster:

       `metrocluster check run`

    e. Visualizzare i risultati del controllo MetroCluster:

       `metrocluster check show`

    f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

       `storage switch show`

    g. Eseguire Config Advisor.

       "Download NetApp: Config Advisor"

    h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

24. Dopo aver sostituito il componente, restituire il componente guasto a NetApp, come descritto nelle istruzioni RMA fornite con il kit. Vedere "Amp per restituzione parti; sostituzioni" per ulteriori informazioni.

Informazioni correlate

"Gestione in-band dei bridge FC-SAS"

Sostituzione di una coppia di bridge FibreBridge 6500N con bridge 7600N o 7500N

Per sfruttare la porta FC2 aggiuntiva sui bridge FibreBridge 7600N o 7500N e ridurre l'utilizzo dei rack, è possibile sostituire senza interruzioni i bridge 6500N e consolidare fino a quattro stack di storage dietro una singola coppia di bridge FibreBridge 7600N o 7500N.

Prima di iniziare

È necessaria la password admin e l'accesso a un server FTP o SCP.

A proposito di questa attività

Utilizzare questa procedura se:

- Si sta sostituendo una coppia di bridge FibreBridge 6500N con bridge FibreBridge 7600N o 7500N.

  Dopo la sostituzione, entrambi i ponti della coppia devono essere dello stesso modello.

- In precedenza, è stato sostituito un singolo bridge FibreBridge 6500N con un bridge 7600N o 7500N e ora si sta sostituendo il secondo bridge della coppia.
- Si dispone di una coppia di bridge FibreBridge 7600N o 7500N con porte SAS disponibili e si stanno consolidando gli stack di storage SAS attualmente connessi tramite bridge FibreBridge 6500N.

Questa procedura è senza interruzioni e richiede circa due ore per essere completata.

Informazioni correlate

"Sostituzione di un singolo bridge FC-SAS"

Verifica della connettività dello storage

Prima di sostituire i bridge, verificare la connettività del bridge e dello storage. Familiarizzare con l'output dei comandi consente di confermare successivamente la connettività dopo aver apportato modifiche alla configurazione.

È possibile eseguire questi comandi dal prompt admin di uno qualsiasi dei moduli controller nella configurazione MetroCluster del sito sottoposto a manutenzione.

1. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:

   ```
   run local sysconfig -v
   ```

   L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

   ```
   node_A_1> run local sysconfig -v
   ```

```
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
```

```
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Sostituzione a caldo dei bridge FibreBridge 6500N per creare una coppia di bridge FibreBridge 7600N o 7500N

Per sostituire a caldo uno o due bridge FibreBridge 6500N e creare una configurazione con una coppia di bridge FibreBridge 7600N o 7500N, è necessario sostituire i bridge uno alla volta e seguire la procedura di cablaggio corretta. Il nuovo cablaggio è diverso da quello originale.

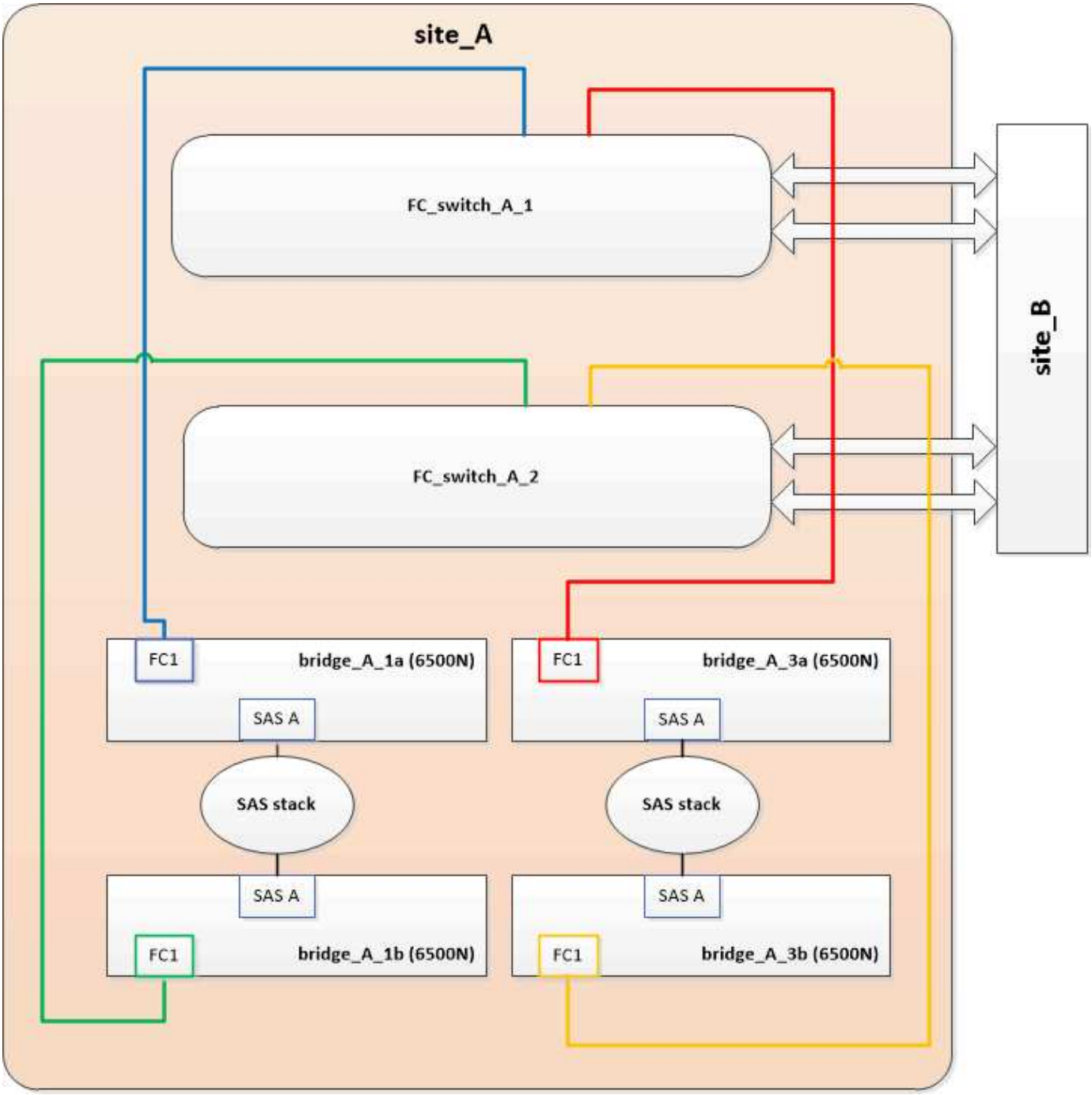
A proposito di questa attività

È possibile utilizzare questa procedura anche se sono soddisfatte le seguenti condizioni:

- Si sta sostituendo una coppia di bridge FibreBridge 6500N collegati allo stesso stack di storage SAS.
- In precedenza è stato sostituito un bridge FibreBridge 6500N nella coppia e lo stack di storage è configurato con un bridge FibreBridge 6500N e un bridge FibreBridge 7600N o 7500N.

  In questo caso, si dovrebbe iniziare con il passaggio seguente per sostituire a caldo il ponte FibreBridge 6500N inferiore con un ponte FibreBridge 7600N o 7500N.

Il seguente diagramma mostra un esempio della configurazione iniziale, in cui quattro bridge FibreBridge 6500N collegano due stack di storage SAS:



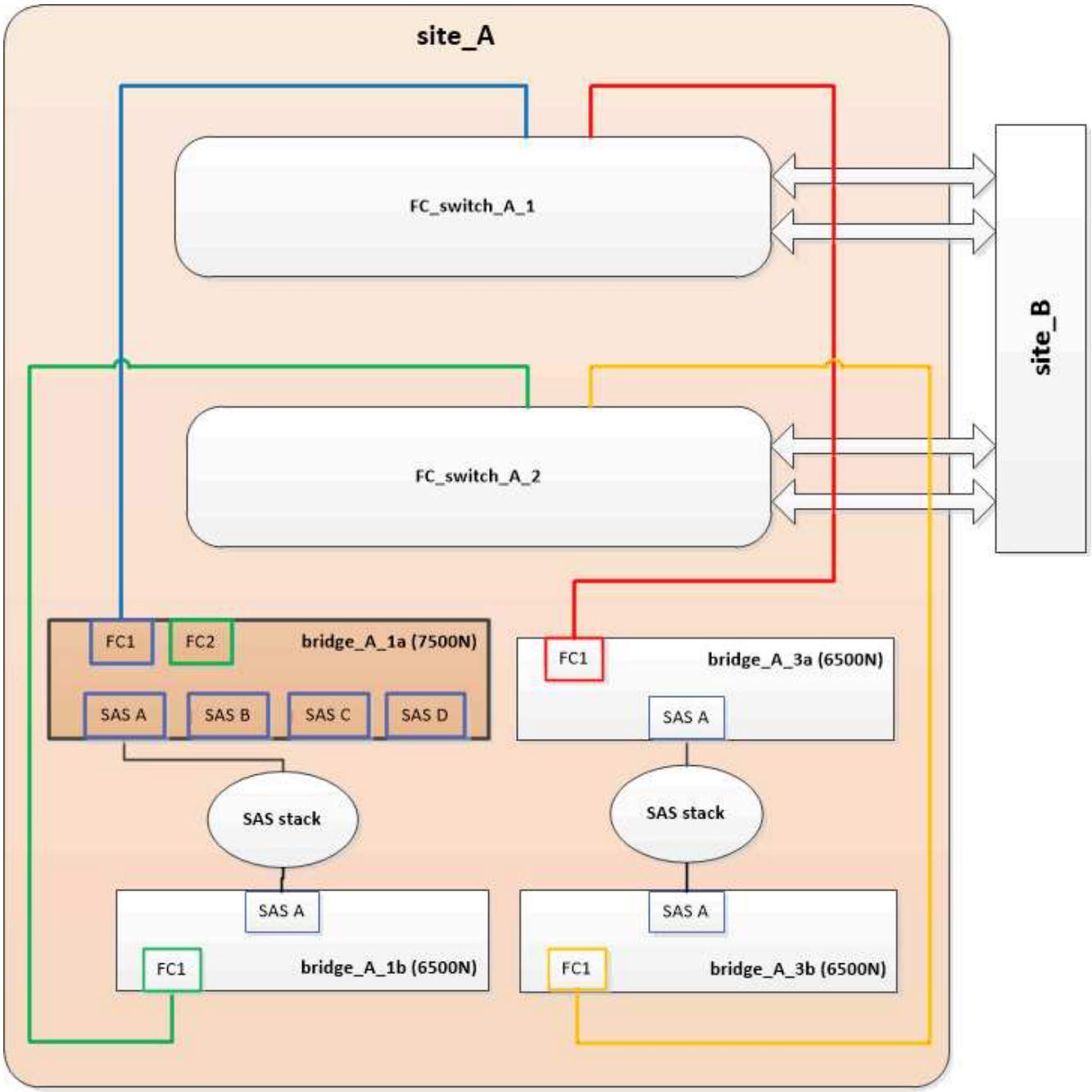
Fasi

1. Utilizzando le seguenti linee guida, sostituire a caldo il ponte FibreBridge 6500N superiore con un ponte FibreBridge 7600N o 7500N utilizzando la procedura descritta nella "Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N":

   - Collegare la porta FC1 del bridge FibreBridge 7600N o 7500N allo switch o al controller.

     Si tratta della stessa connessione effettuata alla porta FC1 del bridge FibreBridge 6500N.

   - Non collegare la porta FC2 del bridge FibreBridge 7600N o 7500N in questo momento. Il seguente diagramma mostra che il bridge_A_1a è stato sostituito ed è ora un bridge FibreBridge 7600N o 7500N:



2. Verificare la connettività ai dischi collegati al bridge e che il nuovo FibreBridge 7500N sia visibile nella configurazione:

```
run local sysconfig -v
```

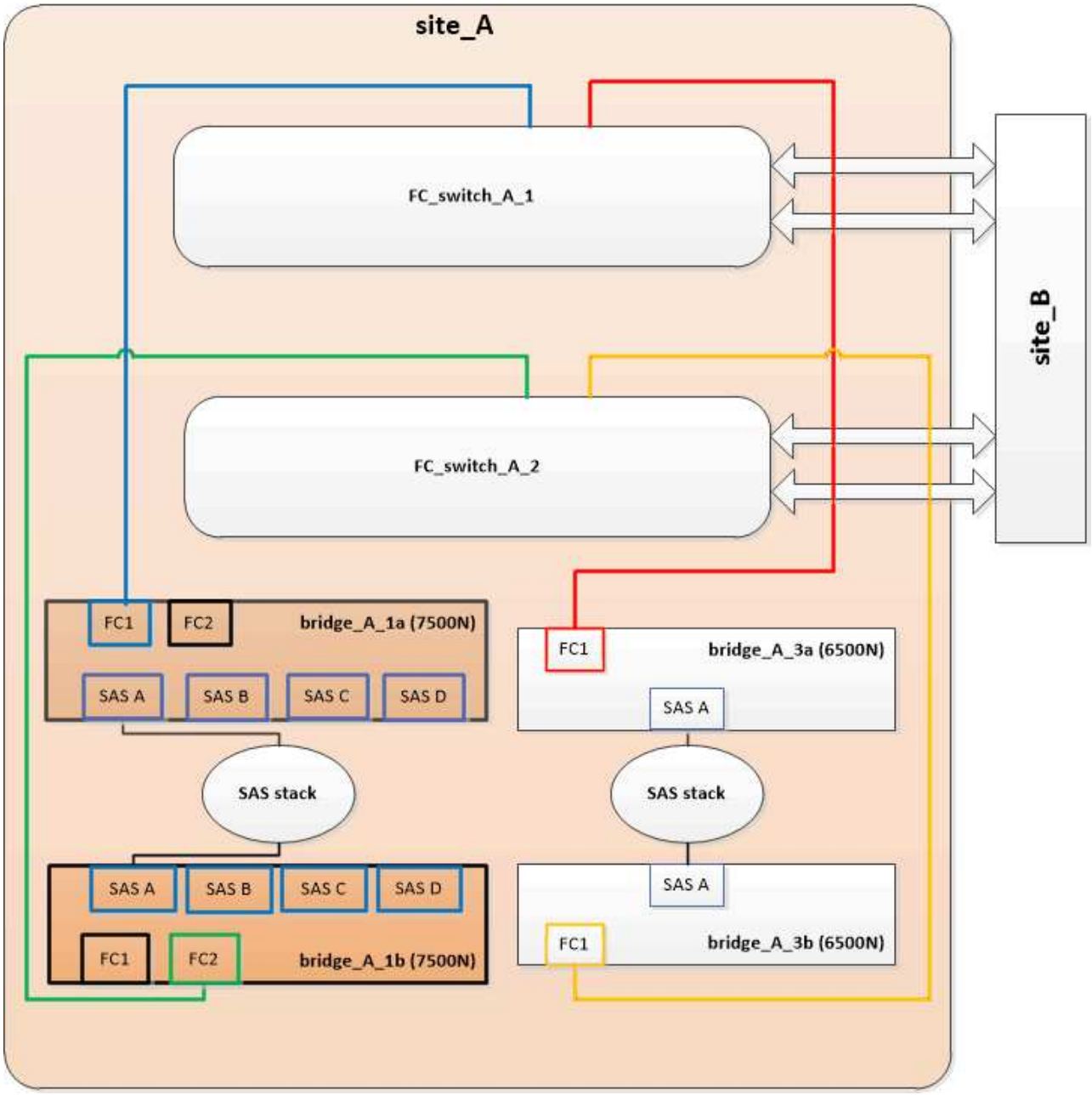
```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
```

```
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104**<===**
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

3. Utilizzando le seguenti linee guida, sostituire a caldo il ponte FibreBridge 6500N inferiore con un ponte FibreBridge 7600N o 7500N utilizzando la procedura descritta nella "Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N":
   - Collegare la porta FC2 del bridge FibreBridge 7600N o 7500N allo switch o al controller.

     Si tratta della stessa connessione effettuata alla porta FC1 del bridge FibreBridge 6500N.

   - Non collegare la porta FC1 del bridge FibreBridge 7600N o 7500N in questo momento.



4. Verificare la connettività ai dischi collegati al bridge:

```
run local sysconfig -v
```

L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
```

```
.
.
.
```

Cablaggio delle porte SAS del bridge durante il consolidamento dello storage mediante bridge FibreBridge 7600N o 7500N

Quando si consolidano più stack di storage SAS dietro una singola coppia di bridge FibreBridge 7600N o 7500N con porte SAS disponibili, è necessario spostare i cavi SAS superiore e inferiore sui nuovi bridge.

A proposito di questa attività

Le porte SAS del bridge FibreBridge 6500N utilizzano connettori QSFP. Le porte SAS bridge FibreBridge 7600N o 7500N utilizzano connettori mini-SAS.

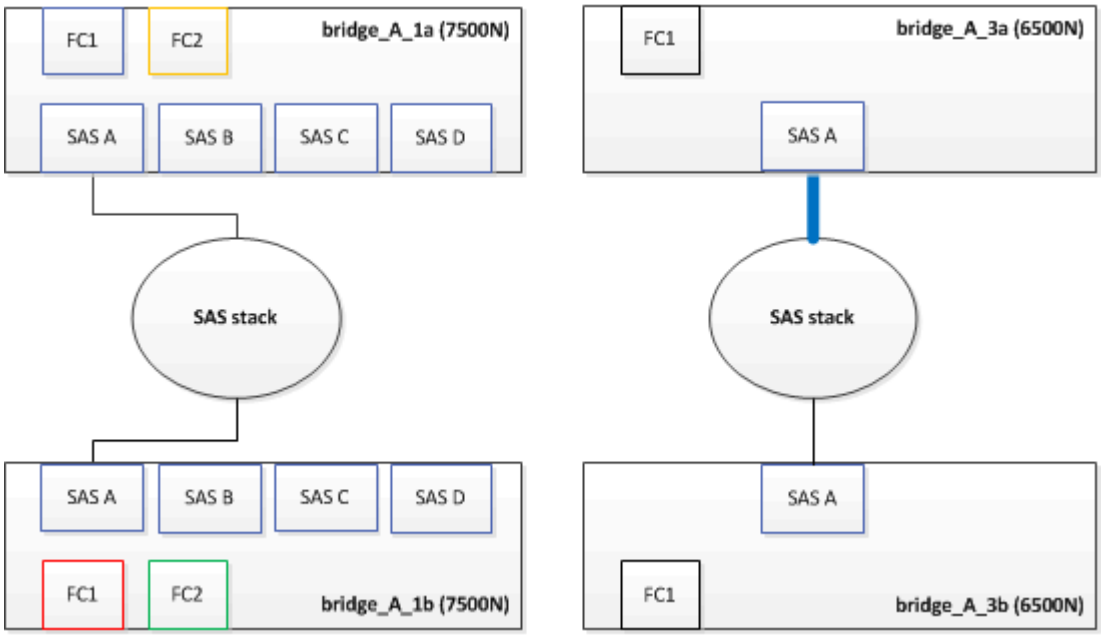
> Se si inserisce un cavo SAS nella porta errata, quando si rimuove il cavo da una porta SAS, è necessario attendere almeno 120 secondi prima di collegarlo a una porta SAS diversa. In caso contrario, il sistema non riconosce che il cavo è stato spostato su un'altra porta.

> Attendere almeno 10 secondi prima di collegare la porta. I connettori dei cavi SAS sono dotati di chiave; se orientati correttamente in una porta SAS, il connettore scatta in posizione e il LED LNK della porta SAS dello shelf di dischi si illumina di verde. Per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso il basso (nella parte inferiore del connettore).

Fasi

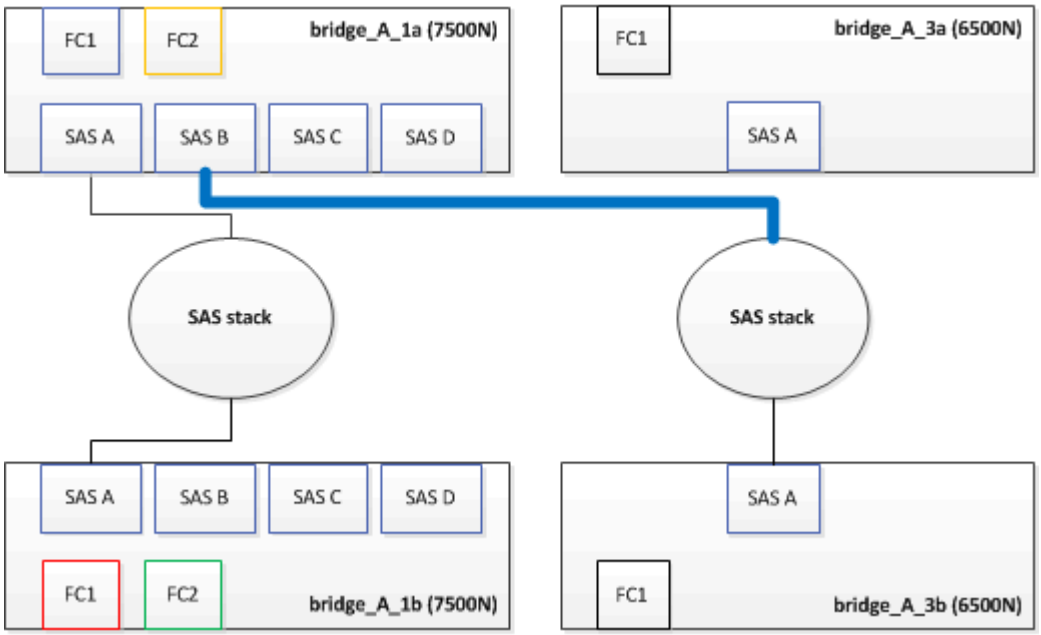
1. Rimuovere il cavo che collega la porta SAS A del bridge superiore FibreBridge 6500N allo shelf SAS superiore, accertandosi di annotare la porta SAS sullo shelf di storage a cui si collega.

   Il cavo viene visualizzato in blu nel seguente esempio:



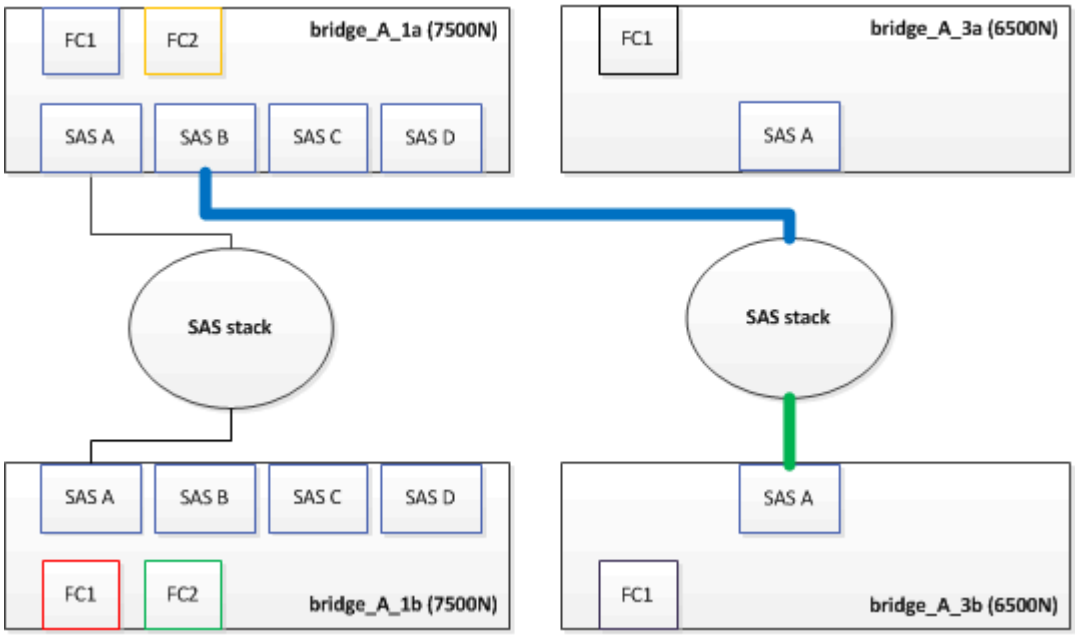
2. Utilizzando un cavo con connettore mini-SAS, collegare la stessa porta SAS sullo shelf di storage alla porta SAS B del bridge superiore FibreBridge 7600N o 7500N.

Il cavo viene visualizzato in blu nel seguente esempio:



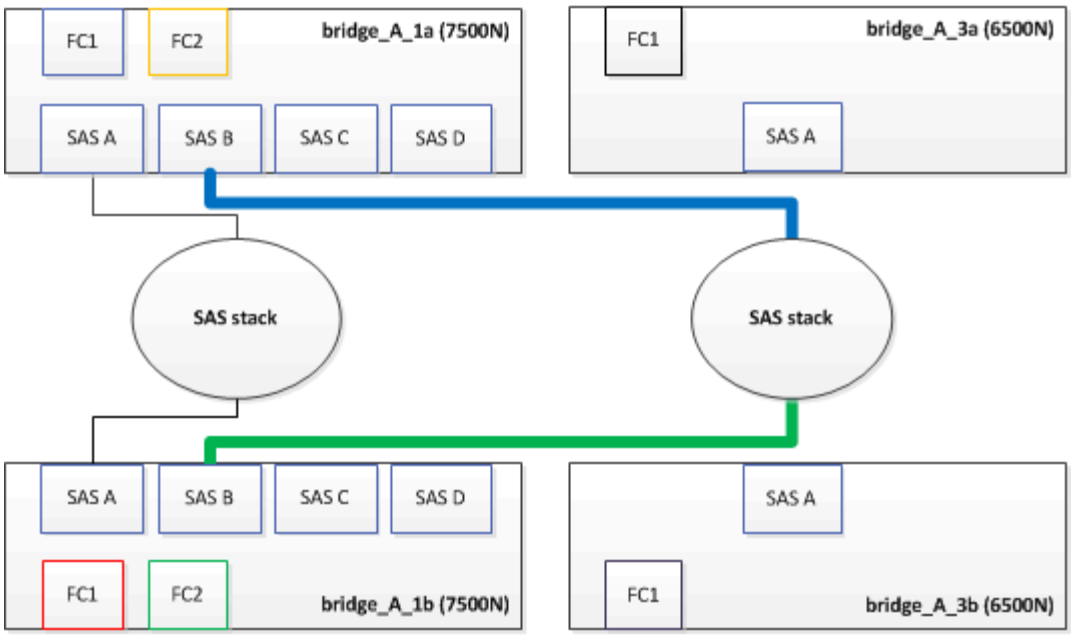
3. Rimuovere il cavo che collega la porta SAS A del bridge FibreBridge 6500N inferiore allo shelf SAS superiore, accertandosi di annotare la porta SAS sullo shelf di storage a cui si collega.

   Questo cavo viene visualizzato in verde nel seguente esempio:



4. Utilizzando un cavo con connettore mini-SAS, collegare la stessa porta SAS sullo shelf di storage alla porta SAS B del bridge inferiore FibreBridge 7600N o 7500N.

   Questo cavo viene visualizzato in verde nel seguente esempio:



5. Verificare la connettività ai dischi collegati al bridge:

```
run local sysconfig -v
```

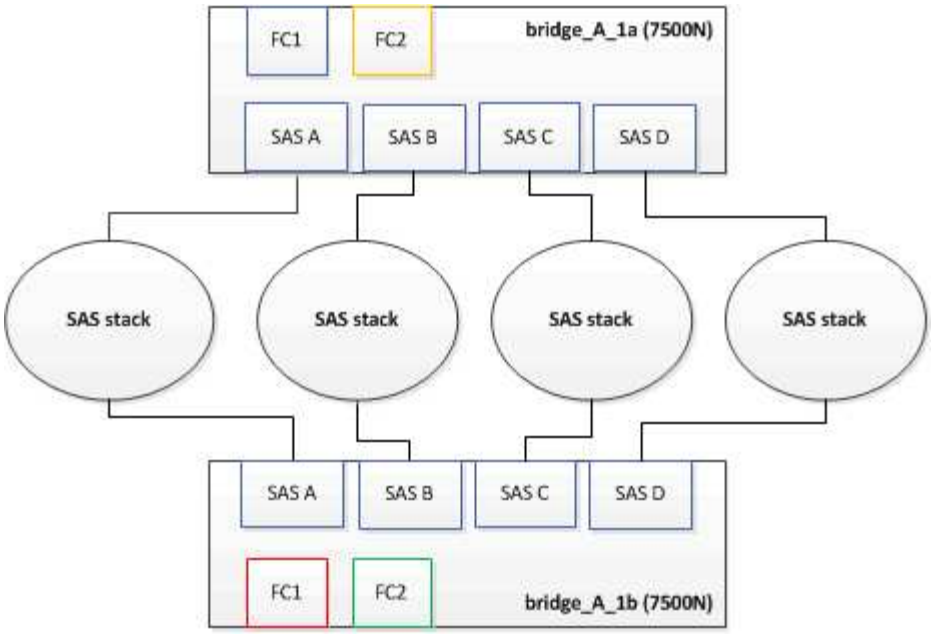
L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
```

```
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

6. Rimuovere i vecchi bridge FibreBridge 6500N che non sono più connessi allo storage SAS.
7. Attendere due minuti affinché il sistema riconosca le modifiche.
8. Se il sistema non è stato cablato correttamente, rimuovere il cavo, correggere il cablaggio, quindi ricollegare il cavo corretto.
9. Se necessario, ripetere i passaggi precedenti per spostare fino a due stack SAS aggiuntivi dietro i nuovi bridge FibreBridge 7600N o 7500N, utilizzando le porte SAS C e quindi D.

   Ogni stack SAS deve essere collegato alla stessa porta SAS sul bridge superiore e inferiore. Ad esempio, se la connessione superiore dello stack è collegata alla porta SAS B del bridge superiore, la connessione inferiore deve essere collegata alla porta SAS B del bridge inferiore.



Aggiornamento dello zoning durante l'aggiunta di bridge FibreBridge 7600N o 7500N a una configurazione

La suddivisione in zone deve essere modificata quando si sostituiscono i bridge FibreBridge 6500N con i bridge FibreBridge 7600N o 7500N e si utilizzano entrambe le porte FC sui bridge FibreBridge 7600N o 7500N. Le modifiche richieste dipendono dal fatto che si stia eseguendo una versione di ONTAP precedente alla 9.1 o alla 9.1 e successive.

Aggiornamento dello zoning durante l'aggiunta di bridge FibreBridge 7500N a una configurazione (prima di ONTAP 9.1)

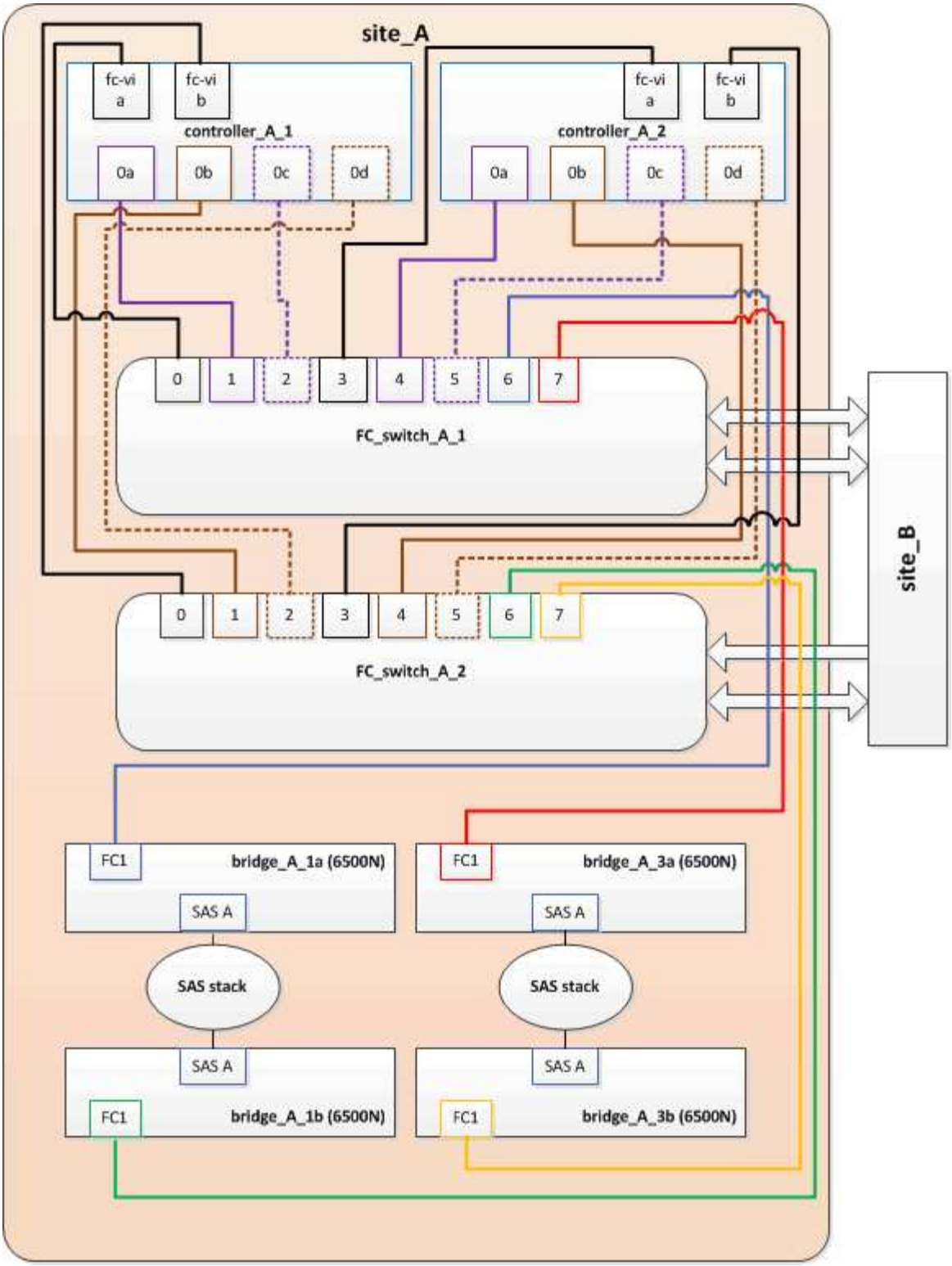
La zoning deve essere modificata quando si sostituiscono i bridge FibreBridge 6500N con i bridge FibreBridge 7500N e si utilizzano entrambe le porte FC sui bridge FibreBridge 7500N. Ciascuna zona non può avere più di quattro porte di iniziatore. La suddivisione in zone utilizzata dipende dal fatto che si stia utilizzando ONTAP prima della versione 9.1 o 9.1 e successive

A proposito di questa attività

Lo zoning specifico in questa attività è per le versioni di ONTAP precedenti alla versione 9.1.

Le modifiche di zoning sono necessarie per evitare problemi con ONTAP, che richiede che non più di quattro porte FC Initiator possano avere un percorso per un disco. Dopo aver eseguito la creazione di una copia degli shelf, l'attuale suddivisione in zone renderebbe ciascun disco raggiungibile da otto porte FC. È necessario modificare lo zoning per ridurre a quattro le porte iniziatore in ciascuna zona.

Il seguente diagramma mostra lo zoning sul sito_A prima delle modifiche:



Fasi

1. Aggiornare le zone di storage per gli switch FC rimuovendo metà delle porte iniziatore da ciascuna zona esistente e creando nuove zone per le porte FC2 FibreBridge 7500N.

   Le zone per le nuove porte FC2 conterranno le porte iniziatore rimosse dalle zone esistenti. Nei diagrammi, queste zone sono mostrate con linee tratteggiate.

   Per ulteriori informazioni sui comandi di zoning, consultare le sezioni switch FC di "Installazione e configurazione di Fabric-Attached MetroCluster" oppure "Estensione dell'installazione e della

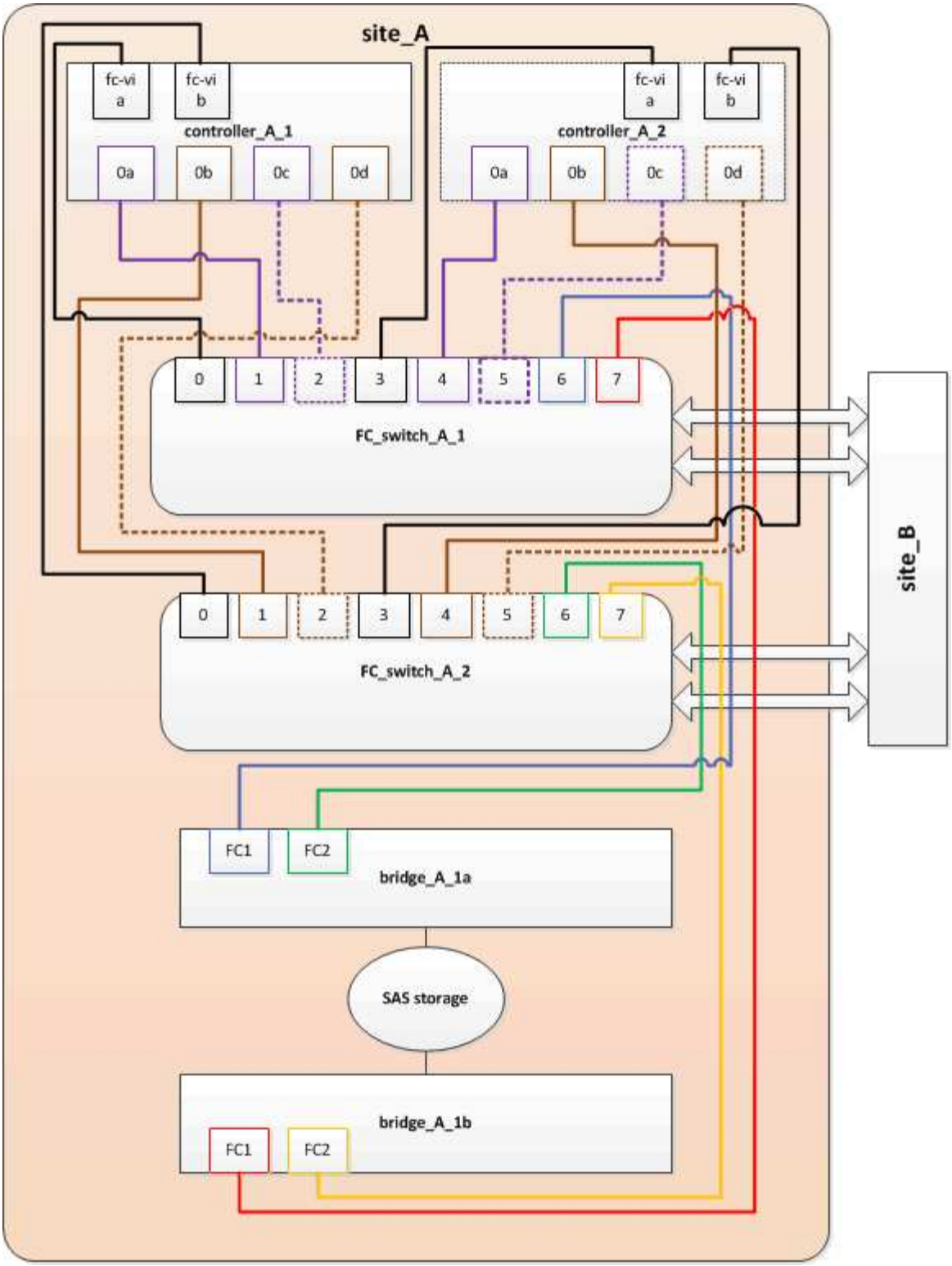
configurazione di MetroCluster".

Gli esempi seguenti mostrano le zone di storage e le porte di ciascuna zona prima e dopo il consolidamento. Le porte sono identificate da _dominio, coppie di porte.

- Il dominio 5 è costituito dallo switch FC_switch_A_1.
- Il dominio 6 è costituito dallo switch FC_switch_A_2.
- Il dominio 7 è costituito dallo switch FC_switch_B_1.
- Il dominio 8 è costituito dallo switch FC_switch_B_2.

Prima o dopo il consolidamento	Zona	Domini e porte	Colori nei diagrammi (i diagrammi mostrano solo il sito A)
Prima del consolidamento. Sui quattro bridge FibreBridge 6500N è presente una zona per ciascuna porta FC.	STOR_A_1A-FC1	5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,6	Viola + viola tratteggiato + blu
STOR_A_1B-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,6	Marrone + marrone tratteggiato + verde	STOR_A_2A-FC1
5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,7	Viola + viola tratteggiato + rosso	STOR_A_2B-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,7
Marrone + marrone tratteggiato + arancione	Dopo il consolidamento. È presente una zona per ciascuna porta FC sui due bridge FibreBridge 7500N.	STOR_A_1A-FC1	7,1; 7,4; 5,1; 5,4; 5,6
Viola + blu	STOR_A_1B-FC1	7,2; 7,5; 5,2; 5,5; 5,7	Viola tratteggiato + rosso
STOR_A_1A-FC2	8,1; 8,4; 6,1; 6,4; 6,6	Marrone + verde	STOR_A_1B-FC2

Il seguente diagramma mostra lo zoning nel sito_A dopo il consolidamento:



Aggiornamento dello zoning durante l'aggiunta di bridge FibreBridge 7600N o 7500N a una configurazione (ONTAP 9.1 e versioni successive)

La suddivisione in zone deve essere modificata quando si sostituiscono i bridge FibreBridge 6500N con i bridge FibreBridge 7600N o 7500N e si utilizzano entrambe le porte FC sui bridge FibreBridge 7600N o 7500N. Ciascuna zona non può avere più di quattro porte di iniziatore.

A proposito di questa attività

- Questa attività si applica a ONTAP 9.1 e versioni successive.
- I bridge FibreBridge 7600N sono supportati in ONTAP 9.6 e versioni successive.
- Lo zoning specifico in questa attività è per ONTAP 9.1 e versioni successive.
- Le modifiche di zoning sono necessarie per evitare problemi con ONTAP, che richiede che non più di quattro porte FC Initiator possano avere un percorso per un disco.

  Dopo aver eseguito la creazione di una copia degli shelf, l'attuale suddivisione in zone renderebbe ciascun disco raggiungibile da otto porte FC. È necessario modificare lo zoning per ridurre a quattro le porte iniziatore in ciascuna zona.

Fase

1. Aggiornare le zone di storage per gli switch FC rimuovendo metà delle porte iniziatore da ciascuna zona esistente e creando nuove zone per le porte FC2 FibreBridge 7600N o 7500N.

   Le zone per le nuove porte FC2 conterranno le porte iniziatore rimosse dalle zone esistenti.

   Fare riferimento alla sezione relativa allo switch FC di "Installazione e configurazione di Fabric-Attached MetroCluster" per informazioni dettagliate sui comandi di zoning.

Collegamento della porta FC del secondo bridge quando si aggiungono bridge FibreBridge 7600N o 7500N a una configurazione

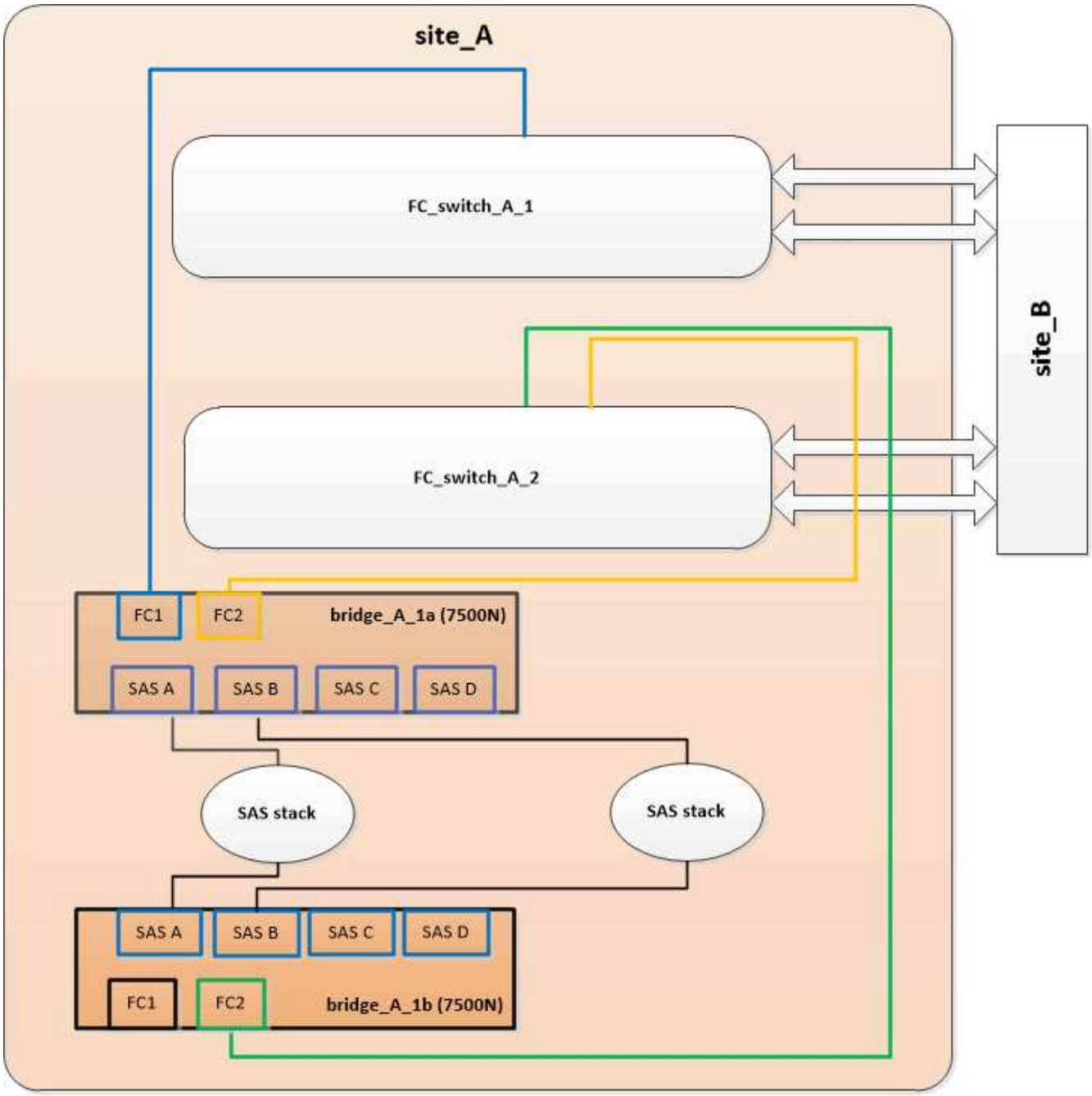
Per fornire percorsi multipli agli stack di storage, è possibile collegare la seconda porta FC su ciascun bridge FibreBridge 7600N o 7500N dopo aver aggiunto il bridge FibreBridge 7600N o 7500N alla configurazione.

Prima di iniziare

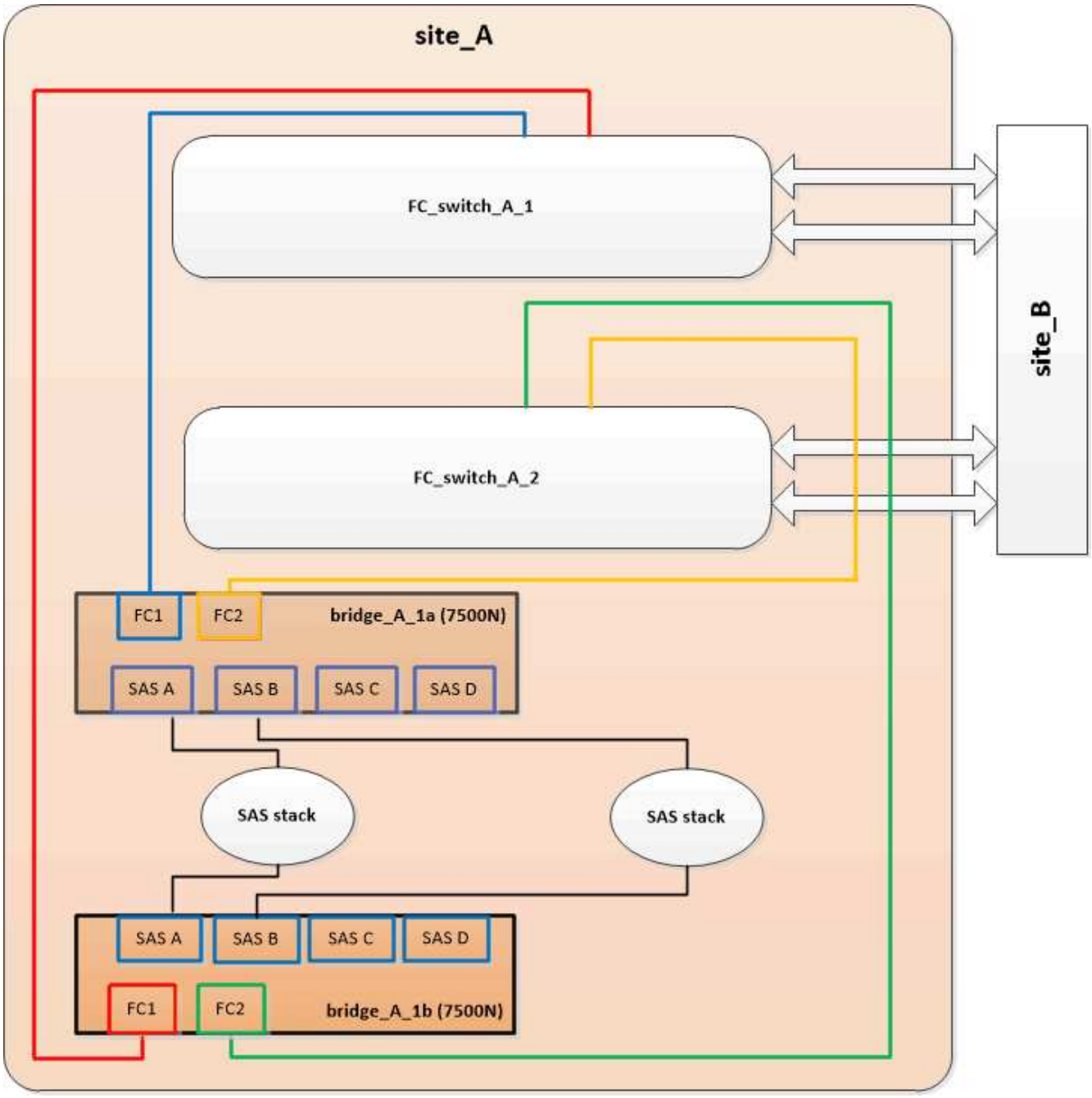
Lo zoning deve essere stato regolato in modo da fornire zone per le seconde porte FC.

Fasi

1. Collegare la porta FC2 del ponte superiore alla porta corretta su FC_switch_A_2.



2. Collegare la porta FC1 del bridge inferiore alla porta corretta su FC_switch_A_1.



3. Verificare la connettività ai dischi collegati al bridge:

   ```
   run local sysconfig -v
   ```

   L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
   System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
   System Serial Number: 940001025465 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   ```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Disattivazione delle porte SAS inutilizzate sui bridge FC-SAS

Dopo aver modificato il cablaggio del bridge, disattivare eventuali porte SAS inutilizzate sui bridge FC-SAS per evitare avvisi di monitoraggio dello stato di salute relativi alle porte inutilizzate.

Fasi

1. Disattivare le porte SAS inutilizzate sul bridge FC-SAS superiore:

   a. Accedere alla CLI del bridge.

   b. Disattivare le porte inutilizzate.

   > Se è stato configurato un bridge atto 7500N, tutte le porte SAS (Da A a D) sono attivate per impostazione predefinita ed è necessario disattivare le porte SAS non utilizzate:
   >
   > `SASPortDisable` *`sas port`*

   Se si utilizzano le porte SAS A e B, è necessario disattivare le porte SAS C e D. Nell'esempio seguente, le porte SAS C e D inutilizzate sono disattivate:

   ```
   Ready. *
   SASPortDisable C

   SAS Port C has been disabled.

   Ready. *
   SASPortDisable D

   SAS Port D has been disabled.

   Ready. *
   ```

   c. Salvare la configurazione del bridge:
   `SaveConfiguration`

   L'esempio seguente mostra che le porte SAS C e D sono state disattivate. L'asterisco non viene più visualizzato, a indicare che la configurazione è stata salvata.

```
Ready. *
SaveConfiguration

Ready.
```

2. Ripetere il passaggio precedente sul bridge FC-SAS inferiore.

Requisiti per l'utilizzo di altre interfacce per configurare e gestire i bridge FibreBridge

È possibile utilizzare la combinazione di una porta seriale, Telnet e FTP per gestire i bridge FibreBridge invece delle interfacce di gestione consigliate. Il sistema deve soddisfare i requisiti dell'interfaccia applicabile prima di installare i bridge.

È possibile utilizzare una porta seriale o Telnet per configurare il bridge e la porta di gestione Ethernet 1 e per gestire il bridge. È possibile utilizzare FTP per aggiornare il firmware del bridge.

> Il *Manuale d'installazione e di funzionamento di FibreBridge atto* per il tuo modello bridge contiene ulteriori informazioni sulle interfacce di gestione.

È possibile accedere a questo documento sul sito Web di atto utilizzando il link fornito nella pagina ATTO Fibrebridge Description.

Porta seriale

Quando si utilizza la porta seriale per configurare e gestire un bridge e per configurare la porta di gestione Ethernet 1, il sistema deve soddisfare i seguenti requisiti:

- Un cavo seriale (che collega la porta seriale del bridge a una porta seriale (COM) del computer utilizzato per la configurazione)

  La porta seriale del bridge è RJ-45 e ha lo stesso pin-out dei controller.

- Un programma di emulazione di terminale come Hyperterminal, Teraterm o putty per accedere alla console

  Il programma terminale deve essere in grado di registrare l'output dello schermo in un file.

Telnet

Quando si utilizza Telnet per configurare e gestire un bridge, il sistema deve soddisfare i seguenti requisiti:

- Un cavo seriale (che collega la porta seriale del bridge a una porta seriale (COM) del computer utilizzato per la configurazione)

  La porta seriale del bridge è RJ-45 e ha lo stesso pin-out dei controller.

- (Consigliato) un nome utente e una password non predefiniti (per l'accesso al bridge)
- Un programma di emulazione di terminale come Hyperterminal, Teraterm o putty per accedere alla console

  Il programma terminale deve essere in grado di registrare l'output dello schermo in un file.

- Un indirizzo IP, una subnet mask e informazioni sul gateway per la porta di gestione Ethernet 1 su ciascun bridge

FTP

Quando si utilizza FTP per aggiornare il firmware del bridge, il sistema deve soddisfare i seguenti requisiti:

- Un cavo Ethernet standard (che collega la porta di gestione Ethernet del bridge 1 alla rete)

- (Consigliato) un nome utente e una password non predefiniti (per l'accesso al bridge)

Sostituzione a caldo di un modulo alimentatore guasto

In caso di modifica dello stato di un modulo di alimentazione al bridge, è possibile rimuovere e installare il modulo di alimentazione.

È possibile visualizzare il cambiamento di stato di un modulo di alimentazione tramite i LED sul bridge. È inoltre possibile visualizzare lo stato dei moduli di alimentazione tramite la GUI ExpressNAV e la CLI del bridge, tramite la porta seriale o Telnet.

- Questa procedura è NDO (senza interruzioni) e richiede circa 15 minuti per essere completata.
- È necessaria la password admin e l'accesso a un server FTP o SCP.

> 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.

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 proposito di questa attività**
>
> 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.

Informazioni correlate

"Sostituzione a caldo di un bridge con un bridge sostitutivo dello stesso modello"

"Scambio a caldo di un FibreBridge 7500N con un bridge 7600N"

"Scambio a caldo di un bridge FibreBridge 6500N con un bridge FibreBridge 7600N o 7500N"

"Aggiunta a caldo di uno stack di shelf e bridge di dischi SAS"

Gestione di un bridge FibreBridge da ONTAP

A partire da ONTAP 9.5, è possibile utilizzare l'interfaccia utente di ONTAP per passare i comandi FibreBridge al bridge e visualizzare i risultati di tali comandi.

A proposito di questa attività

> 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. Eseguire il comando FiberBridge applicabile all'interno di `storage bridge run-cli` comando:

   `storage bridge run-cli -name` *`bridge-name`* `-command` *`"command-text"`*

   Il seguente comando esegue FibreBridge `SASPortDisable` Dal prompt di ONTAP per disattivare la porta SAS b sul bridge:

   ```
   cluster_A::> storage bridge run-cli -name "SASPortDisable b"

   SAS Port B has been disabled.
   Ready
   cluster_A::>
   ```

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.

- 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 riabilitare 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 sprotegge 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
   ```

Manutenzione e sostituzione dello switch FC

Aggiornamento o downgrade del firmware su uno switch Brocade FC

Per aggiornare o eseguire il downgrade del firmware su uno switch Brocade FC, è necessario utilizzare i comandi specifici di Brocade per disattivare lo switch, eseguire e verificare la modifica del firmware, riavviare e riabilitare lo switch.

- È necessario disporre dei file del firmware.
- Il sistema deve essere collegato correttamente.
- Tutti i percorsi verso gli shelf di storage devono essere disponibili.
- Gli stack degli shelf di dischi devono essere stabili.
- Il fabric dello switch FC deve essere integro.
- Non è possibile che nel sistema siano presenti componenti guasti.
- Il sistema deve funzionare normalmente.
- È necessario disporre della password admin e dell'accesso a un server FTP o SCP.

Il fabric dello switch viene disattivato durante un aggiornamento o un downgrade del firmware e la configurazione MetroCluster si basa sul secondo fabric per continuare a funzionare.

A partire da Fabric OS 9,0.1, SNMPv2 non è supportato dagli switch Brocade. Se esegui l'upgrade a Fabric OS 9.0.1 o versione successiva, devi utilizzare SNMPv3 per il monitoraggio dello stato di salute. Per ulteriori informazioni, vedere "Configurazione di SNMPv3 in una configurazione MetroCluster".

Questa attività deve essere eseguita su ciascuno switch fabric in successione in modo che tutti gli switch eseguano la stessa versione del firmware.

Questa procedura è senza interruzioni e richiede circa un'ora per essere completata.

Fasi

1. Accedere a ciascuno switch del fabric.

   Gli esempi riportati di seguito utilizzano lo switch `FC_switch_A_1`.

2. Disattivare ciascuno switch nel fabric:

   `switchCfgPersistentDisable`

   Se questo comando non è disponibile, eseguire `switchDisable` comando.

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. Scaricare la versione del firmware desiderata:

   `firmwareDownload`

   Quando viene richiesto il nome del file, è necessario specificare la sottodirectory o il percorso relativo al file del firmware.

   È possibile eseguire `firmwareDownload` contemporaneamente su entrambi gli switch, ma prima di passare alla fase successiva è necessario consentire il download e il commit corretti del firmware.

```
FC_switch_A_1:admin> firmwaredownload
Server Name or IP Address: 10.64.203.188
User Name: test
File Name: v7.3.1b
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password:
Server IP: 10.64.203.188, Protocol IPv4
Checking system settings for firmwaredownload...
System settings check passed.
```

4. Verificare che il firmware sia stato scaricato e che sia stato eseguito il commit su entrambe le partizioni:

   firmwareShow

   Il seguente esempio mostra che il download del firmware è completo man mano che entrambe le immagini vengono aggiornate:

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. Riavviare gli switch:

   reboot

   Alcune versioni del firmware eseguono automaticamente un'operazione di reboot al termine del download del firmware. Il riavvio in questa fase è necessario anche se è stato eseguito il riavvio di haReboot.

```
FC_switch_A_1:admin> reboot
```

6. Verificare se il nuovo firmware è per un livello di firmware intermedio o per una release finale specificata.

   Se il download riguarda il livello di firmware intermedio, eseguire i due passi precedenti fino a quando non viene installata la release specificata.

7. Abilitare gli switch:

   switchCfgPersistentEnable

   Se questo comando non è disponibile, lo switch deve trovarsi in `enabled` dopo `reboot` il comando viene eseguito.

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. Verificare che gli switch siano in linea e che tutti i dispositivi siano collegati correttamente:

   switchShow

```
FC_switch_A_1:admin> switchShow
```

9. Verificare che le informazioni sull'utilizzo del buffer per un gruppo di porte o tutti i gruppi di porte nello switch siano visualizzate correttamente:

   portbuffershow

```
FC_switch_A_1:admin> portbuffershow
```

10. Verificare che la configurazione corrente di una porta sia visualizzata correttamente:

    portcfgshow

```
FC_switch_A_1:admin> portcfgshow
```

    Verificare le impostazioni della porta, ad esempio velocità, modalità, trunking, crittografia, E la compressione, nell'uscita Inter-Switch link (ISL). Verificare che le impostazioni della porta non siano state influenzate dal download del firmware.

11. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

    a. Verificare che il sistema sia multipercorso:
       node run -node *node-name* sysconfig -a

    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
       system health alert show

    c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
       metrocluster show

    d. Eseguire un controllo MetroCluster:
       metrocluster check run

    e. Visualizzare i risultati del controllo MetroCluster:
       metrocluster check show

    f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli interruttori (se presenti):
       storage switch show

    g. Eseguire Config Advisor.

       "Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

12. Attendere 15 minuti prima di ripetere questa procedura per il secondo fabric dello switch.

Aggiornamento o downgrade del firmware su uno switch FC Cisco

Per aggiornare o eseguire il downgrade del firmware su uno switch FC Cisco, è necessario utilizzare i comandi specifici di Cisco per disattivare lo switch, eseguire e verificare l'aggiornamento, riavviare e riabilitare lo switch.

- Il sistema deve essere collegato correttamente.
- Tutti i percorsi verso gli shelf di storage devono essere disponibili.
- Gli stack degli shelf di dischi devono essere stabili.
- Il fabric dello switch FC deve essere integro.
- Tutti i componenti del sistema devono essere integri.
- Il sistema deve funzionare normalmente.
- È necessaria la password admin e l'accesso a un server FTP o SCP.

Il fabric dello switch viene disattivato durante l'aggiornamento o il downgrade del firmware e la configurazione MetroCluster si basa sul secondo fabric per continuare a funzionare.

È necessario ripetere questa attività su ciascuno switch fabric in successione per assicurarsi che tutti gli switch eseguano la stessa versione del firmware.

È necessario disporre dei file del firmware.

Questa procedura è senza interruzioni e richiede circa un'ora per essere completata.

Fasi

1. Accedere a ciascuno switch del fabric.

   Negli esempi, gli switch sono chiamati FC_switch_A_1 e FC_switch_B_1.

2. Determinare se nella directory bootflash su ogni switch è presente spazio sufficiente:

   `dir bootflash`

   In caso contrario, eliminare i file del firmware indesiderati utilizzando `delete bootflash:file_name` comando.

3. Copiare i file di sistema e kickstart sugli switch:

   `copy` *`source_filetarget_file`*

   Nell'esempio seguente, il file kickstart (`m9200-s2ek9-kickstart-mz.5.2.1.bin`) e il file di sistema (`m9200-s2ek9-mz.5.2.1.bin`) Si trovano sul server FTP 10.10.10.55 in `/firmware/` percorso.

   L'esempio seguente mostra i comandi emessi su FC_switch_A_1:

```
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-
mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin
bootflash:m9200-s2ek9-mz.5.2.1.bin
```

4. Disattivare tutte le VSAN su entrambi gli switch in questo fabric.

   Per disattivare le reti VSAN, attenersi alla seguente procedura:

   a. Aprire il terminale di configurazione:

      `config t`

   b. Inserire: **`vsan database`**

   c. Controllare lo stato delle reti VSAN:

      `show vsan`

      Tutte le reti VSAN devono essere attive.

   d. Sospendere le VSAN:

      `vsan vsan-num suspend`

      Esempio: `vsan 10 suspend`

   e. Controllare nuovamente lo stato delle reti VSAN:

      `show vsan`+ tutti i VSAN devono essere sospesi.

   f. Uscire dal terminale di configurazione:

      `end`

   g. Salvare la configurazione.

      `copy running-config startup-config`

      Nell'esempio seguente viene visualizzato l'output per FC_switch_A_1:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up
```

```
vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 80 information
         name:MC2_STOR_2_80  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# vsan 1 suspend
FC_switch_A_1(config-vsan-db)# vsan 30 suspend
FC_switch_A_1(config-vsan-db)# vsan 40 suspend
FC_switch_A_1(config-vsan-db)# vsan 70 suspend
FC_switch_A_1(config-vsan-db)# vsan 80 suspend
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
FC_switch_A_1# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
```

```
        loadbalancing:src-id/dst-id
        operational state:down

vsan 40 information
        name:MC1_STOR_2_40  state:suspended
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:down

vsan 70 information
        name:MC2_FCVI_2_70  state:suspended
        interoperability mode:default
        loadbalancing:src-id/dst-id
        operational state:down

vsan 80 information
        name:MC2_STOR_2_80  state:suspended
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan
```

5. Installare il firmware desiderato sugli switch:

   install all system bootflash:*systemfile_name* kickstart bootflash:*kickstartfile_name*

   L'esempio seguente mostra i comandi emessi su FC_switch_A_1:

```
FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin
kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
Enter Yes to confirm the installation.
```

6. Verificare la versione del firmware su ciascun switch per assicurarsi che sia stata installata la versione corretta:

   show version

7. Abilitare tutte le VSAN su entrambi gli switch in questo fabric.

   Utilizzare la seguente procedura per attivare le reti VSAN:

   a. Aprire il terminale di configurazione:

config t

b. Inserire: **vsan database**

c. Controllare lo stato delle reti VSAN:

show vsan

Le VSAN devono essere sospese.

d. Attivare le VSAN:

no vsan *vsan-num* suspend

Esempio: `no vsan 10 suspend`

e. Controllare nuovamente lo stato delle reti VSAN:

show vsan

Tutte le reti VSAN devono essere attive.

f. Uscire dal terminale di configurazione:

end

g. Salvare la configurazione:

copy running-config startup-config

Nell'esempio seguente viene visualizzato l'output per FC_switch_A_1:

```
FC_switch_A_1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 30 information
         name:MC1_FCVI_2_30  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 40 information
         name:MC1_STOR_2_40  state:suspended
         interoperability mode:default
```

```
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 70 information
         name:MC2_FCVI_2_70  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:down

vsan 80 information
         name:MC2_STOR_2_80  state:suspended
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:down

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# no vsan 1 suspend
FC_switch_A_1(config-vsan-db)# no vsan 30 suspend
FC_switch_A_1(config-vsan-db)# no vsan 40 suspend
FC_switch_A_1(config-vsan-db)# no vsan 70 suspend
FC_switch_A_1(config-vsan-db)# no vsan 80 suspend
FC_switch_A_1(config-vsan-db)#
FC_switch_A_1(config-vsan-db)# show vsan
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 30 information
         name:MC1_FCVI_2_30  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id
         operational state:up

vsan 40 information
         name:MC1_STOR_2_40  state:active
         interoperability mode:default
         loadbalancing:src-id/dst-id/oxid
         operational state:up

vsan 70 information
         name:MC2_FCVI_2_70  state:active
```

```
        interoperability mode:default
        loadbalancing:src-id/dst-id
        operational state:up

vsan 80 information
        name:MC2_STOR_2_80  state:active
        interoperability mode:default
        loadbalancing:src-id/dst-id/oxid
        operational state:up

vsan 4079:evfp_isolated_vsan

vsan 4094:isolated_vsan

FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1#
```

8. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      node run -node *node-name* sysconfig -a

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      system health alert show

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      metrocluster show

   d. Eseguire un controllo MetroCluster:

      metrocluster check run

   e. Visualizzare i risultati del controllo MetroCluster:

      metrocluster check show

   f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

      storage switch show

   g. Eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.
9. Ripetere questa procedura per il secondo fabric switch.

Aggiornamento a nuovi switch Brocade FC

Se si esegue l'aggiornamento a nuovi switch FC Brocade, è necessario sostituire gli switch nel primo fabric, verificare che la configurazione MetroCluster sia completamente operativa, quindi sostituire gli switch nel secondo fabric.

- La configurazione di MetroCluster deve essere in buone condizioni e in condizioni di funzionamento normali.
- I fabric switch MetroCluster sono costituiti da quattro switch Brocade.

  Le illustrazioni riportate nelle fasi seguenti mostrano gli interruttori correnti.

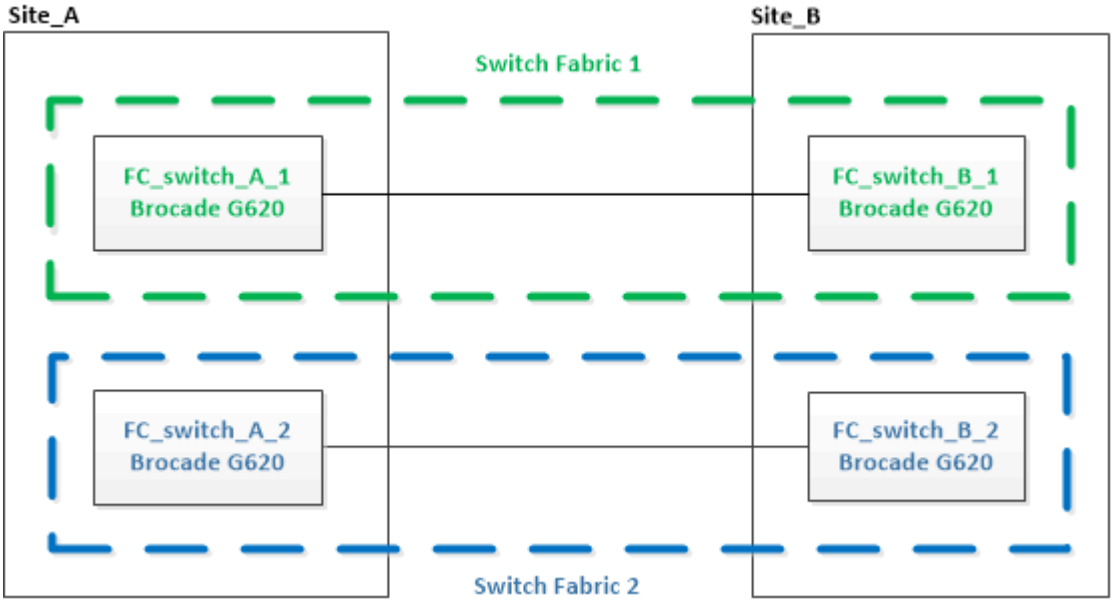
- Gli switch devono utilizzare il firmware supportato più recente.

  "Tool di matrice di interoperabilità NetApp"

- Questa procedura è senza interruzioni e richiede circa due ore per essere completata.
- È necessaria la password admin e l'accesso a un server FTP o SCP.

I fabric degli switch vengono aggiornati uno alla volta.

Al termine di questa procedura, tutti e quattro gli switch verranno aggiornati ai nuovi switch.

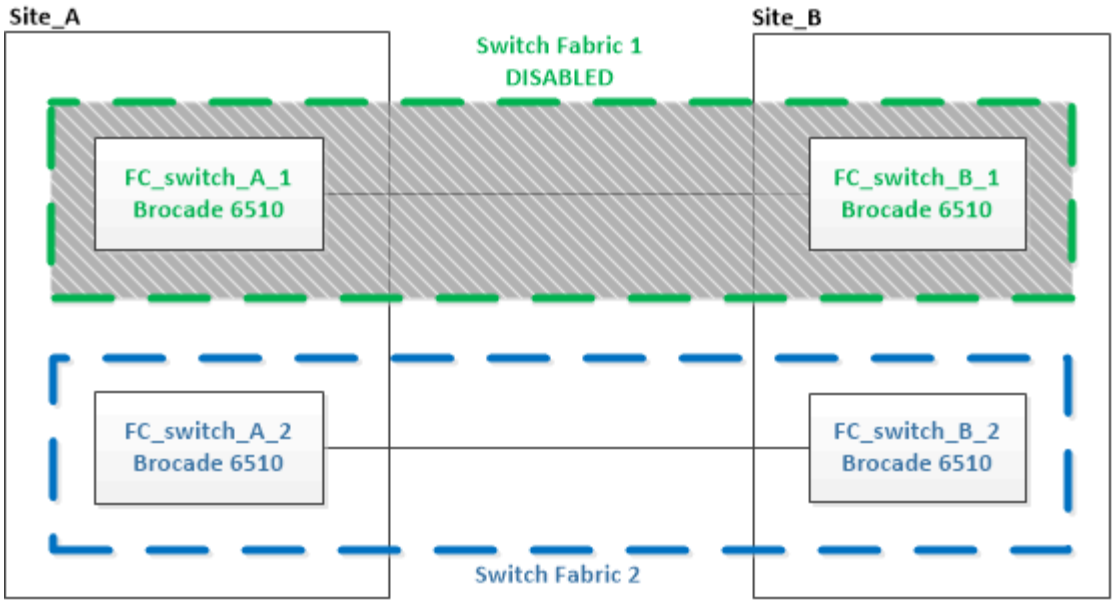


Fasi

1. Disattivare il primo fabric dello switch:

   `FC_switch_A_1:admin> switchCfgPersistentDisable`

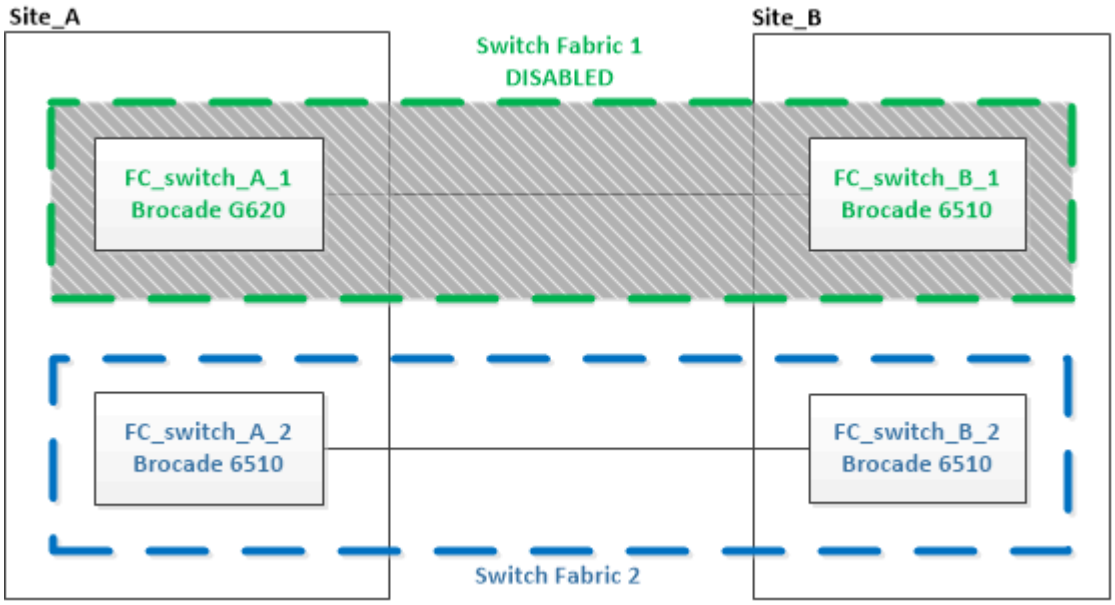
   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```



2. Sostituire i vecchi switch in un sito MetroCluster.

   a. Scollegare e rimuovere lo switch disattivato.

   b. Installare il nuovo switch nel rack.



   c. Disattivare i nuovi switch:

   `switchCfgPersistentDisable`

   Il comando disattiva entrambi gli switch nel fabric dello switch.

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

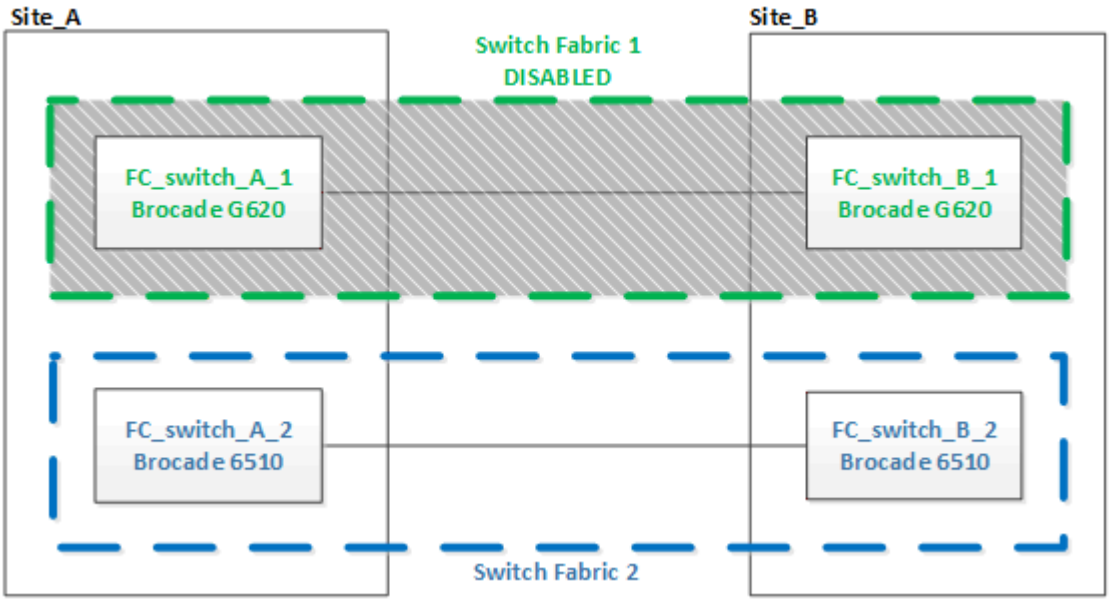
   d. Collegare il nuovo switch utilizzando le assegnazioni delle porte consigliate.

"Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"

"Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

e. Ripetere questi passaggi secondari sul sito MetroCluster del partner per sostituire il secondo switch nel primo fabric.

   Entrambi gli switch del fabric 1 sono stati sostituiti.



3. Accendere i nuovi switch e lasciarli avviare.
4. Scaricare i file RCF per il nuovo switch.
5. Applicare i file RCF a entrambi i nuovi switch del fabric, seguendo le istruzioni riportate nella pagina di download.
6. Salvare la configurazione dello switch:

   ```
   cfgSave
   ```

7. Attendere 10 minuti per consentire alla configurazione di stabilizzarsi.
8. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:

   ```
   run local sysconfig -v
   ```

   L'output mostra i dischi collegati alle porte dell'iniziatore sul controller e identifica gli shelf collegati ai bridge FC-SAS:

   ```
   node_A_1> run local sysconfig -v
   NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
   System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
   System Serial Number: 940001025471 (node_A_1)
   System Rev: 70
   System Storage Configuration: Multi-Path HA**<=== Configuration should
   ```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
```

```
.
```

9. Tornare al prompt dello switch, verificare la versione del firmware dello switch:

   ```
   firmwareShow
   ```

   Gli switch devono utilizzare il firmware supportato più recente.

   "Tool di matrice di interoperabilità NetApp"

10. Simulare un'operazione di switchover:

    a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
       `set -privilege advanced`

       Quando viene richiesto di passare alla modalità avanzata, rispondere con "y" e visualizzare il prompt della modalità avanzata (*).

    b. Eseguire l'operazione di switchover con `-simulate` parametro:

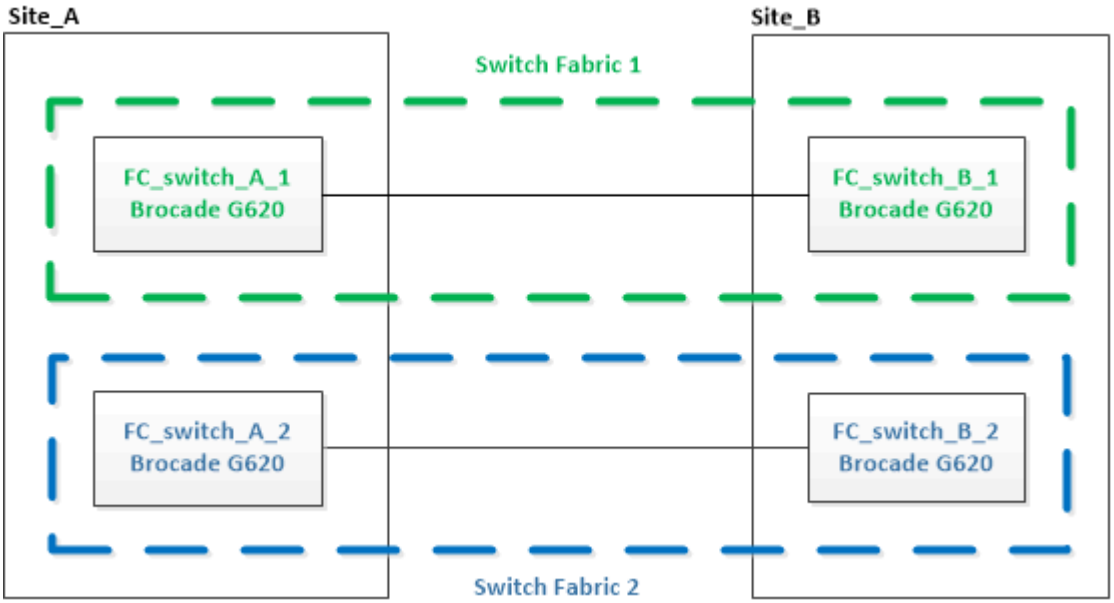
       ```
       metrocluster switchover -simulate
       ```

    c. Tornare al livello di privilegio admin:

       ```
       set -privilege admin
       ```

11. Ripetere i passaggi precedenti sul secondo fabric dello switch.

Dopo aver ripetuto i passaggi, tutti e quattro gli switch sono stati aggiornati e la configurazione MetroCluster funziona normalmente.



Sostituzione di uno switch FC Brocade

Per sostituire uno switch guasto, è necessario utilizzare questa procedura specifica di Brocade.

È necessaria la password admin e l'accesso a un server FTP o SCP.

Negli esempi seguenti, FC_switch_A_1 è lo switch integro e FC_switch_B_1 è lo switch compromesso. L'utilizzo della porta dello switch negli esempi è illustrato nella seguente tabella:

Connessioni delle porte	Porte
Connessioni FC-VI	0, 3
Connessioni HBA	1, 2, 4, 5
Connessioni bridge FC-SAS	6, 7
Connessioni ISL	10, 11

Gli esempi mostrano due bridge FC-SAS. Se si dispone di altre porte, è necessario disattivarle e attivarle successivamente.

Questa procedura è senza interruzioni e richiede circa due ore per essere completata.

L'utilizzo della porta dello switch deve seguire le assegnazioni consigliate.

- "Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"
- "Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Fasi

1. Spegnere lo switch in sostituzione disattivando le porte ISL dello switch integro nel fabric e le porte FC-VI e HBA dello switch non funzionante (se lo switch non funzionante è ancora in funzione):

   a. Disattivare le porte ISL sullo switch integro per ciascuna porta:

   `portcfgpersistentdisable` *`port-number`*

   ```
   FC_switch_A_1:admin> portcfgpersistentdisable 10
   FC_switch_A_1:admin> portcfgpersistentdisable 11
   ```

   b. Se lo switch non funzionante è ancora in funzione, disattivare le porte FC-VI e HBA dello switch per ciascuna porta:

   `portcfgpersistentdisable` *`port-number`*

   ```
   FC_switch_B_1:admin> portcfgpersistentdisable 0
   FC_switch_B_1:admin> portcfgpersistentdisable 1
   FC_switch_B_1:admin> portcfgpersistentdisable 2
   FC_switch_B_1:admin> portcfgpersistentdisable 3
   FC_switch_B_1:admin> portcfgpersistentdisable 4
   FC_switch_B_1:admin> portcfgpersistentdisable 5
   ```

2. Se l'interruttore non funzionante è ancora in funzione, raccogliere l'uscita da `switchshow` comando.

```
FC_switch_B_1:admin> switchshow
    switchName: FC_switch_B_1
    switchType: 71.2
    switchState:Online
    switchMode: Native
    switchRole: Subordinate
    switchDomain:       2
    switchId:   fffc01
    switchWwn:  10:00:00:05:33:86:89:cb
    zoning:             OFF
    switchBeacon:       OFF
```

3. Avviare e preconfigurare il nuovo switch prima di installarlo fisicamente:
   a. Accendere il nuovo switch e lasciarlo avviare.
   b. Controllare la versione del firmware sullo switch per verificare che corrisponda alla versione degli altri switch FC:

      `firmwareShow`

   c. Configurare il nuovo switch seguendo i passaggi indicati nella sezione "Configurare manualmente gli switch Brocade FC".

      A questo punto, il nuovo switch non viene collegato alla configurazione MetroCluster.

   d. Disattivare le porte FC-VI, HBA e storage sul nuovo switch e le porte collegate ai bridge FC-SAS.

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5

FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. Sostituire fisicamente lo switch:
   a. Spegnere lo switch FC compromesso.
   b. Spegnere lo switch FC sostitutivo.
   c. Scollegare e rimuovere lo switch compromesso, prestando attenzione a quali cavi sono collegati a quali porte.
   d. Installare lo switch sostitutivo nel rack.

e. Collegare lo switch sostitutivo esattamente come lo switch precedente era cablato.

f. Accendere il nuovo switch FC.

5. Se si desidera attivare la crittografia ISL, completare le attività applicabili in "Installazione e configurazione di Fabric-Attached MetroCluster".

   Se si attiva la crittografia ISL, è necessario completare le seguenti attività:

   - Disattivare il fabric virtuale
   - Impostare il payload
   - Impostare il criterio di autenticazione
   - Abilitare la crittografia ISL sugli switch Brocade

6. Completare la configurazione del nuovo switch:

   a. Abilitare gli ISL:

      `portcfgpersistentenable` *`port-number`*

      ```
      FC_switch_B_1:admin> portcfgpersistentenable 10
      FC_switch_B_1:admin> portcfgpersistentenable 11
      ```

   b. Verificare la configurazione dello zoning:

      ```
      cfg show
      ```

   c. Sullo switch sostitutivo (FC_switch_B_1 nell'esempio), verificare che gli ISL siano in linea:

      ```
      switchshow
      ```

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

d. Abilitare le porte di storage che si collegano ai bridge FC.

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

e. Abilitare le porte storage, HBA e FC-VI.

L'esempio seguente mostra i comandi utilizzati per attivare le porte che collegano gli adattatori HBA:

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

L'esempio seguente mostra i comandi utilizzati per attivare le porte che collegano gli adattatori FC-VI:

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

7. Verificare che le porte siano in linea:

```
switchshow
```

8. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      ```
      system health alert show
      ```

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      ```
      metrocluster show
      ```

   d. Eseguire un controllo MetroCluster:

      ```
      metrocluster check run
      ```

   e. Visualizzare i risultati del controllo MetroCluster:

      ```
      metrocluster check show
      ```

   f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

      ```
      storage switch show
      ```

   g. Eseguire "Config Advisor".
   h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Ridenominazione di uno switch FC Brocade

Potrebbe essere necessario rinominare uno switch FC Brocade per garantire un nome coerente in tutta la configurazione.

Fasi

1. Disabilitare in modo persistente lo switch o gli switch in un fabric:

   `switchcfgpersistentdisable`

   L'esempio seguente mostra l'output per **`switchcfgpersistentdisable`** comando:

   ```
   7840_FCIP_2:admin> switchcfgpersistentdisable
   Switch's persistent state set to 'disabled'
   2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is DEGRADED.
   2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is OFFLINE.

   7840_FCIP_2:admin>
   ```

2. Rinominare lo switch o gli switch:

   `switchname` *`new-switch-name`*

   Se si stanno rinominando entrambi gli switch nel fabric, utilizzare lo stesso comando su ogni switch.

   L'esempio seguente mostra l'output per **`switchname` *`new-switch-name`*** comando:

   ```
   7840_FCIP_2:admin> switchname FC_switch_1_B
   Committing configuration...
   Done.
   Switch name has been changed.Please re-login into the switch for the
   change to be applied.
   2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B,
   Switch name has been successfully changed to FC_switch_1_B.
   7840_FCIP_2:admin>
   ```

3. Riavviare lo switch:

   `reboot`

   Se si stanno rinominando entrambi gli switch nel fabric, riavviare entrambi gli switch. Una volta completato il riavvio, lo switch viene rinominato in tutte le posizioni.

   L'esempio seguente mostra l'output per **`reboot`** comando:

```
7840_FCIP_2:admin> reboot
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
2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840,
System is about to reload.
Rebooting! Fri Mar  9 07:42:11 CET 2018

Broadcast message from root (ttyS0) Fri Mar  9 07:42:11 2018...

The system is going down for reboot NOW !!
INIT: Switching to runlevel: 6
INIT:
2018/03/09-07:50:48, [ESM-1013], 146104, FID 128, INFO, FC_switch_1_B,
DP0 Configuration replay has completed.
2018/03/09-07:50:48, [ESM-1011], 146105, FID 128, INFO, FC_switch_1_B,
DP0 is ONLINE.

*** CORE FILES WARNING (03/09/18 - 08:00:00 ) ***
10248 KBytes in 1 file(s)
use "supportsave" command to upload


*** FFDC FILES WARNING (03/09/18 - 08:00:00 ) ***
520 KBytes in 1 file(s)
```

4. Abilitare costantemente gli switch: **`switchcfgpersistentenable`**

   L'esempio seguente mostra l'output per **`switchcfgpersistentenable`** comando:

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch's persistent state set to 'enabled'
FC_switch_1_B:admin>
FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128,
INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B,
VE Tunnel 24 is ONLINE.

FC_switch_1_B:admin>


FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address  Media Speed   State       Proto
==================================================
   0   0   060000   id    16G     Online      FC  F-Port
50:0a:09:81:06:a5:5a:08
   1   1   060100   id    16G     Online      FC  F-Port
50:0a:09:83:06:a5:5a:08
```

5. Verificare che la modifica del nome dello switch sia visibile dal prompt del cluster ONTAP:

   `storage switch show`

   L'esempio seguente mostra l'output per **`storage switch show`** comando:

```
cluster_A::*> storage switch show
  (storage switch show)
                      Symbolic                                Is
Monitor
Switch                Name     Vendor  Model Switch WWN       Monitored
Status
--------------------- -------- ------- ----- ---------------- ---------
-------
Brocade_172.20.7.90
                      RTP-FC01-510Q40
                               Brocade Brocade7840
                                             1000c4f57c904bc8 true
ok
Brocade_172.20.7.91
                      RTP-FC02-510Q40
                               Brocade Brocade7840
                                             100050eb1a9aa579 true
ok
Brocade_172.20.7.92
```

Disattivazione della crittografia sugli switch Brocade FC

Potrebbe essere necessario disattivare la crittografia sugli switch Brocade FC.

Fasi

1. Inviare un messaggio AutoSupport da entrambi i siti indicando l'inizio della manutenzione.

```
cluster_A::> autosupport invoke -node * -type all -message MAINT=4h
```

```
cluster_B::> autosupport invoke -node * -type all -message MAINT=4h
```

2. Verificare il funzionamento della configurazione MetroCluster dal cluster A.
   a. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale: **`metrocluster show`**

   ```
   cluster_A::> metrocluster show
   ```

   b. Eseguire un controllo MetroCluster: **`metrocluster check run`**

```
cluster_A::> metrocluster check run
```

c. Visualizzare i risultati del controllo MetroCluster:
`metrocluster check show`

```
cluster_A::> metrocluster check show
```

3. Controllare lo stato di entrambi gli interruttori:

`fabric show`

```
switch_A_1:admin> fabric show
```

```
switch_B_1:admin> fabric show
```

4. Disattivare entrambi gli switch:

`switchdisable`

```
switch_A_1:admin> switchdisable
```

```
switch_B_1:admin> switchdisable
```

5. Verificare i percorsi disponibili per i nodi su ciascun cluster:

`sysconfig`

```
cluster_A::> system node run -node node-name -command sysconfig -a
```

```
cluster_B::> system node run -node node-name -command sysconfig -a
```

Poiché il fabric dello switch è ora disattivato, la configurazione dello storage di sistema dovrebbe essere ha a percorso singolo.

6. Controllare lo stato dell'aggregato per entrambi i cluster.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

L'output del sistema dovrebbe mostrare che gli aggregati sono mirrorati e normali per entrambi i cluster:

```
mirrored,normal
```

7. Ripetere i passaggi seguenti dal prompt di amministrazione su entrambi gli switch.

   a. Mostra quali porte sono crittografate:
   portenccompshow

   ```
   switch_A_1:admin> portenccompshow
   ```

   b. Disattivare la crittografia sulle porte crittografate:
   portcfgencrypt – disable *port-number*

   ```
   switch_A_1:admin> portcfgencrypt --disable 40
   switch_A_1:admin> portcfgencrypt --disable 41
   switch_A_1:admin> portcfgencrypt --disable 42
   switch_A_1:admin> portcfgencrypt --disable 43
   ```

   c. Impostare il tipo di autenticazione su tutti:

   authUtil --set -a all

```
switch_A_1:admin> authUtil --set -a all
```

   a. Impostare il criterio di autenticazione sullo switch. su off:
   authutil --policy -sw off

   ```
   switch_A_1:admin> authutil --policy -sw off
   ```

   b. Impostare il gruppo di autenticazione Diffie-Hellman su * :
   authutil --set -g *

   ```
   switch_A_1:admin> authUtil --set -g *
   ```

   c. Eliminare il database delle chiavi segrete:
   secAuthSecret --remove -all

```
switch_A_1:admin> secAuthSecret --remove -all
```

d. Verificare che la crittografia sia disattivata sulle porte:
portenccompshow

```
switch_A_1:admin> portenccompshow
```

e. Attivare lo switch:
switchenable

```
switch_A_1:admin> switchenable
```

f. Confermare lo stato degli ISL:
islshow

```
switch_A_1:admin> islshow
```

8. Verificare i percorsi disponibili per i nodi su ciascun cluster:

sysconfig

```
cluster_A::> system node run -node * -command sysconfig -a
```

```
cluster_B::> system node run -node * -command sysconfig -a
```

L'output del sistema dovrebbe indicare che la configurazione dello storage di sistema è stata nuovamente modificata in Quad-Path ha.

9. Controllare lo stato dell'aggregato per entrambi i cluster.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

Il sistema dovrebbe mostrare che gli aggregati sono mirrorati e normali per entrambi i cluster, come mostrato nell'output di sistema seguente:

```
mirrored,normal
```

10. Verificare il funzionamento della configurazione MetroCluster dal cluster A.
    a. Eseguire un controllo MetroCluster:
    metrocluster check run

    ```
    cluster_A::> metrocluster check run
    ```

    b. Visualizzare i risultati del controllo MetroCluster:
    metrocluster check show

    ```
    cluster_A::> metrocluster check show
    ```

11. Inviare un messaggio AutoSupport da entrambi i siti indicando la fine della manutenzione.

```
cluster_A::> autosupport invoke -node node-name -type all -message
MAINT=END
```

```
cluster_B::> autosupport invoke -node node-name -type all -message
MAINT=END
```

Modifica delle proprietà ISL, delle porte ISL o della configurazione IOD/OOOD su uno switch Brocade

Potrebbe essere necessario aggiungere gli ISL a uno switch se si sta aggiungendo o aggiornando hardware come controller o switch aggiuntivi o più veloci.

Prima di iniziare

Assicurarsi che il sistema sia configurato correttamente, che tutti gli switch fabric siano operativi e che non siano presenti errori.

Se l'apparecchiatura sul collegamento ISL cambia e la nuova configurazione del collegamento non supporta più la configurazione corrente----trunking e consegna ordinata----allora il fabric deve essere riconfigurato per la policy di routing corretta: In-order-delivery (IOD) o out-of-order-delivery (OOOD).

> Per apportare modifiche all'OOD dal software ONTAP, attenersi alla seguente procedura: "Configurazione della consegna in-order o out-of-order dei frame sul software ONTAP"

Fasi

1. Disattivare le porte FCVI e HBA dello storage:

   `portcfgpersistentdisable` *`port number`*

   Per impostazione predefinita, le prime 8 porte (porte da 0 a 7) vengono utilizzate per FCVI e Storage HBA. Le porte devono essere costantemente disattivate in modo che rimangano disattivate in caso di riavvio dello switch.

L'esempio seguente mostra che le porte ISL 0-7 sono disabilitate su entrambi gli switch:

```
Switch_A_1:admin> portcfgpersistentdisable 0-7
Switch_B_1:admin> portcfgpersistentdisable 0-7
```

2. Modificare le porte ISL secondo necessità.

Opzione	Fase

Per modificare la velocità di una porta ISL…	Utilizzare `portcfgspeed port number port speed` comando su entrambi gli switch del fabric.
	
	Nell'esempio seguente, la velocità della porta ISL viene modificata da 40 Gbps a 16 Gbps:
	
	`brocade_switch_A_1:admin> portcfgspeed 40 16`
	
	È possibile verificare che la velocità sia cambiata utilizzando `switchshow` comando:
	
	`brocade_switch_A_1:admin> switchshow`
	
	Viene visualizzato il seguente output:
	
	`. . .`
	`40 40 062800 id 16G No_Sync FC Disabled`
	`. . .`

Per modificare la distanza di una porta ISL…	Utilizzare `portcfglongdistance port number port distance` comando su entrambi gli switch nel fabric.
Per rimuovere un ISL…	Scollegare il tirante.
Per aggiungere un ISL…	Inserire gli SFP nelle porte che si stanno aggiungendo come porte ISL. Assicurarsi che queste porte siano elencate nella "Installare un MetroCluster collegato al fabric" per lo switch a cui si desidera aggiungerli.
Per spostare un ISL…	Il trasferimento di un ISL equivale alla rimozione e all'aggiunta di un ISL. Innanzitutto, rimuovere l'ISL scollegando il collegamento, quindi inserire gli SFP nelle porte che si stanno aggiungendo come porte ISL.

Quando si apportano modifiche alle porte ISL, potrebbe essere necessario applicare ulteriori impostazioni consigliate dal fornitore di WDM. Fare riferimento alla documentazione del fornitore WDM per le indicazioni.

3. Riconfigurare per la consegna fuori ordine (OOD) o la consegna in-order (IOD).

> Se i criteri di routing rimangono invariati, non è necessario riconfigurare e questo passaggio può essere ignorato. La configurazione ONTAP deve corrispondere alla configurazione fabric. Se il fabric è configurato per OOD, anche ONTAP deve essere configurato per OOD. Lo stesso vale per IOD.

Questo passaggio deve essere eseguito nei seguenti scenari:

- Più di un ISL ha formato una linea prima della modifica, ma dopo la modifica, il trunking non è più supportato. In questo caso, è necessario configurare il fabric per OOD.
- C'è un ISL prima della modifica e più ISL dopo la modifica.
- Se più ISL formano una linea, configurare la struttura per IOD. Se più ISL **non possono** formare un trunk, configurare il fabric per OOD.
- Disattivare in modo persistente gli switch utilizzando `switchcfgpersistentdisable` come illustrato nell'esempio seguente:

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

i. Configurare la modalità trunking per ogni ISL `portcfgtrunkport port number` come mostrato nella seguente tabella:

Scenario	Fasi

Configurare l'ISL per il trunking (IOD)	Impostare `portcfgtrunkport port number` a 1:
	`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`

Configurare l'ISL per il trunking	Impostare `portcfgtrunkport port number` a 0:
	`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`

ii. Configurare il fabric per IOD o OOOD secondo necessità.

Scenario	Fasi

Configurare il fabric per IOD	Impostare le tre impostazioni di IOD, APT e DLS utilizzando `iodset`, `aptpolicypolicy`, e. `dlsreset` comandi come mostrato nell'esempio seguente:
	
	`Switch_A_1:admin> iodset`
	`Switch_A_1:admin> aptpolicy 1`
	`Policy updated successfully.`
	`Switch_A_1:admin> dlsreset`
	`FC_switch_A_1:admin>portcfgtrunkport 40 1`
	`FC_switch_A_1:admin>portcfgtrunkport 41 1`
	
	`Switch_B_1:admin> iodset`
	`Switch_B_1:admin> aptpolicy 1`
	`Policy updated successfully.`
	`Switch_B_1:admin> dlsreset`
	`FC_switch_B_1:admin>portcfgtrunkport 20 1`
	`FC_switch_B_1:admin>portcfgtrunkport 21 1`

Configurare il fabric per OOD	Impostare le tre impostazioni di IOD, APT e DLS utilizzando `iodreset`, `aptpolicy`*`policy`*, e. `dlsset` comandi come mostrato nell'esempio seguente:
	
	`Switch_A_1:admin> iodreset`
	`Switch_A_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_A_1:admin> dlsset`
	`FC_switch_A_1:admin> portcfgtrunkport 40 0`
	`FC_switch_A_1:admin> portcfgtrunkport 41 0`
	
	`Switch_B_1:admin> iodreset`
	`Switch_B_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_B_1:admin> dlsset`
	`FC_switch_B_1:admin> portcfgtrunkport 40 0`
	`FC_switch_B_1:admin> portcfgtrunkport 41 0`

iii. Abilitare gli switch in modo persistente:

`switchcfgpersistentenable`

```
switch_A_1:admin>switchcfgpersistentenable
switch_B_1:admin>switchcfgpersistentenable
```

+ Se questo comando non esiste, utilizzare `switchenable` come illustrato nell'esempio seguente:

```
brocade_switch_A_1:admin>
switchenable
```

i. Verificare le impostazioni OOOD utilizzando `iodshow`, `aptpolicy`, e. `dlsshow` comandi come mostrato nell'esempio seguente:

```
switch_A_1:admin> iodshow
IOD is not set

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

switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

È necessario eseguire questi comandi su entrambi gli switch.

ii. Verificare le impostazioni IOD utilizzando `iodshow`, `aptpolicy`, e. `dlsshow` comandi come mostrato nell'esempio seguente:

```
switch_A_1:admin> iodshow
IOD is set

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

switch_A_1:admin> dlsshow
DLS is not set
```

È necessario eseguire questi comandi su entrambi gli switch.

4. Verificare che gli ISL siano online e trunked (se l'apparecchiatura di collegamento supporta il trunking) utilizzando `islshow` e. `trunkshow` comandi.

Se FEC è attivato, il valore di disallineamento dell'ultima porta online del fascio di linee potrebbe mostrare una differenza fino a 36, anche se i cavi sono tutti della stessa lunghezza.

Gli ISL sono trunked?	Viene visualizzato il seguente output di sistema…

Sì	Se gli ISL sono trunked, nell'output di viene visualizzato solo un ISL singolo `islshow` comando. A seconda del trunk master, è possibile visualizzare la porta 40 o 41. L'output di `trunkshow` Se una linea con ID "1" elenca entrambi gli ISL fisici sulle porte 40 e 41. Nell'esempio seguente, le porte 40 e 41 sono configurate per l'utilizzo come ISL:
	`switch_A_1:admin> islshow 1:`
	`40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 32.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER`
	`41-> 41 10:00:00:05:33:88:9c:68 2 deskew 15`

No	Se gli ISL non sono trunked, entrambi gli ISL vengono visualizzati separatamente negli output per `islshow` e. `trunkshow`. Entrambi i comandi elencano gli ISL con il loro ID “1” e “2”. Nell’esempio seguente, le porte “40” e “41” sono configurate per l’utilizzo come ISL:
	
	`switch_A_1:admin> islshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC`
	`2: 41-> 41 10:00:00:05:33:88:9c:68 2 switch_B_1 sp: 16.000G bw: 16.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40 10:00:00:05:33:88:9c:68 2 deskew 51 MASTER`
	`2: 41-> 41 10:00:00:05:33:88:9c:68 2 deskew 48 MASTER`

5. Eseguire `spinfab` Su entrambi gli switch per verificare che gli ISL siano integri:

```
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. Attivare le porte disattivate al passaggio 1:

   `portenable` *`port number`*

   L’esempio seguente mostra le porte ISL da “0” a “7” attivate:

```
brocade_switch_A_1:admin> portenable 0-7
```

Sostituzione di uno switch FC Cisco

Per sostituire uno switch FC Cisco guasto, è necessario utilizzare i passaggi specifici di Cisco.

Prima di iniziare

È necessaria la password admin e l’accesso a un server FTP o SCP.

A proposito di questa attività

Questa procedura è senza interruzioni e richiede circa due ore per essere completata.

Negli esempi di questa procedura, FC_switch_A_1 è lo switch integro e FC_switch_B_1 è lo switch compromesso. L’utilizzo della porta dello switch negli esempi è illustrato nella seguente tabella:

Ruolo	Porte
Connessioni FC-VI	1, 4

Connessioni HBA	2, 3, 5, 6
Connessioni bridge FC-SAS	7, 8
Connessioni ISL	36, 40

Gli esempi mostrano due bridge FC-SAS. Se si dispone di altre porte, è necessario disattivarle e attivarle successivamente.

L'utilizzo della porta dello switch deve seguire le assegnazioni consigliate.

- "Assegnazioni delle porte per switch FC quando si utilizza ONTAP 9.0"
- "Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Fasi

1. Disattivare le porte ISL sullo switch integro per escludere lo switch compromesso.

   Questi passaggi vengono eseguiti sullo switch integro.

   a. Accedere alla modalità di configurazione:
   `conf t`

   b. Disattivare le porte ISL sullo switch integro con `interface` e. `shut` comandi.

   ```
   FC_switch_A_1# conf t
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config)# shut
   FC_switch_A_1(config)# interface fc1/40
   FC_switch_A_1(config)# shut
   ```

   c. Uscire dalla modalità di configurazione e copiare la configurazione nella configurazione di avvio.

   ```
   FC_switch_A_1(config)# end
   FC_switch_A_1# copy running-config startup-config
   FC_switch_A_1#
   ```

2. Disfare le porte FC-VI e HBA dello switch non funzionante (se ancora in funzione).

   Questi passaggi vengono eseguiti sullo switch compromesso.

   a. Accedere alla modalità di configurazione:

   `conf t`

   b. Se lo switch non funzionante è ancora in funzione, disattivare le porte FC-VI e HBA sullo switch non funzionante con i comandi di interfaccia e di chiusura.

```
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
```

c. Uscire dalla modalità di configurazione e copiare la configurazione nella configurazione di avvio.

```
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. Se lo switch non funzionante è ancora in funzione, determinare il numero WWN dello switch:

   `show wwn switch`

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:e3:86:50
FC_switch_B_1#
```

4. Avviare e preconfigurare lo switch sostitutivo prima di installarlo fisicamente.

   A questo punto, lo switch sostitutivo non viene collegato alla configurazione MetroCluster. Le porte ISL sullo switch partner sono disattivate (in modalità di chiusura) e offline.

   a. Accendere lo switch sostitutivo e lasciarlo avviare.
   b. Controllare la versione del firmware sullo switch sostitutivo per verificare che corrisponda alla versione degli altri switch FC:

      `show version`

   c. Configurare lo switch sostitutivo come descritto nella *Guida all'installazione e alla configurazione di MetroCluster*, ignorando la sezione "Configurazione dello zoning su uno switch FC Cisco".

      "Installazione e configurazione di Fabric-Attached MetroCluster"

   La configurazione dello zoning verrà eseguita più avanti in questa procedura.

   a. Disattivare le porte FC-VI, HBA e storage sullo switch sostitutivo.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/7-8
FC_switch_B_1(config)# shut
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

5. Sostituire fisicamente lo switch compromesso:
   a. Spegnere l'interruttore per i problemi.
   b. Spegnere lo switch sostitutivo.
   c. Scollegare e rimuovere lo switch compromesso, prestando attenzione a quali cavi sono collegati a quali porte.
   d. Installare lo switch sostitutivo nel rack.
   e. Collegare lo switch sostitutivo esattamente come lo switch compromesso era cablato.
   f. Accendere lo switch sostitutivo.
6. Abilitare le porte ISL sullo switch sostitutivo.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#
```

7. Verificare che le porte ISL dello switch sostitutivo siano in funzione:

```
show interface brief
```

8. Regolare lo zoning sullo switch sostitutivo in modo che corrisponda alla configurazione MetroCluster:
   a. Distribuire le informazioni di zoning dal fabric sano.

      In questo esempio, FC_switch_B_1 è stato sostituito e le informazioni di zoning sono recuperate da FC_switch_A_1:

```
FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end
```

b. Sullo switch sostitutivo, verificare che le informazioni di zoning siano state recuperate correttamente dallo switch integro:

```
show zone
```

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. Individuare i WWN degli switch.

In questo esempio, i due WWN dello switch sono i seguenti:

- FC_switch_A_1: 20:00:54:7f:ee:b8:24:c0
- FC_switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

d. Rimuovere i membri di zona che non appartengono ai WWN dei due switch.

   In questo esempio, “no member interface” nell’output indica che i seguenti membri non sono associati al WWN dello switch di uno dei due switch del fabric e devono essere rimossi:

   - Nome della zona FC-VI_zone_1_10 vsan 10
     - interfaccia fc1/1 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/2 swwn 20:00:54:7f:ee:e3:86:50
   - Nome zona STOR_zone_1_20_25A vsan 20
     - interfaccia fc1/5 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/11 swwn 20:00:54:7f:ee:e3:86:50
   - Nome zona STOR_zone_1_20_25B vsan 20
     - interfaccia fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - interfaccia fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/11 swwn 20:00:54:7f:ee:e3:86:50 il seguente esempio mostra la rimozione di queste interfacce:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan
20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

e. Aggiungere le porte dello switch sostitutivo alle zone.

   Tutti i cavi dello switch sostitutivo devono essere identici a quelli dello switch compromesso:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

f. Verificare che lo zoning sia configurato correttamente:

```
show zone
```

Il seguente esempio di output mostra le tre zone:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

g. Abilitare la connettività allo storage e ai controller.

   L’esempio seguente mostra l’utilizzo della porta:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      `node run -node node-name sysconfig -a`

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      `system health alert show`

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      `metrocluster show`

   d. Eseguire un controllo MetroCluster:

      `metrocluster check run`

   e. Visualizzare i risultati del controllo MetroCluster:

      `metrocluster check show`

   f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

      `storage switch show`

   g. Eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Modifica della velocità delle porte ISL su uno switch FC Cisco

Potrebbe essere necessario modificare la velocità delle porte ISL su uno switch per

migliorare la qualità dell'ISL. Gli ISL che viaggiano su distanze maggiori potrebbero aver bisogno di una riduzione della velocità per migliorare la qualità.

Per garantire la connettività ISL, è necessario completare tutti i passaggi su entrambi gli switch.

1. Disattivare le porte ISL degli ISL che si desidera modificare in base alla velocità di su entrambi gli switch del fabric:

   FC_switch_A_1# config t

   Immettere i comandi di configurazione, uno per riga. Terminare con CTRL-Z dopo aver immesso tutti i comandi di configurazione.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# shut
      FC_switch_A_1(config)# end
   ```

2. Modificare la velocità delle porte ISL su entrambi gli switch del fabric:

   FC_switch_A_1# config t

   Immettere i comandi di configurazione, uno per riga. Terminare con CTRL-Z dopo aver immesso tutti i comandi di configurazione.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# switchport speed 16000
   ```

   > Le velocità delle porte sono 16 = 16,000 Gbps, 8 = 8,000 Gbps, 4 = 4,000 Gbps.

   Assicurarsi che queste porte ISL per lo switch siano elencate nella *Guida all'installazione e alla configurazione di Fabric-Attached MetroCluster*.

3. Abilitare tutte le porte ISL (se non attivate) su entrambi gli switch del fabric:

   FC_switch_A_1# config t

   Immettere i comandi di configurazione, uno per riga. Terminare con CTRL-Z dopo aver immesso tutti i comandi di configurazione.

   ```
   FC_switch_A_1(config)# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

4. Verificare che gli ISL siano stati stabiliti tra entrambi gli switch:

   show topology isl

```
-----------------------------------------------------------------------
--------
    __________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

-----------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

5. Ripetere la procedura per il secondo fabric dello switch.

Aggiunta di LSL a uno switch Cisco

Potrebbe essere necessario aggiungere gli ISL a uno switch se si sta aggiungendo o aggiornando hardware come controller aggiuntivi o più veloci o switch più veloci.

Per garantire la connettività ISL, è necessario completare anche i passaggi completati su uno switch.

Fasi

1. Disattivare le porte ISL degli ISL da aggiungere su entrambi gli switch del fabric:

   `FC_switch_A_1#config t`

   Immettere i comandi di configurazione, uno per riga. Terminare con CTRL-Z dopo aver inserito tutti i comandi di configurazione.

   ```
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end
   ```

2. Inserire gli SFP nelle porte che si stanno aggiungendo come porte ISL e cablarli come indicato nella *Guida all'installazione e alla configurazione*.

   Assicurarsi che queste porte siano elencate nella *Guida all'installazione e alla configurazione* dello switch a cui si desidera aggiungerle.

3. Configurare le porte ISL in base alla *Guida all'installazione e alla configurazione*.

4. Abilitare tutte le porte ISL (se non attivate) su entrambi gli switch del fabric:

   FC_switch_A_1# config t

   Immettere i comandi di configurazione, uno per riga. Terminare con CTRL-Z.

   ```
   FC_switch_A_1# interface fc1/36
      FC_switch_A_1(config-if)# no shut
      FC_switch_A_1(config)# end
   ```

5. Verificare che gli ISL siano stati stabiliti tra entrambi gli switch:

   show topology isl

6. Ripetere la procedura sul secondo fabric:

   ```
   ---------------------------------------------------------------------------
   --------
       __________Local_________ _________Remote_________ VSAN Cost I/F  PC
   I/F  Band
        PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
   Speed width

   ---------------------------------------------------------------------------
   --------
         1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
   16g   64g
         1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
   16g   64g
   ```

Modificare il vendor o il modello di uno switch FC

Potrebbe essere necessario cambiare il vendor di uno switch FC da Cisco a Brocade o viceversa, modificare il modello dello switch o entrambi.

A proposito di questa attività

- Questa procedura si applica quando si utilizzano interruttori convalidati NetApp.
- È necessario eseguire i passaggi di questa procedura su un tessuto alla volta, per entrambi i fabric nella configurazione.

Fasi

1. controllare lo stato della configurazione.

   a. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verificare che il mirroring sia attivato su ciascun nodo: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Verificare che i componenti di MetroCluster siano in buone condizioni: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

   d. Verificare che non siano presenti avvisi sullo stato di salute: **`system health alert show`**

2. Configurare il nuovo switch prima dell'installazione.

   Seguire la procedura descritta in "Configurare gli switch FC".

3. Scollegare i collegamenti dal vecchio interruttore staccando i collegamenti nell'ordine seguente:
   a. Se le interfacce del cluster locale sono collegate a uno switch:
      i. Scollegare le interfacce del cluster locale
      ii. Disconnettere gli ISL del cluster locale
   b. Scollegare le interfacce FC MetroCluster.
   c. Scollegare gli ISL MetroCluster.
4. Spegnere il vecchio interruttore, rimuovere i cavi e sostituire fisicamente il vecchio interruttore con il nuovo.
5. Collegare gli interruttori nel seguente ordine:

   È necessario seguire la procedura descritta in "Installare e cablare i componenti dell'MetroCluster".

   a. Collegare gli ISL al sito remoto.
   b. Collegare le interfacce FC MetroCluster.
   c. Collegare le interfacce del cluster locale.

      Se le interfacce del cluster locale sono collegate a uno switch:

      i. Collegare le interfacce del cluster locale.
      ii. Collegare via cavo gli ISL del cluster locale.
6. Accendere l'interruttore.

7. Verificare che la configurazione di MetroCluster sia corretta ripetendo la configurazione [Fase 1].
8. Ripetere i passaggi da 1 a 7 per il secondo fabric nella configurazione.

Manutenzione e sostituzione dello switch IP

Sostituire uno switch IP o modificare l'utilizzo degli switch IP MetroCluster esistenti

Potrebbe essere necessario sostituire uno switch guasto, aggiornare o eseguire il downgrade di uno switch o modificare l'utilizzo degli switch IP MetroCluster esistenti.

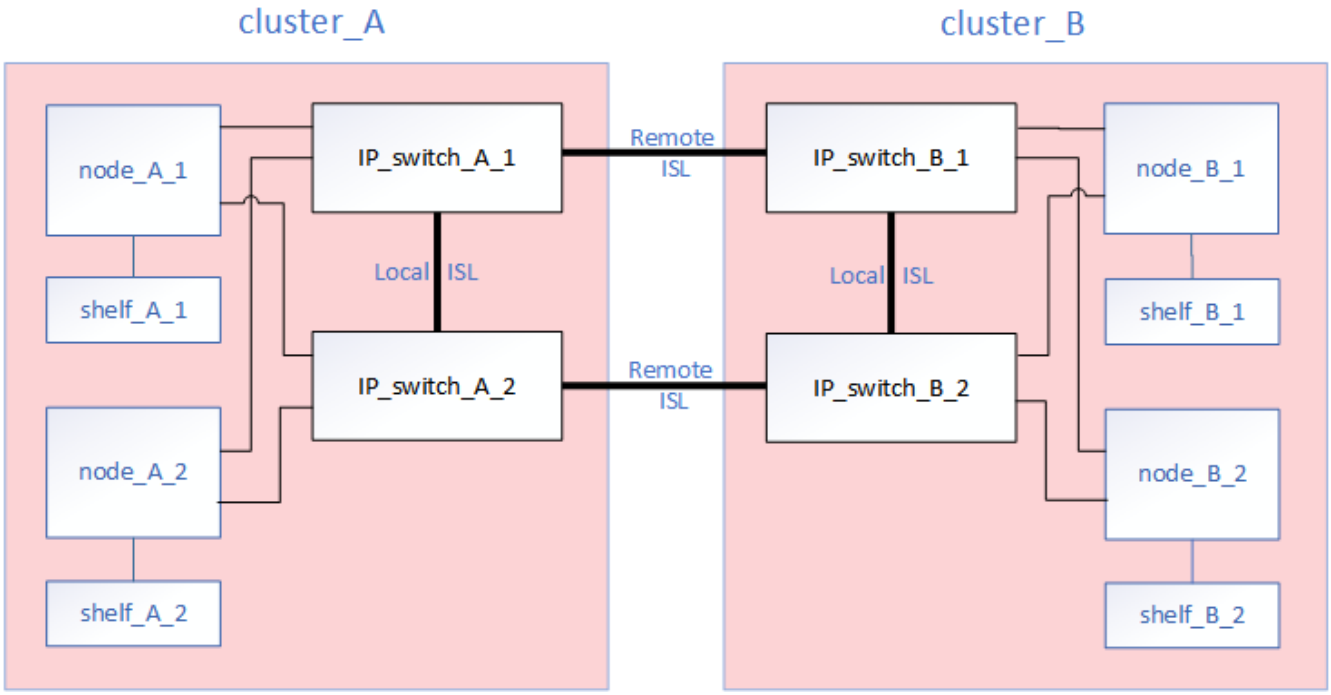
Questa procedura si applica quando si utilizzano switch validati da NetApp. Se si utilizzano switch compatibili con MetroCluster, rivolgersi al fornitore dello switch.

Questa procedura supporta le seguenti conversioni:

- Modifica del vendor, del tipo o di entrambi gli switch. Il nuovo switch può essere lo stesso del vecchio switch in caso di guasto oppure è possibile modificare il tipo di switch (aggiornare o eseguire il downgrade dello switch).

  Ad esempio, per espandere una configurazione MetroCluster IP da una singola configurazione a quattro nodi utilizzando controller AFF A400 e switch BES-53248 a una configurazione a otto nodi utilizzando controller AFF A400, è necessario modificare gli switch in un tipo supportato per la configurazione, in quanto gli switch BES-53248 non sono supportati nella nuova configurazione.

  Se si desidera sostituire uno switch guasto con lo stesso tipo di switch, sostituire solo lo switch guasto. Se si desidera aggiornare o eseguire il downgrade di uno switch, è necessario regolare due switch che si trovano nella stessa rete. Due switch si trovano nella stessa rete quando sono collegati con un collegamento inter-switch (ISL) e non si trovano nello stesso sito. Ad esempio, la rete 1 include IP_switch_A_1 e IP_switch_B_1, mentre la rete 2 include IP_switch_A_2 e IP_switch_B_2, come mostrato nel diagramma seguente:



> Se si sostituisce uno switch o si esegue l'aggiornamento a switch diversi, è possibile preconfigurare gli switch installando il firmware dello switch e il file RCF.

- Convertire una configurazione IP MetroCluster in una configurazione IP MetroCluster utilizzando switch MetroCluster di storage condiviso.

  Ad esempio, se si dispone di una configurazione MetroCluster IP regolare utilizzando i controller AFF A700 e si desidera riconfigurare MetroCluster per collegare gli shelf NS224 agli stessi switch.

  > - Se si aggiungono o rimuovono shelf in una configurazione MetroCluster IP utilizzando switch MetroCluster IP storage condiviso, seguire la procedura descritta in "Aggiunta di shelf a un MetroCluster IP utilizzando switch MetroCluster per lo storage condiviso"
  > - La configurazione IP di MetroCluster potrebbe già essere collegata direttamente agli shelf NS224 o a switch di storage dedicati.

Foglio di lavoro sull'utilizzo delle porte

Di seguito viene riportato un esempio di foglio di lavoro per la conversione di una configurazione MetroCluster IP in una configurazione storage condivisa che collega due shelf NS224 utilizzando gli switch esistenti.

Definizioni dei fogli di lavoro:

- Configurazione esistente: Il cablaggio della configurazione MetroCluster esistente.
- Nuova configurazione con shelf NS224: La configurazione di destinazione in cui gli switch sono condivisi tra lo storage e MetroCluster.

I campi evidenziati in questo foglio di lavoro indicano quanto segue:

- Verde: Non è necessario modificare il cablaggio.
- Giallo: È necessario spostare le porte con la stessa configurazione o con una configurazione diversa.
- Blu: Porte nuove connessioni.

PORT USAGE OVERVIEW Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G							
Switch port	Existing configuration				New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2		Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'		MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'			Cluster Port 'A'	Cluster Port 'B'
3							
4							
5					Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6						NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster			ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'		MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'			Port 'A'	Port 'B'
11							
12							
13					ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14							
15							
16							
17					MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18						Storage Port 'A'	Storage Port 'B'
19							
20							
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G		Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22						NSM-B, e0a	NSM-B, e0b
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							
34							
35							
36							

Fasi

1. controllare lo stato della configurazione.

   a. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verificare che il mirroring sia attivato su ciascun nodo: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

   c. Verificare che i componenti di MetroCluster siano in buone condizioni: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Verificare che non siano presenti avvisi sullo stato di salute: **`system health alert show`**

2. Configurare il nuovo switch prima dell'installazione.

   Se si stanno riutilizzando gli switch esistenti, passare a. Fase 4.

   > Se si stanno aggiornando o eseguendo il downgrade degli switch, è necessario configurare tutti gli switch della rete.

   Seguire le istruzioni della sezione *Configurazione degli switch IP* in "Installazione e configurazione di MetroCluster IP."

   Assicurarsi di applicare il file RCF corretto per lo switch _A_1, _A_2, _B_1 o _B_2. Se il nuovo switch è lo stesso del vecchio switch, è necessario applicare lo stesso file RCF.

   Se si esegue l'aggiornamento o il downgrade di uno switch, applicare il file RCF più recente supportato per il nuovo switch.

3. Eseguire il comando port show per visualizzare le informazioni relative alle porte di rete:

   `network port show`

   a. Modifica tutte le LIF del cluster per disattivare l'indirizzamento automatico:

   ```
   network interface modify -vserver <vserver_name> -lif <lif_name>
   -auto-revert false
   ```

4. Disconnetti le connessioni dal vecchio switch.

> Si scollegano solo le connessioni che non utilizzano la stessa porta nelle configurazioni precedenti e nuove. Se si utilizzano nuovi switch, è necessario scollegare tutte le connessioni.

Rimuovere i collegamenti nel seguente ordine:

a. Scollegare le interfacce del cluster locale
b. Disconnettere gli ISL del cluster locale
c. Scollegare le interfacce IP di MetroCluster
d. Disconnettere gli ISL MetroCluster

   Nell'esempio [port_usage_worksheet], gli switch non cambiano. Gli ISL MetroCluster vengono ricollocati e devono essere disconnessi. Non è necessario scollegare le connessioni contrassegnate in verde sul foglio di lavoro.

5. Se si utilizzano nuovi switch, spegnere il vecchio switch, rimuovere i cavi e rimuovere fisicamente il vecchio switch.

   Se si stanno riutilizzando gli switch esistenti, passare a. Fase 6.

   > Non collegare * i nuovi switch ad eccezione dell'interfaccia di gestione (se utilizzata).

6. Configura gli switch esistenti.

   Se gli switch sono già stati preconfigurati, è possibile saltare questo passaggio.

   Per configurare gli switch esistenti, seguire la procedura per installare e aggiornare il firmware e i file RCF:

   - "Aggiornamento del firmware sugli switch IP MetroCluster"
   - "Aggiornare i file RCF sugli switch IP MetroCluster"

7. Collegare gli switch.

   Seguire la procedura descritta nella sezione *collegamento degli switch IP* di "Installazione e configurazione di MetroCluster IP".

   Collegare gli switch nel seguente ordine (se necessario):

   a. Collegare gli ISL al sito remoto.
   b. Collegare le interfacce IP di MetroCluster.
   c. Collegare le interfacce del cluster locale.

   > - Se il tipo di switch è diverso, le porte utilizzate potrebbero essere diverse da quelle del vecchio switch. Se si stanno aggiornando o eseguendo il downgrade degli switch, **NON** collegare gli ISL locali. Collegare gli ISL locali solo se si aggiornano o si esegue il downgrade degli switch nella seconda rete e entrambi gli switch in un sito sono dello stesso tipo e del medesimo cablaggio.
   > - Se si sta aggiornando Switch-A1 e Switch-B1, eseguire i passaggi da 1 a 6 per gli switch Switch-A2 e Switch-B2.

8. Finalizzare il cablaggio del cluster locale.

a. Se le interfacce del cluster locale sono collegate a uno switch:

   i. Collegare via cavo gli ISL del cluster locale.

b. Se le interfacce del cluster locale sono **non** collegate a uno switch:

   i. Utilizzare "Migrare a un ambiente cluster NetApp con switch" procedura per convertire un cluster senza switch in un cluster con switch. Utilizzare le porte indicate nella "Installazione e configurazione di MetroCluster IP" Oppure i file di cablaggio RCF per collegare l'interfaccia cluster locale.

9. Accendere lo switch o gli switch.

   Se il nuovo switch è lo stesso, accendere il nuovo switch. Se si stanno aggiornando o eseguendo il downgrade degli switch, accendere entrambi gli switch. La configurazione può funzionare con due switch diversi in ogni sito fino all'aggiornamento della seconda rete.

10. Verificare che la configurazione di MetroCluster sia corretta ripetendo la configurazione Fase 1.

    Se si aggiornano o si esegue il downgrade degli switch nella prima rete, potrebbero essere visualizzati alcuni avvisi relativi al clustering locale.

    > Se si esegue l'aggiornamento o il downgrade delle reti, ripetere tutti i passaggi per la seconda rete.

11. Modifica tutte le LIF del cluster per riattivare l'indirizzamento automatico:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. In alternativa, spostare gli shelf NS224.

    Se si sta riconfigurando una configurazione IP MetroCluster che non collega gli shelf NS224 agli switch IP MetroCluster, utilizzare la procedura appropriata per aggiungere o spostare gli shelf NS224:

    - "Aggiunta di shelf a un MetroCluster IP utilizzando switch MetroCluster per lo storage condiviso"
    - "Migrazione da un cluster senza switch con storage direct-attached"
    - "Migrare da una configurazione senza switch con storage collegato a switch riutilizzando gli switch storage"

Aggiornamento del firmware sugli switch IP MetroCluster

Potrebbe essere necessario aggiornare il firmware su uno switch IP MetroCluster.

È necessario ripetere questa attività su ciascuno switch in successione.

Fasi

1. Controllare lo stato della configurazione.

   a. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster:

```
metrocluster show
```

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

b. Verificare che il mirroring sia attivato su ciascun nodo:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Verificare che i componenti di MetroCluster siano in buone condizioni:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

a. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Installare il software sul primo switch.

> È necessario installare il software dello switch sugli switch nel seguente ordine: Switch_A_1, switch_B_1, switch_A_2, switch_B_2.

Seguire i passaggi per l'installazione del software dello switch nell'argomento pertinente delle informazioni *Installazione e configurazione IP MetroCluster* a seconda che il tipo di switch sia Broadcom o Cisco:

- "Download e installazione del software EFOS dello switch Broadcom"
- "Download e installazione del software NX-OS dello switch Cisco"

3. Ripetere il passaggio precedente per ciascuno degli switch.
4. Ripetere il passaggio 1 per verificare lo stato della configurazione.

Aggiornare i file RCF sugli switch IP MetroCluster

Potrebbe essere necessario aggiornare un file RCF su uno switch IP MetroCluster. Ad esempio, se la versione del file RCF in esecuzione sugli switch non è supportata dalla versione ONTAP, dalla versione firmware dello switch o da entrambe.

Verificare che il file RCF sia supportato

Se si sta modificando la versione di ONTAP o la versione del firmware dello switch, è necessario verificare di disporre di un file RCF supportato per tale versione. Se si utilizza il generatore RCF, viene generato il file RCF corretto.

Fasi

1. Utilizzare i seguenti comandi degli switch per verificare la versione del file RCF:

Da questo switch…	Eseguire questo comando…
Switch Broadcom	`(IP_switch_A_1) # show clibanner`
Switch Cisco	`IP_switch_A_1# show banner motd`

   Per entrambi gli switch, individuare la riga nell'output che indica la versione del file RCF. Ad esempio, il seguente output proviene da uno switch Cisco, che indica che la versione del file RCF è "v1.80".

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Per controllare quali file sono supportati per una versione, uno switch e una piattaforma ONTAP specifici, utilizzare RcfFileGenerator. Se è possibile generare il file RCF per la configurazione in uso o a cui si desidera eseguire l'aggiornamento, il file è supportato.
3. Per verificare che il firmware dello switch sia supportato, fare riferimento a quanto segue:
   - "Hardware Universe"
   - "Interoperabilità NetApp"

Aggiornare i file RCF

Se si sta installando un nuovo firmware dello switch, è necessario installare il firmware dello switch prima di aggiornare il file RCF.

A proposito di questa attività

- Questa procedura interrompe il traffico sullo switch in cui viene aggiornato il file RCF. Il traffico riprenderà una volta applicato il nuovo file RCF.
- Eseguire le operazioni su un interruttore alla volta, nell'ordine seguente: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

Fasi

1. Verificare lo stato della configurazione.

   a. Verificare che i componenti di MetroCluster siano integri:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

      L'operazione viene eseguita in background.

   b. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

      Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id 38
```

b. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire la procedura per il fornitore dello switch:

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"
   - "Ripristino delle impostazioni predefinite dello switch NVIDIA IP SN2100"

3. Scaricare e installare il file RCF IP, a seconda del fornitore dello switch.
   - "Download e installazione dei file Broadcom IP RCF"
   - "Download e installazione dei file Cisco IP RCF"
   - "Download e installazione dei file RCF NVIDIA IP"

> Se si dispone di una configurazione di rete L2 condivisa o L3, potrebbe essere necessario regolare le porte ISL sugli switch intermedi/clienti. La modalità switchport potrebbe passare dalla modalità 'access' alla modalità 'trunk'. Procedere all'aggiornamento della seconda coppia di switch (A_2, B_2) solo se la connettività di rete tra gli switch A_1 e B_1 è completamente operativa e la rete funziona correttamente.

Aggiornare i file RCF sugli switch IP Cisco utilizzando CleanUpFiles

Potrebbe essere necessario aggiornare un file RCF su uno switch IP Cisco. Ad esempio, un aggiornamento ONTAP o un aggiornamento del firmware dello switch richiedono un nuovo file RCF.

A proposito di questa attività

- A partire dalla versione 1.4a di RcfFileGenerator, è disponibile una nuova opzione per modificare (aggiornare, eseguire il downgrade o sostituire) la configurazione dello switch sugli switch IP Cisco senza eseguire una "cancellazione in scrittura".
- Lo switch Cisco 9336C-FX2 è dotato di due tipi di storage di switch diversi con nomi diversi nell'RCF. Utilizzare la tabella seguente per determinare il tipo di storage Cisco 9336C-FX2 corretto per la propria configurazione:

Se si sta collegando il seguente dispositivo di archiviazione…	Scegliere il tipo di storage Cisco 9336C-FX2…	Banner/MOTD file RCF di esempio
• Shelf SAS collegati direttamente • Shelf NVMe connessi direttamente • Shelf NVMe connessi a switch storage dedicati	9336C-FX2 - solo archiviazione diretta	`* Switch : NX9336C (direct storage, L2 Networks, direct ISL)`
• Shelf SAS collegati direttamente • Shelf NVMe connessi agli switch IP MetroCluster È richiesto almeno uno shelf NVMe connesso a Ethernet	9336C-FX2 – Storage SAS ed Ethernet	`* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)`

Prima di iniziare

È possibile utilizzare questo metodo se la configurazione soddisfa i seguenti requisiti:

- Viene applicata la configurazione RCF standard.
- Il "RcfFileGenerator" Deve essere in grado di creare lo stesso file RCF applicato, con la stessa versione e configurazione (piattaforme, VLAN).
- Il file RCF applicato non è stato fornito da NetApp per una configurazione speciale.
- Il file RCF non è stato modificato prima dell'applicazione.
- Prima di applicare il file RCF corrente, sono state seguite le procedure per ripristinare le impostazioni predefinite dello switch.
- Non sono state apportate modifiche alla configurazione dello switch (porta) dopo l'applicazione dell'RCF.

  Se non si soddisfano questi requisiti, non è possibile utilizzare i CleanUpFiles creati durante la generazione dei file RCF. Tuttavia, è possibile sfruttare la funzione per creare file CleanUpFiles generici — la pulitura che utilizza questo metodo deriva dall'output di `show running-config` ed è la best practice.

È necessario aggiornare gli switch nel seguente ordine: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. In alternativa, è possibile aggiornare gli switch Switch_A_1 e Switch_B_1 contemporaneamente, seguiti dagli switch Switch_A_2 e Switch_B_2.

Fasi

1. Determinare la versione corrente del file RCF e le porte e le VLAN utilizzate: `IP_switch_A_1# show banner motd`

   È necessario ottenere queste informazioni da tutti e quattro gli switch e completare la seguente tabella di informazioni.

```
* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*              MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*

#
IP_switch_A_1#
```

Da questo output, è necessario raccogliere le informazioni mostrate nelle due tabelle seguenti.

Informazioni generiche	MetroCluster	Dati
Versione del file RCF		1.81

Tipo di switch		NX9336
Tipologia di rete		Reti L2, ISL diretto
Tipo di storage		Storage SAS
Piattaforme	1	AFF A400
	2	FAS9000

Informazioni sulla VLAN	Rete	Configurazione di MetroCluster	Switchport	Sito A	Sito B
Cluster locale VLAN	Rete 1	1	1, 2	111	222
		2	3, 4	151	251
	Rete 2	1	1, 2	111	222
		2	3, 4	151	251
VLAN MetroCluster	Rete 1	1	9, 10	119	119
		2	11, 12	159	159
	Rete 2	1	9, 10	219	219
		2	11, 12	259	259

2. Crea i file RCF e CleanUpFiles oppure crea file generici per la configurazione corrente.

   Se la configurazione soddisfa i requisiti indicati nei prerequisiti, selezionare **opzione 1**. Se la configurazione **non** soddisfa i requisiti indicati nei prerequisiti, selezionare **opzione 2**.

Opzione 1: Creare i file RCF e CleanUpFiles

Utilizzare questa procedura se la configurazione soddisfa i requisiti.

Fasi

a. Utilizzare RcfFileGenerator 1.4a (o versione successiva) per creare i file RCF con le informazioni recuperate nel passaggio 1. La nuova versione di RcfFileGenerator crea un set aggiuntivo di CleanUpFiles che è possibile utilizzare per ripristinare alcune configurazioni e preparare lo switch ad applicare una nuova configurazione RCF.

b. Confrontare il motd del banner con i file RCF attualmente applicati. I tipi di piattaforma, il tipo di switch, la porta e l'utilizzo della VLAN devono essere identici.

> È necessario utilizzare CleanUpFiles della stessa versione del file RCF e per la stessa configurazione. L'utilizzo di CleanUpFile non funziona e potrebbe richiedere un ripristino completo dello switch.

> La versione di ONTAP per la quale viene creato il file RCF non è rilevante. È importante solo la versione del file RCF.

> Il file RCF (anche se è della stessa versione) potrebbe elencare un numero inferiore o superiore di piattaforme. Assicurarsi che la piattaforma sia presente nell'elenco.

Opzione 2: Creazione di file CleanUpFiles generici

Utilizzare questa procedura se la configurazione **non** soddisfa tutti i requisiti.

Fasi

a. Recuperare l'output di `show running-config` da ogni switch.

b. Aprire lo strumento RcfFileGenerator e fare clic su "Create generic CleanUpFiles" (Crea file di pulizia generici) nella parte inferiore della finestra

c. Copiare l'output recuperato al punto 1 dal commutatore 'uno' nella finestra superiore. È possibile rimuovere o lasciare l'output predefinito.

d. Fare clic su "Create CUF Files" (Crea file CUF).

e. Copiare l'output dalla finestra inferiore in un file di testo (questo file è CleanUpFile).

f. Ripetere i passaggi c, d ed e per tutti gli switch della configurazione.

   Al termine di questa procedura, si dovrebbero avere quattro file di testo, uno per ogni switch. È possibile utilizzare questi file nello stesso modo dei CleanUpFiles che è possibile creare utilizzando l'opzione 1.

3. Crea i "nuovi" file RCF per la nuova configurazione. Creare questi file nello stesso modo in cui sono stati creati nel passaggio precedente, ad eccezione della scelta della versione del file ONTAP e RCF corrispondente.

   Dopo aver completato questo passaggio, si dovrebbero avere due set di file RCF, ciascuno costituito da dodici file.

4. Scaricare i file sul bootflash.

   a. Scaricare i CleanUpFiles creati in Creare i file RCF e CleanUpFiles oppure creare file CleanUpFiles generici per la configurazione corrente

   > Questo file CleanUpFile si applica al file RCF corrente e **NON** al nuovo RCF a cui si desidera eseguire l'aggiornamento.

   Esempio di CleanUpFile per Switch-A1: `Cleanup_NX9336_v1.81_Switch-A1.txt`

   b. Scarica i "nuovi" file RCF creati in Creare i "nuovi" file RCF per la nuova configurazione.

   Esempio di file RCF per Switch-A1: `NX9336_v1.90_Switch-A1.txt`

   c. Scaricare i CleanUpFiles creati in Creare i "nuovi" file RCF per la nuova configurazione. Questo passaggio è facoltativo: È possibile utilizzare il file in futuro per aggiornare la configurazione dello switch. Corrisponde alla configurazione attualmente applicata.

   Esempio di CleanUpFile per Switch-A1: `Cleanup_NX9336_v1.90_Switch-A1.txt`

   > Utilizzare CleanUpFile per la versione RCF corretta (corrispondente). Se si utilizza un CleanUpFile per una versione RCF diversa o per una configurazione diversa, la pulizia della configurazione potrebbe non funzionare correttamente.

   Il seguente esempio copia i tre file nella flash di avvio:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_xxx_xxx_xxx_xxx/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_xxx_xxx_xxx_xxxNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+

> Viene richiesto di specificare Virtual Routing and Forwarding (VRF).

5. Applicare il file CleanUpFile o il file CleanUpFile generico.

   Alcune configurazioni vengono ripristinate e gli switchport vengono "offline".

   a. Verificare che non vi siano modifiche in sospeso alla configurazione di avvio: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Se viene visualizzato l'output di sistema, salvare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

> L'output del sistema indica che la configurazione di avvio e la configurazione in esecuzione sono diverse e in sospeso. Se non si salvano le modifiche in sospeso, non è possibile eseguire il rollback utilizzando un ricaricamento dello switch.

   a. Applicare il comando CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config

IP_switch_A_1#
```

> Lo script potrebbe impiegare del tempo per tornare al prompt dello switch. Nessun output previsto.

7. Visualizzare la configurazione in esecuzione per verificare che la configurazione sia stata cancellata: `show running-config`

   La configurazione corrente dovrebbe mostrare:

   - Non sono configurate mappe di classe ed elenchi di accesso IP
   - Non sono configurate mappe di policy
   - Nessuna policy di servizio configurata
   - Nessun profilo porta configurato
   - Tutte le interfacce Ethernet (ad eccezione di mgmt0 che non devono mostrare alcuna configurazione e deve essere configurata solo la VLAN 1).

     Se uno degli elementi sopra indicati è configurato, potrebbe non essere possibile applicare una nuova configurazione del file RCF. Tuttavia, è possibile tornare alla configurazione precedente ricaricando lo switch **senza** salvare la configurazione in esecuzione nella configurazione di avvio. Lo switch verrà configurato in precedenza.

8. Applicare il file RCF e verificare che le porte siano in linea.

   a. Applicare i file RCF.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```

> Durante l'applicazione della configurazione vengono visualizzati alcuni messaggi di avviso. I messaggi di errore generalmente non sono previsti. Tuttavia, se si è connessi con SSH, potrebbe essere visualizzato il seguente errore: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

b. Una volta applicata la configurazione, verificare che il cluster e le porte MetroCluster siano in linea con uno dei seguenti comandi: `show interface brief`, `show cdp neighbors`, o. `show lldp neighbors`

> Se è stata modificata la VLAN per il cluster locale e si è aggiornato il primo switch del sito, il monitoraggio dello stato del cluster potrebbe non riportare lo stato come "integro" perché le VLAN delle configurazioni precedenti e nuove non corrispondono. Dopo l'aggiornamento del secondo switch, lo stato dovrebbe tornare a essere integro.

Se la configurazione non viene applicata correttamente o non si desidera mantenere la configurazione, è possibile tornare alla configurazione precedente ricaricando lo switch **senza** salvare la configurazione in esecuzione nella configurazione di avvio. Lo switch verrà configurato in precedenza.

9. Salvare la configurazione e ricaricare lo switch.

```
IP_switch_A_1# copy running-config startup-config

IP_switch_A_1# reload
```

Ridenominazione di uno switch IP Cisco

Potrebbe essere necessario rinominare uno switch IP Cisco per fornire un nome coerente per tutta la configurazione.

Negli esempi di questa attività, il nome dello switch viene modificato da `myswitch` a. `IP_switch_A_1`.

1. Accedere alla modalità di configurazione globale:

   `configure terminal`

   L'esempio seguente mostra il prompt della modalità di configurazione. Entrambi i prompt mostrano il nome dello switch di `myswitch`.

   ```
   myswitch# configure terminal
   myswitch(config)#
   ```

2. Rinominare lo switch:

   `switchname new-switch-name`

   Se si stanno rinominando entrambi gli switch nel fabric, utilizzare lo stesso comando su ogni switch.

   Il prompt CLI cambia per riflettere il nuovo nome:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Uscire dalla modalità di configurazione:

   `exit`

   Viene visualizzato il prompt di livello superiore:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Copiare la configurazione corrente in esecuzione nel file di configurazione di avvio:

   `copy running-config startup-config`

5. Verificare che la modifica del nome dello switch sia visibile dal prompt del cluster ONTAP.

   Si noti che viene visualizzato il nuovo nome dello switch e il vecchio nome dello switch (`myswitch`) non viene visualizzato.

   a. Accedere alla modalità avanzata dei privilegi, premendo **`y`** quando richiesto:
      `set -privilege advanced`
   b. Visualizzare i dispositivi collegati:
      `network device-discovery show`
   c. Tornare alla modalità privilegi di amministratore:
      `set -privilege admin`

      L'esempio seguente mostra che lo switch viene visualizzato con il nuovo nome, `IP_switch_A_1`:

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Aggiunta, rimozione o modifica delle porte ISL senza interruzioni sugli switch IP Cisco

Potrebbe essere necessario aggiungere, rimuovere o modificare le porte ISL sugli switch IP Cisco. È possibile convertire porte ISL dedicate in porte ISL condivise o modificare la velocità delle porte ISL su uno switch IP Cisco.

A proposito di questa attività

Se si stanno convertendo porte ISL dedicate in porte ISL condivise, assicurarsi che le nuove porte soddisfino il "Requisiti per le porte ISL condivise".

Per garantire la connettività ISL, è necessario completare tutti i passaggi su entrambi gli switch.

La seguente procedura presuppone la sostituzione di un ISL da 10 GB collegato alla porta dello switch eth1/24/1 con due ISL da 100 GB collegati alle porte dello switch 17 e 18.

> Se si utilizza uno switch Cisco 9336C-FX2 in una configurazione condivisa che collega NS224 shelf, la modifica degli ISL potrebbe richiedere un nuovo file RCF. Non è necessario un nuovo file RCF se la velocità attuale e quella nuova dell'ISL è 40Gbps e 100Gbps. Tutte le altre modifiche alla velocità ISL richiedono un nuovo file RCF. Ad esempio, la modifica della velocità ISL da 40Gbps a 100Gbps non richiede un nuovo file RCF, ma la modifica della velocità ISL da 10Gbps a 40Gbps richiede un nuovo file RCF.

Prima di iniziare

Fare riferimento alla sezione **interruttori** della "NetApp Hardware Universe" per verificare i ricetrasmettitori supportati.

Fasi

1. Disattivare le porte ISL degli ISL su entrambi gli switch del fabric che si desidera modificare.

   > Le porte ISL correnti devono essere disattivate solo se vengono spostate su un'altra porta o se la velocità dell'ISL cambia. Se si aggiunge una porta ISL con la stessa velocità degli ISL esistenti, passare alla fase 3.

   Immettere un solo comando di configurazione per ogni riga e premere Ctrl-Z dopo aver immesso tutti i comandi, come illustrato nell'esempio seguente:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/24/1
   switch_A_1(config-if)# shut
   switch_A_1(config-if)#
   switch_A_1#

   switch_B_1# conf t
   switch_B_1(config)# int eth1/24/1
   switch_B_1(config-if)# shut
   switch_B_1(config-if)#
   switch_B_1#
   ```

2. Rimuovere i cavi e i ricetrasmettitori esistenti.
3. Modificare la porta ISL secondo necessità.

> Se si utilizzano gli switch Cisco 9336C-FX2 in una configurazione condivisa che collega gli shelf NS224 ed è necessario aggiornare il file RCF e applicare la nuova configurazione per le nuove porte ISL, seguire i passaggi da a. "Aggiornare i file RCF sugli switch IP MetroCluster."

Opzione	Fase
Per modificare la velocità di una porta ISL…	Collegare i nuovi ISL alle porte designate in base alla velocità. Assicurarsi che le porte ISL dello switch siano elencate nella sezione *Installazione e configurazione IP MetroCluster*.
Per aggiungere un ISL…	Inserire i QFSP nelle porte che si stanno aggiungendo come porte ISL. Assicurarsi che siano elencati nella sezione *Installazione e configurazione IP MetroCluster* e cablarli di conseguenza.

4. Abilitare tutte le porte ISL (se non attivate) su entrambi gli switch del fabric iniziando dal seguente comando:

```
switch_A_1# conf t
```

Immettere un solo comando di configurazione per riga e premere Ctrl-Z dopo aver immesso tutti i comandi:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Verificare che gli ISL e i canali delle porte per gli ISL siano stabiliti tra entrambi gli switch:

```
switch_A_1# show int brief
```

Le interfacce ISL dovrebbero essere visualizzate nell'output del comando, come mostrato nell'esempio

seguente:

```
Switch_A_1# show interface brief
--------------------------------------------------------------------------
--------
Ethernet        VLAN    Type Mode   Status  Reason                 Speed
Port
Interface
Ch #
--------------------------------------------------------------------------
--------
Eth1/17         1       eth  access down    XCVR not inserted
auto(D) --
Eth1/18         1       eth  access down    XCVR not inserted
auto(D) --

--------------------------------------------------------------------------
------------------
Port-channel VLAN    Type Mode   Status  Reason
Speed   Protocol
Interface
--------------------------------------------------------------------------
------------------
Po10         1       eth  trunk  up      none
a-100G(D)  lacp
Po11         1       eth  trunk  up      none
a-100G(D)  lacp
```

6. Ripetere la procedura per il fabric 2.

Modificare indirizzo, maschera di rete e gateway in una configurazione IP MetroCluster

A partire da ONTAP 9.10.1, è possibile modificare le seguenti proprietà di un'interfaccia IP MetroCluster: Indirizzo IP, maschera e gateway. È possibile utilizzare qualsiasi combinazione di parametri per l'aggiornamento.

Potrebbe essere necessario aggiornare queste proprietà, ad esempio, se viene rilevato un indirizzo IP duplicato o se un gateway deve essere modificato in caso di rete di livello 3 a causa di modifiche alla configurazione del router.

È possibile modificare solo un'interfaccia alla volta. L'interfaccia verrà rallentata fino a quando le altre interfacce non saranno aggiornate e le connessioni non verranno ristabilita.

Utilizzare `metrocluster configuration-settings interface modify` Per modificare qualsiasi proprietà dell'interfaccia IP di MetroCluster.

> Questi comandi modificano la configurazione di un nodo specifico per una determinata porta. Per ripristinare la connettività di rete completa, sono necessari comandi simili su altre porte. Analogamente, anche gli switch di rete devono aggiornare la configurazione. Ad esempio, se il gateway viene aggiornato, idealmente viene modificato su entrambi i nodi di una coppia ha, poiché sono identici. Inoltre, anche lo switch connesso a tali nodi deve aggiornare il gateway.

Utilizzare `metrocluster configuration-settings interface show`, `metrocluster connection` controllare e. `metrocluster connection show` comandi per verificare che tutta la connettività funzioni in tutte le interfacce.

Modificare l'indirizzo IP, la netmask e il gateway

1. Aggiornare l'indirizzo IP, la netmask e il gateway per un singolo nodo e interfaccia: `metrocluster configuration-settings interface modify`

   Il comando seguente mostra come aggiornare l'indirizzo IP, la netmask e il gateway:

```
cluster_A::* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsi13:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsi14:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsi15:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsi16:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful
```

2. verificare che la connettività funzioni per tutte le interfacce: `metrocluster configuration-settings interface show`

   Il seguente comando mostra come verificare che tutte le connessioni funzionino per tutte le interfacce:

```
cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR              Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.12.201  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.200  255.255.255.0   192.168.20.1
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.12.101  255.255.254.0   192.168.12.1
completed
                 Home Port: e0b-20
                      192.168.20.101  255.255.255.0   192.168.20.1
completed
      cluster_B node_B_1
                 Home Port: e0a-10
                      192.168.11.151  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.150  255.255.255.0   192.168.21.1
completed
                node_B_2
                 Home Port: e0a-10
                      192.168.11.250  255.255.255.0   192.168.11.1
completed
                 Home Port: e0b-20
                      192.168.21.250  255.255.255.0   192.168.21.1
completed
8 entries were displayed.
```

3. verificare che tutte le connessioni funzionino:

   `metrocluster configuration-settings connection show`

Il seguente comando mostra come verificare che tutte le connessioni funzionino:

```
cluster_A::*> metrocluster configuration-settings connection show
  (metrocluster configuration-settings connection show)
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A node_A_2
                 Home Port: e0a-10
                      192.168.10.200  192.168.10.101  HA Partner
completed
                 Home Port: e0a-10
                      192.168.10.200  192.168.11.250  DR Partner
completed
                 Home Port: e0a-10
                      192.168.10.200  192.168.11.151  DR Auxiliary
completed
                 Home Port: e0b-20
                      192.168.20.200  192.168.20.100  HA Partner
completed
                 Home Port: e0b-20
                      192.168.20.200  192.168.21.250  DR Partner
completed
                 Home Port: e0b-20
                      192.168.20.200  192.168.21.150  DR Auxiliary
completed
                node_A_1
                 Home Port: e0a-10
                      192.168.10.101  192.168.10.200  HA Partner
completed
                 Home Port: e0a-10
                      192.168.10.101  192.168.11.151  DR Partner
completed
                 Home Port: e0a-10
                      192.168.10.101  192.168.11.250  DR Auxiliary
completed
                 Home Port: e0b-20
                      192.168.20.100  192.168.20.200  HA Partner
completed
                 Home Port: e0b-20
                      192.168.20.100  192.168.21.150  DR Partner
completed
                 Home Port: e0b-20
                      192.168.20.100  192.168.21.250  DR Auxiliary
completed
```

Modificare l'indirizzo IP di uno switch o di un bridge atto per il monitoraggio dello stato di salute

Dopo aver modificato gli indirizzi IP degli switch back-end FC MetroCluster e dei bridge ATTO, è necessario sostituire i vecchi indirizzi IP per il monitoraggio dello stato di salute con i nuovi valori.

- Modificare l'indirizzo IP di uno switch
- Modificare un indirizzo IP del bridge atto

Modificare l'indirizzo IP di uno switch

Sostituire il vecchio indirizzo IP di monitoraggio dello stato di uno switch back-end FC MetroCluster.

Prima di iniziare

Fare riferimento alla documentazione del fornitore dello switch per il modello di switch in uso per modificare l'indirizzo IP dello switch prima di modificare l'indirizzo IP per il monitoraggio dello stato di salute.

Fasi

1. Eseguire `::> storage switch show` e nell'output, annotare gli switch che segnalano gli errori.
2. Rimuovere le voci dello switch con i vecchi indirizzi IP:

   ```
   ::> storage switch remove -name switch_name
   ```

3. Aggiungere gli switch con nuovi indirizzi IP:

   ```
   ::> storage switch add -name switch_name -address new_IP_address -managed-by
   in-band
   ```

4. Verificare i nuovi indirizzi IP e verificare che non vi siano errori:

   ```
   ::> storage switch show
   ```

5. Se necessario, aggiornare le voci:

   ```
   ::> set advanced

   ::*> storage switch refresh

   ::*> set admin
   ```

Modificare un indirizzo IP del bridge atto

Sostituire il vecchio indirizzo IP per il monitoraggio dello stato di salute di un bridge ATTO.

Fasi

1. Eseguire `::> storage bridge show` E nell'output, annotare i bridge ATTO che segnalano gli errori.
2. Rimuovere le voci del bridge ATTO con i vecchi indirizzi IP:

```
::> storage bridge remove -name ATTO_bridge_name
```

3. Aggiungere i bridge ATTO con i nuovi indirizzi IP:

```
::> storage bridge add -name ATTO_bridge_name -address new_IP_address -managed
-by in-band
```

4. Verificare i nuovi indirizzi IP e verificare che non vi siano errori:

```
::> storage bridge show
```

5. Se necessario, aggiornare le voci:

```
::> set advanced

::*> storage bridge refresh

::*> set admin
```

Identificazione dello storage in una configurazione MetroCluster IP

Se è necessario sostituire un disco o un modulo shelf, è necessario prima identificare la posizione.

Identificazione degli shelf locali e remoti

Quando si visualizzano le informazioni sugli shelf da un sito MetroCluster, tutti i dischi remoti si trovano su 0 m, l'adattatore host iSCSI virtuale. Ciò significa che l'accesso ai dischi avviene tramite le interfacce IP di MetroCluster. Tutti gli altri dischi sono locali.

Dopo aver identificato se uno shelf è remoto (su 0 m), è possibile identificare ulteriormente l'unità o lo shelf in base al numero di serie o, in base alle assegnazioni degli shelf ID nella configurazione, in base all'ID dello shelf.

> Nelle configurazioni MetroCluster IP che eseguono ONTAP 9.4, l'ID shelf non deve essere univoco tra i siti MetroCluster. Questo include sia shelf interni (0) che shelf esterni. Il numero di serie è coerente se visualizzato da qualsiasi nodo su uno dei siti MetroCluster.

Gli shelf ID devono essere univoci all'interno del gruppo di disaster recovery (DR), ad eccezione dello shelf interno.

Una volta identificato il modulo del disco o dello shelf, è possibile sostituire il componente utilizzando la procedura appropriata.

"Manutenzione degli shelf di dischi DS460C DS224C e DS212C"

Esempio di output sysconfig -A.

Nell'esempio riportato di seguito viene utilizzato il `sysconfig -a` Per visualizzare i dispositivi su un nodo nella configurazione IP MetroCluster. Questo nodo ha i seguenti shelf e dispositivi collegati:

- Slot 0: Dischi interni (dischi locali)
- Slot 3: ID shelf esterno 75 e 76 (dischi locali)
- Slot 0: Virtual iSCSI host adapter 0m (dischi remoti)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
```

```
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
```

```
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
```

```
node_A_1::>
```

Aggiunta di shelf a un MetroCluster IP utilizzando switch Storage MetroCluster condivisi

Potrebbe essere necessario aggiungere shelf NS224 a un MetroCluster utilizzando switch Storage MetroCluster condivisi.

A partire da ONTAP 9.10.1, è possibile aggiungere shelf NS224 da un MetroCluster utilizzando gli switch storage/MetroCluster condivisi. È possibile aggiungere più shelf alla volta.

Prima di iniziare

- I nodi devono eseguire ONTAP 9.9.1 o versione successiva.
- Tutti gli shelf NS224 attualmente connessi devono essere collegati agli stessi switch di MetroCluster (configurazione storage condiviso/switch MetroCluster).
- Questa procedura non può essere utilizzata per convertire una configurazione con shelf NS224 collegati direttamente o shelf NS224 collegati a switch Ethernet dedicati in una configurazione che utilizza switch storage/MetroCluster condivisi.

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che l'aggiornamento è in corso.

   a. Immettere il seguente comando:

      ```
      system node autosupport invoke -node * -type all -message "Maint=10h Adding
      or Removing NS224 shelves"_
      ```

      Questo esempio specifica una finestra di manutenzione di 10 ore. A seconda del piano, potrebbe essere necessario dedicare più tempo.

      Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Ripetere il comando sul cluster partner.

Verifica dello stato della configurazione MetroCluster

Prima di eseguire la transizione, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      ```
      system health alert show
      ```

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      ```
      metrocluster show
      ```

   d. Eseguire un controllo MetroCluster:

      ```
      metrocluster check run
      ```

   e. Visualizzare i risultati del controllo MetroCluster:

      ```
      metrocluster check show
      ```

   f. Eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   g. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.
2. Verificare che il cluster funzioni correttamente:

   ```
   cluster show -vserver Cluster
   ```

   ```
   cluster_A::> cluster show -vserver Cluster
   Node           Health  Eligibility   Epsilon
   -------------- ------  -----------   -------
   node_A_1    true    true          false
   node_A_2    true    true          false

   cluster_A::>
   ```

3. Verificare che tutte le porte del cluster siano installate:

   ```
   network port show -ipspace cluster
   ```

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verificare che tutte le LIF del cluster siano operative:

   `network interface show -vserver Cluster`

   Ogni LIF del cluster dovrebbe visualizzare true per is Home e avere uno stato Admin/Oper di up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verificare che l'autorevert sia attivato su tutte le LIF del cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Applicazione del nuovo file RCF agli switch

> Se lo switch è già configurato correttamente, è possibile saltare queste sezioni successive e passare direttamente a. Configurazione della crittografia MACsec sugli switch Cisco 9336C, se applicabile o a. Collegamento del nuovo shelf NS224.

- È necessario modificare la configurazione dello switch per aggiungere shelf.
- Consultare i dettagli del cablaggio all'indirizzo "Assegnazioni delle porte della piattaforma".
- È necessario utilizzare lo strumento **RcfFileGenerator** per creare il file RCF per la configurazione. Il "RcfFileGenerator" fornisce inoltre una panoramica del cablaggio per porta per ogni switch. Assicurarsi di scegliere il numero corretto di shelf. Insieme al file RCF vengono creati file aggiuntivi che forniscono un layout di cablaggio dettagliato corrispondente alle opzioni specifiche. Utilizzare questa panoramica dei cavi per verificare il cablaggio durante il cablaggio dei nuovi shelf.

Aggiornamento dei file RCF sugli switch IP MetroCluster

Se si sta installando un nuovo firmware dello switch, è necessario installare il firmware dello switch prima di aggiornare il file RCF.

Questa procedura interrompe il traffico sullo switch in cui viene aggiornato il file RCF. Il traffico riprenderà una volta applicato il nuovo file RCF.

Fasi

1. Verificare lo stato della configurazione.

   a. Verificare che i componenti di MetroCluster siano integri:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

L'operazione viene eseguita in background.

b. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Per verificare lo stato dell'operazione MetroCluster check in corso, utilizzare il comando: **`metrocluster operation history show -job-id 38`**

b. Verificare che non siano presenti avvisi sullo stato di salute: **`system health alert show`**

2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

Ripristino delle impostazioni predefinite dello switch IP Cisco

Prima di installare una nuova versione software e gli RCF, è necessario cancellare la configurazione dello switch Cisco ed eseguire la configurazione di base.

È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.

1. Ripristinare le impostazioni predefinite dello switch:

a. Cancellare la configurazione esistente: `write erase`

b. Ricaricare il software dello switch: `reload`

Il sistema viene riavviato e viene avviata la configurazione guidata. Durante l'avvio, se viene visualizzato il messaggio Interrompi provisioning automatico e continua con la normale configurazione?(sì/no)[n], dovresti rispondere `yes` per procedere.

c. Nella configurazione guidata, immettere le impostazioni di base dello switch:

- Password amministratore
- Nome dello switch
- Configurazione della gestione fuori banda
- Gateway predefinito
- Servizio SSH (RSA) al termine della configurazione guidata, lo switch si riavvia.

d. Quando richiesto, immettere il nome utente e la password per accedere allo switch.

L'esempio seguente mostra i prompt e le risposte del sistema durante la configurazione dello switch. Le staffe angolari (<<<) mostra dove inserire le informazioni.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

Inserire le informazioni di base nel successivo set di prompt, inclusi nome dello switch, indirizzo di gestione e gateway, quindi selezionare SSH con RSA.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
   Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
   Number of rsa key bits <1024-2048> [1024]:
 Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
 Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

L’ultimo set di prompt completa la configurazione:

```
The following configuration will be applied:
 password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
 no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[##########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Salvare la configurazione:

```
IP_switch-A-1# copy running-config startup-config
```

3. Riavviare lo switch e attendere che lo switch si ricarichi:

```
IP_switch-A-1# reload
```

4. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Download e installazione del software NX-OS dello switch Cisco

È necessario scaricare il file del sistema operativo dello switch e il file RCF su ciascun switch nella configurazione IP MetroCluster.

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per copiare i file sui centralini.

Questa procedura deve essere ripetuta su ciascuno switch IP nella configurazione IP di MetroCluster.

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

1. Scaricare il file software NX-OS supportato.

   "Download del software Cisco"

2. Copiare il software dello switch sullo switch: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In questo esempio, il file nxos.7.0.3.I4.6.bin viene copiato dal server SFTP 10.10.99.99 al bootflash locale:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verificare su ogni switch che i file NX-OS dello switch siano presenti nella directory bootflash di ogni switch: `dir bootflash:`

   Il seguente esempio mostra che i file sono presenti su IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installare il software dello switch: `install all nxos bootflash:nxos.version-number.bin`

   Lo switch viene ricaricato (riavviato) automaticamente dopo l'installazione del software dello switch.

   L'esempio seguente mostra l'installazione del software su IP_switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
-- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Attendere che lo switch si ricarichi, quindi accedere allo switch.

   Una volta riavviato lo switch, viene visualizzato il prompt di login:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verificare che il software dello switch sia stato installato: `show version`

   L'esempio seguente mostra l'output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Ripetere questa procedura sui tre switch IP rimanenti nella configurazione IP MetroCluster.

Configurazione della crittografia MACsec sugli switch Cisco 9336C

Se lo si desidera, è possibile configurare la crittografia MACsec sulle porte ISL WAN che vengono eseguite tra i siti. È necessario configurare MACsec dopo aver applicato il file RCF corretto.

> La crittografia MACsec può essere applicata solo alle porte ISL WAN.

Requisiti di licenza per MACsec

MACsec richiede una licenza di sicurezza. Per una spiegazione completa dello schema di licenza di Cisco NX-OS e su come ottenere e richiedere le licenze, consultare la "Guida alle licenze di Cisco NX-OS"

Abilitazione degli ISL WAN con crittografia Cisco MACsec nelle configurazioni IP di MetroCluster

È possibile attivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

1. Accedere alla modalità di configurazione globale: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Abilitare MACsec e MKA sul dispositivo: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copiare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Disattivazione della crittografia Cisco MACsec

Potrebbe essere necessario disattivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

> Se si disattiva la crittografia, è necessario eliminare anche le chiavi.

1. Accedere alla modalità di configurazione globale: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disattivare la configurazione MACsec sul dispositivo: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

> Selezionando l'opzione no si ripristina la funzione MACsec.

3. Selezionare l'interfaccia già configurata con MACsec.

È possibile specificare il tipo di interfaccia e l'identità. Per una porta Ethernet, utilizzare slot/porta ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Rimuovere il portachiavi, il criterio e il portachiavi fallback configurati sull'interfaccia per rimuovere la configurazione MACsec: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Ripetere i passaggi 3 e 4 su tutte le interfacce in cui è configurato MACsec.
6. Copiare la configurazione in esecuzione nella configurazione di avvio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configurazione di una catena di chiavi MACsec e delle chiavi

Per ulteriori informazioni sulla configurazione di una catena di chiavi MACsec, consultare la documentazione Cisco relativa allo switch.

Collegamento del nuovo shelf NS224

Fasi

1. Installare il kit per il montaggio su guida fornito con lo shelf utilizzando il volantino di installazione fornito nella confezione del kit.
2. Installare e fissare lo shelf sulle staffe di supporto e sul rack o sull'armadietto utilizzando il volantino di installazione.
3. Collegare i cavi di alimentazione allo shelf, fissarli con il fermo del cavo di alimentazione, quindi collegare i cavi di alimentazione a diverse fonti di alimentazione per garantire la resilienza.

   Uno shelf si accende quando viene collegato a una fonte di alimentazione; non dispone di interruttori di alimentazione. Quando funziona correttamente, il LED bicolore di un alimentatore si illumina di verde.

4. Impostare l'ID dello shelf su un numero univoco all'interno della coppia ha e nella configurazione.
5. Collegare le porte dello shelf nel seguente ordine:
   a. Collegare NSM-A, e0a allo switch (Switch-A1 o Switch-B1)
   b. Collegare NSM-B, e0a allo switch (Switch-A2 o Switch-B2)
   c. Collegare NSM-A, e0b allo switch (Switch-A1 o Switch-B1)
   d. Collegare NSM-B, e0b allo switch (Switch-A2 o Switch-B2)
6. Utilizzare il layout di cablaggio generato dallo strumento **RcfFileGenerator** per collegare lo shelf alle porte

appropriate.

Una volta collegato correttamente il nuovo shelf, ONTAP lo rileva automaticamente sulla rete.

Aggiunta a caldo di storage a una configurazione MetroCluster FC

Aggiunta a caldo di uno shelf di dischi SAS in una configurazione MetroCluster FC a collegamento diretto mediante cavi ottici SAS

È possibile utilizzare i cavi ottici SAS per aggiungere a caldo uno shelf di dischi SAS a uno stack esistente di shelf di dischi SAS in una configurazione MetroCluster FC a collegamento diretto o come nuovo stack a un HBA SAS o a una porta SAS integrata del controller.

- Questa procedura è senza interruzioni e richiede circa due ore per essere completata.
- È necessaria la password admin e l'accesso a un server FTP o SCP.
- Se si aggiunge uno shelf IOM12 a uno stack di shelf IOM6, vedere "Aggiunta a caldo di shelf IOM12 a una pila di shelf IOM6".

Questa attività si applica a una configurazione MetroCluster FC in cui lo storage è collegato direttamente ai controller di storage mediante cavi SAS. Non si applica alle configurazioni MetroCluster FC che utilizzano bridge FC-SAS o fabric switch FC.

Fasi

1. Seguire le istruzioni per l'aggiunta a caldo di uno shelf di dischi SAS nella *Guida all'installazione* del modello di shelf di dischi per eseguire le seguenti operazioni per aggiungere a caldo uno shelf di dischi:
   a. Installare uno shelf di dischi per un'aggiunta a caldo.
   b. Accendere gli alimentatori e impostare l'ID dello shelf per un componente aggiuntivo a caldo.
   c. Cablare lo shelf di dischi aggiunto a caldo.
   d. Verificare la connettività SAS.

Aggiunta a caldo di storage SAS a una configurazione FC MetroCluster collegata a ponte

Aggiunta a caldo di uno stack di shelf di dischi SAS a una coppia esistente di bridge FibreBridge 7600N o 7500N

È possibile aggiungere a caldo uno stack di shelf di dischi SAS a una coppia esistente di bridge FibreBridge 7600N o 7500N dotati di porte disponibili.

Prima di iniziare

- È necessario aver scaricato l'ultima versione del firmware dello shelf di dischi e dischi.
- Tutti gli shelf di dischi nella configurazione MetroCluster (shelf esistenti) devono eseguire la stessa versione del firmware. Se uno o più dischi o shelf non utilizzano la versione più recente del firmware, aggiornare il firmware prima di collegare i nuovi dischi o shelf.

"Download NetApp: Firmware del disco"

"Download NetApp: Firmware shelf di dischi"

- I bridge FibreBridge 7600N o 7500N devono essere collegati e disporre di porte SAS disponibili.

A proposito di questa attività

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.

È possibile utilizzare l'interfaccia grafica di ATTO ExpressNAV per configurare e gestire un bridge e per aggiornare il firmware del bridge. È possibile 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. Queste opzioni includono l'utilizzo di una porta seriale o Telnet per configurare e gestire un bridge e per configurare la porta di gestione Ethernet 1 e l'utilizzo di FTP per aggiornare il firmware del bridge. Se si sceglie una di queste interfacce di gestione, è necessario soddisfare i requisiti applicabili in "Altre interfacce di gestione del bridge".

> Se si inserisce un cavo SAS nella porta errata, quando si rimuove il cavo da una porta SAS, è necessario attendere almeno 120 secondi prima di collegarlo a una porta SAS diversa. In caso contrario, il sistema non riconosce che il cavo è stato spostato su un'altra porta.

Fasi

1. Mettere a terra l'utente.
2. Dalla console di uno dei controller, verificare che l'assegnazione automatica dei dischi sia abilitata nel sistema:

   ```
   storage disk option show
   ```

   La colonna Auto Assign (assegnazione automatica) indica se l'assegnazione automatica del disco è attivata.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

3. Su ciascun bridge della coppia, attivare la porta SAS che si connette al nuovo stack:

   ```
   SASPortEnable port-letter
   ```

   La stessa porta SAS (B, C o D) deve essere utilizzata su entrambi i bridge.

4. Salvare la configurazione e riavviare ciascun bridge:

   ```
   SaveConfiguration Restart
   ```

5. Collegare gli shelf di dischi ai bridge:

a. Collegare a margherita gli shelf di dischi in 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.

b. Per ogni stack di shelf di dischi, collegare il cavo IOM A del primo shelf alla porta SAS A di FibreBridge A, quindi collegare il cavo IOM B dell'ultimo shelf alla porta SAS A di FibreBridge B.

   "Installazione e configurazione di Fabric-Attached MetroCluster"

   "Estensione dell'installazione e della configurazione di MetroCluster"

   Ogni bridge ha un percorso per la propria pila di shelf di dischi; il bridge A si collega al lato A dello stack attraverso il primo shelf e il bridge B si collega al lato B dello stack attraverso l'ultimo shelf.

   La porta SAS bridge B è disattivata.

6. Verificare che ciascun bridge sia in grado di rilevare tutte le unità disco e gli shelf di dischi a cui è collegato il bridge.

Se si utilizza…	Quindi…
GUI ExpressNAV	a. In un browser Web supportato, inserire l'indirizzo IP di un bridge nella casella del browser. Viene visualizzata la home page di ATTO FibreBridge, che contiene un link. b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge. Viene visualizzata la pagina di stato di atto FibreBridge con un menu a sinistra. c. Fare clic su **Avanzate** nel menu. d. Visualizzare i dispositivi connessi: `sastargets` e. Fare clic su **Invia**.
Connessione alla porta seriale	Visualizzare i dispositivi connessi: `sastargets`

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.

Se all'inizio dell'output viene visualizzato il testo "respesse tronced", è possibile utilizzare Telnet per connettersi al bridge e visualizzare l'output utilizzando `sastargets` comando.

Il seguente output indica 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        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

7. Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi appropriati nello stack.

Se l'output è…	Quindi…
Esatto	Ripetere il passaggio precedente per ogni bridge rimanente.
Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo la procedura per collegare gli shelf di dischi ai bridge. b. Ripetere il passaggio precedente per ogni bridge rimanente.

8. Aggiornare il firmware del disco alla versione più recente dalla console di sistema:

   `disk_fw_update`

   Eseguire questo comando su entrambi i controller.

   "Download NetApp: Firmware del disco"

9. Aggiornare il firmware dello shelf di dischi alla versione più recente utilizzando le istruzioni per il firmware scaricato.

   È possibile eseguire i comandi della procedura dalla console di sistema di uno dei controller.

   "Download NetApp: Firmware shelf di dischi"

10. Se il sistema non dispone dell'assegnazione automatica dei dischi attivata, assegnare la proprietà dei dischi.

    "Gestione di dischi e aggregati"

    > Se si suddivide la proprietà di un singolo stack di shelf di dischi tra più controller, è necessario disattivare l'assegnazione automatica dei dischi (`storage disk option modify -autoassign off *` da entrambi i nodi del cluster) prima di assegnare la proprietà del disco; in caso contrario, quando si assegna un disco singolo, i dischi rimanenti potrebbero essere assegnati automaticamente allo stesso controller e pool.

> Non è necessario aggiungere dischi ad aggregati o volumi fino a quando il firmware del disco e del firmware dello shelf di dischi non sono stati aggiornati e le fasi di verifica di questa attività non sono state completate.

11. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
    a. Verificare che il sistema sia multipercorso:

    ```
    node run -node node-name sysconfig -a
    ```

    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

    ```
    system health alert show
    ```

    c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

    ```
    metrocluster show
    ```

    d. Eseguire un controllo MetroCluster:

    ```
    metrocluster check run
    ```

    e. Visualizzare i risultati del controllo MetroCluster:

    ```
    metrocluster check show
    ```

    f. Verificare la presenza di eventuali avvisi sullo stato di salute sui bridge dopo l'aggiunta dei nuovi stack:

    ```
    storage bridge show
    ```

    g. Eseguire Config Advisor.

    "Download NetApp: Config Advisor"

    h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.
12. Se applicabile, ripetere questa procedura per il sito del partner.

Aggiunta a caldo di uno stack di shelf di dischi SAS e bridge a un sistema MetroCluster

È possibile aggiungere a caldo (senza interruzioni) un intero stack, inclusi i bridge, al sistema MetroCluster. Gli switch FC devono disporre di porte disponibili ed è necessario aggiornare lo zoning dello switch per riflettere le modifiche.

A proposito di questa attività

- Questa procedura può essere utilizzata per aggiungere uno stack utilizzando i bridge FibreBridge 7600N o 7500N.
- 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. Queste opzioni includono l'utilizzo di una porta seriale o Telnet per configurare e gestire un bridge, la configurazione della porta di gestione Ethernet 1 e l'utilizzo di FTP per aggiornare il firmware del bridge. Se si sceglie una di queste interfacce di gestione, il sistema deve soddisfare i requisiti applicabili in "Altre interfacce di gestione del bridge"

Preparazione all'aggiunta a caldo di uno stack di shelf e bridge di dischi SAS

La preparazione all'aggiunta a caldo di uno stack di shelf di dischi SAS e di una coppia di bridge implica il download di documenti, nonché del firmware del disco e dello shelf di dischi.

Prima di iniziare

- Il sistema deve essere una configurazione supportata e deve essere in esecuzione una versione supportata di ONTAP.

  "Tool di matrice di interoperabilità NetApp"

- Tutti i dischi e gli shelf di dischi del sistema devono disporre della versione più recente del firmware.

  Prima di aggiungere shelf, è possibile aggiornare il firmware del disco e dello shelf nella configurazione MetroCluster.

  "Upgrade, revert o downgrade"

- Ogni switch FC deve disporre di una porta FC per il collegamento di un bridge.

  > Potrebbe essere necessario aggiornare lo switch FC in base alla compatibilità dello switch FC.

- Per utilizzare l'interfaccia grafica di ATTO ExpressNAV: Internet Explorer 8 o 9 o Mozilla Firefox 3, 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 utilizzando le informazioni riportate nella procedura.

Fasi

1. Scarica o visualizza i seguenti documenti dal sito di supporto NetApp:
   - "Tool di matrice di interoperabilità NetApp"
   - La *Guida all'installazione e al servizio* per il modello di shelf di dischi.
2. Scaricare i contenuti dal sito Web atto e dal sito Web di NetApp:
   a. Accedere alla pagina ATTO FibreBridge Description (Descrizione di ATTO FibreBridge).
   b. Utilizzando il collegamento nella pagina ATTO FibreBridge Description, accedere al sito Web atto e scaricare quanto segue:
      - *ATTO FibreBridge Installation and Operation Manual* per il tuo modello di bridge.
      - ATTO barra di navigazione (sul computer in uso per la configurazione).
   c. Accedere alla pagina di download del firmware ATTO FibreBridge facendo clic su **Continue** (continua) alla fine della pagina ATTO FibreBridge Description (Descrizione di ATTO FibreBridge), quindi procedere come segue:
      - Scaricare il file del firmware del bridge come indicato nella pagina di download.

In questa fase, si sta completando solo la parte di download delle istruzioni fornite nei collegamenti. Il firmware di ciascun bridge viene aggiornato in un secondo momento, quando richiesto in "Aggiunta a caldo della pila di shelf" sezione.

- Fare una copia della pagina di download del firmware ATTO FibreBridge e delle note sulla versione per riferimento in seguito.

3. Scaricare il firmware più recente per lo shelf di dischi e dischi ed eseguire una copia della parte di installazione delle istruzioni per riferimento in seguito.

   Tutti gli shelf di dischi nella configurazione MetroCluster (sia i nuovi shelf che gli shelf esistenti) devono eseguire la stessa versione del firmware.

   > In questa fase, si sta completando solo la parte di download delle istruzioni fornite nei collegamenti e si sta creando una copia delle istruzioni di installazione. Il firmware viene aggiornato su ciascun disco e shelf di dischi in un secondo momento, quando richiesto nella "Aggiunta a caldo della pila di shelf" sezione.

   a. Scaricare il firmware del disco ed eseguire una copia delle istruzioni del firmware del disco per riferimento in seguito.

      "Download NetApp: Firmware del disco"

   b. Scaricare il firmware dello shelf di dischi ed eseguire una copia delle istruzioni del firmware dello shelf di dischi per riferimento in seguito.

      "Download NetApp: Firmware shelf di dischi"

4. Raccogliere l'hardware e le informazioni necessarie per utilizzare le interfacce di gestione del bridge consigliate: GUI ExpressNAV atto e utility barra di navigazione atto:

   a. Procurarsi un cavo Ethernet standard per il collegamento dalla porta di gestione Ethernet del bridge 1 alla rete.

   b. Determinare un nome utente e una password non predefiniti per l'accesso ai bridge.

      Si consiglia di modificare il nome utente e la password predefiniti.

   c. Ottenere un indirizzo IP, una subnet mask e 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.

5. Procurarsi quattro viti per ciascun bridge per montare saldamente le staffe "L" del bridge sulla parte anteriore del rack.

   Le aperture delle staffe "L" del ponte sono conformi allo standard ETA-310-X per rack da 19" (482.6 mm).

6. Se necessario, aggiornare lo zoning dello switch FC per ospitare i nuovi bridge aggiunti alla configurazione.

   Se si utilizzano i file di configurazione di riferimento forniti da NetApp, le zone sono state create per tutte le porte, quindi non è necessario effettuare aggiornamenti di zoning. Per ciascuna porta dello switch che si collega alle porte FC del bridge deve essere presente una zona di storage.

Aggiunta a caldo di uno stack di shelf e bridge di dischi SAS

È possibile aggiungere a caldo uno stack di shelf di dischi SAS e bridge per aumentare la capacità dei bridge.

Il sistema deve soddisfare tutti i requisiti per aggiungere a caldo uno stack di shelf e bridge di dischi SAS.

"Preparazione all'aggiunta a caldo di uno stack di shelf e bridge di dischi SAS"

- L'aggiunta a caldo di uno stack di shelf e bridge di dischi SAS è una procedura senza interruzioni se vengono soddisfatti tutti i requisiti di interoperabilità.

  "Tool di matrice di interoperabilità NetApp"

  "Utilizzo dello strumento matrice di interoperabilità per trovare le informazioni MetroCluster"

- Multipath ha è l'unica configurazione supportata per i sistemi MetroCluster che utilizzano bridge.

  Entrambi i moduli controller devono avere accesso attraverso i bridge agli shelf di dischi in ogni stack.

- È necessario aggiungere a caldo un numero uguale di shelf di dischi in ogni sito.
- 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.

> 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.

> Se si inserisce un cavo SAS nella porta errata, quando si rimuove il cavo da una porta SAS, è necessario attendere almeno 120 secondi prima di collegarlo a una porta SAS diversa. In caso contrario, il sistema non riconosce che il cavo è stato spostato su un'altra porta.

Fasi

1. Mettere a terra l'utente.
2. Dalla console di uno dei moduli controller, verificare se l'assegnazione automatica dei dischi nel sistema è abilitata:

   ```
   storage disk option show
   ```

   La colonna Auto Assign (assegnazione automatica) indica se l'assegnazione automatica del disco è attivata.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

3. Disattivare le porte dello switch per il nuovo stack.
4. 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.

5. 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.

6. Configurare il bridge.

   Se le informazioni di configurazione sono state recuperate dal vecchio bridge, utilizzare le informazioni per configurare il nuovo bridge.

   Annotare il nome utente e la password designati.

   Il *Manuale d'installazione e funzionamento di FibreBridge atto* per il tuo modello di bridge contiene le informazioni più aggiornate sui comandi disponibili e su come utilizzarli.

   > 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.

      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 l'interfaccia CLI, è necessario eseguire il seguente comando:

  `set bridgename bridgename`

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.

7. 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 dallo switch 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`

a. 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 disattivare la porta:
     `FCPortDisable port-number`

b. 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.

8. Accesso sicuro al bridge e salvataggio della configurazione del bridge.

   a. Dal prompt del controller, controllare lo stato dei bridge:

      ```
      storage bridge show
      ```

      L'output mostra quale bridge non è protetto.

   b. Verificare 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 il comando seguente:
      `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.

9. Aggiornare il firmware FibreBridge su ciascun bridge.

   Se il nuovo bridge è dello stesso tipo del bridge partner, eseguire l'aggiornamento allo stesso firmware del bridge partner. Se il nuovo bridge è di tipo diverso da quello del bridge partner, eseguire l'aggiornamento al firmware più recente supportato dal bridge e dalla versione di ONTAP. Consultare la sezione "aggiornamento del firmware su un bridge FibreBridge" in *manutenzione MetroCluster*.

10. collega gli shelf di dischi ai bridge:

    a. Collegare a margherita gli shelf di dischi in ogni stack.

       La *Guida all'installazione* per il modello di shelf di dischi fornisce informazioni dettagliate sugli shelf di dischi con concatenamento a margherita.

    b. Per ogni stack di shelf di dischi, collegare IOM A del primo shelf alla porta SAS A su FibreBridge A, quindi collegare IOM B dell'ultimo shelf alla porta SAS A su FibreBridge B.

       "Installazione e configurazione di Fabric-Attached MetroCluster"

       "Estensione dell'installazione e della configurazione di MetroCluster"

Ogni bridge ha un percorso per la propria pila di shelf di dischi; il bridge A si collega al lato A dello stack attraverso il primo shelf e il bridge B si collega al lato B dello stack attraverso l'ultimo shelf.

La porta SAS bridge B è disattivata.

11. verificare che ciascun bridge sia in grado di rilevare tutti i dischi e gli shelf di dischi a cui è collegato il bridge.

Se si utilizza…	Quindi…
GUI ExpressNAV	a. In un browser Web supportato, inserire l'indirizzo IP di un bridge nella casella del browser. Viene visualizzata la home page di ATTO FibreBridge, che contiene un link. b. Fare clic sul collegamento, quindi immettere il nome utente e la password designati al momento della configurazione del bridge. Viene visualizzata la pagina di stato di atto FibreBridge con un menu a sinistra. c. Fare clic su **Avanzate** nel menu. d. Visualizzare i dispositivi collegati: `sastargets` e. Fare clic su **Invia**.
Connessione alla porta seriale	Visualizzare i dispositivi connessi: `sastargets`

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.

Se la risposta di testo troncata viene visualizzata all'inizio dell'output, è possibile utilizzare Telnet per connettersi al bridge e visualizzare l'output utilizzando `sastargets` comando.

Il seguente output indica 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        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

12. Verificare che l'output del comando indichi che il bridge è collegato a tutti i dischi e gli shelf di dischi appropriati nello stack.

Se l'output è…	Quindi…
Esatto	Ripetere Fase 11 per ogni bridge rimanente.
Non corretto	a. Verificare l'eventuale presenza di cavi SAS allentati o correggere il cablaggio SAS ripetendo le operazioni Fase 10. b. Ripetere Fase 11.

13. Se si sta configurando una configurazione Fabric-Attached MetroCluster, collegare ciascun bridge agli switch FC locali utilizzando i cavi mostrati nella tabella per la configurazione, il modello di switch e il modello di bridge FC-SAS:

> Gli switch Brocade e Cisco utilizzano una diversa numerazione delle porte, come illustrato nelle tabelle seguenti.

- Sugli switch Brocade, la prima porta è numerata "0".
- Sugli switch Cisco, la prima porta è numerata "1".

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)											
GRUPPO DR 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Componente	Porta	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2

Stack 1	bridge _x_1a	FC1	8		8		8		8		10	
FC2	-	8	-	8	-	8	-	8	-	10	bridge _x_1B	FC1
9	-	9	-	9	-	9	-	11	-	FC2	-	9
-	9	-	9	-	9	-	11	Stack 2	bridge _x_2a	FC1	10	-
10	-	10	-	10	-	14	-	FC2	-	10	-	10
-	10	-	10	-	14	bridge _x_2B	FC1	11	-	11	-	11
-	11	-	17	-	FC2	-	11	-	11	-	11	-
11	-	17	Stack 3	bridge _x_3a	FC1	12	-	12	-	12	-	12
-	18	-	FC2	-	12	-	12	-	12	-	12	-
18	bridge _x_3B	FC1	13	-	13	-	13	-	13	-	19	-
FC2	-	13	-	13	-	13	-	13	-	19	Stack y	bridge _x_ya
FC1	14	-	14	-	14	-	14	-	20	-	FC2	-
14	-	14	-	14	-	14	-	20	bridge _x_yb	FC1	15	-
15	-	15	-	15	-	21	-	FC2		15		15

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando entrambe le porte FC (FC1 e FC2)									
GRUPPO DR 2									
		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G720	
Componente	Porta	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	interruttore 2

Stack 1	bridge_x_51a	FC1	26	-	32	-	56	-	32	-
FC2	-	26	-	32	-	56	-	32	bridge_x_51b	FC1
27	-	33	-	57	-	33	-	FC2	-	27
-	33	-	57	-	33	Stack 2	bridge_x_52a	FC1	30	-
34	-	58	-	34	-	FC2	-	30	-	34
-	58	-	34	bridge_x_52b	FC1	31	-	35	-	59
-	35	-	FC2	-	31	-	35	-	59	-
35	Stack 3	bridge_x_53a	FC1	32	-	36	-	60	-	36
-	FC2	-	32	-	36	-	60	-	36	bridge_x_53b
FC1	33	-	37	-	61	-	37	-	FC2	-
33	-	37	-	61	-	37	Stack y	bridge_x_5ya	FC1	34
-	38	-	62	-	38	-	FC2	-	34	-
38	-	62	-	38	bridge_x_5yb	FC1	35	-	39	-
63	-	39	-	FC2	-	35	-	39	-	63

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)											
GRUPPO DR 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Componente	Porta	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2	Interruttore 1	Interruttore 2

Stack 1	bridge_x_1a	8		8		8		8		10	
bridge_x_1b	-	8	-	8	-	8	-	8	-	10	Stack 2
bridge_x_2a	9	-	9	-	9	-	9	-	11	-	bridge_x_2b
-	9	-	9	-	9	-	9	-	11	Stack 3	bridge_x_3a
10	-	10	-	10	-	10	-	14	-	bridge_x_4b	-
10	-	10	-	10	-	10	-	14	Stack y	bridge_x_ya	11
-	11	-	11	-	11	-	15	-	bridge_x_yb	-	11

Configurazioni che utilizzano FibreBridge 7500N o 7600N utilizzando una sola porta FC (FC1 o FC2)									
GRUPPO DR 2									
		Brocade G720		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520	
Stack 1	bridge_x_51a	32	-	26	-	32	-	56	-
bridge_x_51b	-	32	-	26	-	32	-	56	Stack 2
bridge_x_52a	33	-	27	-	33	-	57	-	bridge_x_52b
-	33	-	27	-	33	-	57	Stack 3	bridge_x_53a
34	-	30	-	34	-	58	-	bridge_x_54b	-
34	-	30	-	34	-	58	Stack y	bridge_x_ya	35

-	31	-	35	-	59	-	bridge_x_yb	-	35

14. Se si sta configurando un sistema MetroCluster collegato tramite bridge, collegare ciascun bridge ai moduli controller:
    a. Collegare la porta FC 1 del bridge a una porta FC da 16 GB o 8 GB sul modulo controller in cluster_A.
    b. Collegare la porta FC 2 del bridge alla porta FC della stessa velocità del modulo controller in cluster_A.
    c. Ripetere questi passaggi secondari sugli altri bridge successivi fino a quando tutti i bridge non sono stati cablati.
15. Aggiornare il firmware del disco alla versione più recente dalla console di sistema:

    ```
    disk_fw_update
    ```

    Eseguire questo comando su entrambi i moduli controller.

    "Download NetApp: Firmware del disco"

16. Aggiornare il firmware dello shelf di dischi alla versione più recente utilizzando le istruzioni per il firmware scaricato.

    È possibile eseguire i comandi della procedura dalla console di sistema di uno dei moduli controller.

    "Download NetApp: Firmware shelf di dischi"

17. Se il sistema non dispone dell'assegnazione automatica dei dischi attivata, assegnare la proprietà dei dischi.

    "Gestione di dischi e aggregati"

    > Se si suddivide la proprietà di un singolo stack di shelf di dischi tra più moduli controller, è necessario disattivare l'assegnazione automatica dei dischi su entrambi i nodi del cluster (`storage disk option modify -autoassign off *`) prima di assegnare la proprietà del disco; in caso contrario, quando si assegna un disco singolo, i dischi rimanenti potrebbero essere assegnati automaticamente allo stesso modulo controller e pool.

    > Non è necessario aggiungere dischi ad aggregati o volumi fino a quando il firmware del disco e del firmware dello shelf di dischi non sono stati aggiornati e le fasi di verifica di questa attività non sono state completate.

18. Abilitare le porte dello switch per il nuovo stack.
19. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
    a. Verificare che il sistema sia multipercorso:
    `node run -node node-name sysconfig -a`
    b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
    `system health alert show`
    c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
    `metrocluster show`

d. Eseguire un controllo MetroCluster:
```
metrocluster check run
```
e. Visualizzare i risultati del controllo MetroCluster:
```
metrocluster check show
```
f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli interruttori (se presenti):
```
storage switch show
```
g. Eseguire Config Advisor.

   "Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

20. Se applicabile, ripetere questa procedura per il sito del partner.

Informazioni correlate

"Gestione in-band dei bridge FC-SAS"

Aggiungere a caldo uno shelf di dischi SAS a uno stack di shelf di dischi SAS

Preparazione all'aggiunta a caldo di shelf di dischi SAS

La preparazione all'aggiunta a caldo di uno shelf di dischi SAS comporta il download di documenti, nonché del firmware del disco e dello shelf di dischi.

- Il sistema deve essere una configurazione supportata e deve essere in esecuzione una versione supportata di ONTAP.
- Tutti i dischi e gli shelf di dischi del sistema devono disporre della versione più recente del firmware.

  Prima di aggiungere shelf, è possibile aggiornare il firmware del disco e dello shelf nella configurazione MetroCluster.

  "Upgrade, revert o downgrade"

> Un insieme di moduli IOM12 e IOM6 è supportato all'interno dello stesso stack se il sistema esegue una versione supportata di ONTAP. Per stabilire se la tua versione di ONTAP supporta la combinazione di shelf, Fare riferimento al tool di matrice di interoperabilità (IMT).https://mysupport.netapp.com/NOW/products/interoperability[NetApp interoperabilità] se la versione di ONTAP in uso non è supportata e non è possibile aggiornare o eseguire il downgrade dei moduli IOM sullo stack esistente o sul nuovo shelf da aggiungere a una combinazione supportata di moduli IOM, è necessario eseguire una delle seguenti operazioni:

- Avviare un nuovo stack su una nuova porta SAS (se supportata dalla coppia di bridge).
- Avviare un nuovo stack su una coppia di bridge aggiuntiva.

Fasi

1. Scarica o visualizza i seguenti documenti dal sito di supporto NetApp:
   - "Tool di matrice di interoperabilità NetApp"
   - La *Guida all'installazione* per il modello di shelf di dischi.

2. Verificare che lo shelf di dischi che si sta aggiungendo a caldo sia supportato.

   "Tool di matrice di interoperabilità NetApp"

3. Scarica l'ultima versione del firmware per shelf di dischi e dischi:

   In questa fase, si sta completando solo la parte di download delle istruzioni fornite nei collegamenti. Seguire la procedura descritta in "Aggiunta a caldo di uno shelf di dischi" sezione per l'installazione dello shelf di dischi.

   a. Scaricare il firmware del disco ed eseguire una copia delle istruzioni del firmware del disco per riferimento in seguito.

      "Download NetApp: Firmware del disco"

   b. Scaricare il firmware dello shelf di dischi ed eseguire una copia delle istruzioni del firmware dello shelf di dischi per riferimento in seguito.

      "Download NetApp: Firmware shelf di dischi"

Aggiunta a caldo di uno shelf di dischi

È possibile aggiungere a caldo uno shelf di dischi quando si desidera aumentare lo storage senza alcuna riduzione delle performance.

- Il sistema deve soddisfare tutti i requisiti di "Preparazione all'aggiunta a caldo di shelf di dischi SAS".
- Per aggiungere a caldo uno shelf, l'ambiente deve soddisfare uno dei seguenti scenari:
  - Sono presenti due bridge FibreBridge 7500N collegati a uno stack di shelf di dischi SAS.
  - Sono presenti due bridge FibreBridge 7600N collegati a uno stack di shelf di dischi SAS.
  - Si dispone di un bridge FibreBridge 7500N e di un bridge FibreBridge 7600N collegati a uno stack di shelf di dischi SAS.
- Questa procedura consente di aggiungere a caldo uno shelf di dischi all'ultimo shelf di dischi in uno stack.

  Questa procedura viene scritta con il presupposto che l'ultimo shelf di dischi in uno stack sia collegato da IOM A bridge A e da IOM B a bridge B.

- Si tratta di una procedura senza interruzioni.
- È necessario aggiungere a caldo un numero uguale di shelf di dischi in ogni sito.
- Se si aggiungono a caldo più shelf di dischi, è necessario aggiungere a caldo uno shelf di dischi alla volta.

  Ogni coppia di bridge FibreBridge 7500N o 7600N può supportare fino a quattro stack.

L'aggiunta a caldo di uno shelf di dischi richiede l'aggiornamento del firmware del disco sul shelf di dischi aggiunto a caldo eseguendo il `storage disk firmware update` comando in modalità avanzata. L'esecuzione di questo comando può causare interruzioni se il firmware dei dischi esistenti nel sistema è una versione precedente.

Se si inserisce un cavo SAS nella porta errata, quando si rimuove il cavo da una porta SAS, è necessario attendere almeno 120 secondi prima di collegarlo a una porta SAS diversa. In caso contrario, il sistema non riconosce che il cavo è stato spostato su un'altra porta.

Fasi

1. Mettere a terra l'utente.
2. Verificare la connettività dello shelf di dischi dalla console di sistema di uno dei controller:

   `sysconfig -v`

   L'output è simile a quanto segue:

   - Ciascun bridge su una linea separata e sotto ogni porta FC a cui è visibile; ad esempio, l'aggiunta a caldo di uno shelf di dischi a un set di bridge FibreBridge 7500N produce il seguente output:

     ```
     FC-to-SAS Bridge:
     cisco_A_1-1:9.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100189
     cisco_A_1-2:1.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100162
     ```

   - Ogni shelf di dischi su una linea separata sotto ogni porta FC a cui è visibile:

     ```
     Shelf   0: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     Shelf   1: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     ```

   - Ciascun disco su una linea separata sotto ciascuna porta FC a cui è visibile:

     ```
     cisco_A_1-1:9.126L1   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
     (879097968 520B/sect)
     cisco_A_1-1:9.126L2   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
     (879097968 520B/sect)
     ```

3. Verificare che l'assegnazione automatica dei dischi sia attivata dalla console di uno dei controller:

   `storage disk option show`

   Il criterio di assegnazione automatica viene visualizzato nella colonna Auto Assign (assegnazione automatica).

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

4. Se nel sistema non è attivata l'assegnazione automatica dei dischi o se i dischi nello stesso stack appartengono a entrambi i controller, assegnare i dischi ai pool appropriati.

   "Gestione di dischi e aggregati"

   > Se si suddivide un singolo stack di shelf di dischi tra due controller, l'assegnazione automatica dei dischi deve essere disattivata prima di assegnare la proprietà dei dischi; in caso contrario, quando si assegna un singolo disco, i dischi rimanenti potrebbero essere assegnati automaticamente allo stesso controller e pool.
   >
   > Il `storage disk option modify -node` *`node-name`* `-autoassign off` il comando disattiva l'assegnazione automatica del disco.

   > I dischi non devono essere aggiunti ad aggregati o volumi fino a quando il firmware del disco e dello shelf non sono stati aggiornati.

5. Aggiornare il firmware dello shelf di dischi alla versione più recente utilizzando le istruzioni per il firmware scaricato.

   È possibile eseguire i comandi della procedura dalla console di sistema di uno dei controller.

   "Download NetApp: Firmware shelf di dischi"

6. Installare e cablare lo shelf di dischi:

   > Non forzare un connettore in una porta. I cavi mini-SAS sono inseriti; quando orientati correttamente in una porta SAS, il cavo SAS scatta in posizione e il LED LNK della porta SAS dello shelf di dischi si illumina di verde.per gli shelf di dischi, inserire un connettore per cavo SAS con la linguetta rivolta verso l'alto (sul lato superiore del connettore).

   a. Installare lo shelf di dischi, accenderlo e impostare l'ID dello shelf.

      La *Guida all'installazione* per il modello di shelf di dischi fornisce informazioni dettagliate sull'installazione di shelf di dischi.

      > È necessario spegnere e riaccendere lo shelf di dischi e mantenere gli ID dello shelf univoci per ogni shelf di dischi SAS all'interno dell'intero sistema di storage.

   b. Scollegare il cavo SAS dalla porta IOM B dell'ultimo shelf dello stack, quindi ricollegarlo alla stessa porta del nuovo shelf.

      L'altra estremità del cavo rimane collegata al ponte B.

   c. Collegare a margherita il nuovo shelf di dischi collegando le nuove porte IOM dello shelf (di IOM A e IOM B) alle ultime porte IOM dello shelf (di IOM A e IOM B).

   La *Guida all'installazione* per il modello di shelf di dischi fornisce informazioni dettagliate sugli shelf di dischi con concatenamento a margherita.

7. Aggiornare il firmware del disco alla versione più recente dalla console di sistema.

   "Download NetApp: Firmware del disco"

a. Passare al livello di privilegio avanzato:
   `set -privilege advanced`

   Devi rispondere con **`y`** quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

b. Aggiornare il firmware del disco alla versione più recente dalla console di sistema:
   `storage disk firmware update`

c. Tornare al livello di privilegio admin:
   `set -privilege admin`

d. Ripetere i passaggi precedenti sull'altro controller.

8. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che il sistema sia multipercorso:

      `node run -node node-name sysconfig -a`

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:
      `system health alert show`

   c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
      `metrocluster show`

   d. Eseguire un controllo MetroCluster:
      `metrocluster check run`

   e. Visualizzare i risultati del controllo MetroCluster:

      `metrocluster check show`

   f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

      `storage switch show`

   g. Eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

9. Se si stanno aggiungendo a caldo più shelf di dischi, ripetere i passaggi precedenti per ogni shelf di dischi che si sta aggiungendo a caldo.

Aggiunta a caldo di uno shelf di dischi IOM12 a uno stack di shelf di dischi IOM6 in una configurazione MetroCluster con collegamento a ponte

A seconda della versione di ONTAP in uso, è possibile aggiungere a caldo uno shelf di dischi IOM12 a uno stack di shelf di dischi IOM6 in una configurazione MetroCluster con collegamento a ponte.

Per eseguire questa procedura, vedere "Shelf hot-adding con moduli IOM12 a uno stack di shelf con moduli IOM6".

Rimozione a caldo dello storage da una configurazione MetroCluster FC

È possibile rimuovere a caldo gli shelf di dischi, ovvero rimuovere fisicamente gli shelf che hanno rimosso gli aggregati dai dischi, da una configurazione MetroCluster FC in grado di gestire i dati. Puoi rimuovere a caldo uno o più shelf da qualsiasi punto all'interno di una pila di shelf o rimuovere una pila di shelf.

- Il sistema deve essere una configurazione ha multipath, multipath, ha quad-path o quad-path.
- In una configurazione MetroCluster FC a quattro nodi, la coppia ha locale non può trovarsi in uno stato di Takeover.
- È necessario aver già rimosso tutti gli aggregati dai dischi negli shelf che si stanno rimuovendo.

  > Se si tenta di eseguire questa procedura su configurazioni FC non MetroCluster con aggregati sullo shelf che si sta rimuovendo, si potrebbe causare il malfunzionamento del sistema con un panic su più dischi.

  La rimozione degli aggregati implica la suddivisione degli aggregati mirrorati sugli shelf che si stanno rimuovendo e la ricreazione degli aggregati mirrorati con un altro set di dischi.

  "Gestione di dischi e aggregati"

- È necessario rimuovere la proprietà del disco dopo aver rimosso gli aggregati dai dischi negli shelf che si stanno rimuovendo.

  "Gestione di dischi e aggregati"

- Se si rimuovono uno o più shelf dall'interno di uno stack, è necessario aver preso in considerazione la distanza per evitare gli shelf che si stanno rimuovendo.

  Se i cavi attuali non sono abbastanza lunghi, è necessario disporre di cavi più lunghi.

Questa attività si applica alle seguenti configurazioni MetroCluster FC:

- Configurazioni MetroCluster FC a collegamento diretto, in cui gli shelf di storage sono collegati direttamente ai controller di storage con cavi SAS
- Configurazioni MetroCluster FC con collegamento a fabric o bridge, in cui gli shelf di storage sono collegati mediante bridge FC-SAS

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:
      `node run -node node-name sysconfig -a`
   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      `system health alert show`

   c. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale:
      `metrocluster show`

d. Eseguire un controllo MetroCluster:

```
metrocluster check run
```

e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

```
storage switch show
```

g. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Verificare che sugli shelf non siano presenti unità mailbox: **`storage failover mailbox-disk show`**
4. Rimuovere lo shelf seguendo i passaggi per lo scenario pertinente.

Scenario	Fasi
Per rimuovere un aggregato quando lo shelf contiene unmirrored, mirrored o entrambi i tipi di aggregato…	a. Utilizzare `storage aggregate delete -aggregate` *`aggregate name`* comando per rimuovere l'aggregato. b. Utilizzare la procedura standard per rimuovere la proprietà di tutti i dischi nello shelf, quindi rimuovere fisicamente lo shelf. Per rimuovere a caldo gli shelf, seguire le istruzioni riportate nella *SAS Disk Shelf Service Guide* relativa al modello di shelf in uso.

Per rimuovere un plesso da un aggregato mirrorato, è necessario eseguire il mirroring dell'aggregato.	a. Identificare il plesso che si desidera rimuovere utilizzando `run -node local sysconfig -r` comando.
	
	Nell'esempio seguente, è possibile identificare il plex dalla linea `Plex /dpg_mcc_8020_13_a1_aggr1/plex0`. In questo caso, il plex da specificare è "plex0".
	
	``
	dpgmcc_8020_13_a1a2::storage aggregate> run -node local sysconfig -r
	*** This system has taken over dpg-mcc-8020-13-a1
	Aggregate dpg_mcc_8020_13_a1_aggr1 (online, raid_dp, mirrored) (block checksums)
	  Plex /dpg_mcc_8020_13_a1_aggr1/plex0 (online, normal, active, pool0)
	  RAID group /dpg_mcc_8020_13_a1_aggr1/plex0/rg0 (normal, block checksums)
	  RAID Disk Device HA SHELF BAY CHAN Pool Type RPM Used (MB/blks) Phys (MB/blks)
	  --------- ------ ------------- ---- ---- ---- ----- --------------
	  dparity mcc-cisco-8Gb-fab-2:1-1.126L16 0c 32 15 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	  parity mcc-cisco-8Gb-fab-2:1-1.126L18 0c 32 17 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	  data mcc-cisco-8Gb-fab-2:1-1.126L19 0c 32 18 FC:B 0 SAS 15000 272000/557056000 274845/562884296
	  data mcc-cisco-8Gb-
	``
	
	1014

Sostituzione senza interruzioni di uno shelf in una configurazione stretch MetroCluster

Puoi sostituire gli shelf di dischi senza interruzioni in una configurazione stretch MetroCluster con uno shelf di dischi completamente popolato o uno shelf di dischi e trasferire i componenti dallo shelf che stai rimuovendo.

Il modello di shelf di dischi che si sta installando deve soddisfare i requisiti di sistema storage specificati nella "Hardware Universe", Che include i modelli di shelf supportati, i tipi di dischi supportati, il numero massimo di shelf di dischi in uno stack e le versioni ONTAP supportate.

Fasi

1. Mettere a terra l'utente.
2. Identificare tutti gli aggregati e i volumi che hanno dischi del loop che contengono lo shelf che si sta sostituendo e prendere nota del nome del plex interessato.

   Entrambi i nodi potrebbero contenere dischi del loop dello shelf interessato e aggregati host o volumi host.

3. Scegliere una delle due opzioni seguenti in base allo scenario di sostituzione che si sta pianificando.
   - Se si sta sostituendo uno shelf completo di dischi, inclusi chassis, dischi e moduli i/o (IOM), eseguire l'azione corrispondente come descritto nella tabella seguente:

Scenario	Azione
Il plesso interessato contiene meno dischi dallo shelf interessato.	Sostituire i dischi uno per uno sullo shelf interessato con parti di ricambio di un altro shelf. Dopo aver completato la sostituzione del disco, è possibile portare il plex offline.
Il plesso interessato contiene più dischi di quelli presenti nello shelf interessato.	Spostare il plex offline ed eliminare il plex.
Il plesso interessato contiene qualsiasi disco dello shelf interessato.	Spostare il plex offline ma non eliminarlo.

   - Se si sta sostituendo solo lo chassis dello shelf di dischi e nessun altro componente, attenersi alla seguente procedura:
     i. Offline i plex interessati dal controller in cui sono ospitati:

     ```
     aggregate offline
     ```

     ii. Verificare che i plessi siano offline:

     ```
     aggregate status -r
     ```

4. Identificare le porte SAS del controller a cui è collegato lo shelf loop interessato e disattivare le porte SAS su entrambi i controller del sito:

```
storage port disable -node node_name -port SAS_port
```

Lo shelf loop interessato è collegato a entrambi i siti.

5. Attendere che ONTAP riconosca l'assenza del disco.
   a. Verificare che il disco non sia presente:

      `sysconfig -a` oppure `sysconfig -r`

   b. Utilizzare `storage aggregate plex delete -aggregate aggr_name -plex plex_name` comando per rimuovere il plex.

      plex definisce il nome del plex, ad esempio "plex3" o "plex6".

   c. Utilizzare la procedura standard per rimuovere la proprietà di tutti i dischi nello shelf, quindi rimuovere fisicamente lo shelf.

      Per rimuovere a caldo gli shelf, seguire le istruzioni riportate nella *SAS Disk Shelf Service Guide* relativa al modello di shelf in uso.

6. Spegnere l'interruttore di alimentazione sullo shelf di dischi.
7. Scollegare tutti i cavi di alimentazione dallo shelf di dischi.
8. Annotare le porte da cui si scollegano i cavi in modo da poter collegare il nuovo shelf di dischi allo stesso modo.
9. Scollegare e rimuovere i cavi che collegano lo shelf di dischi agli altri shelf di dischi o al sistema di storage.
10. Rimuovere lo shelf del disco dal rack.

    Per rendere lo shelf di dischi più leggero e facile da manovrare, rimuovere gli alimentatori e l'IOM. Se si desidera installare uno chassis per shelf di dischi, rimuovere anche i dischi o i supporti. In caso contrario, evitare di rimuovere i dischi o i supporti, se possibile, poiché una manipolazione eccessiva può causare danni al disco interno.

11. Installare e fissare lo shelf di dischi sostitutivo sulle staffe di supporto e sul rack.
12. Se è stato installato uno chassis per shelf di dischi, reinstallare gli alimentatori e IOM.
13. Riconfigurare lo stack di shelf di dischi collegando tutti i cavi alle porte dello shelf di dischi sostitutivi esattamente come sono stati configurati sullo shelf di dischi rimosso.
14. Accendere lo shelf di dischi sostitutivo e attendere che i dischi si accendano.
15. Modificare l'ID dello shelf del disco con un ID univoco compreso tra 0 e 98.
16. Abilitare le porte SAS precedentemente disattivate.
    a. Attendere che ONTAP riconosca che i dischi sono stati inseriti.
    b. Verificare che i dischi siano inseriti:

       `sysconfig -a` oppure `sysconfig -r`

17. Se si sta sostituendo lo shelf completo di dischi (chassis per shelf di dischi, dischi, IOM), attenersi alla seguente procedura:

    > Se si sta sostituendo solo lo chassis dello shelf di dischi e nessun altro componente, passare alla fase 19.

    a. Determinare se l'assegnazione automatica del disco è attivata (on).

       `storage disk option modify -autoassign`

    L'assegnazione dei dischi avviene automaticamente.

    a. Se l'assegnazione automatica del disco non è attivata, assegnare manualmente la proprietà del disco.

18. Sposta di nuovo online i plex:

```
FC_A    1   SAS 15000
  272000/557056000
  280104/573653840
```

```
aggregate online plex name
```

19. Ricreare eventuali plex cancellati eseguendo il mirroring dell'aggregato.
20. Monitorare i plessi mentre iniziano la risincronizzazione:

```
aggregate status -r <aggregate name>
```

21. Verificare che il sistema storage funzioni come previsto:

```
system health alert show
```

Sostituzione senza interruzioni di uno shelf in una configurazione MetroCluster collegata al fabric

Potrebbe essere necessario sapere come sostituire uno shelf senza interruzioni in una configurazione Fabric-Attached MetroCluster.

> Questa procedura deve essere utilizzata solo in una configurazione Fabric-Attached MetroCluster.

Disattivazione dell'accesso allo shelf

È necessario disattivare l'accesso allo shelf prima di sostituire i moduli dello shelf.

Controllare lo stato generale della configurazione. Se il sistema non risulta integro, risolvere il problema prima di procedere.

Fasi

1. Da entrambi i cluster, offline tutti i plessi con dischi nello shelf stack interessato:

   ```
   aggr offline plex_name
   ```

   L'esempio mostra i comandi per l'offlining dei plex per un controller che esegue l'ONTAP in cluster.

   ```
   cluster_A_1::> storage aggregate plex offline -aggr aggrA_1_0 -plex
   plex0
   cluster_A_1::> storage aggregate plex offline -aggr dataA_1_data -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr aggrA_2_0 -plex
   plex0
   cluster_A_2::> storage aggregate plex offline -aggr dataA_2_data -plex
   plex0
   ```

2. Verificare che i plessi siano offline:

   ```
   aggr status -raggr_name
   ```

   L'esempio mostra i comandi per verificare che gli aggregati siano offline per un controller che esegue

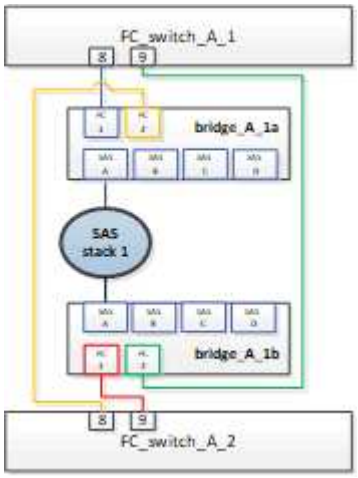
cmode.

```
Cluster_A_1::> storage aggregate show -aggr aggrA_1_0
Cluster_A_1::> storage aggregate show -aggr dataA_1_data
Cluster_A_2::> storage aggregate show -aggr aggrA_2_0
Cluster_A_2::> storage aggregate show -aggr dataA_2_data
```

3. Disattivare le porte SAS o dello switch a seconda che i bridge che collegano lo shelf di destinazione collegino un singolo stack SAS o due o più stack SAS:

   - Se i bridge collegano un singolo stack SAS, disattivare le porte dello switch a cui sono collegati i bridge utilizzando il comando appropriato per lo switch.

     L'esempio seguente mostra una coppia di bridge che collegano un singolo stack SAS, che contiene lo shelf di destinazione:



     Le porte 8 e 9 di ogni switch collegano i bridge alla rete.

     Nell'esempio seguente vengono mostrate le porte 8 e 9 disabilitate su uno switch Brocade.

```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9

FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

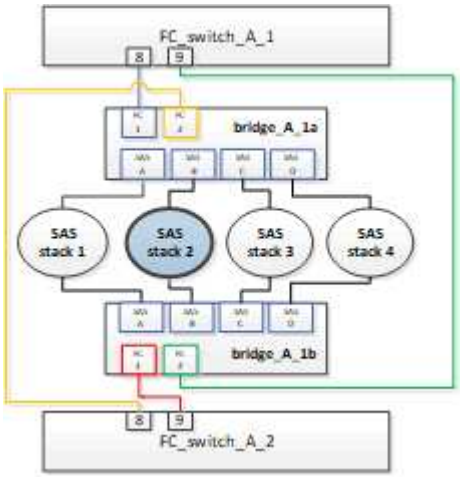
     L'esempio seguente mostra la disattivazione delle porte 8 e 9 su uno switch Cisco.

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

- Se i bridge collegano due o più stack SAS, disattivare le porte SAS che collegano i bridge allo shelf di destinazione:
  `SASportDisable` *`port number`*

  L'esempio seguente mostra una coppia di bridge che collegano quattro stack SAS. Lo stack SAS 2 contiene lo shelf di destinazione:



La porta SAS B collega i bridge allo shelf di destinazione. Disattivando solo la porta SAS B su entrambi gli shelf, gli altri stack SAS possono continuare a servire i dati durante la procedura di sostituzione.

In questo caso, disattivare la porta SAS che collega il bridge allo shelf di destinazione:

`SASportDisable` *`port number`*

L'esempio seguente mostra che la porta SAS B è disattivata dal bridge e verifica che sia disattivata. È necessario ripetere il comando su entrambi i bridge.

```
Ready. *
SASPortDisable B

SAS Port B has been disabled.
```

4. Se in precedenza le porte dello switch sono state disattivate, verificare che siano disattivate:

   `switchShow`

   L'esempio mostra che le porte dello switch sono disattivate su uno switch Brocade.

   ```
   FC_switch_A_1:admin> switchShow
   FC_switch_A_2:admin> switchShow
   ```

   L'esempio mostra che le porte dello switch sono disattivate su uno switch Cisco.

   ```
   FC_switch_A_1# show interface fc1/6
   FC_switch_A_2# show interface fc1/6
   ```

5. Attendere che ONTAP si renda conto che il disco è mancante.
6. Spegnere lo shelf che si desidera sostituire.

Sostituzione dello shelf

Rimuovere fisicamente tutti i cavi e lo shelf prima di inserire e collegare i nuovi shelf e moduli.

Fasi

1. Rimuovere tutti i dischi e scollegare tutti i cavi dallo shelf da sostituire.
2. Rimuovere i moduli dello shelf.
3. Inserire il nuovo ripiano.
4. Inserire i nuovi dischi nel nuovo shelf.
5. Inserire i moduli dello shelf.
6. Cablare lo shelf (SAS o Power).
7. Accendere lo shelf.

Riabilitare l'accesso e verificare il funzionamento

Una volta sostituito lo shelf, è necessario riabilitare l'accesso e verificare che il nuovo shelf funzioni correttamente.

Fasi

1. Verificare che lo shelf si accenda correttamente e che siano presenti i collegamenti sui moduli IOM.
2. Abilitare le porte dello switch o la porta SAS in base ai seguenti scenari:

Opzione	Fase

Se in precedenza sono state disattivate le porte dello switch	a. Abilitare le porte dello switch:
	
	`portEnable` *`port number`*
	
	L'esempio mostra la porta dello switch attivata su uno switch Brocade.
	
	`Switch_A_1:admin> portEnable 6`
	`Switch_A_2:admin> portEnable 6`
	
	L'esempio mostra la porta dello switch abilitata su uno switch Cisco.
	
	`Switch_A_1# conf t`
	`Switch_A_1(config)# int fc1/6`
	`Switch_A_1(config)# no shut`
	`Switch_A_1(config)# end`
	
	`Switch_A_2# conf t`
	`Switch_A_2(config)# int fc1/6`
	`Switch_A_2(config)# no shut`
	`Switch_A_2(config)# end`

Se in precedenza è stata disattivata una porta SAS	a. Abilitare la porta SAS che collega lo stack alla posizione dello shelf:
	
	`SASportEnable` *`port number`*
	
	L'esempio mostra che la porta SAS A è abilitata dal bridge e verifica che sia abilitata.
	
	`Ready. *`
	`SASPortEnable A`
	
	`SAS Port A has been enabled.`

3. Se in precedenza le porte dello switch sono state disattivate, verificare che siano attivate e in linea e che tutti i dispositivi siano collegati correttamente:

   `switchShow`

   L'esempio mostra `switchShow` Comando per verificare che uno switch Brocade sia in linea.

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

L'esempio mostra `switchShow` Comando per verificare che uno switch Cisco sia in linea.

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

> Dopo alcuni minuti, ONTAP rileva l'inserimento di nuovi dischi e visualizza un messaggio per ogni nuovo disco.

4. Verificare che i dischi siano stati rilevati da ONTAP:

   `sysconfig -a`

5. Online i plex offline in precedenza:

   `aggr online`*`plex_name`*

   L'esempio mostra i comandi per posizionare i plex su un controller che esegue cmode di nuovo online.

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

   I plessi iniziano a risincronizzarsi.

> È possibile monitorare l'avanzamento della risincronizzazione utilizzando `aggr status -`*`raggr_name`* comando.

Quando migrare i volumi root in una nuova destinazione

Potrebbe essere necessario spostare i volumi root in un altro aggregato root all'interno di una configurazione MetroCluster a due o quattro nodi.

Migrazione dei volumi root all'interno di una configurazione MetroCluster a due nodi

Per migrare i volumi root in un nuovo aggregato root all'interno di una configurazione MetroCluster a due nodi, fare riferimento a. "Come spostare mroot in un nuovo aggregato root in un Clustered MetroCluster a 2 nodi con switchover". Questa procedura illustra come migrare senza interruzioni i volumi root durante un'operazione di switchover MetroCluster. Questa procedura è leggermente diversa da quella utilizzata in una configurazione a quattro nodi.

Migrazione dei volumi root all'interno di una configurazione MetroCluster a quattro nodi

Per migrare i volumi root in un nuovo aggregato root all'interno di una configurazione MetroCluster a quattro nodi, è possibile utilizzare "nodo di sistema migra-root" controllare rispettando i seguenti requisiti.

- È possibile utilizzare il nodo di sistema migra-root per spostare gli aggregati root all'interno di una configurazione MetroCluster a quattro nodi.
- Tutti gli aggregati root devono essere sottoposti a mirroring.
- È possibile aggiungere nuovi shelf su entrambi i siti con dischi più piccoli per ospitare l'aggregato root.
- Prima di collegare nuovi dischi, è necessario controllare i limiti dei dischi supportati dalla piattaforma.

  "NetApp Hardware Universe"

- Se si sposta l'aggregato root su dischi più piccoli, è necessario adattare le dimensioni minime del volume root della piattaforma per garantire il salvataggio di tutti i file core.

> La procedura a quattro nodi può essere applicata anche a una configurazione a otto nodi.

Spostamento di un volume di metadati nelle configurazioni MetroCluster

È possibile spostare un volume di metadati da un aggregato a un altro in una configurazione MetroCluster. È possibile spostare un volume di metadati quando l'aggregato di origine viene decommissionato o non viene eseguito il mirroring o per altri motivi che rendono l'aggregato non idoneo.

- Per eseguire questa attività, è necessario disporre dei privilegi di amministratore del cluster.
- L'aggregato di destinazione deve essere mirrorato e non deve trovarsi nello stato degradato.
- Lo spazio disponibile nell'aggregato di destinazione deve essere maggiore del volume di metadati che si sta spostando.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Identificare il volume di metadati da spostare:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identificare un aggregato di destinazione idoneo:

   `metrocluster check config-replication show-aggregate-eligibility`

   Il seguente comando identifica gli aggregati in cluster_A idonei per ospitare i volumi di metadati:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

Nell'esempio precedente, Node_A_1_aggr2 e Node_A_2_aggr2 sono idonei.

4. Avviare l'operazione di spostamento del volume:

   volume move start -vserver *svm_name* -volume *metadata_volume_name* -destination -aggregate *destination_aggregate_name*

   Il seguente comando sposta il volume di metadati `MDV_CRS_14c00d4ac9f311e7922800a0984395f1` da `aggregate Node_A_1_aggr1` a. `aggregate Node_A_1_aggr2`:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verificare lo stato dell'operazione di spostamento del volume:

   `volume move show -volume vol_constituent_name`

6. Tornare al livello di privilegio admin:

   `set -privilege admin`

Ridenominazione di un cluster nelle configurazioni MetroCluster

La ridenominazione di un cluster in una configurazione MetroCluster implica l'esecuzione delle modifiche e la verifica, sia sul cluster locale che su quello remoto, della corretta applicazione della modifica.

Fasi

1. Visualizzare i nomi dei cluster utilizzando

   `metrocluster node show`

   comando:

   ```
   cluster_1::*> metrocluster node show
   DR                              Configuration  DR
   Group Cluster Node              State          Mirroring Mode
   ----- ------- ------------------ -------------- ---------
   --------------------
   1     cluster_1
                 node_A_1           configured     enabled   normal
                 node_A_2           configured     enabled   normal
         cluster_2
                 node_B_1           configured     enabled   normal
                 node_B_2           configured     enabled   normal
   4 entries were displayed.
   ```

2. Rinominare il cluster:

   `cluster identity modify -name new_name`

   Nell'esempio seguente, il `cluster_1` il cluster viene rinominato `cluster_A`:

   ```
   cluster_1::*> cluster identity modify -name cluster_A
   ```

3. Verificare sul cluster locale che il cluster rinominato sia in esecuzione normalmente:

   `metrocluster node show`

Nell'esempio seguente, il nuovo rinominato `cluster_A` funziona normalmente:

```
cluster_A::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

4. Rinominare il cluster remoto:

   `cluster peer modify-local-name -name` *`cluster_2`* `-new-name` *`cluster_B`*

   Nell'esempio seguente, `cluster_2` viene rinominato `cluster_B`:

```
cluster_A::> cluster peer modify-local-name -name cluster_2 -new-name
cluster_B
```

5. Verificare sul cluster remoto che il cluster locale sia stato rinominato e che funzioni normalmente:

   `metrocluster node show`

   Nell'esempio seguente, il nuovo rinominato `cluster_B` funziona normalmente:

```
cluster_B::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
      cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
4 entries were displayed.
```

6. Ripetere questa procedura per ogni cluster che si desidera rinominare.

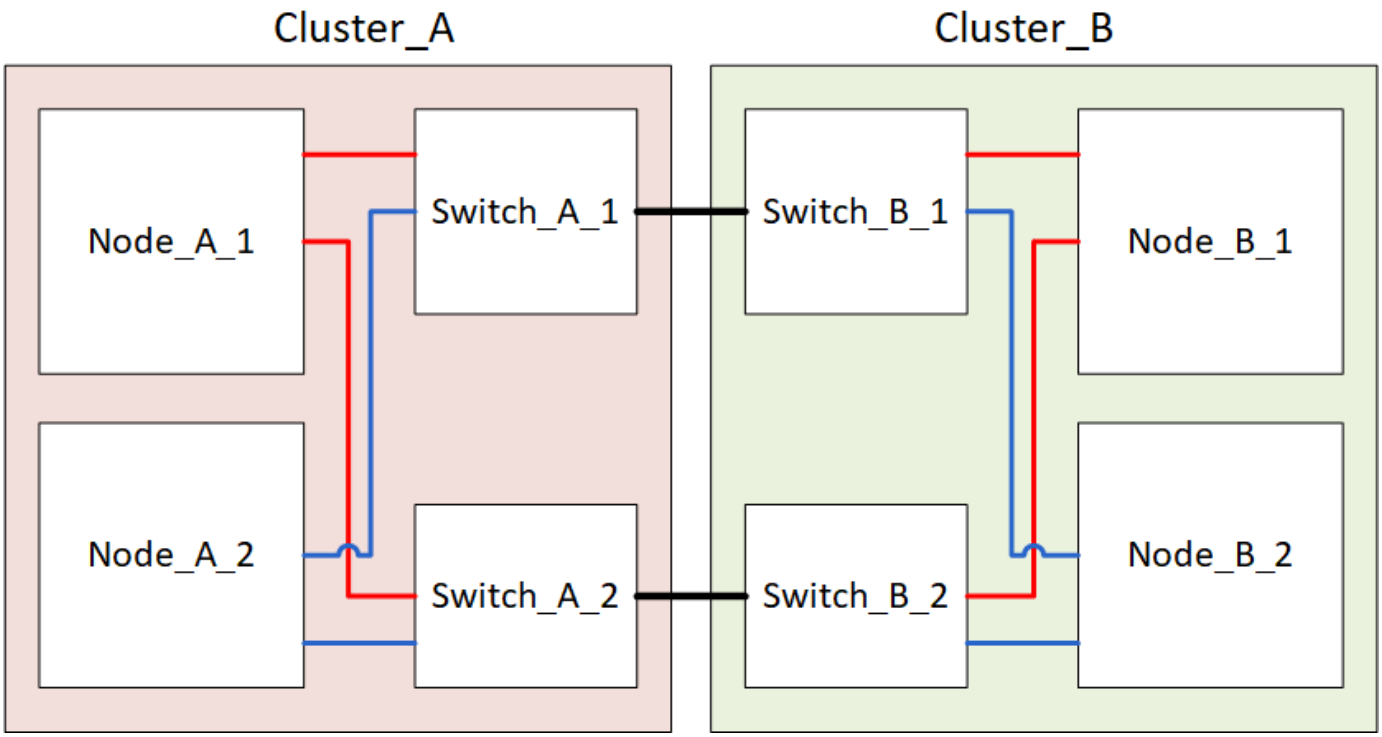
Spegnere e riaccendere un singolo sito MetroCluster

Spegnere e riaccendere un singolo sito in una configurazione IP di MetroCluster

Se è necessario eseguire la manutenzione del sito o spostare un singolo sito in una configurazione IP MetroCluster, è necessario sapere come spegnere e riaccendere il sito.

Per spostare e riconfigurare un sito (ad esempio per l'espansione da un cluster a quattro nodi a uno a otto nodi), non è possibile completare contemporaneamente le attività. Questa procedura descrive solo le fasi necessarie per eseguire la manutenzione del sito o per spostare un sito senza modificarne la configurazione.

Il seguente diagramma mostra una configurazione MetroCluster. Il cluster_B è spento per la manutenzione.



Spegnere un sito MetroCluster

È necessario spegnere un sito e tutte le apparecchiature prima di iniziare la manutenzione o il trasferimento del sito.

A proposito di questa attività

Tutti i comandi dei seguenti passaggi vengono emessi dal sito che rimane acceso.

Fasi

1. Prima di iniziare, verificare che gli aggregati non mirrorati nel sito siano offline.
2. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

```
system health alert show
```

c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

```
metrocluster show
```

d. Eseguire un controllo MetroCluster:
```
metrocluster check run
```

e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

```
storage switch show
```

g. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

3. Dal sito in cui si desidera rimanere attivi, implementare lo switchover:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Il completamento dell'operazione può richiedere alcuni minuti.

4. Monitorare e verificare il completamento dello switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Se si dispone di una configurazione MetroCluster IP con ONTAP 9.6 o versione successiva, attendere che i plex del sito di emergenza siano online e che le operazioni di riparazione vengano completate automaticamente.

   Nelle configurazioni IP di MetroCluster che eseguono ONTAP 9,5 o versione precedente, i nodi del sito di disastro non si avviano automaticamente su ONTAP e i plex rimangono offline.

6. Spostare offline tutti i volumi e le LUN che appartengono agli aggregati senza mirror.
   a. Spostare i volumi offline.

      ```
      cluster_A::* volume offline <volume name>
      ```

   b. Spostare i LUN offline.

      ```
      cluster_A::* lun offline lun_path <lun_path>
      ```

7. Sposta aggregati senza mirror offline: `storage aggregate offline`

   ```
   cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
   ```

8. A seconda della configurazione e della versione di ONTAP, identificare e spostare offline i plex interessati che si trovano nel sito di emergenza (Cluster_B).

   Devi spostare i seguenti plessi offline:

   - Plessi non mirrorati che risiedono su dischi situati nel sito di disastro.

     Se non si spostano offline i plex non di mirroring del sito di disastro, potrebbe verificarsi un'interruzione quando il sito di disastro viene successivamente spento.

   - Plessi mirrorati che risiedono su dischi situati nel sito di disastro per il mirroring aggregato. Una volta spostati offline, i plex non sono accessibili.

   a. Identificare i plessi interessati.

      I plex di proprietà dei nodi nel sito sopravvissuto sono costituiti da dischi Pool1. I plex di proprietà dei nodi nel sito di disastro sono costituiti da dischi Pool0.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

I plex interessati sono quelli remoti al cluster A. La seguente tabella indica se i dischi sono locali o remoti rispetto al cluster A:

Nodo	Dischi nel pool	I dischi devono essere impostati offline?	Esempio di plessi da spostare offline
Nodo _A_1 e nodo _A_2	Dischi nel pool 0	No I dischi sono locali nel cluster A.	-
Dischi nel pool 1	Sì. I dischi sono remoti nel cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nodo _B_1 e nodo _B_2

Dischi nel pool 0	Sì. I dischi sono remoti nel cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Dischi nel pool 1

b. Sposta i plessi interessati offline:

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

> Eseguire questa operazione per tutti i plessi che hanno dischi remoti a Cluster_A.

9. Le porte dello switch ISL sono costantemente offline in base al tipo di switch.
10. Arrestare i nodi eseguendo il seguente comando su ciascun nodo:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Spegnere l'apparecchiatura in caso di disastro.

    È necessario spegnere le seguenti apparecchiature nell'ordine indicato:

    - Switch IP MetroCluster
    - Controller di storage
    - Shelf di storage

Spostamento del sito spento di MetroCluster

Una volta spento il sito, è possibile iniziare il lavoro di manutenzione. La procedura è la stessa sia che i componenti MetroCluster vengano ricollocati all'interno dello stesso data center sia che vengano ricollocati in un data center diverso.

- Il cavo dell'hardware deve essere identico a quello del sito precedente.
- Se la velocità, la lunghezza o il numero di InterSwitch link (ISL) sono stati modificati, è necessario riconfigurare tutti.

Fasi

1. Verificare che il cablaggio di tutti i componenti sia registrato attentamente in modo che possa essere ricollegato correttamente nella nuova posizione.
2. Spostare fisicamente tutto l'hardware, i controller di storage, gli switch IP, i FibreBridge e gli shelf di storage.
3. Configurare le porte ISL e verificare la connettività tra siti.

a. Accendere gli switch IP.

> Non * accendere altre apparecchiature.

4. Utilizzare gli strumenti sugli switch (se disponibili) per verificare la connettività tra siti.

> Procedere solo se i collegamenti sono correttamente configurati e stabili.

5. Disattivare nuovamente i collegamenti se risultano stabili.

Accensione della configurazione MetroCluster e ripristino del normale funzionamento

Una volta completata la manutenzione o spostato il sito, è necessario accendere il sito e ripristinare la configurazione MetroCluster.

A proposito di questa attività

Tutti i comandi descritti di seguito vengono emessi dal sito di accensione.

Fasi

1. Accendere gli interruttori.

   Accendere prima gli interruttori. Potrebbero essere stati accesi durante la fase precedente se il sito è stato trasferito.

   a. Riconfigurare il collegamento interswitch (ISL) se necessario o se non è stato completato come parte del trasferimento.
   b. Abilitare l'ISL se la scherma è stata completata.
   c. Verificare l'ISL.

2. Accendere i controller di archiviazione e attendere che venga visualizzato `LOADER` prompt. I controller non devono essere completamente avviati.

   Se l'avvio automatico è attivato, premere `Ctrl+C` per interrompere l'avvio automatico dei controller.

3. Accendere gli scaffali, lasciando abbastanza tempo per accenderli completamente.
   a. Verificare che gli shelf e i dischi sui bridge siano chiaramente visibili.

      È possibile utilizzare un comando come `sastargets` Sulla CLI atto.

4. Verificare che la memoria locale sia visibile dal nodo in modalità manutenzione:

   ```
   disk show -v
   ```

5. Ristabilire la configurazione MetroCluster.

   Seguire le istruzioni riportate in "Verificare che il sistema sia pronto per lo switchback" Per eseguire operazioni di healing e switchback in base alla configurazione MetroCluster.

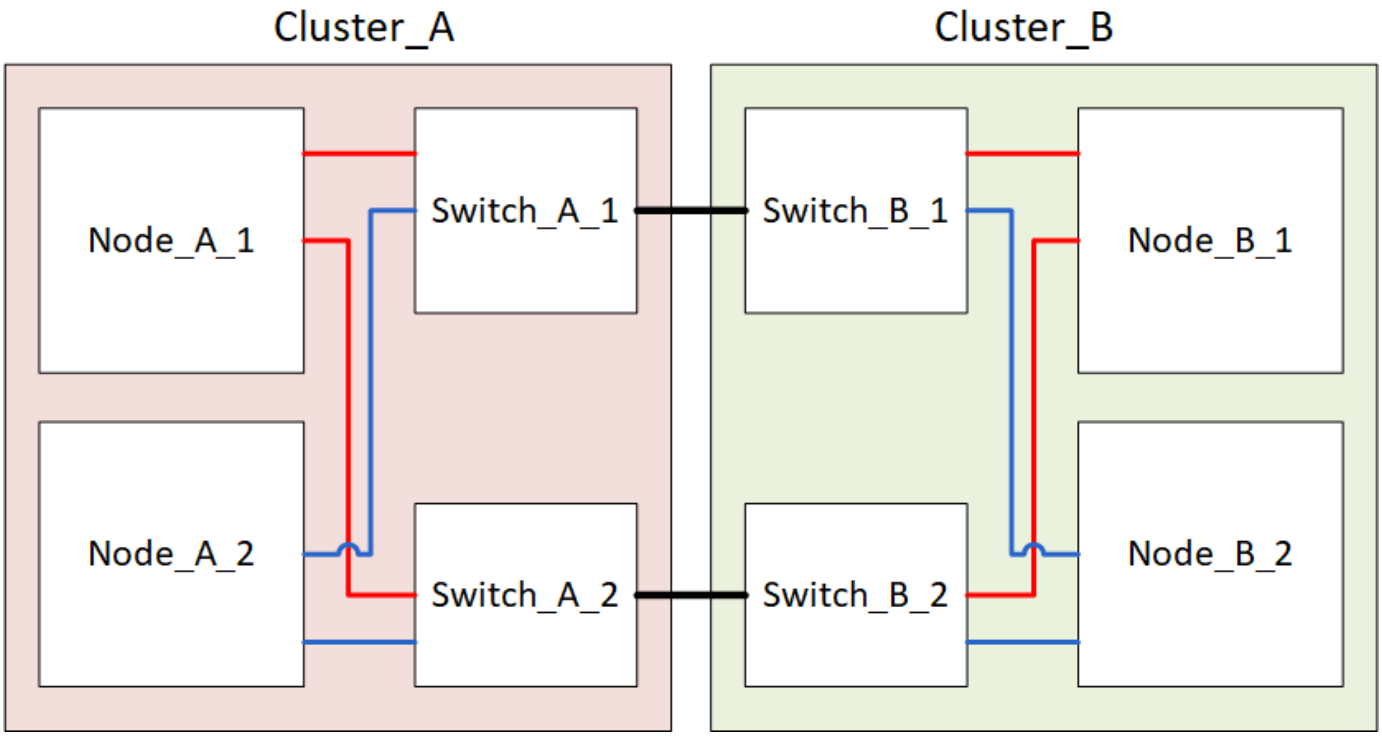
Spegnere e riaccendere un singolo sito in una configurazione MetroCluster FC

Se è necessario eseguire la manutenzione del sito o spostare un singolo sito in una

configurazione FC MetroCluster, è necessario sapere come spegnere e riaccendere il sito.

Per spostare e riconfigurare un sito (ad esempio per l'espansione da un cluster a quattro nodi a uno a otto nodi), non è possibile completare contemporaneamente le attività. Questa procedura descrive solo le fasi necessarie per eseguire la manutenzione del sito o per spostare un sito senza modificarne la configurazione.

Il seguente diagramma mostra una configurazione MetroCluster. Il cluster_B è spento per la manutenzione.



Spegnere un sito MetroCluster

È necessario spegnere un sito e tutte le apparecchiature prima di iniziare la manutenzione o il trasferimento del sito.

A proposito di questa attività

Tutti i comandi dei seguenti passaggi vengono emessi dal sito che rimane acceso.

Fasi

1. Prima di iniziare, verificare che gli aggregati non mirrorati nel sito siano offline.
2. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

      ```
      system health alert show
      ```

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

```
metrocluster show
```

d. Eseguire un controllo MetroCluster:
```
metrocluster check run
```

e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

```
storage switch show
```

g. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

3. Dal sito in cui si desidera rimanere attivi, implementare lo switchover:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

Il completamento dell'operazione può richiedere alcuni minuti.

Gli aggregati senza mirror saranno online solo dopo uno switchover se i dischi remoti dell'aggregato sono accessibili. In caso di errore degli ISL, il nodo locale potrebbe non essere in grado di accedere ai dati nei dischi remoti senza mirror. Il guasto di un aggregato può causare il riavvio del nodo locale.

4. Monitorare e verificare il completamento dello switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. Spostare offline tutti i volumi e le LUN che appartengono agli aggregati senza mirror.
   a. Spostare i volumi offline.

      ```
      cluster_A::* volume offline <volume name>
      ```

   b. Spostare i LUN offline.

      ```
      cluster_A::* lun offline lun_path <lun_path>
      ```

6. Sposta aggregati senza mirror offline: `storage aggregate offline`

   ```
   cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
   ```

7. A seconda della configurazione e della versione di ONTAP, identificare e spostare offline i plex interessati che si trovano nel sito di emergenza (Cluster_B).

   Devi spostare i seguenti plessi offline:

   - Plessi non mirrorati che risiedono su dischi situati nel sito di disastro.

     Se non si spostano offline i plex non di mirroring del sito di disastro, potrebbe verificarsi un'interruzione quando il sito di disastro viene successivamente spento.

   - Plessi mirrorati che risiedono su dischi situati nel sito di disastro per il mirroring aggregato. Una volta spostati offline, i plex non sono accessibili.

   a. Identificare i plessi interessati.

      I plex di proprietà dei nodi nel sito sopravvissuto sono costituiti da dischi Pool1. I plex di proprietà dei nodi nel sito di disastro sono costituiti da dischi Pool0.

```
Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

I plex interessati sono quelli remoti al cluster A. La seguente tabella indica se i dischi sono locali o remoti rispetto al cluster A:

Nodo	Dischi nel pool	I dischi devono essere impostati offline?	Esempio di plessi da spostare offline
Nodo _A_1 e nodo _A_2	Dischi nel pool 0	No I dischi sono locali nel cluster A.	-
Dischi nel pool 1	Sì. I dischi sono remoti nel cluster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nodo _B_1 e nodo _B_2

Dischi nel pool 0	Sì. I dischi sono remoti nel cluster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Dischi nel pool 1

b. Sposta i plessi interessati offline:

`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+

> Eseguire questa operazione per tutti i plessi che hanno dischi remoti a Cluster_A.

8. Le porte dello switch ISL sono costantemente offline in base al tipo di switch.

Tipo di switch	Azione

Per gli switch FC Brocade…	a. Utilizzare `portcfgpersistentdisable <port>` per disattivare in modo permanente le porte, come illustrato nell'esempio seguente. Questa operazione deve essere eseguita su entrambi gli switch del sito sopravvissuto.
	
	`Switch_A_1:admin> portcfgpersistentdisable 14`
	`Switch_A_1:admin> portcfgpersistentdisable 15`
	`Switch_A_1:admin>`
	
	b. Verificare che le porte siano disattivate utilizzando `switchshow` comando mostrato nell'esempio seguente:
	
	`Switch_A_1:admin> switchshow`
	`switchName: Switch_A_1`
	`switchType: 109.1`
	`switchState: Online`
	`switchMode: Native`
	`switchRole: Principal`
	`switchDomain: 2`
	`switchId: fffc02`
	`switchWwn: 10:00:00:05:33:88:9c:68`
	`zoning: ON (T5_T6)`
	`switchBeacon: OFF`
	`FC Router: OFF`
	`FC Router BB Fabric ID: 128`
	`Address Mode: 0`
	
	`Index Port Address Media Speed State Proto`
	`==========`
	`...`
	`14 14 020e00 id 16G No_Light FC`
	`Disabled (Persistent)`
	`15 15 020f00 id 16G No_Light FC`
	`Disabled (Persistent)`
	`...`
	`Switch_A_1:admin>`

Per gli switch FC Cisco…	a. Utilizzare `interface` per disattivare in modo persistente le porte. Nell'esempio seguente vengono mostrate le porte 14 e 15 disabilitate:
	
	`Switch_A_1# conf t`
	`Switch_A_1(config)# interface fc1/14-15`
	`Switch_A_1(config)# shut`
	
	`Switch_A_1(config-if)# end`
	`Switch_A_1# copy running-config startup-config`
	
	b. Verificare che la porta dello switch sia disattivata utilizzando `show interface brief` come illustrato nell'esempio seguente:
	
	`Switch_A_1# show interface brief`
	`Switch_A_1`

9. Spegnere l'apparecchiatura in caso di disastro.

   Le seguenti apparecchiature devono essere spente nell'ordine indicato:

   - Switch FC MetroCluster
   - Storage controller: Gli storage controller devono trovarsi attualmente nella `LOADER` è necessario spegnerli completamente.
   - Shelf di storage
   - ATTO FibreBridge (se presente)

Spostamento del sito spento di MetroCluster

Una volta spento il sito, è possibile iniziare il lavoro di manutenzione. La procedura è la stessa sia che i componenti MetroCluster vengano ricollocati all'interno dello stesso data center sia che vengano ricollocati in un data center diverso.

- Il cavo dell'hardware deve essere identico a quello del sito precedente.
- Se la velocità, la lunghezza o il numero di InterSwitch link (ISL) sono stati modificati, è necessario riconfigurare tutti.

Fasi

1. Verificare che il cablaggio di tutti i componenti sia registrato attentamente in modo che possa essere ricollegato correttamente nella nuova posizione.
2. Spostare fisicamente tutto l'hardware, i controller di storage, gli switch FC, i FibreBridge e gli shelf di storage.
3. Configurare le porte ISL e verificare la connettività tra siti.

   a. Accendere gli switch FC.

Non * accendere altre apparecchiature.

b. Attivare le porte.

Abilitare le porte in base ai tipi di switch corretti nella seguente tabella:

Tipo di switch	Comando

Per gli switch FC Brocade…	i. Utilizzare `portcfgpersistentenable <port number>` per abilitare in modo permanente la porta. Questa operazione deve essere eseguita su entrambi gli switch del sito sopravvissuto. L'esempio seguente mostra le porte 14 e 15 attivate sullo switch_A_1. ``` switch_A_1:admin> portcfgpersistentenable 14 switch_A_1:admin> portcfgpersistentenable 15 switch_A_1:admin> ``` ii. Verificare che la porta dello switch sia abilitata: `switchshow` L'esempio seguente mostra che le porte 14 e 15 sono attivate: ``` switch_A_1:admin> switchshow switchName: Switch_A_1 switchType: 109.1 switchState: Online switchMode: Native switchRole: Principal switchDomain: 2 switchId: fffc02 switchWwn: 10:00:00:05:33:88:9c:68 zoning: ON (T5_T6) switchBeacon: OFF FC Router: OFF FC Router BB Fabric ID: 128 Address Mode: 0 Index Port Address Media Speed State Proto == ==== ... 14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" 15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream) ... switch_A_1:admin> ```

Per gli switch FC Cisco…	i. Inserire il `interface` per attivare la porta. L'esempio seguente mostra le porte 14 e 15 attivate sullo switch_A_1. ``` switch_A_1# conf t switch_A_1(config)# interface fc1/14-15 switch_A_1(config)# no shut switch_A_1(config-if)# end switch_A_1# copy running-config startup-config ``` ii. Verificare che la porta dello switch sia abilitata: `show interface brief` ``` switch_A_1# show interface brief switch_A_1# ```

4. Utilizzare gli strumenti sugli switch (se disponibili) per verificare la connettività tra siti.

   Procedere solo se i collegamenti sono correttamente configurati e stabili.

5. Disattivare nuovamente i collegamenti se risultano stabili.

   Disattivare le porte in base all'utilizzo di switch Brocade o Cisco, come illustrato nella tabella seguente:

Tipo di switch	Comando

Per gli switch FC Brocade…	a. Inserire il `portcfgpersistentdisable <port_number>` per disattivare in modo permanente la porta.
	
	Questa operazione deve essere eseguita su entrambi gli switch del sito sopravvissuto. L'esempio seguente mostra le porte 14 e 15 disattivate sullo switch_A_1:
	
	`switch_A_1:admin> portpersistentdisable 14`
	`switch_A_1:admin> portpersistentdisable 15`
	`switch_A_1:admin>`
	
	b. Verificare che la porta dello switch sia disattivata: `switchshow`
	
	L'esempio seguente mostra che le porte 14 e 15 sono disattivate:
	
	`switch_A_1:admin> switchshow`
	`switchName: Switch_A_1`
	`switchType: 109.1`
	`switchState:  Online`
	`switchMode: Native`
	`switchRole: Principal`
	`switchDomain:  2`
	`switchId:  fffc02`
	`switchWwn:  10:00:00:05:33:88:9c:68`
	`zoning:  ON (T5_T6)`
	`switchBeacon:  OFF`
	`FC Router:  OFF`
	`FC Router BB Fabric ID: 128`
	`Address Mode:  0`
	
	`Index Port Address Media Speed State Proto`
	`==========`
	`...`
	`14  14  020e00  id  16G  No_Light FC  Disabled (Persistent)`
	`15  15  020f00  id  16G  No_Light FC  Disabled (Persistent)`
	`...`
	`switch_A_1:admin>`

Per gli switch FC Cisco…	a. Disattivare la porta utilizzando `interface` comando.
	
	L'esempio seguente mostra le porte fc1/14 e fc1/15 disattivate sullo switch A_1:
	
	`switch_A_1# conf t`
	
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Verificare che la porta dello switch sia disattivata utilizzando `show interface brief` comando.
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

Accensione della configurazione MetroCluster e ripristino del normale funzionamento

Una volta completata la manutenzione o spostato il sito, è necessario accendere il sito e ripristinare la configurazione MetroCluster.

A proposito di questa attività

Tutti i comandi descritti di seguito vengono emessi dal sito di accensione.

Fasi

1. Accendere gli interruttori.

   Accendere prima gli interruttori. Potrebbero essere stati accesi durante la fase precedente se il sito è stato trasferito.

   a. Riconfigurare il collegamento interswitch (ISL) se necessario o se non è stato completato come parte del trasferimento.
   b. Abilitare l'ISL se la scherma è stata completata.
   c. Verificare l'ISL.
2. Disattivare gli ISL sugli switch FC.
3. Accendere i controller di archiviazione e attendere che venga visualizzato `LOADER` prompt. I controller non devono essere completamente avviati.

   Se l'avvio automatico è attivato, premere `Ctrl+C` per interrompere l'avvio automatico dei controller.

4. Accendere gli shelf e attendere il tempo necessario per l'accensione completa.

5. Accendere i bridge FibreBridge.
   a. Sugli switch FC, verificare che le porte che collegano i bridge siano in linea.

      È possibile utilizzare un comando come `switchshow` Per switch Brocade, e. `show interface brief` Per switch Cisco.

   b. Verificare che gli shelf e i dischi sui bridge siano chiaramente visibili.

      È possibile utilizzare un comando come `sastargets` Sulla CLI atto.

6. Abilitare gli ISL sugli switch FC.

   Attivare le porte in base all'utilizzo di switch Brocade o Cisco, come mostrato nella tabella seguente:

Tipo di switch	Comando

Per gli switch FC Brocade…	a. Inserire il `portcfgpersistentenable <port>` per abilitare in modo persistente le porte. Questa operazione deve essere eseguita su entrambi gli switch del sito sopravvissuto.
	
	L'esempio seguente mostra le porte 14 e 15 attivate sullo switch_A_1:
	
	`Switch_A_1:admin> portcfgpersistentenable 14`
	`Switch_A_1:admin> portcfgpersistentenable 15`
	`Switch_A_1:admin>`
	
	b. Verificare che la porta dello switch sia abilitata utilizzando il segno `switchshow` comando:
	
	`switch_A_1:admin> switchshow`
	`switchName: Switch_A_1`
	`switchType: 109.1`
	`switchState: Online`
	`switchMode: Native`
	`switchRole: Principal`
	`switchDomain: 2`
	`switchId: fffc02`
	`switchWwn: 10:00:00:05:33:88:9c:68`
	`zoning: ON (T5_T6)`
	`switchBeacon: OFF`
	`FC Router: OFF`
	`FC Router BB Fabric ID: 128`
	`Address Mode: 0`
	
	`Index Port Address Media Speed State Proto`
	`==========`
	`...`
	`14 14 020e00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1"`
	`15 15 020f00 id 16G Online FC E-Port 10:00:00:05:33:86:89:cb "Switch_A_1" (downstream)`
	`...`
	`switch_A_1:admin>`

Per gli switch FC Cisco…	a. Utilizzare `interface` per abilitare le porte.
	
	L'esempio seguente mostra l'abilitazione della porta fc1/14 e fc1/15 sullo switch A_1:
	
	`switch_A_1# conf t`
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# no shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Verificare che la porta dello switch sia disattivata:
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

7. Verificare che lo storage sia visibile dal sito sopravvissuto. Riportare online i plesso offline. In questo modo vengono rieseguite le operazioni di risync e viene ristabilita SyncMirror.
8. Ristabilire la configurazione MetroCluster.

   Seguire le istruzioni riportate in "Verificare che il sistema sia pronto per lo switchback" Per eseguire operazioni di healing e switchback in base alla configurazione MetroCluster.

Spegnere un'intera configurazione MetroCluster

Spegnimento di un'intera configurazione IP MetroCluster

Prima di iniziare la manutenzione o il trasferimento, è necessario spegnere l'intera configurazione IP di MetroCluster e tutte le apparecchiature.

> A partire da ONTAP 9.8, la **`storage switch`** il comando viene sostituito con **`system switch`**. La procedura riportata di seguito mostra **`storage switch`** Ma se si utilizza ONTAP 9.8 o versione successiva, il comando **`system switch`** è preferibile utilizzare il comando.

1. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster.
   a. Verificare che la configurazione e la modalità operativa di MetroCluster siano normali.
      `metrocluster show`
   b. Eseguire il seguente comando:
      `metrocluster interconnect show`
   c. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:
      `run local sysconfig -v`

d. Eseguire il seguente comando:
storage port show

e. Eseguire il seguente comando:
storage switch show

f. Eseguire il seguente comando:
network interface show

g. Eseguire il seguente comando:
network port show

h. Eseguire il seguente comando:
network device-discovery show

i. Eseguire un controllo MetroCluster:
metrocluster check run

j. Visualizzare i risultati del controllo MetroCluster:
metrocluster check show

k. Eseguire il seguente comando:
metrocluster configuration-settings interface show

2. Se necessario, disattivare AUSO modificando IL dominio di errore AUSO in

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

> In una configurazione IP MetroCluster, il dominio di errore AUSODISABLED è già impostato su 'ausodisabled', a meno che la configurazione non sia configurata con il supporto ONTAP.

3. Verificare la modifica utilizzando il comando

metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Arrestare i nodi:

halt

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. Spegnere le seguenti apparecchiature presso il sito:
   - Controller di storage
   - Switch IP MetroCluster
   - Shelf di storage
6. Attendere trenta minuti, quindi accendere tutti gli shelf di storage, gli switch IP MetroCluster e i controller di storage.
7. Dopo aver acceso i controller, verificare la configurazione MetroCluster da entrambi i siti.

   Per verificare la configurazione, ripetere il passaggio 1.

8. Eseguire i controlli del ciclo di alimentazione.
   a. Verificare che tutte le SVM di origine della sincronizzazione siano online:
      `vserver show`
   b. Avviare tutte le SVM di origine della sincronizzazione non in linea:
      `vserver start`

Spegnimento di un'intera configurazione MetroCluster FC

Prima di iniziare la manutenzione o il trasferimento del sito, è necessario spegnere l'intera configurazione MetroCluster FC e tutte le apparecchiature.

A proposito di questa attività

È necessario eseguire le fasi di questa procedura da entrambi i siti, contemporaneamente.

> 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. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster.
   a. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale.
      `metrocluster show`
   b. Confermare la connettività ai dischi immettendo il seguente comando su uno qualsiasi dei nodi MetroCluster:
      `run local sysconfig -v`
   c. Eseguire il seguente comando:
      `storage bridge show`
   d. Eseguire il seguente comando:
      `storage port show`
   e. Eseguire il seguente comando:
      `storage switch show`

f. Eseguire il seguente comando:
network port show

g. Eseguire un controllo MetroCluster:
metrocluster check run

h. Visualizzare i risultati del controllo MetroCluster:
metrocluster check show

2. Disattivare AUSO modificando IL dominio di errore AUSO in

auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

3. Verificare la modifica utilizzando il comando

metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Arrestare i nodi utilizzando il seguente comando: **halt**
   - Per una configurazione MetroCluster a quattro o otto nodi, utilizzare **inhibit-takeover** e. **skip-lif-migration-before-shutdown** parametri:

     ```
     system node halt -node node1_SiteA -inhibit-takeover true -ignore
     -quorum-warnings true -skip-lif-migration-before-shutdown true
     ```

   - Per una configurazione MetroCluster a due nodi, utilizzare il comando:

     ```
     system node halt -node node1_SiteA -ignore-quorum-warnings true
     ```

5. Spegnere le seguenti apparecchiature presso il sito:
   - Controller di storage
   - Switch FC MetroCluster (se in uso e la configurazione non è una configurazione stretch a due nodi)
   - ATTO FibreBridges
   - Shelf di storage
6. Attendere trenta minuti, quindi accendere la seguente apparecchiatura presso il sito:

- Shelf di storage
- ATTO FibreBridges
- Switch FC MetroCluster
- Controller di storage

7. Dopo aver acceso i controller, verificare la configurazione MetroCluster da entrambi i siti.

   Per verificare la configurazione, ripetere il passaggio 1.

8. Eseguire i controlli del ciclo di alimentazione.
   a. Verificare che tutte le SVM di origine della sincronizzazione siano online:
      `vserver show`
   b. Avviare tutte le SVM di origine della sincronizzazione non in linea:
      `vserver start`

Riconfigurazione del layout di uno switch FC configurato prima di ONTAP 9.x.

Se il layout dello switch FC esistente è stato configurato prima di ONTAP 9.1, è necessario riconfigurare il layout delle porte e applicare i file di configurazione di riferimento (RCF) più recenti. Questa procedura si applica solo alle configurazioni MetroCluster FC.

Prima di iniziare

È necessario identificare gli switch FC presenti nel dominio fabric.

È necessaria la password admin e l'accesso a un server FTP o SCP.

È necessario eseguire questa attività se il layout dello switch FC esistente è stato configurato prima di ONTAP 9.1. Non è necessario eseguire l'aggiornamento da un layout di switch esistente configurato per ONTAP 9.1 o versione successiva.

A proposito di questa attività

Questa procedura è senza interruzioni e richiede circa quattro ore per il completamento (esclusi rack e stack) quando i dischi vengono azzerati.

Invio di un messaggio AutoSupport personalizzato prima della riconfigurazione degli switch

Prima di riconfigurare gli switch, devi inviare un messaggio AutoSupport per informare il supporto tecnico di NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours*
```

intervallo di manutenzione in ore specifica la durata della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

3. Ripetere questi passaggi sul sito del partner.

Verifica dello stato della configurazione MetroCluster

Verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che i componenti di MetroCluster siano integri:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   L'operazione viene eseguita in background.

2. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

   Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

   ```
   -----------
   cluster_A::*> metrocluster check show

   Component           Result
   ------------------- ---------
   nodes               ok
   lifs                ok
   config-replication  ok
   aggregates          warning
   clusters            ok
   connections         not-applicable
   volumes             ok
   7 entries were displayed.
   ```

3. Per verificare lo stato dell'operazione MetroCluster check in corso, utilizzare il comando:

   ```
   metrocluster operation history show -job-id 38
   ```

4. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

Verifica degli errori di configurazione di MetroCluster in corso

È possibile utilizzare lo strumento Config Advisor disponibile sul sito del supporto NetApp per verificare la presenza di errori di configurazione comuni.

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.

1. Scarica lo strumento Config Advisor.

   "Download NetApp: Config Advisor"

2. Eseguire Config Advisor, esaminare l'output e seguire i consigli per risolvere eventuali problemi.

Disattivazione persistente degli switch

È necessario disattivare gli switch nel fabric in modo persistente per modificarne la configurazione.

Per disattivare gli switch, eseguire i comandi sulla riga di comando dello switch; i comandi utilizzati per questo non sono comandi ONTAP.

Fasi

1. Disattivare in modo persistente lo switch:
   - Utilizzare il seguente comando per disattivare uno switch Brocade in modo persistente:

     ```
     FC_switch_A_1:admin> switchCfgPersistentDisable
     ```

   - Utilizzare il seguente comando per disattivare uno switch Cisco in modo persistente:

     ```
     vsan [vsna #] suspend
     ```

Determinazione del nuovo layout di cablaggio

È necessario determinare il cablaggio dei nuovi moduli controller e dei nuovi shelf di dischi per gli switch FC esistenti.

Questa attività deve essere eseguita in ogni sito MetroCluster.

Fasi

1. Utilizzare "Installazione e configurazione di Fabric-Attached MetroCluster" Per determinare il layout del cablaggio per il tipo di switch, utilizzando l'utilizzo della porta per una configurazione MetroCluster a otto nodi.

   L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo descritto nella documentazione in modo da poter utilizzare i file di configurazione di riferimento (RCF).

   > Non utilizzare questa procedura se il cablaggio non può utilizzare RCF.

Applicazione dei file RCF e ricablaggio degli switch

È necessario applicare i file di configurazione di riferimento (RCF) appropriati per riconfigurare gli switch in modo da ospitare i nuovi nodi. Dopo aver applicato i file RCF, è possibile recuperare gli switch.

L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo descritto in "Installazione e configurazione di Fabric-Attached MetroCluster" In modo da poter utilizzare gli RCF.

Fasi

1. Individuare i file RCF per la configurazione.

   È necessario utilizzare i file RCF corrispondenti al modello di switch in uso.

2. Applicare i file RCF seguendo le istruzioni nella pagina Download e regolando le impostazioni ISL in base alle necessità.
3. Verificare che la configurazione dello switch sia stata salvata.
4. Collegare entrambi i bridge FC-SAS agli switch FC, utilizzando il layout di cablaggio creato nella sezione "Ddefinizione del nuovo layout di cablaggio".
5. Verificare che le porte siano in linea:
   - Per gli switch Brocade, utilizzare `switchshow` comando.
   - Per gli switch Cisco, utilizzare `show interface brief` comando.
6. Collegare le porte FC-VI dai controller agli switch.
7. Dai nodi esistenti, verificare che le porte FC-VI siano in linea:

   ```
   metrocluster interconnect adapter show

   metrocluster interconnect mirror show
   ```

Abilitare gli switch in modo persistente

È necessario abilitare gli switch nel fabric in modo persistente.

Fasi

1. Abilitare costantemente lo switch:
   - Per gli switch Brocade, utilizzare `switchCfgPersistentenable` comando.
   - Per gli switch Cisco, utilizzare il comando no `suspend` comando. Il seguente comando abilita costantemente uno switch Brocade:

     ```
     FC_switch_A_1:admin> switchCfgPersistentenable
     ```

     Il seguente comando abilita uno switch Cisco:

   ```
   vsan [vsna #]no suspend
   ```

Verifica dello switchover, della riparazione e dello switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

1. Utilizzare le procedure per lo switchover negoziato, la riparazione e lo switchback descritte in "Gestione MetroCluster e disaster recovery".

Assegnazioni delle porte per switch FC

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.

A proposito di questa attività

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	Switch Brocade modelli 6505, 6510, 6520, 7840, G620, G610 e DCX 8510-8	
		Si connette 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

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 tabella seguente mostra l'utilizzo delle porte del controller sui modelli Brocade 6505, 6510 o DCX 8510-8:

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_3	Porta FC-VI A.	6	-
controller_x_3	Porta FC-VI b	-	6
controller_x_3	Porta HBA a	7	-
controller_x_3	Porta HBA b	-	7
controller_x_3	Porta HBA c	8	-
controller_x_3	Porta HBA d	-	8
controller_x_4	Porta FC-VI A.	9	-
controller_x_4	Porta FC-VI b	-	9
controller_x_4	Porta HBA a	10	-
controller_x_4	Porta HBA b	-	10
controller_x_4	Porta HBA c	11	-
controller_x_4	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 o 7600N:

Ponte	Porta Bridge	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
bridge_x_1a	FC2	-	12
bridge_x_1b	FC1	13	-
bridge_x_1b	FC2	-	13
bridge_x_2a	FC1	14	-
bridge_x_2a	FC2	-	14
bridge_x_2b	FC1	15	-
bridge_x_2b	FC2	-	15
bridge_x_3a	FC1	16	-

Ponte	Porta Bridge	FC_switch_x_1	FC_switch_x_2
bridge_x_3a	FC2	-	16
bridge_x_3b	FC1	17	-
bridge_x_3b	FC2	-	17
bridge_x_4a	FC1	18	-
bridge_x_4a	FC2	-	18
bridge_x_4b	FC1	19	-
bridge_x_4b	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 per gli switch Brocade 6505, 6510 o DCX 8510-8:

Porta ISL	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. La seguente tabella mostra l'utilizzo degli switch Brocade 6505, 6510 e DCX 8510-8.

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
controller_x_1	Porta FC-VI b	-	0
controller_x_1	Porta HBA a	1	-
controller_x_1	Porta HBA b	-	1
controller_x_1	Porta HBA c	2	-
controller_x_1	Porta HBA d	-	2
controller_x_2	Porta FC-VI A.	3	-
controller_x_2	Porta FC-VI b	-	3
controller_x_2	Porta HBA a	4	-
controller_x_2	Porta HBA b	-	4
controller_x_2	Porta HBA c	5	-
controller_x_2	Porta HBA d	-	5

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 o 7600N. È possibile cablare altri bridge alle porte da 18 a 23.

Bridge FibreBridge 7500	Porta	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1a	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
bridge_x_1b	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
bridge_x_2a	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
bridge_x_2b	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
bridge_x_3a	FC2	-	10	-	14
bridge_x_3b	FC1	11	-	15	-
bridge_x_3b	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
bridge_x_4a	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
bridge_x_4b	FC2	-	13	-	17
		è possibile cablare altri bridge attraverso la porta 19, quindi le porte da 24 a 47			

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:

Porta ISL	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
Porta ISL 1	20	20	8	8

Porta ISL	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
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. La seguente tabella mostra i cavi per gli switch Brocade 6505, 6510 e DCX 8510-8.

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	0	-
controller_x_1	Porta FC-VI b	-	0
controller_x_1	Porta HBA a	1	-
controller_x_1	Porta HBA b	-	1
controller_x_1	Porta HBA c	2	-
controller_x_1	Porta HBA d	-	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 bridge FibreBridge 7500N o 7600N con switch Brocade 6505, 6510 e DCX 8510-8. È possibile cablare altri bridge alle porte da 18 a 23.

Bridge FibreBridge 7500	Porta	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1a	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
bridge_x_1b	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
bridge_x_2a	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
bridge_x_2b	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
bridge_x_3a	FC2	-	10	-	14

Bridge FibreBridge 7500	Porta	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_3a	FC1	11	-	15	-
bridge_x_3a	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
bridge_x_4a	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
bridge_x_4b	FC2	-	13	-	17
		è possibile cablare altri bridge attraverso la porta 19, quindi le porte da 24 a 47		è possibile cablare altri bridge tramite la porta 23	

Utilizzo della porta Brocade per gli ISL in una configurazione MetroCluster a due nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo delle porte ISL per gli switch Brocade 6505, 6510 e DCX 8510-8:

Porta ISL	FC_switch_x_1 (6510 o DCX 8510-8)	FC_switch_x_2 (6510 o DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
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 9148 e 9148S:

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_3	Porta FC-VI A.	7	-
controller_x_3	Porta FC-VI b	-	7
controller_x_3	Porta HBA a	8	-
controller_x_3	Porta HBA b	-	8
controller_x_3	Porta HBA c	9	-
controller_x_3	Porta HBA d	-	9
controller_x_4	Porta FC-VI A.	10	-
controller_x_4	Porta FC-VI b	-	10

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_4	Porta HBA a	11	-
controller_x_4	Porta HBA b	-	11
controller_x_4	Porta HBA c	13	-
controller_x_4	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 bridge FibreBridge 7500N o 7600N con switch Cisco 9148 o 9148S.

Bridge FibreBridge 7500	Porta	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	14	14
bridge_x_1a	FC2	-	-
bridge_x_1b	FC1	15	15
bridge_x_1b	FC2	-	-
bridge_x_2a	FC1	17	17
bridge_x_2a	FC2	-	-
bridge_x_2b	FC1	18	18
bridge_x_2b	FC2	-	-
bridge_x_3a	FC1	19	19
bridge_x_3a	FC2	-	-
bridge_x_3b	FC1	21	21
bridge_x_3b	FC2	-	-
bridge_x_4a	FC1	22	22
bridge_x_4a	FC2	-	-
bridge_x_4b	FC1	23	23
bridge_x_4b	FC2	-	-

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 MetroCluster a otto nodi con ONTAP 9.0

La seguente tabella mostra l'utilizzo della porta ISL per gli switch Cisco 9148 e 9148S:

Porte ISL	FC_switch_x_1	FC_switch_x_2
Porta ISL 1	12	12
Porta ISL 2	16	16

Porte ISL	FC_switch_x_1	FC_switch_x_2
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 9148, 9148S e 9250i:

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	1	-
controller_x_1	Porta FC-VI b	-	1
controller_x_1	Porta HBA a	2	-
controller_x_1	Porta HBA b	-	2
controller_x_1	Porta HBA c	3	-
controller_x_1	Porta HBA d	-	3
controller_x_2	Porta FC-VI A.	4	-
controller_x_2	Porta FC-VI b	-	4
controller_x_2	Porta HBA a	5	-
controller_x_2	Porta HBA b	-	5
controller_x_2	Porta HBA c	6	-
controller_x_2	Porta HBA d	-	6

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 bridge FibreBridge 7500N o 7600N con switch Cisco 9148, 9148S o 9250i. È possibile collegare ulteriori bridge alle porte da 15 a 32 seguendo lo stesso schema.

Bridge FibreBridge 7500	Porta	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1a	FC2	-	7
bridge_x_1b	FC1	8	-
bridge_x_1b	FC2	-	8
bridge_x_2a	FC1	9	-
bridge_x_2a	FC2	-	9
bridge_x_2b	FC1	10	-
bridge_x_2b	FC2	-	10

Bridge FibreBridge 7500	Porta	FC_switch_x_1	FC_switch_x_2
bridge_x_3a	FC1	11	-
bridge_x_3a	FC2	-	11
bridge_x_3b	FC1	12	-
bridge_x_3b	FC2	-	12
bridge_x_4a	FC1	13	-
bridge_x_4a	FC2	-	13
bridge_x_4b	FC1	14	-
bridge_x_4b	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 per gli switch Cisco 9148 e 9148S:

Porta ISL	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 9148, 9148S e 9250i:

Componente	Porta	FC_switch_x_1	FC_switch_x_2
controller_x_1	Porta FC-VI A.	1	-
controller_x_1	Porta FC-VI b	-	1
controller_x_1	Porta HBA a	2	-
controller_x_1	Porta HBA b	-	2
controller_x_1	Porta HBA c	3	-
controller_x_1	Porta HBA d	-	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 bridge FibreBridge 7500N o 7600N con switch Cisco 9148, 9148S e 9250i. È possibile collegare ulteriori bridge alle porte da 15 a 32 seguendo lo stesso schema.

Bridge FibreBridge 7500	Porta	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1a	FC2	-	7
bridge_x_1b	FC1	8	-
bridge_x_1b	FC2	-	8
bridge_x_2a	FC1	9	-
bridge_x_2a	FC2	-	9
bridge_x_2b	FC1	10	-
bridge_x_2b	FC2	-	10
bridge_x_3a	FC1	11	-
bridge_x_3a	FC2	-	11
bridge_x_3b	FC1	12	-
bridge_x_3b	FC2	-	12
bridge_x_4a	FC1	13	-
bridge_x_4a	FC2	-	13
bridge_x_4b	FC1	14	-
bridge_x_4b	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 per gli switch Cisco 9148 o 9148S:

Porta ISL	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		Switch Brocade modello G720
		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		Switch Brocade modello G720
		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_51a	1	32	56	20
26	32	bridge_x_51b	2	32	56	20	26
32	Stack 2	bridge_x_52a	1	33	57	21	27
33	bridge_x_52b	2	33	57	21	27	33
Stack 3	bridge_x_53a	1	34	58	22	30	34
bridge_x_54b	2	34	58	22	30	34	Stack y
bridge_x_ya	1	35	59	23	31	35	bridge_x_yb

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 **Nota**: 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	

Utilizzo dello strumento matrice di interoperabilità per trovare le informazioni MetroCluster

Quando si imposta la configurazione MetroCluster, è possibile utilizzare lo strumento di interoperabilità per assicurarsi di utilizzare le versioni software e hardware supportate.

"Tool di matrice di interoperabilità NetApp"

Dopo aver aperto la matrice di interoperabilità, è possibile utilizzare il campo soluzione storage per selezionare la soluzione MetroCluster in uso.

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.

Dove trovare ulteriori informazioni

Ulteriori informazioni sulla configurazione, il funzionamento e il monitoraggio di una configurazione MetroCluster sono disponibili nella documentazione completa di NetApp.

Informazioni	Soggetto
"Documentazione MetroCluster"	• Tutte le informazioni MetroCluster
"Architettura e progettazione della soluzione NetApp MetroCluster"	• Panoramica tecnica della configurazione e del funzionamento di MetroCluster. • Best practice per la configurazione di MetroCluster.
"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Installazione e configurazione di MetroCluster IP"	• Architettura IP di MetroCluster • Collegamento della configurazione IP di MetroCluster • Configurazione di MetroCluster in ONTAP
"Documentazione NetApp: Guide e risorse sui prodotti"	• Monitoraggio della configurazione e delle prestazioni di MetroCluster
"Installazione e configurazione del software MetroCluster Tiebreaker"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster

Transizione da MetroCluster FC a MetroCluster IP

Scelta della procedura di transizione

Quando si passa a una configurazione MetroCluster IP, è necessario disporre di una combinazione di modelli di piattaforma supportati. È inoltre necessario assicurarsi che la piattaforma IP di MetroCluster sia delle dimensioni appropriate per il carico che si sta passando dalla configurazione FC di MetroCluster alla configurazione IP di MetroCluster.

La seguente tabella mostra le combinazioni di piattaforme supportate. È possibile passare da piattaforme nella colonna di sinistra a piattaforme elencate come supportate nelle colonne a destra, come indicato dalle celle colorate della tabella.

Ad esempio, è supportata la transizione da una configurazione MetroCluster FC costituita da moduli controller AFF8060 a una configurazione IP costituita da moduli controller AFF A400.

		Target MetroCluster IP platform									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster FC platform	FAS8020 AFF8020 FAS8040 AFF8040										
	FAS8060 AFF8060 FAS8080 AFF8080										
	FAS8200 AFF A300			Note 1							Note 1
	AFF A400 ASA A400										Note 1
	FAS9000 AFF A700										Note 2
	FAS9500 AFF A900 ASA A900										Note 3

- Nota 1: Questa combinazione di piattaforme richiede ONTAP 9.11.1 o versione successiva.
- Nota 2: È necessario disporre di un'interfaccia da 40 GbE per le interfacce cluster locali sui nodi FC. Questa combinazione di piattaforme richiede ONTAP 9.11.1 o versione successiva.
- Nota 3: È necessario disporre di un'interfaccia 100GbE per le interfacce cluster locali sui nodi FC. Questa combinazione di piattaforme richiede ONTAP 9.11.1 o versione successiva.
- Tutte le procedure di transizione richiedono ONTAP 9.8 o versioni successive, salvo diversamente indicato nelle note o come richiesto da una singola piattaforma.
- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, se si dispone di una configurazione a otto nodi, tutti e otto i nodi devono utilizzare la stessa versione di ONTAP.

- Non superare i limiti di oggetti della "parte inferiore" delle piattaforme nella combinazione. Applicare il limite inferiore di oggetti delle due piattaforme.
- Se i limiti della piattaforma di destinazione sono inferiori ai limiti MetroCluster, è necessario riconfigurare il MetroCluster in modo che sia pari o inferiore ai limiti della piattaforma di destinazione prima di aggiungere i nuovi nodi.
- Fare riferimento a. "Hardware Universe" per i limiti della piattaforma.

Selezionare una procedura di transizione in base alla configurazione MetroCluster FC esistente.

Una procedura di transizione sostituisce il fabric switch FC back-end o la connessione FC-VI con una rete switch IP. La procedura esatta dipende dalla configurazione iniziale.

Le piattaforme originali e gli switch FC (se presenti) vengono ritirati al termine della procedura di transizione.

Avvio della configurazione	Disruptivo o senza interruzioni	Requisiti	Procedura
Otto nodi	Senza interruzioni	I nuovi shelf di storage sono supportati sulle nuove piattaforme.	"Collegamento alla procedura"
Quattro nodi	Senza interruzioni	I nuovi shelf di storage sono supportati sulle nuove piattaforme.	"Collegamento alla procedura"
Due nodi	Disgregativo	I nuovi shelf di storage sono supportati sia sulle piattaforme originali che su quelle nuove.	"Collegamento alla procedura"
Due nodi	Disgregativo	I nuovi shelf di storage sono supportati sia sulle piattaforme originali che su quelle nuove. I vecchi shelf di storage devono essere ritirati.	"Collegamento alla procedura"
Due nodi	Disgregativo	I vecchi shelf di storage non sono supportati sulle nuove piattaforme. I vecchi shelf di storage devono essere ritirati.	"Collegamento alla procedura"

Transizione senza interruzioni da una configurazione MetroCluster FC a una configurazione MetroCluster IP (ONTAP 9.8 e versioni successive)

Transizione senza interruzioni da una configurazione MetroCluster FC a una configurazione MetroCluster IP (ONTAP 9.8 e versioni successive)

È possibile eseguire transizioni senza interruzioni di carichi di lavoro e dati da una configurazione MetroCluster FC esistente a una nuova configurazione MetroCluster IP.

A partire da ONTAP 9.13.1, questa procedura è supportata nelle configurazioni IP di MetroCluster in cui MetroCluster e gli shelf di dischi sono connessi agli stessi switch IP (configurazione di uno storage condiviso).

A partire da ONTAP 9.13.1, è possibile eseguire una transizione senza interruzioni di carichi di lavoro e dati da una configurazione MetroCluster FC a otto nodi esistente a una nuova configurazione MetroCluster IP.

A partire da ONTAP 9.8, è possibile eseguire una transizione senza interruzioni di carichi di lavoro e dati da una configurazione MetroCluster FC a quattro nodi esistente a una nuova configurazione MetroCluster IP.

- Questa procedura è senza interruzioni.

  La configurazione MetroCluster può continuare a fornire dati durante l'operazione.

- Questa procedura si applica solo alle configurazioni MetroCluster FC a quattro e otto nodi.

  Se si dispone di una configurazione MetroCluster FC a due nodi, vedere "Scelta della procedura di transizione".

- Questa procedura descrive i passaggi necessari per la transizione di un gruppo DR FC a quattro nodi. Se si dispone di una configurazione a otto nodi (due gruppi DR FC), è necessario ripetere l'intera procedura per ciascun gruppo DR FC.
- È necessario soddisfare tutti i requisiti e seguire tutte le fasi della procedura.

Prepararsi alla transizione da una configurazione MetroCluster FC a una configurazione MetroCluster IP

Requisiti per la transizione FC-IP senza interruzioni

Prima di avviare il processo di transizione, è necessario assicurarsi che la configurazione soddisfi i requisiti.

- Se si dispone di una configurazione a otto nodi, tutti i nodi devono eseguire ONTAP 9.13.1 o versione successiva.
- Se si dispone di una configurazione a quattro nodi, tutti i nodi devono eseguire ONTAP 9.8 o versione successiva.
- Le piattaforme esistenti e nuove devono essere una combinazione supportata per la transizione.

  "Piattaforme supportate per una transizione senza interruzioni"

- Deve supportare una configurazione del cluster con switch.

"NetApp Hardware Universe"

- Deve soddisfare tutti i requisiti e i cavi descritti nelle *procedure di installazione e configurazione di MetroCluster*.

  "Installazione e configurazione di Fabric-Attached MetroCluster"

  "Estensione dell'installazione e della configurazione di MetroCluster"

Impatto della transizione sui componenti hardware di MetroCluster

Dopo aver completato la procedura di transizione, i componenti principali della configurazione MetroCluster esistente sono stati sostituiti o riconfigurati.

- **Moduli controller**

  I moduli controller esistenti vengono sostituiti da nuovi moduli controller. I moduli controller esistenti vengono dismessi al termine delle procedure di transizione.

- **Storage shelf**

  I dati vengono spostati dai vecchi shelf ai nuovi shelf. I vecchi shelf vengono dismessi al termine delle procedure di transizione.

- **MetroCluster (back-end) e switch cluster**

  La funzionalità dello switch back-end viene sostituita dal fabric dello switch IP. Se la configurazione MetroCluster FC include switch FC e bridge FC-SAS, questi vengono dismessi al termine di questa procedura.

  Se la configurazione MetroCluster FC utilizzava switch cluster per l'interconnessione del cluster, in alcuni casi possono essere riutilizzati per fornire il fabric dello switch IP back-end. Gli switch cluster riutilizzati devono essere riconfigurati con RCF specifici per piattaforma e switch. procedure.

  Se la configurazione MetroCluster FC non utilizza switch cluster, vengono aggiunti nuovi switch IP per fornire il fabric switch back-end.

  "Considerazioni sugli switch IP"

- **Cluster peering network**

  Per la nuova configurazione IP di MetroCluster, è possibile utilizzare la rete di peering cluster fornita dal cliente. Il peering del cluster viene configurato sui nodi IP MetroCluster come parte della procedura di transizione.

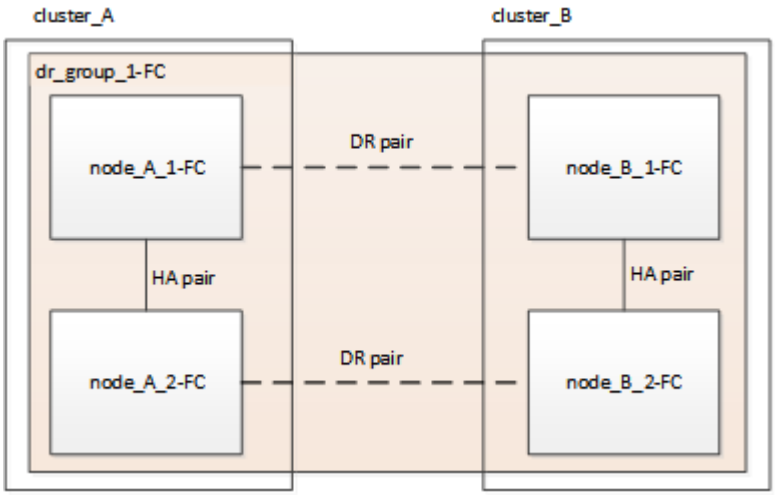
Workflow per la transizione MetroCluster senza interruzioni

È necessario seguire il workflow specifico per garantire una transizione senza interruzioni. Scegli il flusso di lavoro per la tua configurazione:

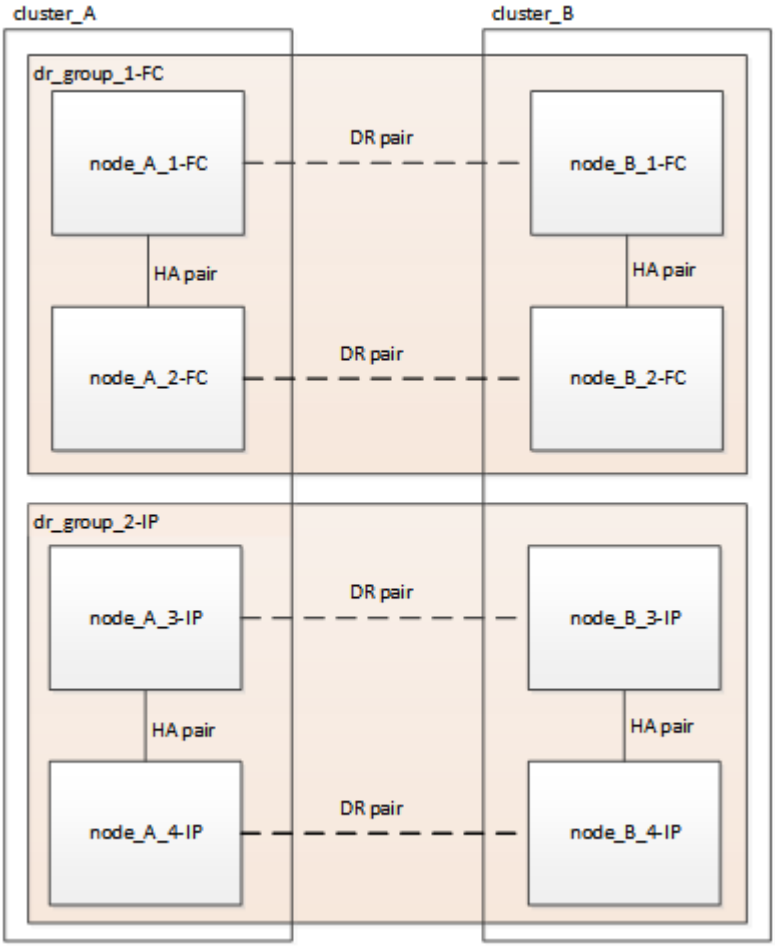
- Workflow di transizione della configurazione FC a quattro nodi
- Workflow di transizione della configurazione FC a otto nodi

Workflow di transizione della configurazione FC a quattro nodi

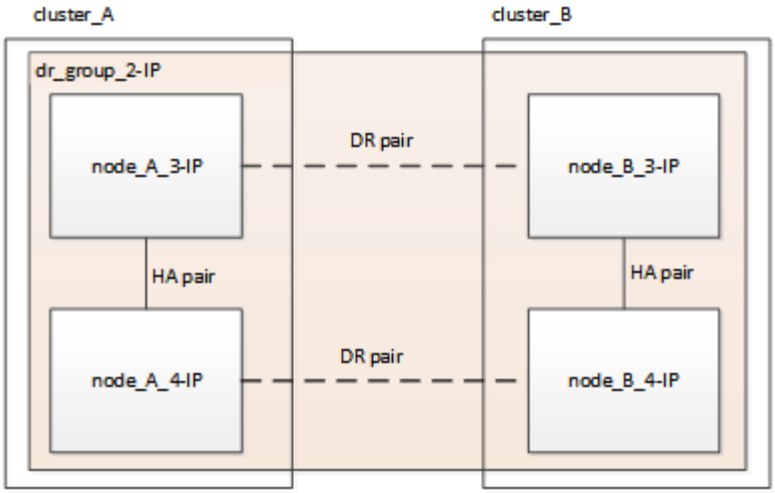
Il processo di transizione inizia con una configurazione FC MetroCluster a quattro nodi funzionante.



I nuovi nodi IP MetroCluster vengono aggiunti come secondo gruppo DR.

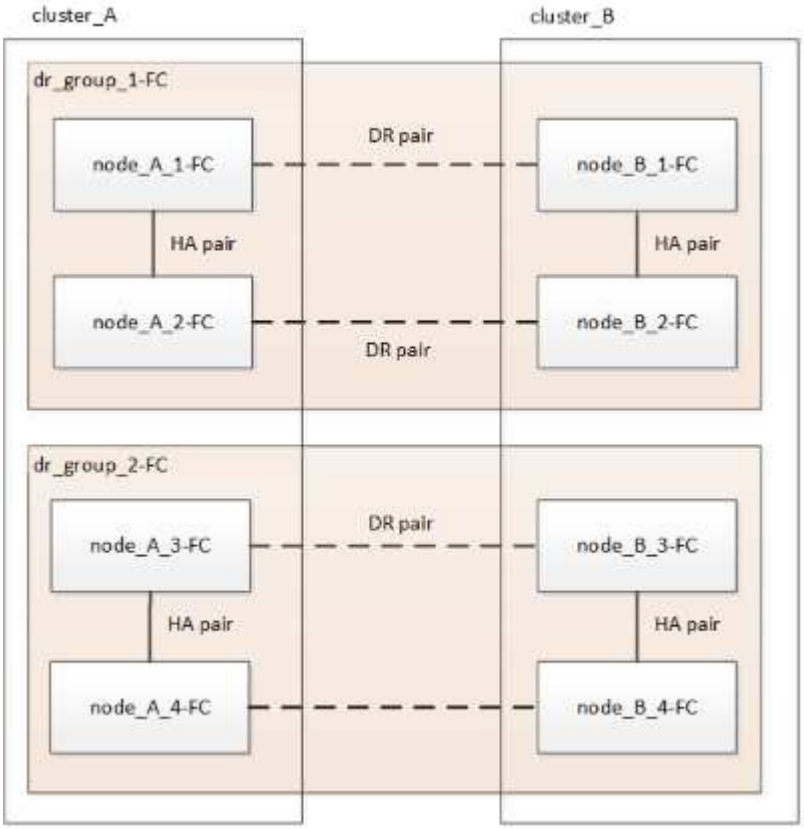


I dati vengono trasferiti dal vecchio gruppo DR al nuovo gruppo DR, quindi i vecchi nodi e il relativo storage vengono rimossi dalla configurazione e dismessi. Il processo termina con una configurazione IP MetroCluster a quattro nodi.

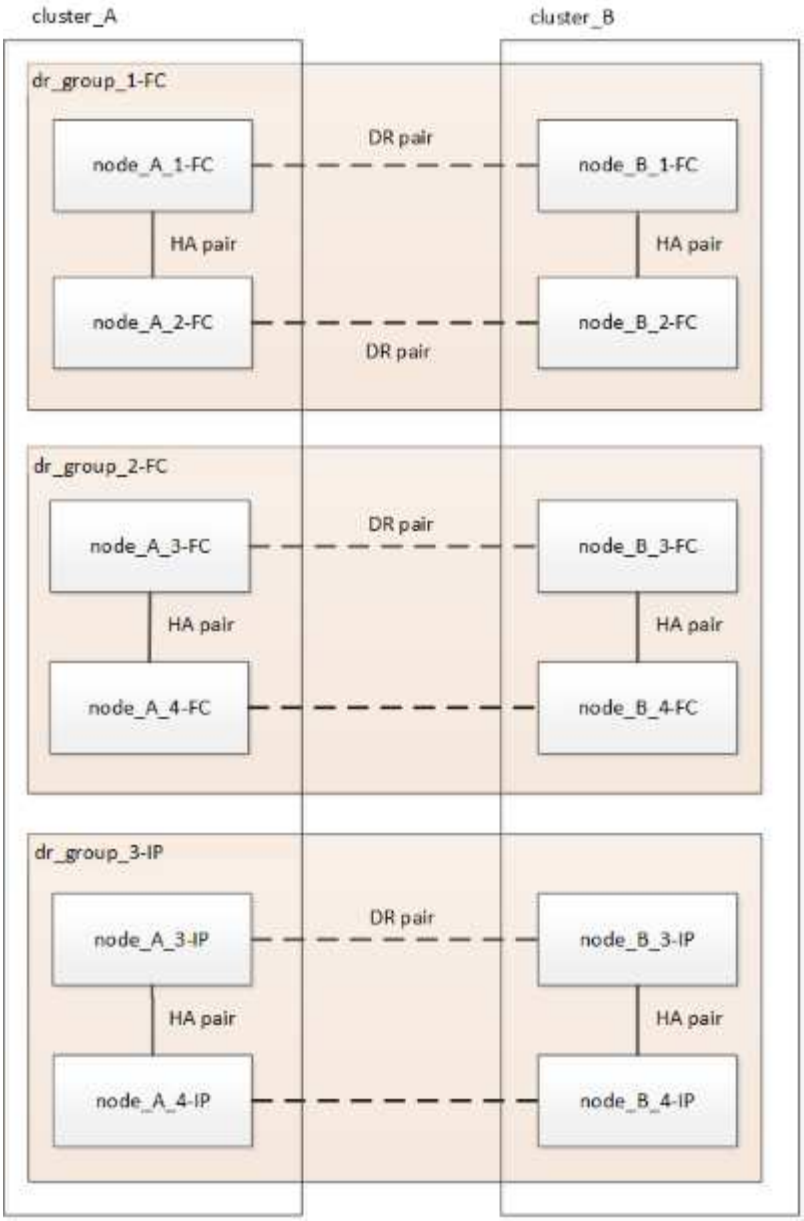


Workflow di transizione della configurazione FC a otto nodi

Il processo di transizione inizia con una configurazione FC MetroCluster a otto nodi funzionante.

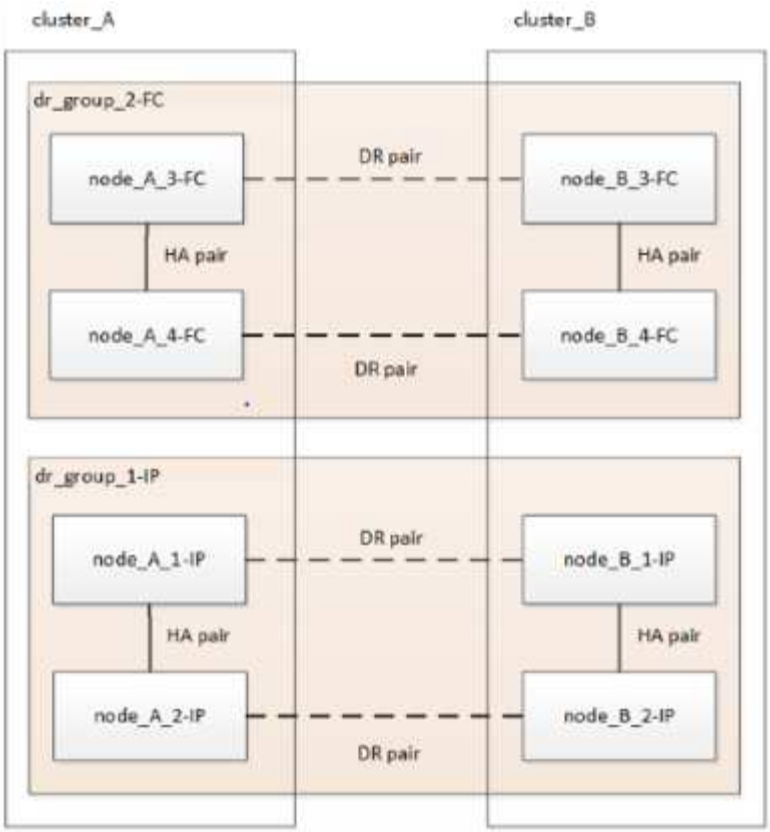


I nuovi nodi IP MetroCluster vengono aggiunti come terzo gruppo DR.

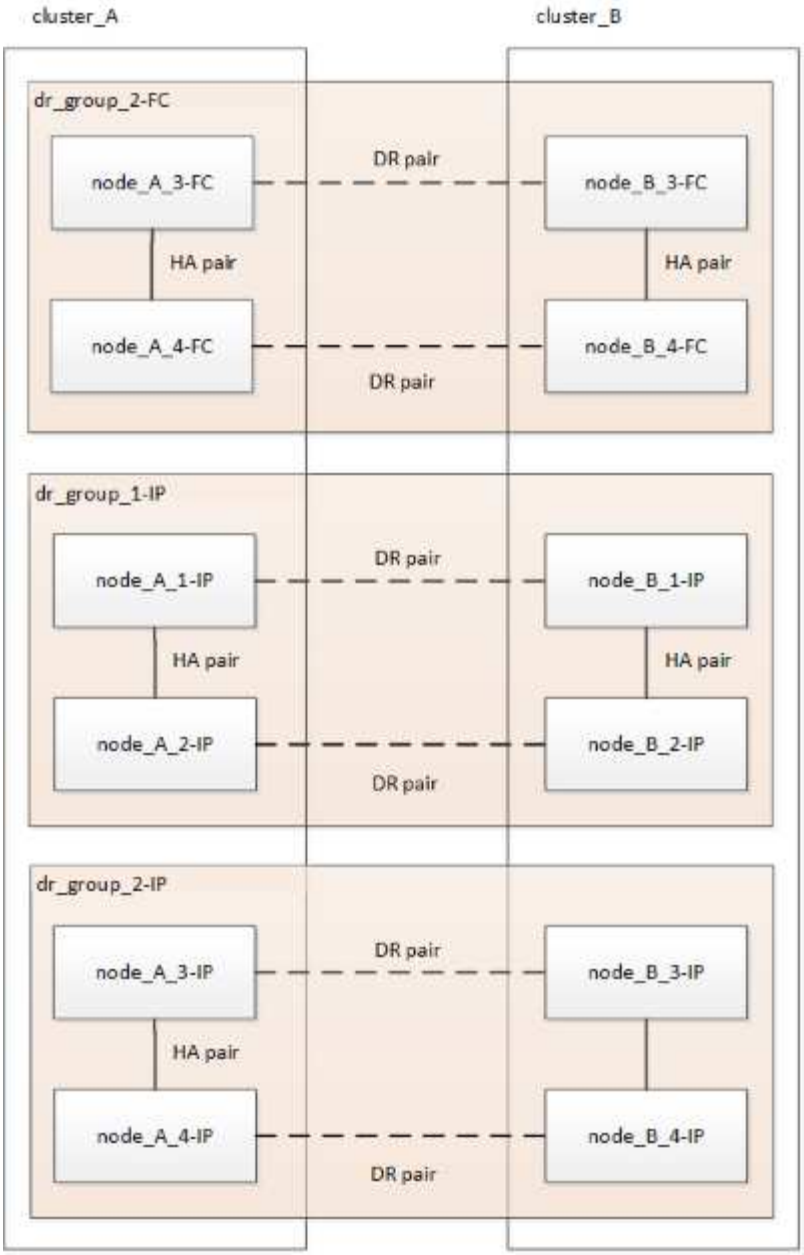


I dati vengono trasferiti da DR_Group_1-FC a DR_Group_1-IP, quindi i vecchi nodi e il relativo storage vengono rimossi dalla configurazione e dismessi.

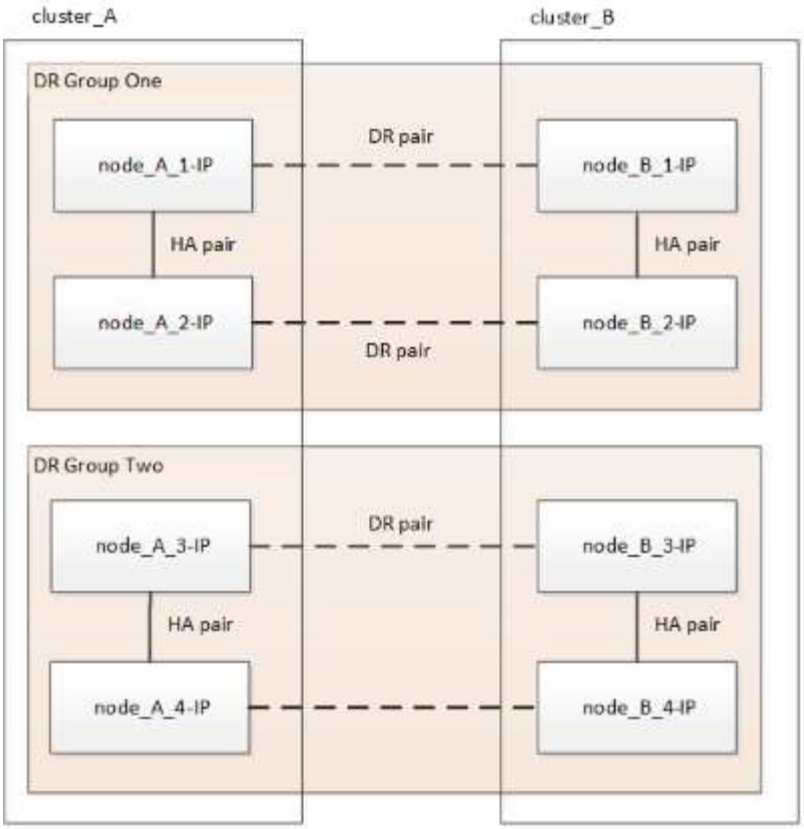
> Se si desidera passare da una configurazione FC a otto nodi a una configurazione IP a quattro nodi, è necessario trasferire tutti i dati in DR_Group_1-FC e DR_Group_2-FC al nuovo gruppo DR IP (DR_Group_1-IP). È quindi possibile decommissionare entrambi i gruppi DR FC. Una volta rimossi i gruppi FC DR, il processo termina con una configurazione IP MetroCluster a quattro nodi.



Aggiungere i restanti nodi IP MetroCluster alla configurazione MetroCluster esistente. Ripetere la procedura per trasferire i dati dai nodi DR_Group_2-FC ai nodi DR_Group_2-IP.

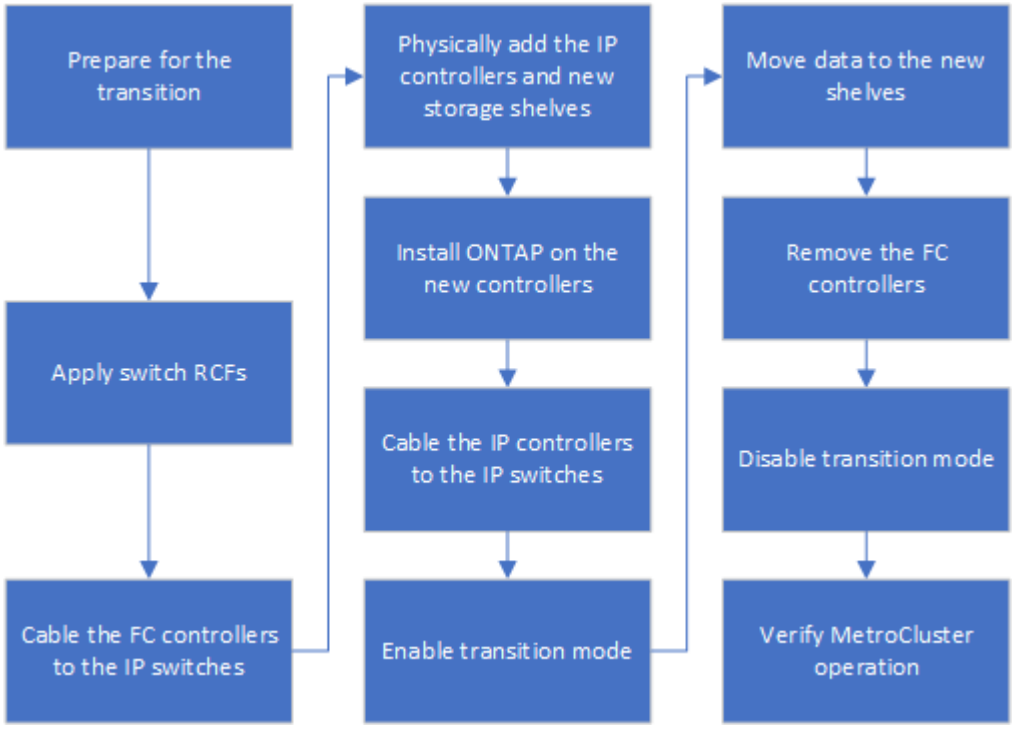


Dopo aver rimosso DR_Group_2-FC, il processo termina con una configurazione IP MetroCluster a otto nodi.



Workflow del processo di transizione

Per eseguire la transizione della configurazione MetroCluster, utilizzare il seguente flusso di lavoro.



Considerazioni sugli switch IP

Assicurarsi che gli switch IP siano supportati. Se il modello di switch esistente è

supportato sia dalla configurazione MetroCluster FC originale che dalla nuova configurazione MetroCluster IP, è possibile riutilizzare gli switch esistenti.

Switch supportati

È necessario utilizzare gli switch forniti da NetApp.

- L'utilizzo di switch compatibili con MetroCluster (switch non validati e forniti da NetApp) non è supportato per la transizione.
- Gli switch IP devono essere supportati come switch di cluster sia dalla configurazione MetroCluster FC che dalla configurazione MetroCluster IP.
- Gli switch IP possono essere riutilizzati nella nuova configurazione MetroCluster IP se MetroCluster FC è un cluster con switch e gli switch del cluster IP sono supportati dalla configurazione MetroCluster IP.
- I nuovi switch IP vengono in genere utilizzati nei seguenti casi:
  - MetroCluster FC è un cluster senza switch, pertanto sono necessari nuovi switch.
  - MetroCluster FC è un cluster con switch, ma gli switch IP esistenti non sono supportati nella configurazione MetroCluster IP.
  - Si desidera utilizzare switch diversi per la configurazione IP MetroCluster.

Per informazioni sul modello di piattaforma e sul supporto dello switch, consulta la sezione *NetApp Hardware Universe*.

"NetApp Hardware Universe"

Operazioni di switchover, riparazione e switchback durante la transizione senza interruzioni

A seconda della fase del processo di transizione, le operazioni di switchover, riparazione e switchback di MetroCluster utilizzano il flusso di lavoro MetroCluster FC o MetroCluster IP.

La seguente tabella mostra i flussi di lavoro utilizzati nelle diverse fasi del processo di transizione. In alcune fasi, lo switchover e lo switchback non sono supportati.

- Nel flusso di lavoro MetroCluster FC, le fasi di switchover, riparazione e switchback sono quelle utilizzate da una configurazione MetroCluster FC.
- Nel flusso di lavoro IP di MetroCluster, le fasi di switchover, riparazione e switchback sono quelle utilizzate da una configurazione IP di MetroCluster.
- Nel flusso di lavoro unificato, quando sono configurati entrambi i nodi FC e IP, le operazioni dipendono dall'esecuzione di NSO o USO. I dettagli sono riportati nella tabella.

Per informazioni sui flussi di lavoro FC e IP di MetroCluster per lo switchover, la riparazione e lo switchback, vedere "Comprensione della protezione dei dati e del disaster recovery di MetroCluster".

Lo switchover automatico non pianificato non è disponibile durante il processo di transizione.

Fase della transizione	Lo switchover negoziato utilizza questo workflow…	Lo switchover non pianificato utilizza questo workflow…

Prima che i nodi IP MetroCluster si siano Uniti al cluster	FC MetroCluster	FC MetroCluster
Dopo che i nodi IP MetroCluster sono entrati a far parte del cluster, prima di `metrocluster configure` viene eseguito il comando	Non supportato	FC MetroCluster
Dopo il `metrocluster configure` il comando è stato emesso. Lo spostamento del volume può essere in corso.	Unificato: Tutti i nodi del sito remoto rimangono attivi e la riparazione viene eseguita automaticamente	Unificato: • Gli aggregati mirrorati di proprietà del nodo MetroCluster FC vengono mirrorati se lo storage è accessibile, tutti gli altri vengono degradati dopo lo switchover. • Tutti i nodi del sito remoto sono in grado di avviarsi. • Il `heal aggregate` e. `heal root` i comandi devono essere eseguiti manualmente.
I nodi MetroCluster FC non sono stati configurati.	Non supportato	IP MetroCluster
Il `cluster unjoin` Il comando è stato eseguito sui nodi FC MetroCluster.	IP MetroCluster	IP MetroCluster

Messaggi di avviso e supporto dello strumento durante la transizione

Durante la transizione potrebbero essere visualizzati messaggi di avviso. Questi avvisi possono essere ignorati in modo sicuro. Inoltre, alcuni strumenti non sono disponibili durante la transizione.

- GLI AR potrebbero inviare un avviso durante la transizione.

  Questi avvisi possono essere ignorati e dovrebbero scomparire una volta terminata la transizione.

- Il gestore unificato di OnCommand potrebbe inviare un avviso durante la transizione.

  Questi avvisi possono essere ignorati e dovrebbero scomparire una volta terminata la transizione.

- Config Advisor non è supportato durante la transizione.
- System Manager non è supportato durante la transizione.

Esempio di denominazione in questa procedura

Questa procedura utilizza nomi di esempio per identificare i gruppi DR, i nodi e gli switch coinvolti.

Gruppi DR	Cluster_A presso il sito_A.	Cluster_B nel sito_B.
dr_Group_1-FC	• Node_A_1-FC • Node_A_2-FC	• Node_B_1-FC • Node_B_2-FC
dr_Group_2-IP	• Node_A_3-IP • Node_A_4-IP	• Node_B_3-IP • Node_B_4-IP
Switch	Switch iniziali (se la configurazione fabric-attached:) • Switch_A_1-FC • Switch_A_2-FC Switch IP MetroCluster: • Switch_A_1-IP • Switch_A_2-IP	Switch iniziali (se la configurazione fabric-attached): • Switch_B_1-FC • Switch_B_2-FC Switch IP MetroCluster: • Switch_B_1-IP • Switch_B_2-IP

Transizione da configurazioni MetroCluster FC a MetroCluster IP

Verifica dello stato della configurazione MetroCluster

Prima di eseguire la transizione, è necessario verificare lo stato e la connettività della configurazione di MetroCluster

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:`node run -node node-name sysconfig -a`
   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster: `system health alert show`
   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale: `metrocluster show`
   d. Eseguire un controllo MetroCluster: `metrocluster check run`
   e. Visualizzare i risultati del controllo MetroCluster: `metrocluster check show`
   f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti): `storage switch show`
   g. Eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.
2. Verificare che il cluster funzioni correttamente: `cluster show`

```
cluster_A::> cluster show
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1_FC    true    true          false
node_A_2_FC    true    true          false

cluster_A::>
```

3. Verificare che tutte le porte del cluster siano installate: `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1_FC

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verificare che tutte le LIF del cluster siano operative: `network interface show -vserver cluster`

   Ogni LIF del cluster deve visualizzare "true" per "is Home" e "up/up" per "Status Admin/Oper".

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A-1_FC_clus1
                       up/up      169.254.209.69/16  node_A-1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verificare che l'autorevert sia attivato su tutte le LIF del cluster: `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1_FC_clus1
                        true
           node_A_1_FC_clus2
                        true
           node_A_2_FC_clus1
                        true
           node_A_2_FC_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima della transizione.

1. Rimuovere la configurazione MetroCluster esistente dal software Tiebreaker.

   "Rimozione delle configurazioni MetroCluster"

2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Generazione e applicazione di RCF ai nuovi switch IP

Se si utilizzano nuovi switch IP per la configurazione IP MetroCluster, è necessario configurare gli switch con un file RCF personalizzato.

Questa attività è necessaria se si utilizzano nuovi switch.

Se si utilizzano switch esistenti, passare alla sezione "Spostamento delle connessioni del cluster locale".

1. Installare e installare in rack i nuovi switch IP.
2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP"

- "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
- "Ripristino delle impostazioni predefinite dello switch IP Cisco"

3. Se necessario, aggiornare il firmware dello switch a una versione supportata.
4. Utilizzare lo strumento generatore RCF per creare il file RCF in base al fornitore dello switch e ai modelli di piattaforma, quindi aggiornare gli switch con il file.

   Seguire la procedura descritta nella sezione relativa al fornitore dello switch di *Installazione e configurazione IP MetroCluster*.

   "Installazione e configurazione di MetroCluster IP"

   - "Download e installazione dei file Broadcom IP RCF"
   - "Download e installazione dei file Cisco IP RCF"

Spostare le connessioni del cluster locale

È necessario spostare le interfacce del cluster della configurazione MetroCluster FC sugli switch IP.

Spostare le connessioni del cluster sui nodi FC MetroCluster

È necessario spostare le connessioni del cluster sui nodi FC MetroCluster sugli switch IP. La procedura dipende dal fatto che si stiano utilizzando gli switch IP esistenti o i nuovi switch IP.

Questa attività deve essere eseguita su entrambi i siti MetroCluster.

Quali connessioni spostare

La seguente attività presuppone che un modulo controller utilizzi due porte per le connessioni del cluster. Alcuni modelli di moduli controller utilizzano quattro o più porte per la connessione cluster. In tal caso, ai fini di questo esempio, le porte sono divise in due gruppi, alternando le porte tra i due gruppi

La tabella seguente mostra le porte di esempio utilizzate in questa attività.

Numero di connessioni cluster sul modulo controller	Porte del gruppo A.	Porte del gruppo B.
Due	e0a	e0b
Quattro	e0a, e0c	e0b, e0d

- Le porte del gruppo A si collegano allo switch locale_x_1-IP.
- Le porte del gruppo B si collegano allo switch locale_x_2-IP.

La seguente tabella mostra a quali porte switch si connettono i nodi FC. Per lo switch Broadcom BES-53248, l'utilizzo della porta dipende dal modello dei nodi IP MetroCluster.

Modello di switch	Modello di nodo IP MetroCluster	Porte dello switch	Si connette a.
Cisco 3132Q-V, 3232C o 9336C-FX2	Qualsiasi	5	Interfaccia del cluster locale sul nodo FC
		6	Interfaccia del cluster locale sul nodo FC
Broadcom BES-53248	FAS500f/A250	1 - 6	Interfaccia del cluster locale sul nodo FC
	FAS8200/A300	3, 4, 9, 10, 11, 12	Interfaccia del cluster locale sul nodo FC
	FAS8300/A400/FAS8700	1 - 6	Interfaccia del cluster locale sul nodo FC

Spostamento delle connessioni del cluster locale quando si utilizzano nuovi switch IP

Se si utilizzano nuovi switch IP, è necessario spostare fisicamente le connessioni cluster dei nodi FC MetroCluster esistenti sui nuovi switch.

1. Spostare il gruppo di nodi MetroCluster FC A connessioni cluster ai nuovi switch IP.

   Utilizzare le porte descritte in Quali connessioni spostare.

   a. Scollegare tutte le porte del gruppo A dallo switch oppure, se la configurazione MetroCluster FC era un cluster senza switch, scollegarle dal nodo partner.
   b. Scollegare le porte del gruppo A da Node_A_1-FC e Node_A_2-FC.
   c. Collegare le porte del gruppo A di Node_A_1-FC alle porte dello switch per il nodo FC sullo switch_A_1-IP
   d. Collegare le porte del gruppo A di Node_A_2-FC alle porte dello switch per il nodo FC sullo switch_A_1-IP
2. Verificare che tutte le porte del cluster siano installate:

   ```
   network port show -ipspace Cluster
   ```

```
cluster_A::*> network port show -ipspace Cluster

Node: node_A_1-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::*>
```

3. Verificare che i collegamenti interswitch (ISL) tra siti siano attivi e che i canali delle porte siano operativi:

   `show interface brief`

   Nell'esempio seguente, le porte ISL da "eth1/15" a "eth1/20" sono configurate come "PO10" per il collegamento remoto del sito e "eth1/7" a "eth1/8" come "PO1" per l'ISL del cluster locale. Lo stato "eth1/15" - "eth1/20", "eth1/7" - "eth1/8", "PO10" e "PO1" deve essere "up".

```
IP_switch_A_1# show interface brief

--------------------------------------------------------------
Port   VRF          Status   IP Address        Speed      MTU
--------------------------------------------------------------
mgmt0  --            up        100.10.200.20    1000      1500
--------------------------------------------------------------------------
--------
Ethernet     VLAN   Type Mode    Status     Reason              Speed
Port
Interface                                    Ch #
--------------------------------------------------------------------------
--------

...
```

```
Eth1/7        1     eth  trunk    up        none                100G(D)
1
Eth1/8        1     eth  trunk    up        none                100G(D)
1

...

Eth1/15       1     eth  trunk    up        none                100G(D)
10
Eth1/16       1     eth  trunk    up        none                100G(D)
10
Eth1/17       1     eth  trunk    up        none                100G(D)
10
Eth1/18       1     eth  trunk    up        none                100G(D)
10
Eth1/19       1     eth  trunk    up        none                100G(D)
10
Eth1/20       1     eth  trunk    up        none                100G(D)
10

--------------------------------------------------------------------------
--------
Port-channel VLAN  Type Mode   Status   Reason         Speed    Protocol
Interface
--------------------------------------------------------------------------
--------
Po1          1     eth  trunk   up      none            a-100G(D) lacp
Po10         1     eth  trunk   up      none            a-100G(D) lacp
Po11         1     eth  trunk   down    No operational  auto(D)   lacp
                                         members
IP_switch_A_1#
```

4. Verificare che tutte le interfacce visualizzino true nella colonna “is Home”:

   ```
   network interface show -vserver cluster
   ```

   Il completamento di questa operazione potrebbe richiedere alcuni minuti.

```
cluster_A::*> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1-FC_clus2
                       up/up      169.254.49.125/16  node_A_1-FC   e0b
true
            node_A_2-FC_clus1
                       up/up      169.254.47.194/16  node_A_2-FC   e0a
true
            node_A_2-FC_clus2
                       up/up      169.254.19.183/16  node_A_2-FC   e0b
true

4 entries were displayed.

cluster_A::*>
```

5. Eseguire i passaggi sopra riportati su entrambi i nodi (Node_A_1-FC e Node_A_2-FC) per spostare le porte del gruppo B delle interfacce del cluster.
6. Ripetere i passaggi precedenti sul cluster partner “cluster_B”.

Spostamento delle connessioni del cluster locale durante il riutilizzo degli switch IP esistenti

Se si riutilizzano gli switch IP esistenti, è necessario aggiornare il firmware, riconfigurare gli switch con i file RCF (Reference Configure Files) corretti e spostare le connessioni alle porte corrette uno switch alla volta.

Questa attività è necessaria solo se i nodi FC sono collegati a switch IP esistenti e si stanno riutilizzando gli switch.

1. Scollegare le connessioni del cluster locale che si connettono allo switch_A_1_IP
   a. Scollegare le porte del gruppo A dallo switch IP esistente.
   b. Scollegare le porte ISL sullo switch_A_1_IP.

      Per visualizzare l’utilizzo della porta del cluster, consultare le istruzioni di installazione e configurazione della piattaforma.

      "Sistemi AFF A320: Installazione e configurazione"

"Istruzioni per l'installazione e la configurazione dei sistemi AFF A220/FAS2700"

"Istruzioni per l'installazione e la configurazione dei sistemi AFF A800"

"Istruzioni per l'installazione e la configurazione dei sistemi AFF A300"

"Istruzioni per l'installazione e la configurazione dei sistemi FAS8200"

2. Riconfigurare switch_A_1_IP utilizzando i file RCF generati per la combinazione e la transizione della piattaforma.

   Seguire i passaggi della procedura per il fornitore dello switch da *Installazione e configurazione IP MetroCluster*:

   "Installazione e configurazione di MetroCluster IP"

   a. Se necessario, scaricare e installare il nuovo firmware dello switch.

      Utilizzare il firmware più recente supportato dai nodi IP MetroCluster.

      - "Download e installazione del software EFOS dello switch Broadcom"
      - "Download e installazione del software NX-OS dello switch Cisco"

   b. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

      - "Ripristino delle impostazioni predefinite dello switch IP Broadcom" **
      - "Ripristino delle impostazioni predefinite dello switch IP Cisco"

   c. Scaricare e installare il file RCF IP in base al fornitore dello switch.

      - "Download e installazione dei file Broadcom IP RCF"
      - "Download e installazione dei file Cisco IP RCF"

3. Ricollegare le porte del gruppo A allo switch_A_1_IP.

   Utilizzare le porte descritte in Quali connessioni spostare.

4. Verificare che tutte le porte del cluster siano installate:

   ```
   network port show -ipspace cluster
   ```

```
Cluster-A::*> network port show -ipspace cluster

Node: node_A_1_FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

5. Verificare che tutte le interfacce siano sulla porta home:

   `network interface show -vserver Cluster`

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

6. Ripetere tutti i passaggi precedenti su switch_A_2_IP.
7. Ricollegare le porte ISL del cluster locale.
8. Ripetere la procedura descritta in precedenza sul sito_B per lo switch B_1_IP e lo switch B_2_IP.
9. Connettere gli ISL remoti tra i siti.

Verificare che le connessioni del cluster siano spostate e che il cluster sia integro

Per garantire una connettività corretta e che la configurazione sia pronta per procedere con il processo di transizione, è necessario verificare che le connessioni del cluster siano spostate correttamente, che gli switch del cluster siano riconosciuti e che il cluster funzioni correttamente.

1. Verificare che tutte le porte del cluster siano attive e in esecuzione:

   ```
   network port show -ipspace Cluster
   ```

```
Cluster-A::*> network port show -ipspace Cluster

Node: Node-A-1-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: Node-A-2-FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

2. Verificare che tutte le interfacce siano sulla porta home:

   `network interface show -vserver Cluster`

   Il completamento di questa operazione potrebbe richiedere alcuni minuti.

   L'esempio seguente mostra che tutte le interfacce sono vere nella colonna "is Home".

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            Node-A-1_FC_clus1
                       up/up      169.254.209.69/16  Node-A-1_FC   e0a
true
            Node-A-1-FC_clus2
                       up/up      169.254.49.125/16  Node-A-1-FC   e0b
true
            Node-A-2-FC_clus1
                       up/up      169.254.47.194/16  Node-A-2-FC   e0a
true
            Node-A-2-FC_clus2
                       up/up      169.254.19.183/16  Node-A-2-FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

3. Verificare che entrambi gli switch IP locali siano rilevati dai nodi:

```
network device-discovery show -protocol cdp
```

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
Node-A-1-FC
           /cdp
            e0a    Switch-A-3-IP             1/5/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/5/1             N3K-
C3232C
Node-A-2-FC
           /cdp
            e0a    Switch-A-3-IP             1/6/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/6/1             N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. Sullo switch IP, verificare che i nodi IP MetroCluster siano stati rilevati da entrambi gli switch IP locali:

   `show cdp neighbors`

   Eseguire questa operazione su ogni switch.

   Questo esempio mostra come verificare che i nodi vengano rilevati sullo Switch-A-3-IP.

```
(Switch-A-3-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0a
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0a
Switch-A-4-IP(FDO220329A4)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-4-IP(FDO220329A4)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-3-IP(FDO220329B3)
                    Eth1/20        173    R S I s   N3K-C3232C
Eth1/20
Switch-B-3-IP(FDO220329B3)
                    Eth1/21        173    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-3-IP)#
```

Questo esempio mostra come verificare che i nodi vengano rilevati sullo Switch-A-4-IP.

```
(Switch-A-4-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H         FAS8200       e0b
Node-A-2-FC         Eth1/6/1       133    H         FAS8200       e0b
Switch-A-3-IP(FDO220329A3)
                    Eth1/7         175    R S I s   N3K-C3232C    Eth1/7
Switch-A-3-IP(FDO220329A3)
                    Eth1/8         175    R S I s   N3K-C3232C    Eth1/8
Switch-B-4-IP(FDO220329B4)
                    Eth1/20        169    R S I s   N3K-C3232C
Eth1/20
Switch-B-4-IP(FDO220329B4)
                    Eth1/21        169    R S I s   N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP)#
```

Preparazione dei controller IP MetroCluster

È necessario preparare i quattro nuovi nodi IP MetroCluster e installare la versione corretta di ONTAP.

Questa attività deve essere eseguita su ciascuno dei nuovi nodi:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

In questa procedura, si cancella la configurazione sui nodi e si cancella l'area della mailbox sui nuovi dischi.

1. Rack i nuovi controller per la configurazione IP MetroCluster.

   I nodi FC MetroCluster (Node_A_x-FC e Node_B_x-FC) rimangono cablati in questo momento.

2. Collegare i nodi IP MetroCluster agli switch IP come illustrato nella "Cablaggio degli switch IP".
3. Configurare i nodi IP MetroCluster utilizzando le seguenti sezioni:

a. "Raccolta delle informazioni richieste"
b. "Cancellazione della configurazione su un modulo controller"
c. "Verifica dello stato ha-config dei componenti"
d. "Assegnazione manuale dei dischi per il pool 0 (ONTAP 9.4 e versioni successive)"

4. Dalla modalità Maintenance, eseguire il comando halt per uscire dalla modalità Maintenance, quindi eseguire il comando boot_ontap per avviare il sistema e accedere alla configurazione del cluster.

   Non completare la procedura guidata del cluster o del nodo.

5. Ripetere questa procedura sugli altri nodi IP MetroCluster.

Configurare MetroCluster per la transizione

Per preparare la configurazione per la transizione, aggiungere i nuovi nodi alla configurazione MetroCluster esistente e spostare i dati nei nuovi nodi.

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è in corso:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   "maintenance-window-in-hours" specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

2. Ripetere il comando sul cluster partner.

Attivazione della modalità di transizione e disattivazione del cluster ha

È necessario attivare la modalità di transizione MetroCluster per consentire ai nodi vecchi e nuovi di operare insieme nella configurazione MetroCluster e disattivare il cluster ha.

1. Attiva transizione:

   a. Passare al livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

   b. Attiva modalità di transizione:

```
metrocluster transition enable -transition-mode non-disruptive
```

Eseguire questo comando su un solo cluster.

```
cluster_A::*> metrocluster transition enable -transition-mode non-
disruptive

Warning: This command enables the start of a "non-disruptive"
MetroCluster
         FC-to-IP transition. It allows the addition of hardware for
another DR
         group that uses IP fabrics, and the removal of a DR group that
uses FC
         fabrics. Clients will continue to access their data during a
         non-disruptive transition.

         Automatic unplanned switchover will also be disabled by this
command.
Do you want to continue? {y|n}: y

cluster_A::*>
```

a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

2. Verificare che la transizione sia attivata su entrambi i cluster.

```
cluster_A::> metrocluster transition show-mode
Transition Mode

non-disruptive

cluster_A::*>


cluster_B::*> metrocluster transition show-mode
Transition Mode

non-disruptive

Cluster_B::>
```

3. Disattiva cluster ha.

È necessario eseguire questo comando su entrambi i cluster.

```
cluster_A::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_A::*>


cluster_B::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_B::*>
```

4. Verificare che il cluster ha sia disattivato.

È necessario eseguire questo comando su entrambi i cluster.

```
cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>
```

Unione dei nodi IP MetroCluster ai cluster

È necessario aggiungere i quattro nuovi nodi IP MetroCluster alla configurazione MetroCluster esistente.

A proposito di questa attività

È necessario eseguire questa attività su entrambi i cluster.

Fasi

1. Aggiungere i nodi IP MetroCluster alla configurazione MetroCluster esistente.
   a. Collegare il primo nodo IP MetroCluster (Node_A_3-IP) alla configurazione FC MetroCluster esistente.

```
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: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:

Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Collegare il secondo nodo IP MetroCluster (Node_A_4-IP) alla configurazione FC MetroCluster esistente.

2. Ripetere questa procedura per unire Node_B_3-IP e Node_B_4-IP a cluster_B.

Configurazione delle LIF tra cluster, creazione delle interfacce MetroCluster e mirroring degli aggregati root

È necessario creare le LIF di peering del cluster e le interfacce MetroCluster sui nuovi nodi IP MetroCluster.

A proposito di questa attività

La porta home utilizzata negli esempi è specifica per la piattaforma. Utilizzare la porta home appropriata specifica per la piattaforma del nodo IP MetroCluster.

Fasi

1. Sui nuovi nodi IP MetroCluster, "Configurare le LIF dell'intercluster".
2. In ogni sito, verificare che il peering del cluster sia configurato:

   ```
   cluster peer show
   ```

   L'esempio seguente mostra la configurazione del peering del cluster su cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   L'esempio seguente mostra la configurazione del peering del cluster su cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A 1-80-000011 Available ok
   ```

3. Configurare il gruppo di DR per i nodi IP MetroCluster:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   ```
   cluster_A::> metrocluster configuration-settings dr-group create
   -partner-cluster
   cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
   [Job 259] Job succeeded: DR Group Create is successful.
   cluster_A::>
   ```

4. Verificare che il gruppo DR sia stato creato.

```
metrocluster configuration-settings dr-group show
```

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                     Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
2           cluster_A
                                        node_A_3-IP        node_B_3-IP
                                        node_A_4-IP        node_B_4-IP
            cluster_B
                                        node_B_3-IP        node_A_3-IP
                                        node_B_4-IP        node_A_4-IP

4 entries were displayed.

cluster_A::>
```

Si noterà che il gruppo DR per i vecchi nodi FC MetroCluster (gruppo DR 1) non viene elencato quando si esegue `metrocluster configuration-settings dr-group show` comando.

È possibile utilizzare `metrocluster node show` su entrambi i siti per elencare tutti i nodi.

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
      cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
2     cluster_A
              node_A_3-IP      ready to configure
                                                 -         -
              node_A_4-IP      ready to configure
                                                 -         -

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
      cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
2     cluster_B
              node_B_3-IP      ready to configure
                                                 -         -
              node_B_4-IP      ready to configure
                                                 -         -
```

5. Configurare le interfacce IP MetroCluster per i nodi IP MetroCluster appena entrati:

   `metrocluster configuration-settings interface create -cluster-name`

   Vedere "Configurazione e connessione delle interfacce IP di MetroCluster" Per considerazioni sulla configurazione delle interfacce IP.

È possibile configurare le interfacce IP di MetroCluster da entrambi i cluster. Inoltre, a partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3"

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verificare che le interfacce IP MetroCluster siano state create:

```
metrocluster configuration-settings interface show
```

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
2     cluster_A
             node_A_3-IP
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-IP
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Collegare le interfacce IP di MetroCluster:

```
metrocluster configuration-settings connection connect
```

> Il completamento di questo comando potrebbe richiedere alcuni minuti.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verificare che le connessioni siano state stabilite correttamente:

```
metrocluster configuration-settings connection show
```

```
cluster_A::> metrocluster configuration-settings connection show

DR                     Source          Destination
Group Cluster Node     Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_3-IP**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
```

```
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_4-IP
                 Home Port: e1a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.11    DR Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.11    DR Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e1a
```

```
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. Verificare l’assegnazione automatica e il partizionamento dei dischi:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.
cluster_A::>
```

Nei sistemi configurati per Advanced Drive Partitioning (ADP), il tipo di container è "condiviso" piuttosto che "remoto", come mostrato nell'output di esempio.

10. Mirroring degli aggregati root:

```
storage aggregate mirror -aggregate aggr0_node_A_3_IP
```

È necessario completare questo passaggio su ciascun nodo IP MetroCluster.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3_IP

Info: Disks would be added to aggregate "aggr0_node_A_3_IP"on node
"node_A_3-IP"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available for volume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verificare che gli aggregati root siano mirrorati:

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1_FC
           349.0GB   16.84GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2_FC
           349.0GB   16.84GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3_IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_4_IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-FC
raid_dp,

mirrored,
```

Finalizzazione dell’aggiunta dei nodi IP MetroCluster

È necessario incorporare il nuovo gruppo DR nella configurazione MetroCluster e creare aggregati di dati mirrorati sui nuovi nodi.

Fasi

1. Configurare MetroCluster in base all’eventuale presenza di uno o più aggregati di dati:

Se la configurazione di MetroCluster dispone di…	Quindi…

Aggregati di dati multipli	Dal prompt di qualsiasi nodo, configurare MetroCluster: `metrocluster configure <node-name>` Devi eseguire `metrocluster configure` e **non** `metrocluster configure -refresh true`

Un singolo aggregato di dati mirrorato	a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
	
	`set -privilege advanced`
	
	Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e viene visualizzato il prompt della modalità avanzata (*).
	
	b. Configurare MetroCluster con `-allow-with -one-aggregate true` parametro:
	
	`metrocluster configure -allow-with -one-aggregate true -node-name <node-name>`
	
	c. Tornare al livello di privilegio admin:
	
	`set -privilege admin`

La Best practice consiste nell'avere più aggregati di dati mirrorati. Quando è presente un solo aggregato mirrorato, la protezione è inferiore perché i volumi di metadati si trovano sullo stesso aggregato piuttosto che su aggregati separati.

2. Verificare che i nodi siano aggiunti al gruppo di DR:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node-A-1-FC        configured     enabled   normal
              node-A-2-FC        configured     enabled   normal
      Cluster-B
              node-B-1-FC        configured     enabled   normal
              node-B-2-FC        configured     enabled   normal
2     cluster_A
              node-A-3-IP        configured     enabled   normal
              node-A-4-IP        configured     enabled   normal
      Cluster-B
              node-B-3-IP        configured     enabled   normal
              node-B-4-IP        configured     enabled   normal
8 entries were displayed.

cluster_A::>
```

3. Creare aggregati di dati mirrorati su ciascuno dei nuovi nodi MetroCluster:

   `storage aggregate create -aggregate aggregate-name -node node-name -diskcount no-of-disks -mirror true`

   > È necessario creare almeno un aggregato di dati mirrorati per sito. Si consiglia di disporre di due aggregati di dati mirrorati per sito su nodi IP MetroCluster per ospitare i volumi MDV, tuttavia è supportato un singolo aggregato per sito (ma non consigliato). È possibile che un sito di MetroCluster disponga di un singolo aggregato di dati mirrorati e l'altro sito disponga di più aggregato di dati mirrorati.

   Nell'esempio seguente viene illustrata la creazione di un aggregato su Node_A_3-IP.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_3-
IP -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_3-IP" would be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
```

```
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS              -
-
          parity     5.10.16                   SAS              -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS              -
-
          parity     4.20.14                   SAS              -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

4. Verificare che tutti i nodi nel cluster siano integri:

   `cluster show`

   L'output dovrebbe essere visualizzato `true` per `health` campo per tutti i nodi.

5. Verificare che sia possibile il Takeover e che i nodi siano connessi eseguendo il seguente comando su entrambi i cluster:

   `storage failover show`

   ```
   cluster_A::> storage failover show
                                          Takeover
   Node           Partner                 Possible    State Description
   -------------- ------------------------ ---------   ------------------
   Node_FC_1      Node_FC_2                 true       Connected to Node_FC_2
   Node_FC_2      Node_FC_1                 true       Connected to Node_FC_1
   Node_IP_1      Node_IP_2                 true       Connected to Node_IP_2
   Node_IP_2      Node_IP_1                 true       Connected to Node_IP_1
   ```

6. Verificare che tutti i dischi collegati ai nodi IP MetroCluster appena aggiunti siano presenti:

   `disk show`

7. Verificare l'integrità della configurazione di MetroCluster eseguendo i seguenti comandi:

   a. `metrocluster check run`
   b. `metrocluster check show`
   c. `metrocluster interconnect mirror show`
   d. `metrocluster interconnect adapter show`

8. Spostare i volumi MDV_CRS dai vecchi nodi ai nuovi nodi con privilegi avanzati.

   a. Visualizzare i volumi per identificare i volumi MDV:

      > Se si dispone di un singolo aggregato di dati mirrorati per sito, spostare entrambi i volumi MDV in questo singolo aggregato. Se si dispone di due o più aggregati di dati mirrorati, spostare ciascun volume MDV in un aggregato diverso.

      L'esempio seguente mostra i volumi MDV nel volume che mostrano l'output:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Impostare il livello di privilegio avanzato:

```
set -privilege advanced
```

c. Spostare i volumi MDV uno alla volta:

```
volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name
```

L'esempio seguente mostra il comando e l'output per lo spostamento di MDV_CRS_d6b0b313ff5611e9837100a098544e51_A per aggregare data_a3 sul nodo_A_3.

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Utilizzare il comando di visualizzazione del volume per verificare che il volume MDV sia stato spostato correttamente:

```
volume show mdv-name
```

Il seguente output indica che il volume MDV è stato spostato correttamente.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

a. Tornare alla modalità admin:

```
set -privilege admin
```

Spostamento dei dati nei nuovi shelf di dischi

Durante la transizione, i dati vengono spostati dagli shelf di dischi nella configurazione MetroCluster FC alla nuova configurazione MetroCluster IP.

Prima di iniziare

È necessario creare nuove LIF SAN sui nodi di destinazione o IP e connettere gli host prima di spostare i volumi nei nuovi aggregati.

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per

indicare che la manutenzione è stata completata.

a. Immettere il seguente comando: `system node autosupport invoke -node * -type all -message MAINT=end`

b. Ripetere il comando sul cluster partner.

2. Spostare i volumi di dati in aggregati sui nuovi controller, un volume alla volta.

   Seguire la procedura descritta in "Creazione di un aggregato e spostamento dei volumi nei nuovi nodi".

3. Creare LIF SAN sui nodi aggiunti di recente.

   Seguire la procedura descritta in "Aggiornamento dei percorsi LUN per i nuovi nodi".

4. Controllare se sono presenti licenze con blocco di nodo sui nodi FC; in tal caso, è necessario aggiungerli ai nodi appena aggiunti.

   Seguire la procedura descritta in "Aggiunta di licenze con blocco a nodo".

5. Eseguire la migrazione delle LIF dei dati.

   Seguire la procedura descritta in "Spostamento di LIF di dati non SAN e LIF di gestione del cluster nei nuovi nodi" Tuttavia, **non** eseguire gli ultimi due passaggi per migrare le LIF di gestione del cluster.

> - Non è possibile migrare una LIF utilizzata per le operazioni di copy-offload con le API vStorage VMware per l'integrazione array (VAAI).
> - Una volta completata la transizione dei nodi MetroCluster da FC a IP, potrebbe essere necessario spostare le connessioni host iSCSI sui nuovi nodi, vedere "Spostamento degli host iSCSI Linux da MetroCluster FC a nodi IP MetroCluster."

Rimozione dei controller FC MetroCluster

È necessario eseguire attività di pulizia e rimuovere i vecchi moduli controller dalla configurazione MetroCluster.

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è in corso.

   a. Immettere il seguente comando: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      intervallo di manutenzione in ore specifica la durata della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Ripetere il comando sul cluster partner.

2. Identificare gli aggregati ospitati sulla configurazione MetroCluster FC che devono essere cancellati.

   In questo esempio, i seguenti aggregati di dati sono ospitati dal cluster MetroCluster FC_B e devono essere cancellati: aggr_data_a1 e aggr_data_a2.

È necessario eseguire i passaggi per identificare, offline ed eliminare gli aggregati di dati su entrambi i cluster. L'esempio riguarda un solo cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.83GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.02TB    0% online       0 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
```

```
            1.02TB    1.02TB    0% online       0 node_A_2-FC
raid_dp,

mirrored,

normal
aggr_data_a3
            1.37TB    1.35TB    1% online       3 node_A_3-IP
raid_dp,

mirrored,

normal
aggr_data_a4
            1.25TB    1.24TB    1% online       2 node_A_4-IP
raid_dp,

mirrored,

normal
8 entries were displayed.

cluster_B::>
```

3. Controllare se gli aggregati di dati sui nodi FC hanno volumi MDV_aud ed eliminarli prima di eliminare gli aggregati.

   È necessario eliminare i volumi MDV_aud in quanto non possono essere spostati.

4. Portare tutti gli aggregati di dati offline, quindi eliminarli:

   a. Portare l'aggregato offline: `storage aggregate offline -aggregate aggregate-name`

      L'esempio seguente mostra l'aggregato aggr_data_a1 portato offline:

      ```
      cluster_B::> storage aggregate offline -aggregate aggr_data_a1

      Aggregate offline successful on aggregate: aggr_data_a1
      ```

   b. Eliminare l'aggregato: `storage aggregate delete -aggregate aggregate-name`

      Quando richiesto, è possibile distruggere il plex.

      L'esempio seguente mostra l'aggregato aggr_data_a1 che viene cancellato.

```
cluster_B::> storage aggregate delete -aggregate aggr_data_a1
Warning: Are you sure you want to destroy aggregate "aggr_data_a1"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

5. Identificare il gruppo DR FC MetroCluster che deve essere rimosso.

   Nell'esempio seguente, i nodi FC MetroCluster sono nel gruppo DR '1' e questo è il gruppo DR che deve essere rimosso.

```
cluster_B::> metrocluster node show

DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC       configured     enabled   normal
              node_A_2-FC       configured     enabled   normal
      cluster_B
              node_B_1-FC       configured     enabled   normal
              node_B_2-FC       configured     enabled   normal
2     cluster_A
              node_A_3-IP       configured     enabled   normal
              node_A_4-IP       configured     enabled   normal
      cluster_B
              node_B_3-IP       configured     enabled   normal
              node_B_3-IP       configured     enabled   normal
8 entries were displayed.

cluster_B::>
```

6. Spostare la LIF di gestione del cluster da un nodo FC MetroCluster a un nodo IP MetroCluster: `cluster_B::> network interface migrate -vserver svm-name -lif cluster_mgmt -destination-node node-in-metrocluster-ip-dr-group -destination-port available-port`
7. Modificare il nodo home e la porta home della LIF di gestione del cluster: `cluster_B::> network interface modify -vserver svm-name -lif cluster_mgmt -service-policy default-management -home-node node-in-metrocluster-ip-dr-group -home-port lif-port`
8. Spostamento di epsilon da un nodo FC MetroCluster a un nodo IP MetroCluster:
   a. Identificare il nodo attualmente dotato di epsilon: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-FC       true
node_A_2-FC       false
node_A_1-IP       false
node_A_2-IP       false
4 entries were displayed.
```

b. Impostare epsilon su false sul nodo FC MetroCluster (Node_A_1-FC): `cluster modify -node fc-node -epsilon false`

c. Impostare epsilon su true sul nodo IP MetroCluster (Node_A_1-IP): `cluster modify -node ip-node -epsilon true`

d. Verificare che epsilon sia stato spostato nel nodo corretto: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-FC       false
node_A_2-FC       false
node_A_1-IP       true
node_A_2-IP       false
4 entries were displayed.
```

9. Modificare l'indirizzo IP per il peer del cluster dei nodi IP in transizione per ciascun cluster:

a. Identificare il peer cluster_A utilizzando `cluster peer show` comando:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

i. Modificare l'indirizzo IP del peer cluster_A:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

b. Identificare il peer cluster_B utilizzando `cluster peer show` comando:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

i. Modificare l'indirizzo IP del peer cluster_B:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

c. Verificare che l'indirizzo IP del peer del cluster sia aggiornato per ciascun cluster:

i. Verificare che l'indirizzo IP sia aggiornato per ciascun cluster utilizzando `cluster peer show -instance` comando.

Il `Remote Intercluster Addresses` Nei seguenti esempi viene visualizzato l'indirizzo IP aggiornato.

Esempio per cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                      Remote Cluster Name: cluster_B
                      Active IP Addresses: 172.21.178.212,
172.21.178.204
                    Cluster Serial Number: 1-80-000011
                     Remote Cluster Nodes: node_B_3-IP,
                                           node_B_4-IP
                    Remote Cluster Health: true
                  Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+ Esempio per cluster_B.

```
cluster_B::> cluster peer show -instance

                      Peer Cluster Name: cluster_A
           Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                        Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. In ciascun cluster, rimuovere il gruppo di DR contenente i vecchi nodi dalla configurazione MetroCluster FC.

    È necessario eseguire questo passaggio su entrambi i cluster, uno alla volta.

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B" to remove the remote nodes in the
DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed ifthe preparation steps are not completed on
the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_B::>
```

11. Verificare che i nodi siano pronti per essere rimossi dai cluster.

    È necessario eseguire questa operazione su entrambi i cluster.

    > A questo punto, il `metrocluster node show` Il comando mostra solo i nodi FC MetroCluster locali e non mostra più i nodi che fanno parte del cluster partner.

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        ready to configure
                                                -         -
              node_A_2-FC        ready to configure
                                                -         -
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_4-IP        configured     enabled   normal
6 entries were displayed.

cluster_B::>
```

12. Disattiva il failover dello storage per i nodi FC MetroCluster.

    È necessario eseguire questa operazione su ciascun nodo.

```
cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>
```

13. Disunire i nodi MetroCluster FC dai cluster: `cluster unjoin -node node-name`

    È necessario eseguire questa operazione su ciascun nodo.

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC"from the cluster.
You must
         remove the failover partner as well. After the node is removed,
erase
         its configuration and initialize all disks by usingthe "Clean
         configuration and initialize all disks (4)" option from the
boot menu.
Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

14. Spegnere i moduli controller FC MetroCluster e gli shelf di storage.
15. Scollegare e rimuovere i moduli controller FC MetroCluster e gli shelf di storage.

Completamento della transizione

Per completare la transizione, verificare il funzionamento della nuova configurazione IP MetroCluster.

1. Verificare la configurazione dell'IP MetroCluster.

   È necessario eseguire questa operazione su ciascun cluster.

   L'esempio seguente mostra l'output per cluster_A.

```
cluster_A::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_A_1-IP          true    true          true
node_A_2-IP          true    true          false
2 entries were displayed.

cluster_A::>
```

L'esempio seguente mostra l'output per cluster_B.

```
cluster_B::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_B_1-IP          true    true          true
node_B_2-IP          true    true          false
2 entries were displayed.

cluster_B::>
```

2. Abilitare il failover dello storage e l'ha del cluster.

   È necessario eseguire questa operazione su ciascun cluster.

3. Verificare che la funzionalità ha del cluster sia attivata.

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>


cluster_A::> storage  failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1-IP    node_A_2-IP    true     Connected to node_A_2-IP
node_A_2-IP    node_A_1-IP    true     Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. Disattiva la modalità di transizione MetroCluster.

   a. Passare al livello di privilegio avanzato: `set -privilege advanced`
   b. Disattivare la modalità di transizione:`metrocluster transition disable`
   c. Tornare al livello di privilegio admin: `set -privilege admin`

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. Verificare che la transizione sia disattivata:`metrocluster transition show-mode`

   È necessario eseguire questi passaggi su entrambi i cluster.

```
cluster_A::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_A::>
```

```
cluster_B::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_B::>
```

6. Se si dispone di una configurazione a otto nodi, è necessario ripetere l'intera procedura partendo da "Prepararsi alla transizione da una configurazione MetroCluster FC a una configurazione MetroCluster IP" Per ciascuno dei gruppi FC DR.

Invio di un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completata la transizione, devi inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.
   a. Immettere il seguente comando: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Ripetere il comando sul cluster partner.

Ripristino del monitoraggio di Tiebreaker o Mediator

Una volta completata la transizione della configurazione MetroCluster, è possibile riprendere il monitoraggio con l'utility Tiebreaker o Mediator.

1. Utilizzare la procedura appropriata per la configurazione.

Se si utilizza…	Utilizzare questa procedura
Spareggio	"Aggiunta di configurazioni MetroCluster"

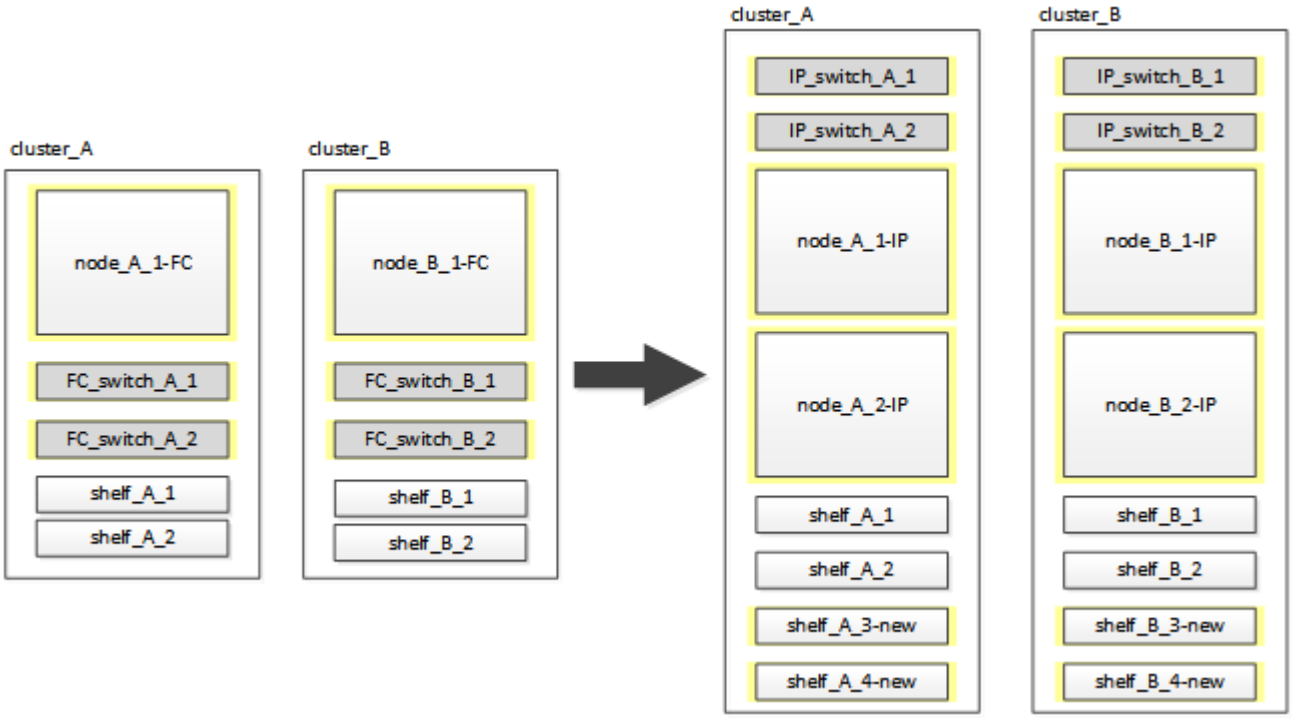
Mediatore	Link:./install-ip/concept_mediator_requirements.html configurazione-del-supporto-ontap-servizio-da-a-metrocluster-ip[Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster]

Transizione senza interruzioni da un MetroCluster FC a due nodi a una configurazione MetroCluster IP a quattro nodi (ONTAP 9.8 e versioni successive)

Transizione dirompente da un MetroCluster FC a due nodi a una configurazione MetroCluster IP a quattro nodi (ONTAP 9.8 e versioni successive)

A partire da ONTAP 9.8, è possibile trasferire carichi di lavoro e dati da una configurazione MetroCluster FC a due nodi esistente a una nuova configurazione MetroCluster IP a quattro nodi. Gli shelf di dischi dai nodi FC MetroCluster vengono spostati nei nodi IP.

L'illustrazione seguente fornisce una vista semplificata della configurazione prima e dopo questa procedura di transizione.



- Questa procedura è supportata nei sistemi che eseguono ONTAP 9.8 e versioni successive.
- Questa procedura ha un'interruzione.
- Questa procedura si applica solo a una configurazione MetroCluster FC a due nodi.

  Se si dispone di una configurazione MetroCluster FC a quattro nodi, vedere "Scelta della procedura di transizione".

- ADP non è supportato nella configurazione IP MetroCluster a quattro nodi creata da questa procedura.

- È necessario soddisfare tutti i requisiti e seguire tutte le fasi della procedura.
- Gli shelf di storage esistenti vengono spostati nei nuovi nodi IP MetroCluster.
- Se necessario, è possibile aggiungere ulteriori shelf di storage alla configurazione.

  Vedere "Riutilizzo degli shelf dei dischi e requisiti dei dischi per una transizione FC-IP senza interruzioni".

Esempio di denominazione in questa procedura

Questa procedura utilizza nomi di esempio per identificare i gruppi DR, i nodi e gli switch coinvolti.

I nodi nella configurazione originale hanno il suffisso -FC, che indica che si trovano in una configurazione Fabric-Attached o Stretch MetroCluster.

Componenti	Cluster_A presso il sito_A.	Cluster_B nel sito_B.
dr_Group_1-FC	• Node_A_1-FC • Shelf_A_1 • Shelf_A_2	• Node_B_1-FC • Shelf_B_1 • Shelf_B_2
dr_Group_2-IP	• Node_A_1-IP • Node_A_2-IP • Shelf_A_1 • Shelf_A_2 • Shelf_A_3-new • Shelf_A_4-new	• Node_B_1-IP • Node_B_2-IP • Shelf_B_1 • Shelf_B_2 • Shelf_B_3-new • Shelf_B_4-new
Switch	• Switch_A_1-FC • Switch_A_2-FC • Switch_A_1-IP • Switch_A_2-IP	• Switch_B_1-FC • Switch_B_2-FC • Switch_B_1-IP • Switch_B_2-IP

Preparazione per una transizione FC-IP senza interruzioni

Requisiti generali per la transizione FC-IP senza interruzioni

Prima di avviare il processo di transizione, è necessario assicurarsi che la configurazione soddisfi i requisiti.

La configurazione MetroCluster FC esistente deve soddisfare i seguenti requisiti:

- Deve essere una configurazione a due nodi e tutti i nodi devono eseguire ONTAP 9.8 o versione successiva.

  Può essere un MetroCluster a due nodi collegato al fabric o allungato.

- Deve soddisfare tutti i requisiti e i cavi descritti nelle *procedure di installazione e configurazione di MetroCluster*.

  "Installazione e configurazione di Fabric-Attached MetroCluster"

  "Estensione dell'installazione e della configurazione di MetroCluster"

- Non può essere configurato con NetApp Storage Encryption (NSE).
- I volumi MDV non possono essere crittografati.

È necessario disporre dell'accesso remoto alla console per tutti e sei i nodi dal sito MetroCluster o pianificare il trasferimento tra i siti come richiesto dalla procedura.

Riutilizzo degli shelf dei dischi e requisiti dei dischi per una transizione FC-IP senza interruzioni

È necessario assicurarsi che sugli shelf di storage siano disponibili dischi di riserva e spazio aggregato root adeguati.

Riutilizzo degli shelf di storage esistenti

Quando si utilizza questa procedura, gli shelf di storage esistenti vengono conservati per l'utilizzo da parte della nuova configurazione. Quando Node_A_1-FC e Node_B_1-FC vengono rimossi, gli shelf di dischi esistenti vengono collegati al nodo_A_1-IP e al nodo_A_2-IP sul cluster_A e al nodo_B_1-IP e al nodo_B_2-IP sul cluster_B.

- Gli shelf di storage esistenti (quelli collegati a Node_A_1-FC e Node_B_1-FC) devono essere supportati dai nuovi modelli di piattaforma.

  Se gli shelf esistenti non sono supportati dai nuovi modelli di piattaforma, vedere "Transizione disgregativa quando gli shelf esistenti non sono supportati sui nuovi controller (ONTAP 9.8 e versioni successive)".

- È necessario assicurarsi di non superare i limiti della piattaforma per i dischi, ecc.

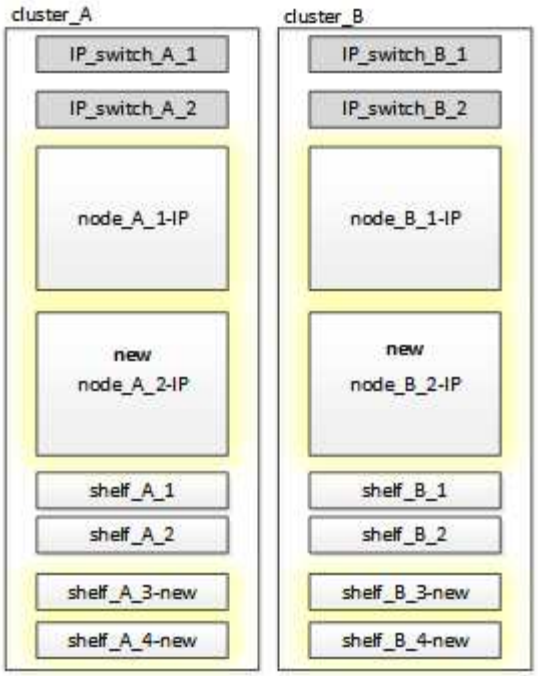
  "NetApp Hardware Universe"

Requisiti di storage per i controller aggiuntivi

Se necessario, è necessario aggiungere storage aggiuntivo per ospitare i due controller aggiuntivi (Node_A_2-IP e Node_B_2-ip), poiché la configurazione sta cambiando da una disposizione a due nodi a una a quattro nodi.

- A seconda delle unità di riserva disponibili negli shelf esistenti, è necessario aggiungere unità aggiuntive per ospitare i controller aggiuntivi nella configurazione.

  Questo potrebbe richiedere ulteriori shelf di storage, come mostrato nell'illustrazione seguente.



È necessario disporre di 14 - 18 unità aggiuntive per il terzo e il quarto controller (Node_A_2-IP e Node_B_2-IP):

- Tre pool0 dischi
- Tre unità pool1
- Due dischi di riserva
- Da sei a dieci dischi per il volume di sistema

- È necessario assicurarsi che la configurazione, inclusi i nuovi nodi, non superi i limiti della piattaforma per la configurazione, inclusi il numero di dischi, la capacità delle dimensioni dell'aggregato root e così via

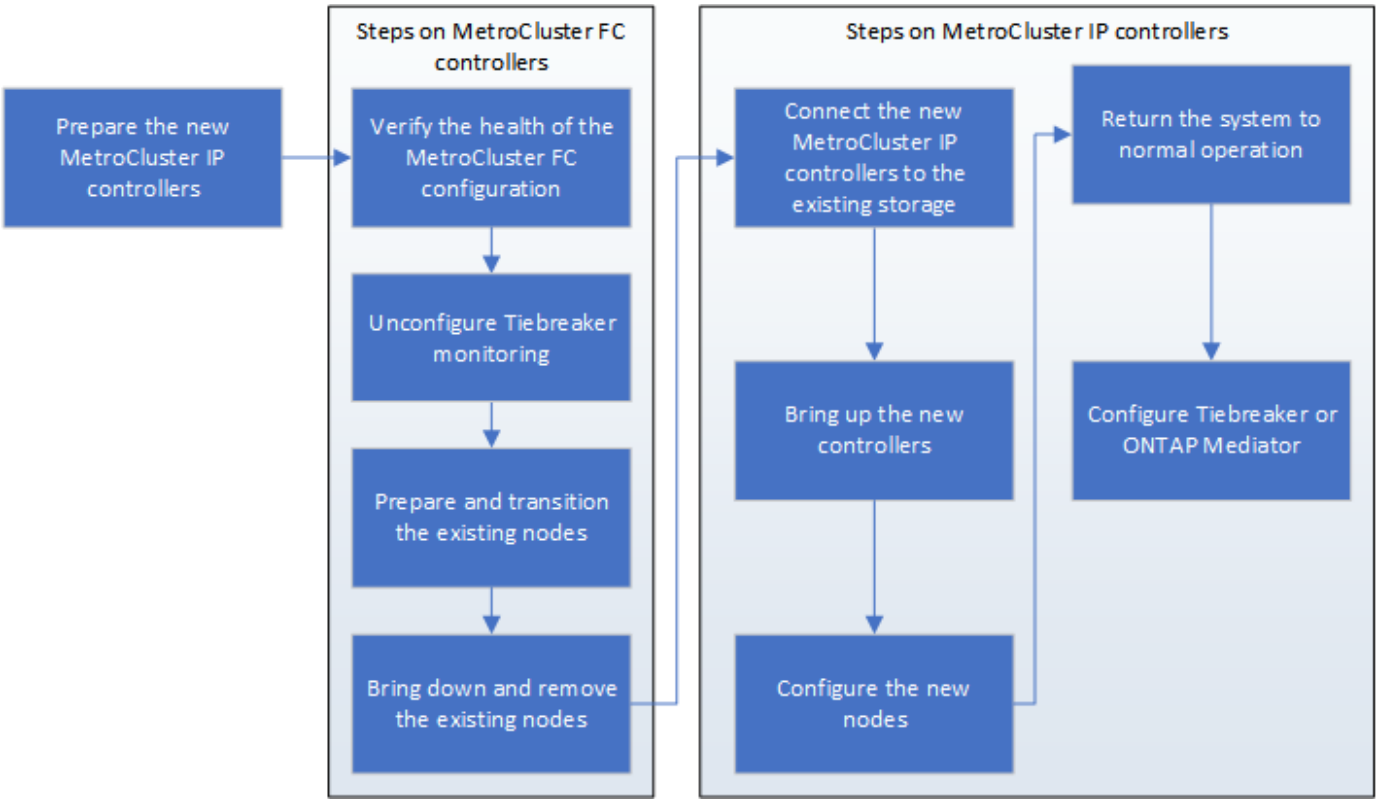
  Queste informazioni sono disponibili per ciascun modello di piattaforma all'indirizzo *NetApp Hardware Universe*.

  "NetApp Hardware Universe"

Workflow per una transizione senza interruzioni

Devi seguire il workflow specifico per garantire una transizione di successo.

Mentre ti prepari per la transizione, pianifica i viaggi tra i siti. Tenere presente che, dopo aver eseguito il racking e il cablaggio dei nodi remoti, è necessario accedere al terminale seriale per i nodi. L'accesso al Service Processor non sarà disponibile fino a quando i nodi non saranno configurati.



Mappatura delle porte dai nodi FC MetroCluster ai nodi IP MetroCluster

È necessario regolare la configurazione di porta e LIF del nodo FC MetroCluster in modo che sia compatibile con quella del nodo IP MetroCluster che lo sostituisce.

A proposito di questa attività

Quando i nuovi nodi vengono avviati per la prima volta durante il processo di aggiornamento, ciascun nodo utilizza la configurazione più recente del nodo che sta sostituendo. Quando si avvia Node_A_1-IP, ONTAP tenta di ospitare le LIF sulle stesse porte utilizzate su Node_A_1-FC.

Durante la procedura di transizione, verranno eseguiti i passaggi sul vecchio e sul nuovo nodo per garantire la corretta configurazione LIF di cluster, gestione e dati.

Fasi

1. Identificare eventuali conflitti tra l'utilizzo della porta FC MetroCluster esistente e l'utilizzo della porta per le interfacce IP MetroCluster sui nuovi nodi.

   È necessario identificare le porte IP MetroCluster sui nuovi controller IP MetroCluster utilizzando la tabella riportata di seguito. Quindi, controllare e registrare l'eventuale presenza di LIF di dati o di LIF del cluster su tali porte sui nodi FC MetroCluster.

   Queste LIF di dati o LIF del cluster in conflitto sui nodi FC MetroCluster verranno spostate nella fase appropriata della procedura di transizione.

   La seguente tabella mostra le porte IP MetroCluster in base al modello di piattaforma. È possibile ignorare la colonna ID VLAN.

Modello di piattaforma	Porta IP MetroCluster	ID VLAN	

AFF A800	e0b	Non utilizzato	
	e1b		
AFF A700 e FAS9000	e5a		
	e5b		
AFF A320	ad esempio		
	e0h		
AFF A300 e FAS8200	e1a		
	e1b		
FAS8300/A400/FAS8700	e1a	10	
	e1b	20	
AFF A250 e FAS500f	e0c	10	
	e0b	20	

È possibile compilare la seguente tabella e fare riferimento a tale tabella più avanti nella procedura di transizione.

Porte	Corrispondenti porte dell'interfaccia IP MetroCluster (dalla tabella precedente)	Le LIF in conflitto su queste porte sui nodi FC MetroCluster
Prima porta IP MetroCluster su Node_A_1-FC		
Seconda porta IP MetroCluster su Node_A_1-FC		
Prima porta IP MetroCluster su Node_B_1-FC		
Seconda porta IP MetroCluster su Node_B_1-FC		

2. Determinare quali porte fisiche sono disponibili sui nuovi controller e quali LIF possono essere ospitate sulle porte.

   L'utilizzo della porta del controller dipende dal modello di piattaforma e dal modello di switch IP che

verranno utilizzati nella configurazione IP di MetroCluster. È possibile ottenere l'utilizzo delle porte delle nuove piattaforme da *NetApp Hardware Universe*.

"NetApp Hardware Universe"

3. Se si desidera, registrare le informazioni sulla porta per Node_A_1-FC e Node_A_1-IP.

   Durante l'esecuzione della procedura di transizione, fare riferimento alla tabella.

   Nelle colonne node_A_1-IP, aggiungere le porte fisiche per il nuovo modulo controller e pianificare gli IPspaces e i domini di trasmissione per il nuovo nodo.

	Node_A_1-FC			Node_A_1-IP		
LIF	Porte	IPspaces	Domini di broadcast	Porte	IPspaces	Domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

4. Se lo si desidera, registrare tutte le informazioni sulla porta per Node_B_1-FC.

   Durante l'esecuzione della procedura di aggiornamento, fare riferimento alla tabella.

   Nelle colonne Node_B_1-IP, aggiungere le porte fisiche per il nuovo modulo controller e pianificare l'utilizzo della porta LIF, gli spazi IPe i domini di broadcast per il nuovo nodo.

	Node_B_1-FC			Node_B_1-IP		
LIF	Porte fisiche	IPspaces	Domini di broadcast	Porte fisiche	IPspaces	Domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

Preparazione dei controller IP MetroCluster

È necessario preparare i quattro nuovi nodi IP MetroCluster e installare la versione corretta di ONTAP.

A proposito di questa attività

Questa attività deve essere eseguita su ciascuno dei nuovi nodi:

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

I nodi devono essere connessi a qualsiasi shelf di storage **nuovo**. Devono **non** essere connessi agli shelf di storage esistenti contenenti dati.

Questi passaggi possono essere eseguiti ora o successivamente nella procedura quando i controller e gli shelf

sono montati in rack. In ogni caso, è necessario assicurarsi di cancellare la configurazione e preparare i nodi **prima** di collegarli agli shelf di storage esistenti e **prima** di apportare eventuali modifiche alla configurazione dei nodi FC MetroCluster.

> Non eseguire questa procedura con i controller IP MetroCluster collegati agli shelf di storage esistenti collegati ai controller FC MetroCluster.

In questa procedura, si cancella la configurazione sui nodi e si cancella l'area della mailbox sui nuovi dischi.

Fasi

1. Collegare i moduli controller ai nuovi shelf di storage.
2. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Lo stato ha per tutti i componenti deve essere "mccip".

3. Se lo stato di sistema visualizzato del controller o dello chassis non è corretto, impostare lo stato ha:

   ```
   ha-config modify controller mccip``ha-config modify chassis mccip
   ```

4. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

5. Ripetere i seguenti passaggi secondari su tutti e quattro i nodi per cancellare la configurazione:

   a. Impostare le variabili ambientali sui valori predefiniti:

      ```
      set-defaults
      ```

   b. Salvare l'ambiente:

      ```
      saveenv
      ```

   ```
   bye
   ```

6. Ripetere i seguenti passaggi secondari per avviare tutti e quattro i nodi utilizzando l'opzione 9a nel menu di boot.

   a. Al prompt DEL CARICATORE, avviare il menu di avvio:

      ```
      boot_ontap menu
      ```

   b. Nel menu di avvio, selezionare l'opzione "9a" per riavviare il controller.

7. Avviare ciascuno dei quattro nodi in modalità Maintenance (manutenzione) utilizzando l'opzione "5" nel menu di avvio.
8. Registrare l'ID di sistema e da ciascuno dei quattro nodi:

   ```
   sysconfig
   ```

9. Ripetere i seguenti passaggi su Node_A_1-IP e Node_B_1-IP.
   a. Assegnare la proprietà di tutti i dischi locali a ciascun sito:

      ```
      disk assign adapter.xx.*
      ```

   b. Ripetere il passaggio precedente per ciascun HBA con shelf di dischi collegati su Node_A_1-IP e Node_B_1-IP.
10. Ripetere i seguenti passaggi su Node_A_1-IP e Node_B_1-IP per cancellare l'area della mailbox su ciascun disco locale.
    a. Distruggere l'area della mailbox su ciascun disco:

       ```
       mailbox destroy local``mailbox destroy partner
       ```

11. Arrestare tutti e quattro i controller:

    ```
    halt
    ```

12. Su ciascun controller, visualizzare il menu di avvio:

    ```
    boot_ontap menu
    ```

13. Su ciascuno dei quattro controller, cancellare la configurazione:

    ```
    wipeconfig
    ```

    Una volta completata l'operazione wpeconfig, il nodo torna automaticamente al menu di boot.

14. Ripetere i seguenti passaggi secondari per riavviare tutti e quattro i nodi utilizzando l'opzione 9a nel menu di boot.
    a. Al prompt DEL CARICATORE, avviare il menu di avvio:

       ```
       boot_ontap menu
       ```

    b. Nel menu di avvio, selezionare l'opzione "9a" per riavviare il controller.
    c. Attendere che il modulo controller completi l'avvio prima di passare al modulo controller successivo.

    Una volta completato "9a", i nodi tornano automaticamente al menu di boot.

15. Spegnere i controller.

Verifica dello stato della configurazione MetroCluster FC

Prima di eseguire la transizione, è necessario verificare lo stato e la connettività della configurazione MetroCluster FC

Questa attività viene eseguita sulla configurazione MetroCluster FC.

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:
   a. Verificare che il sistema sia multipercorso:

      ```
      node run -node node-name sysconfig -a
      ```

b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

```
system health alert show
```

c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

```
metrocluster show
```

d. Eseguire un controllo MetroCluster:

```
metrocluster check run
```

e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

f. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

```
storage switch show
```

g. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

h. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

2. Verificare che i nodi siano in modalità non ha:

```
storage failover show
```

Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima della transizione.

Fasi

1. Rimuovere la configurazione MetroCluster esistente dal software Tiebreaker.

   "Rimozione delle configurazioni MetroCluster"

2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Transizione dei nodi FC MetroCluster

È necessario raccogliere informazioni dai nodi FC MetroCluster esistenti, inviare un messaggio AutoSupport che annuncia l'inizio della manutenzione e trasferire i nodi.

Raccolta di informazioni dai moduli controller esistenti prima della transizione

Prima di effettuare la transizione, è necessario raccogliere informazioni per ciascuno dei nodi.

Questa attività viene eseguita sui nodi esistenti:

- Node_A_1-FC
- Node_B_1-FC

a. Raccogliere l'output dei comandi nella tabella seguente.

Categoria	Comandi	Note
Licenza	licenza di sistema	
Shelf e numero di dischi in ogni shelf, dettagli di storage flash e memoria e NVRAM e schede di rete	nodo di sistema run -node node_name sysconfig	
LIF di gestione di nodi e reti cluster	system node run -node node_name sysconfig network interface show -role "cluster,node-mgmt,data"	
Informazioni SVM	show di vserver	
Informazioni sul protocollo	nfs mostra iscsi mostra cifs show	
Porte fisiche	porta di rete mostra -node node_name -type porta di rete fisica mostra	
Gruppi di failover	i gruppi di failover dell'interfaccia di rete mostrano -vserver vserver_name	Registrare i nomi e le porte dei gruppi di failover che non sono a livello di cluster.
Configurazione della VLAN	porta di rete vlan show -node node_name	Registrare ogni coppia di porte di rete e ID VLAN.
Configurazione del gruppo di interfacce	porta di rete ifgrp show -node node_name -instance	Annotare i nomi dei gruppi di interfacce e le porte ad essi assegnate.
Domini di broadcast	visualizzazione del dominio di broadcast della porta di rete	
IPSpace	visualizzazione di network ipspace	
Info volume	visualizzazione volume e visualizzazione volume - crittografia dei campi	
Info aggregate	show di storage aggregato e storage aggr crittografia show eshow storage aggregato object-store	

Categoria	Comandi	Note
Informazioni sulla proprietà del disco	show di storage aggregato e storage aggr crittografia show eshow storage aggregato object-store	
Crittografia	show di backup di storage failover mailbox-disk e security key-manager	Conservare anche la passphrase utilizzata per attivare il gestore delle chiavi. Nel caso di un gestore di chiavi esterno, sono necessarie le informazioni di autenticazione per il client e il server.
Crittografia	show security key-manager	
Crittografia	programma esterno security key-manager	
Crittografia	systemshell local kenv kmip.init.ipaddr ip-address	
Crittografia	netmask kenv kmip.init.netmask locale di systemshell	
Crittografia	gateway kenv kmip.init.gateway locale di systemshell	
Crittografia	interfaccia systemshell locale kenv kmip.init.interface	

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Ciò impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

Questa attività deve essere eseguita su ciascun sito MetroCluster.

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è in corso.
   a. Immettere il seguente comando: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      intervallo di manutenzione in ore specifica la durata della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Ripetere il comando sul cluster partner.

Transizione, arresto e rimozione dei nodi FC MetroCluster

Oltre all'emissione di comandi sui nodi FC MetroCluster, questa attività include l'apertura fisica e la rimozione dei moduli controller in ogni sito.

Questa attività deve essere eseguita su ciascuno dei vecchi nodi:

- Node_A_1-FC
- Node_B_1-FC

a. Arrestare tutto il traffico client.

b. Su uno dei nodi FC MetroCluster, ad esempio Node_A_1-FC, abilitare la transizione.

   i. Impostare il livello di privilegio avanzato: `set -priv advanced`

   ii. Attiva transizione: `metrocluster transition enable -transition-mode disruptive`

   iii. Tornare alla modalità admin: `set -priv admin`

c. Eseguire il mirroring dell'aggregato root eliminando il plesso remoto degli aggregati root.

   i. Identificare gli aggregati root: `storage aggregate show -root true`

   ii. Visualizzare gli aggregati pool1: `storage aggregate plex show -pool 1`

   iii. Eliminare il plex locale dell'aggregato root: `aggr plex delete aggr-name -plex plex-name`

   iv. Offline il plesso remoto dell'aggregato root: `aggr plex offline root-aggregate -plex remote-plex-for-root-aggregate`

   Ad esempio:

```
# aggr plex offline aggr0_node_A_1-FC_01 -plex plex4
```

d. Confermare il numero di caselle postali, l'assegnazione automatica del disco e la modalità di transizione prima di procedere con i seguenti comandi su ciascun controller:

   i. Impostare il livello di privilegio avanzato: `set -priv advanced`

   ii. Verificare che per ciascun modulo controller siano visualizzate solo tre unità mailbox: `storage failover mailbox-disk show`

   iii. Tornare alla modalità admin: `set -priv admin`

   iv. Verificare che la modalità di transizione sia disgregativa: Mostra MetroCluster Transition

e. Verificare la presenza di eventuali dischi rotti: `disk show -broken`

f. Rimuovere o sostituire eventuali dischi rotti

g. Verificare che gli aggregati siano integri utilizzando i seguenti comandi su Node_A_1-FC e Node_B_1-FC:`storage aggregate show`/

   Il comando show dell'aggregato di storage indica che l'aggregato root è senza mirror.

h. Verificare la presenza di VLAN o gruppi di interfacce: `network port ifgrp show``network port vlan show`

   Se non sono presenti componenti, saltare i due passi seguenti.

i. Visualizzare l'elenco delle LIF utilizzando VLAN o ifgrps: `network interface show -fields home-port,curr-port``network port show -type if-group | vlan`

j. Rimuovere eventuali VLAN e gruppi di interfacce.

È necessario eseguire questi passaggi per tutti i file LIF in tutte le SVM, incluse quelle con il suffisso -mc.

i. Spostare le LIF utilizzando le VLAN o i gruppi di interfacce su una porta disponibile: `network interface modify -vserver vserver-name -lif lif_name -home- port port`

ii. Visualizzare le LIF che non si trovano sulle porte home: `network interface show -is-home false`

iii. Ripristinare tutte le LIF alle rispettive porte home: `network interface revert -vserver vserver_name -lif lif_name`

iv. Verificare che tutte le LIF siano presenti sulle porte home: `network interface show -is -home false`

    Nell'output non dovrebbe essere visualizzato alcun LIF.

v. Rimuovere le porte VLAN e ifgrp dal dominio di broadcast: `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

vi. Verificare che tutte le porte vlan e ifgrp non siano assegnate a un dominio di trasmissione: `network port show -type if-group | vlan`

vii. Elimina tutte le VLAN: `network port vlan delete -node nodename -vlan-name vlan-name`

viii. Elimina gruppi di interfacce: `network port ifgrp delete -node nodename -ifgrp ifgrp-name`

k. Spostare le eventuali LIF necessarie per risolvere i conflitti con le porte dell'interfaccia IP di MetroCluster.

    È necessario spostare i LIF identificati al punto 1 di "Mappatura delle porte dai nodi FC MetroCluster ai nodi IP MetroCluster".

i. Spostare le LIF ospitate sulla porta desiderata su un'altra porta: `network interface modify -lif lifname -vserver vserver-name -home-port new-homeport``network interface revert -lif lifname -vserver vservername`

ii. Se necessario, spostare la porta di destinazione in un dominio IPSpace e broadcast appropriato. `network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast-domain current-broadcast-domain -ports controller-name:current-port``network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port`

l. Arrestare i controller FC MetroCluster (Node_A_1-FC e Node_B_1-FC): `system node halt`

m. Al prompt DEL CARICATORE, sincronizzare i clock hardware tra i moduli controller FC e IP.

i. Sul vecchio nodo MetroCluster FC (Node_A_1-FC), visualizzare la data: `show date`

ii. Sui nuovi controller IP MetroCluster (Node_A_1-IP e Node_B_1-IP), impostare la data visualizzata sul controller originale: `set date mm/dd/yy`

iii. Sui nuovi controller IP MetroCluster (Node_A_1-IP e Node_B_1-IP), verificare la data: `show date`

n. Arrestare e spegnere i moduli controller FC MetroCluster (Node_A_1-FC e Node_B_1-FC), i bridge FC-SAS (se presenti), gli switch FC (se presenti) e ogni shelf di storage collegato a questi nodi.

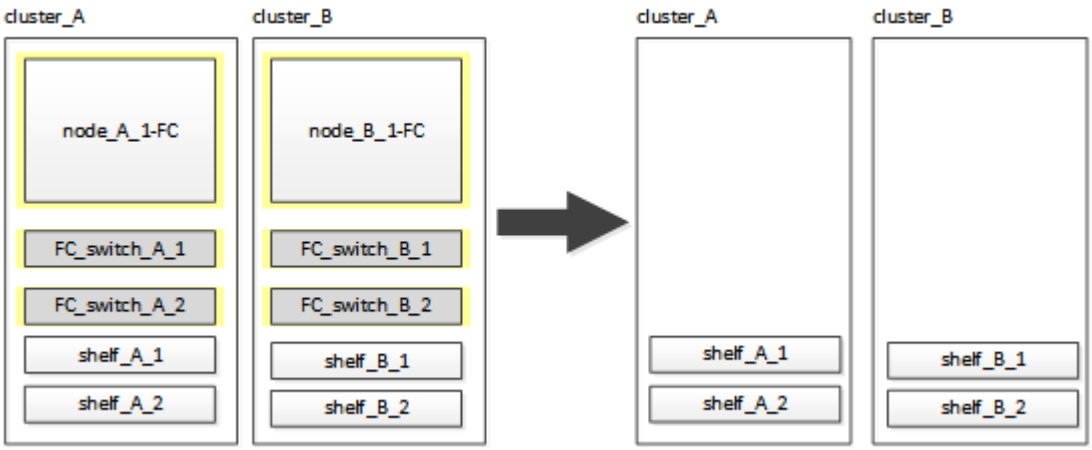
o. Scollega gli shelf dai controller FC MetroCluster e documenta quali shelf sono storage locale per ciascun cluster.

   Se la configurazione utilizza bridge FC-SAS o switch back-end FC, scollegarli e rimuoverli.

p. In modalità di manutenzione sui nodi FC MetroCluster (Node_A_1-FC e Node_B_1-FC), verificare che non siano collegati dischi: `disk show -v`

q. Spegnere e rimuovere i nodi MetroCluster FC.

A questo punto, i controller FC MetroCluster sono stati rimossi e gli shelf sono scollegati da tutti i controller.



Collegamento dei moduli del controller IP MetroCluster

È necessario aggiungere alla configurazione i quattro nuovi moduli controller ed eventuali shelf di storage aggiuntivi. I nuovi moduli controller vengono aggiunti due alla volta.

Configurazione dei nuovi controller

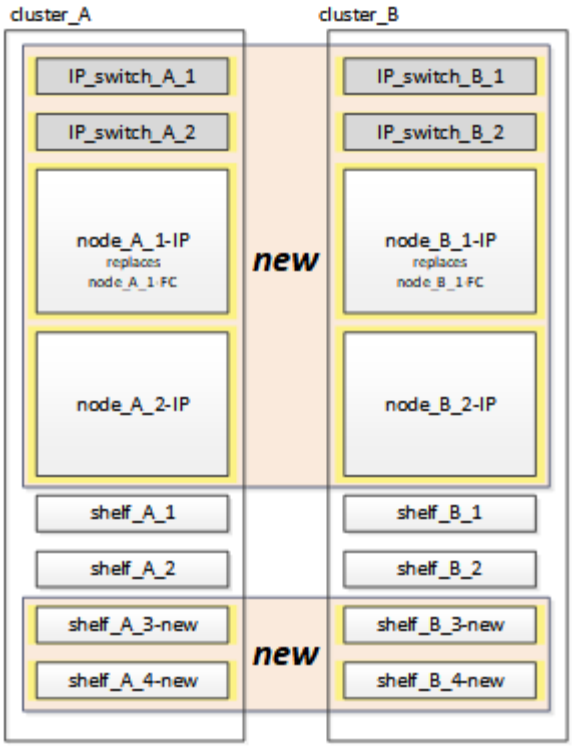
È necessario inserire in rack e collegare i nuovi controller IP MetroCluster agli shelf di storage precedentemente collegati ai controller FC MetroCluster.

A proposito di questa attività

Questi passaggi devono essere eseguiti su ciascuno dei nodi IP di MetroCluster.

- Node_A_1-IP
- Node_A_2-IP
- Node_B_1-IP
- Node_B_2-IP

Nell'esempio seguente, vengono aggiunti due shelf di storage aggiuntivi in ogni sito per fornire storage per ospitare i nuovi moduli controller.



Fasi

1. Pianificare il posizionamento dei nuovi moduli controller e degli shelf di storage in base alle necessità.

   Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di shelf di storage nella configurazione.

2. Mettere a terra l'utente.
3. Rack delle nuove apparecchiature: Controller, shelf di storage e switch IP.

   Non collegare i shelf di storage o gli switch IP in questo momento.

4. Collegare i cavi di alimentazione e la console di gestione ai controller.
5. Verificare che tutti gli shelf di storage siano spenti.
6. Verificare che non vi siano dischi collegati eseguendo la seguente procedura su tutti e quattro i nodi:

   a. Al prompt DEL CARICATORE, avviare il menu di avvio:

      ```
      boot_ontap maint
      ```

   b. Verificare che non siano collegate unità:

      ```
      disk show -v
      ```

   L'output non dovrebbe mostrare dischi.

   a. Arrestare il nodo:

      ```
      halt
      ```

7. Avviare tutti e quattro i nodi utilizzando l'opzione 9a del menu di boot.

a. Al prompt DEL CARICATORE, avviare il menu di avvio:

```
boot_ontap menu
```

b. Nel menu di avvio, selezionare l'opzione "9a" per riavviare il controller.

c. Attendere che il modulo controller completi l'avvio prima di passare al modulo controller successivo.

Una volta completato "9a", i nodi tornano automaticamente al menu di boot.

8. Cablare gli scaffali di stoccaggio.

   Per informazioni sul cablaggio, consultare le procedure di installazione e configurazione del controller per il modello in uso.

   "Documentazione dei sistemi hardware ONTAP"

9. Collegare i controller agli switch IP come descritto in "Cablaggio degli switch IP".
10. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

    Seguire la procedura per il fornitore dello switch:

    - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
    - "Ripristino delle impostazioni predefinite dello switch IP Cisco"

11. Scaricare e installare i file RCF.

    Seguire la procedura per il fornitore dello switch:

    - "Download e installazione dei file RCF Broadcom"
    - "Download e installazione dei file Cisco IP RCF"

12. Accendere il primo nuovo controller (Node_A_1-IP) e premere Ctrl-C per interrompere il processo di avvio e visualizzare il prompt DEL CARICATORE.
13. Avviare il controller in modalità di manutenzione:

    ```
    boot_ontap_maint
    ```

14. Visualizzare l'ID di sistema del controller:

    ```
    sysconfig -v
    ```

15. Verificare che gli shelf della configurazione esistente siano visibili dal nuovo nodo IP MetroCluster:

    ```
    storage show shelf``disk show -v
    ```

16. Arrestare il nodo:

    ```
    halt
    ```

17. Ripetere i passaggi precedenti sull'altro nodo del sito del partner (Site_B).

Connessione e avvio di Node_A_1-IP e Node_B_1-IP

Dopo aver collegato i controller IP MetroCluster e gli switch IP, si passa a Node_A_1-IP e Node_B_1-IP e si

avvia.

Creazione di Node_A_1-IP

È necessario avviare il nodo con l'opzione di transizione corretta.

Fasi

1. Boot node_A_1-IP al menu di boot:

   ```
   boot_ontap menu
   ```

2. Immettere il seguente comando al prompt del menu di avvio per avviare la transizione:

   ```
   boot_after_mcc_transition
   ```

   - Questo comando riassegna tutti i dischi di proprietà di Node_A_1-FC a Node_A_1-IP.
     - I dischi Node_A_1-FC sono assegnati al Node_A_1-IP
     - I dischi Node_B_1-FC sono assegnati al nodo_B_1-IP
   - Il comando esegue inoltre automaticamente altre riassegnazioni di ID di sistema necessarie in modo che i nodi IP MetroCluster possano avviarsi al prompt di ONTAP.
   - Se il comando boot_after_mcc_Transition non riesce per qualsiasi motivo, dovrebbe essere rieseguito dal menu di boot.

> - Se viene visualizzato il seguente prompt, immettere Ctrl-C per continuare. Verifica stato DR MCC in corso… [Enter Ctrl-C(resume), S(status), L(link)]_
> - Se il volume root è stato crittografato, il nodo si arresta con il seguente messaggio. Arresto del sistema, perché il volume root è crittografato (NetApp Volume Encryption) e l'importazione della chiave non è riuscita. Se questo cluster è configurato con un gestore di chiavi esterno (KMIP), controllare lo stato dei server di chiavi.

```
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)?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-
FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of
MetroCluster FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
```

3. Se i volumi di dati sono crittografati, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager key query -node node-name` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia esterne per la gestione delle chiavi".

4. Se il volume root è crittografato, seguire la procedura descritta in "Ripristino della gestione delle chiavi se il volume root è crittografato".

Ripristino della gestione delle chiavi se il volume root è crittografato

Se il volume root è crittografato, è necessario utilizzare speciali comandi di boot per ripristinare la gestione delle chiavi.

Prima di iniziare

Le passphrase devono essere raccolte in precedenza.

Fasi

1. Se si utilizza la gestione delle chiavi integrata, eseguire i seguenti passaggi secondari per ripristinare la configurazione.

   a. Dal prompt DEL CARICATORE, visualizzare il menu di avvio:

   ```
   boot_ontap menu
   ```

   b. Selezionare l'opzione "(10) set onboard key management recovery secrets" dal menu di avvio.

   Rispondere alle richieste in base alle esigenze:

   ```
   This option must be used only in disaster recovery procedures. Are
   you sure? (y or n): y
   Enter the passphrase for onboard key management: passphrase
   Enter the passphrase again to confirm: passphrase

   Enter the backup data: backup-key
   ```

   Il sistema viene avviato dal menu di avvio.

   c. Immettere l'opzione "6" nel menu di avvio.

   Rispondere alle richieste in base alle esigenze:

   ```
   This will replace all flash-based configuration with the last backup
   to
   disks. Are you sure you want to continue?: y

   Following this, the system will reboot a few times and the following
   prompt will be available continue by saying y

   WARNING: System ID mismatch. This usually occurs when replacing a
   boot device or NVRAM cards!
   Override system ID? {y|n} y
   ```

   Dopo il riavvio, il sistema viene visualizzato al prompt DEL CARICATORE.

   d. Dal prompt DEL CARICATORE, visualizzare il menu di avvio:

   ```
   boot_ontap menu
   ```

e. Selezionare nuovamente l'opzione "(10) set onboard key management recovery secrets" (Imposta segreti di ripristino gestione delle chiavi integrate) dal menu di avvio.

   Rispondere alle richieste in base alle esigenze:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

   Il sistema viene avviato dal menu di avvio.

f. Immettere l'opzione "1" nel menu di avvio.

   Se viene visualizzato il seguente prompt, premere Ctrl+C per riprendere il processo.

```
Checking MCC DR state... [enter Ctrl-C(resume), S(status), L(link)]
```

   Il sistema viene avviato dal prompt ONTAP.

g. Ripristinare la gestione delle chiavi integrata:

```
security key-manager onboard sync
```

   Rispondere alle richieste, utilizzando la passphrase precedentemente raccolta:

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster_A":: passphrase
```

2. Se si utilizza la gestione esterna delle chiavi, eseguire le seguenti procedure secondarie per ripristinare la configurazione.

   a. Impostare i bootargs richiesti:

```
setenv bootarg.kmip.init.ipaddr ip-address

setenv bootarg.kmip.init.netmask netmask

setenv bootarg.kmip.init.gateway gateway-address

setenv bootarg.kmip.init.interface interface-id
```

   b. Dal prompt DEL CARICATORE, visualizzare il menu di avvio:

```
boot_ontap menu
```

c. Selezionare l'opzione "(11) Configure node for external key management" (Configura nodo per la gestione delle chiavi esterne) dal menu di avvio.

   Il sistema viene avviato dal menu di avvio.

d. Immettere l'opzione "6" nel menu di avvio.

   Il sistema si avvia più volte. Quando viene richiesto di continuare il processo di avvio, è possibile rispondere affermativamente.

   Dopo il riavvio, il sistema viene visualizzato al prompt DEL CARICATORE.

e. Impostare i bootargs richiesti:

```
setenv bootarg.kmip.init.ipaddr ip-address

setenv bootarg.kmip.init.netmask netmask

setenv bootarg.kmip.init.gateway gateway-address

setenv bootarg.kmip.init.interface interface-id
```

a. Dal prompt DEL CARICATORE, visualizzare il menu di avvio:

```
boot_ontap menu
```

b. Selezionare di nuovo l'opzione "(11) Configure node for external key management" (Configura nodo per la gestione delle chiavi esterne) dal menu di avvio e rispondere alle richieste secondo necessità.

   Il sistema viene avviato dal menu di avvio.

c. Ripristinare la gestione esterna delle chiavi:

```
security key-manager external restore
```

Creazione della configurazione di rete

È necessario creare una configurazione di rete che corrisponda alla configurazione sui nodi FC. Questo perché il nodo IP MetroCluster riproduce la stessa configurazione all'avvio, il che significa che quando si avvia Node_A_1-IP e Node_B_1-IP, ONTAP tenta di ospitare i file LIF sulle stesse porte utilizzate rispettivamente su Node_A_1-FC e Node_B_1-FC.

A proposito di questa attività

Durante la creazione della configurazione di rete, utilizzare il piano creato in "Mappatura delle porte dai nodi FC MetroCluster ai nodi IP MetroCluster" per assisterti.

> Una volta configurati i nodi IP MetroCluster, potrebbe essere necessaria un'ulteriore configurazione per attivare le LIF dei dati.

Fasi

1. Verificare che tutte le porte del cluster si trovino nel dominio di trasmissione appropriato:

   L'IPSpace del cluster e il dominio di broadcast del cluster sono necessari per creare le LIF del cluster

a. Visualizzare gli spazi IP:

```
network ipspace show
```

b. Creare spazi IP e assegnare le porte del cluster in base alle esigenze.

"Configurazione di IPspaces (solo amministratori del cluster)"

c. Visualizzare i domini di trasmissione:

```
network port broadcast-domain show
```

d. Aggiungere eventuali porte del cluster a un dominio di broadcast in base alle esigenze.

"Aggiunta o rimozione di porte da un dominio di broadcast"

e. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

"Creazione di una VLAN"

"Combinazione di porte fisiche per creare gruppi di interfacce"

2. Verificare che le impostazioni MTU siano impostate correttamente per le porte e il dominio di trasmissione e apportare le modifiche utilizzando i seguenti comandi:

```
network port broadcast-domain show

network port broadcast-domain modify -broadcast-domain bcastdomainname -mtu
mtu-value
```

Impostazione delle porte del cluster e delle LIF del cluster

È necessario configurare le porte del cluster e i LIF. I seguenti passaggi devono essere eseguiti sui nodi del sito A che sono stati avviati con aggregati root.

Fasi

1. Identificare l'elenco di LIF utilizzando la porta del cluster desiderata:

```
network interface show -curr-port portname

network interface show -home-port portname
```

2. Per ciascuna porta del cluster, modificare la porta home di una delle LIF di tale porta con un'altra,

a. Immettere Advanced Privilege mode e digitare "y" quando viene richiesto di continuare:

```
set priv advanced
```

b. Se la LIF da modificare è una LIF dati:

```
vserver config override -command "network interface modify -lif lifname
```

```
-vserver vservername -home-port new-datahomeport"
```

c. Se la LIF non è una LIF dati:

```
network interface modify -lif lifname -vserver vservername -home-port new-
datahomeport
```

d. Ripristinare le LIF modificate alla porta home:

```
network interface revert * -vserver vserver_name
```

e. Verificare che non vi siano LIF sulla porta del cluster:

```
network interface show -curr-port portname
```

```
network interface show -home-port portname
```

a. Rimuovere la porta dal dominio di trasmissione corrente:

```
network port broadcast-domain remove-ports -ipspace ipspacename -broadcast
-domain bcastdomainname -ports node_name:port_name
```

b. Aggiungere la porta all'IPSpace del cluster e al dominio di trasmissione:

```
network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain
Cluster -ports node_name:port_name
```

c. Verificare che il ruolo della porta sia stato modificato: `network port show`

d. Ripetere questi passaggi secondari per ciascuna porta del cluster.

e. Tornare alla modalità admin:

```
set priv admin
```

3. Creare le LIF del cluster sulle nuove porte del cluster:

a. Per la configurazione automatica utilizzando l'indirizzo link-local per la LIF del cluster, utilizzare il seguente comando:

```
network interface create -vserver Cluster -lif cluster_lifname -service
-policy default-cluster -home-node a1name -home-port clusterport -auto true
```

b. Per assegnare un indirizzo IP statico alla LIF del cluster, utilizzare il seguente comando:

```
network interface create -vserver Cluster -lif cluster_lifname -service
-policy default-cluster -home-node a1name -home-port clusterport -address
ip-address -netmask netmask -status-admin up
```

Verifica della configurazione LIF in corso

La LIF di gestione dei nodi, la LIF di gestione dei cluster e la LIF di intercluster saranno ancora presenti dopo lo spostamento dello storage dal vecchio controller. Se necessario, è necessario spostare i file LIF nelle porte appropriate.

Fasi

1. Verificare se la LIF di gestione e la LIF di gestione del cluster si trovano già sulla porta desiderata:

   ```
   network interface show -service-policy default-management

   network interface show -service-policy default-intercluster
   ```

   Se le LIF si trovano sulle porte desiderate, è possibile saltare il resto delle fasi di questa attività e passare all'attività successiva.

2. Per ogni nodo, gestione del cluster o LIF di intercluster che non si trovano sulla porta desiderata, modificare la porta home di una delle LIF di tale porta in un'altra porta.

   a. Cambiare destinazione della porta desiderata spostando i file LIF ospitati sulla porta desiderata su un'altra porta:

      ```
      vserver config override -command "network interface modify -lif lifname
      -vserver vservername -home-port new-datahomeport"
      ```

   b. Ripristinare le LIF modificate alla nuova porta home:

      ```
      vserver config override -command "network interface revert -lif lifname
      -vserver _vservername"
      ```

   c. Se la porta desiderata non si trova nel dominio IPSpace e broadcast corretto, rimuovere la porta dal dominio IPSpace e broadcast corrente:

      ```
      network port broadcast-domain remove-ports -ipspace current-ipspace
      -broadcast-domain current-broadcast-domain -ports controller-name:current-
      port
      ```

   d. Spostare la porta desiderata sul dominio IPSpace e broadcast di destra:

      ```
      network port broadcast-domain add-ports -ipspace new-ipspace -broadcast
      -domain new-broadcast-domain -ports controller-name:new-port
      ```

   e. Verificare che il ruolo della porta sia stato modificato:

      ```
      network port show
      ```

   f. Ripetere questi passaggi secondari per ciascuna porta.

3. Spostare nodi, LIF di gestione cluster e LIF di intercluster sulla porta desiderata:

   a. Modificare la porta home di LIF:

      ```
      network interface modify -vserver vserver -lif node_mgmt -home-port port
      -home-node homenode
      ```

   b. Ripristinare la nuova porta home di LIF:

      ```
      network interface revert -lif node_mgmt -vserver vservername
      ```

   c. Modificare la porta home della LIF di gestione del cluster:

```
network interface modify -vserver vserver -lif cluster-mgmt-LIF-name -home
-port port -home-node homenode
```

d. Riportare la LIF di gestione del cluster alla nuova porta home:

```
network interface revert -lif cluster-mgmt-LIF-name -vserver vservername
```

e. Modificare la porta home della LIF dell'intercluster:

```
network interface modify -vserver vserver -lif intercluster-lif-name -home
-node nodename -home-port port
```

f. Riportare la LIF dell'intercluster alla nuova porta home:

```
network interface revert -lif intercluster-lif-name -vserver vservername
```

Portando Node_A_2-IP e Node_B_2-IP

È necessario attivare e configurare il nuovo nodo IP MetroCluster in ogni sito, creando una coppia ha in ogni sito.

Portando Node_A_2-IP e Node_B_2-IP

È necessario avviare i nuovi moduli controller uno alla volta utilizzando l'opzione corretta nel menu di avvio.

A proposito di questa attività

In questi passaggi, si avviano i due nuovi nodi, espandendo quella che era stata una configurazione a due nodi in una configurazione a quattro nodi.

Questi passaggi vengono eseguiti sui seguenti nodi:

- Node_A_2-IP
- Node_B_2-IP

Fasi

1. Avviare i nuovi nodi usando l'opzione di boot "9c".

```
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)? 9c
```

Il nodo viene inizializzato e avviato con l'installazione guidata del nodo, come descritto di seguito.

```
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. .
.
.
```

Se l'opzione "9c" non riesce, attenersi alla seguente procedura per evitare la possibile perdita di dati:

- Non tentare di eseguire l'opzione 9a.
- Scollegare fisicamente gli shelf esistenti che contengono dati dalla configurazione FC MetroCluster originale (shelf_A_1, shelf_A_2, shelf_B_1, shelf_B_2).
- Contattare il supporto tecnico, facendo riferimento all'articolo della Knowledge base "Transizione MetroCluster da FC a IP - opzione 9c non riuscita".

  "Supporto NetApp"

2. Attivare lo strumento AutoSupport seguendo le istruzioni fornite dalla procedura guidata.
3. Rispondere alle richieste per configurare l'interfaccia di gestione dei nodi.

```
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 la modalità di failover dello storage sia impostata su ha:

   `storage failover show -fields mode`

   Se la modalità non è ha, impostarla:

   `storage failover modify -mode ha -node localhost`

   Riavviare il nodo per rendere effettiva la modifica.

5. 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
                                                                  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
```

6. Uscire dalla procedura guidata Node Setup (Configurazione nodo):

```
exit
```

7. Accedere all'account admin utilizzando il nome utente admin.
8. Unirsi al cluster esistente utilizzando la procedura guidata di installazione del cluster.

```
:> cluster setup
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.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

9. Dopo aver completato l'installazione guidata del cluster e averlo chiuso, verificare che il cluster sia attivo e che il nodo funzioni correttamente:

```
cluster show
```

10. Disattiva assegnazione automatica del disco:

    ```
    storage disk option modify -autoassign off -node node_A_2-IP
    ```

11. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager key query -node` *`node-name`* Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia esterne per la gestione delle chiavi".

12. Ripetere i passaggi precedenti sul secondo nuovo modulo controller (Node_B_2-IP).

Verifica delle impostazioni MTU in corso

Verificare che le impostazioni MTU siano impostate correttamente per le porte e il dominio di trasmissione e apportare modifiche.

Fasi

1. Controllare le dimensioni MTU utilizzate nel dominio di trasmissione del cluster:

    ```
    network port broadcast-domain show
    ```

2. Se necessario, aggiornare le dimensioni MTU in base alle necessità:

    ```
    network port broadcast-domain modify -broadcast-domain bcast-domain-name -mtu
    mtu-size
    ```

Configurazione delle LIF tra cluster

Configurare le LIF intercluster richieste per il peering del cluster.

Questa attività deve essere eseguita su entrambi i nuovi nodi, Node_A_2-IP e Node_B_2-IP.

Fase

1. Configurare le LIF dell'intercluster. Vedere "Configurazione delle LIF tra cluster"

Verifica del peering del cluster

Verificare che cluster_A e cluster_B siano peering e che i nodi di ciascun cluster possano comunicare tra loro.

Fasi

1. Verificare la relazione di peering del cluster:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
node_A_1-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
node_A_2-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

2. Ping per verificare che gli indirizzi peer siano raggiungibili:

   `cluster peer ping -originating-node` *`local-node`* `-destination-cluster` *`remote-cluster-name`*

Configurazione dei nuovi nodi e completamento della transizione

Con l'aggiunta dei nuovi nodi, è necessario completare le fasi di transizione e configurare i nodi IP MetroCluster.

Configurazione dei nodi IP MetroCluster e disattivazione della transizione

È necessario implementare le connessioni IP MetroCluster, aggiornare la configurazione MetroCluster e disattivare la modalità di transizione.

1. Formare i nuovi nodi in un gruppo di DR emettendo i seguenti comandi da controller node_A_1-IP:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster peer-cluster-name -local-node local-controller-name -remote-node remote-controller-name

   metrocluster configuration-settings dr-group show
   ```

2. Creare interfacce IP MetroCluster (Node_A_1-IP, Node_A_2-IP, Node_B_1-IP, Node_B_2-IP) — è necessario creare due interfacce per controller; otto interfacce in totale:

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node controller-name -home-port port -address ip-address -netmask
netmask -vlan-id vlan-id``metrocluster configuration-settings interface show
```

> A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".

Il parametro -vlan-id è necessario solo se non si utilizzano gli ID VLAN predefiniti. Solo alcuni sistemi supportano ID VLAN non predefiniti.

> - Alcune piattaforme utilizzano una VLAN per l'interfaccia IP di MetroCluster. Per impostazione predefinita, ciascuna delle due porte utilizza una VLAN diversa: 10 e 20. È inoltre possibile specificare una VLAN diversa (non predefinita) superiore a 100 (tra 101 e 4095) utilizzando `-vlan-id parameter` in `metrocluster configuration-settings interface create` comando.
> - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".

I seguenti modelli di piattaforma possono essere aggiunti alla configurazione MetroCluster esistente se le VLAN utilizzate sono 10/20 o superiori a 100. Se si utilizzano altre VLAN, queste piattaforme non possono essere aggiunte alla configurazione esistente, in quanto l'interfaccia MetroCluster non può essere configurata. Se si utilizza un'altra piattaforma, la configurazione della VLAN non è rilevante in quanto non è richiesta in ONTAP.

Piattaforme AFF	Piattaforme FAS
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

3. Eseguire l'operazione di connessione MetroCluster da controller node_A_1-IP per collegare i siti MetroCluster — questa operazione può richiedere alcuni minuti:

   ```
   metrocluster configuration-settings connection connect
   ```

4. Verificare che i dischi del cluster remoto siano visibili da ciascun controller tramite le connessioni iSCSI:

   ```
   disk show
   ```

   Nella configurazione dovrebbero essere visualizzati i dischi remoti appartenenti agli altri nodi.

5. Eseguire il mirroring dell'aggregato root per Node_A_1-IP e Node_B_1-IP:

   ```
   aggregate mirror -aggregate root-aggr
   ```

6. Assegnare i dischi per Node_A_2-IP e Node_B_2-IP.

   Assegnazioni di dischi del pool 1 già effettuate per Node_A_1-IP e Node_B_1-IP quando il comando

boot_after_mcc_transtion è stato emesso al menu di boot.

a. Eseguire i seguenti comandi su Node_A_2-IP:

```
disk assign disk1disk2disk3 … diskn -sysid node_B_2-IP-controller-sysid
-pool 1 -force
```

b. Eseguire i seguenti comandi su Node_B_2-IP:

```
disk assign disk1disk2disk3 … diskn -sysid node_A_2-IP-controller-sysid
-pool 1 -force
```

7. Verificare che la proprietà dei dischi remoti sia stata aggiornata:

```
disk show
```

8. Se necessario, aggiornare le informazioni di proprietà utilizzando i seguenti comandi:
   a. Accedere alla modalità avanzata dei privilegi e digitare y quando richiesto per continuare:

   ```
   set priv advanced
   ```

   b. Aggiorna proprietà del disco:

   ```
   disk refresh-ownership controller-name
   ```

   c. Tornare alla modalità admin:

   ```
   set priv admin
   ```

9. Eseguire il mirroring degli aggregati root per Node_A_2-IP e Node_B_2-IP:

```
aggregate mirror -aggregate root-aggr
```

10. Verificare che la risincronizzazione dell'aggregato sia stata completata per gli aggregati root e di dati:

```
aggr show``aggr plex show
```

La risincronizzazione può richiedere del tempo, ma deve essere completata prima di procedere con le seguenti operazioni.

11. Aggiornare la configurazione MetroCluster per incorporare i nuovi nodi:
    a. Accedere alla modalità avanzata dei privilegi e digitare y quando richiesto per continuare:

    ```
    set priv advanced
    ```

    b. Aggiornare la configurazione:

Se è stato configurato…	Eseguire questo comando…
Un singolo aggregato in ciascun cluster:	`metrocluster configure -refresh true -allow-with-one-aggregate true`

Più di un singolo aggregato in ciascun cluster	`metrocluster configure -refresh true`

c. Tornare alla modalità admin:

```
set priv admin
```

12. Disattivare la modalità di transizione MetroCluster:
    a. Immettere Advanced Privilege mode e digitare “y” quando viene richiesto di continuare:

    ```
    set priv advanced
    ```

    b. Disattivare la modalità di transizione:

    ```
    metrocluster transition disable
    ```

    c. Tornare alla modalità admin:

    ```
    set priv admin
    ```

Impostazione di LIF dei dati sui nuovi nodi

È necessario configurare le LIF dei dati sui nuovi nodi, Node_A_2-IP e Node_B_2-IP.

Se non è già stata assegnata a un dominio di trasmissione, è necessario aggiungere nuove porte disponibili sui nuovi controller. Se necessario, creare VLAN o gruppi di interfacce sulle nuove porte. Vedere "Gestione della rete"

1. Identificare l’utilizzo corrente delle porte e i domini di trasmissione:

   ```
   network port show``network port broadcast-domain show
   ```

2. Aggiungere porte a domini di trasmissione e VLAN secondo necessità.
   a. Visualizzare gli spazi IP:

   ```
   network ipspace show
   ```

   b. Creare spazi IP e assegnare le porte dati in base alle esigenze.

   "Configurazione di IPspaces (solo amministratori del cluster)"

   c. Visualizzare i domini di trasmissione:

   ```
   network port broadcast-domain show
   ```

   d. Aggiungere eventuali porte dati a un dominio di broadcast in base alle esigenze.

   "Aggiunta o rimozione di porte da un dominio di broadcast"

   e. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

   L’appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo

precedente.

"Creazione di una VLAN"

"Combinazione di porte fisiche per creare gruppi di interfacce"

3. Verificare che le LIF siano ospitate sul nodo appropriato e sulle porte sui nodi IP di MetroCluster (inclusa la SVM con vserver -mc) secondo necessità.

   Consultare le informazioni raccolte in "Creazione della configurazione di rete".

   a. Controllare la porta home dei file LIF:

      ```
      network interface show -field home-port
      ```

   b. Se necessario, modificare la configurazione LIF:

      ```
      vserver config override -command "network interface modify -vserver
      vserver_name -home-port active_port_after_upgrade -lif lif_name -home- node
      new_node_name"
      ```

   c. Ripristinare le LIF alle porte home:

      ```
      network interface revert * -vserver vserver_name
      ```

Creazione delle SVM

A causa delle modifiche apportate alla configurazione LIF, è necessario riavviare le SVM sui nuovi nodi.

Fasi

1. Controllare lo stato delle SVM:

   ```
   metrocluster vserver show
   ```

2. Riavviare le SVM sul cluster_A che non hanno un suffisso “-mc”:

   ```
   vserver start -vserver svm-name -force true
   ```

3. Ripetere i passaggi precedenti sul cluster partner.
4. Verificare che tutte le SVM siano in buono stato:

   ```
   metrocluster vserver show
   ```

5. Verificare che tutti i dati LIF siano online:

   ```
   network interface show
   ```

Spostamento di un volume di sistema nei nuovi nodi

Per migliorare la resilienza, è necessario spostare un volume di sistema dal nodo controller_A_1-IP al nodo controller_A_2-IP e dal nodo_B_1-IP al nodo_B_2-IP. È necessario creare un aggregato mirrorato sul nodo di destinazione per il volume di sistema.

A proposito di questa attività

I volumi di sistema hanno il nome “MDV_CRS_*`*A” o “MDV_CRS** B." Le designazioni "`*A” e “_B” non sono correlate ai riferimenti del sito_A e del sito_B utilizzati in questa sezione; ad esempio, MDV_CRS**_A non è associato al sito_A.

Fasi

1. Assegnare almeno tre dischi pool 0 e tre dischi pool 1 ciascuno per i controller Node_A_2-IP e Node_B_2-IP secondo necessità.
2. Abilitare l’assegnazione automatica del disco.
3. Spostare il volume di sistema _B da Node_A_1-IP a Node_A_2-IP seguendo la procedura descritta di seguito da Site_A.

   a. Creare un aggregato mirrorato su controller node_A_2-IP per contenere il volume di sistema:

   ```
   aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node
   nodename_node_A_2-IP
   ```

   ```
   aggr show
   ```

   L’aggregato mirrorato richiede cinque dischi di riserva pool 0 e cinque pool 1 di proprietà del controller Node_A_2-IP.

   L’opzione avanzata “-force-Small-aggregate true” può essere utilizzata per limitare l’utilizzo del disco a 3 pool 0 e 3 pool 1 di dischi, se i dischi sono in quantità limitata.

   b. Elencare i volumi di sistema associati alla SVM amministrativa:

   ```
   vserver show
   ```

   ```
   volume show -vserver admin-vserver-name
   ```

   È necessario identificare i volumi contenuti negli aggregati di proprietà di Site_A. Vengono visualizzati anche i volumi di sistema Site_B.

4. Spostare il volume di sistema MDV_CRS_*_B per il sito_A nell’aggregato mirrorato creato sul nodo controller_A_2-IP

   a. Verificare la presenza di eventuali aggregati di destinazione:

   ```
   volume move target-aggr show -vserver admin-vserver-name -volume
   system_vol_MDV_B
   ```

   L’aggregato appena creato su Node_A_2-IP dovrebbe essere elencato.

   b. Spostare il volume nell’aggregato appena creato su Node_A_2-IP:

   ```
   set advanced
   ```

   ```
   volume move start -vserver admin-vserver -volume system_vol_MDV_B
   -destination-aggregate new_node_A_2-IP_aggr -cutover-window 40
   ```

   c. Controllare lo stato dell’operazione di spostamento:

```
volume move show -vserver admin-vserver-name -volume system_vol_MDV_B
```

d. Una volta completata l'operazione di spostamento, verificare che il sistema MDV_CRS_*_B sia contenuto nel nuovo aggregato sul nodo_A_2-IP:

```
set admin
```

```
volume show -vserver admin-vserver
```

5. Ripetere i passaggi precedenti su Site_B (Node_B_1-IP e Node_B_2-IP).

Ripristino del normale funzionamento del sistema

È necessario eseguire le fasi finali della configurazione e ripristinare il normale funzionamento della configurazione MetroCluster.

Verifica del funzionamento di MetroCluster e assegnazione dei dischi dopo la transizione

Verificare che MetroCluster funzioni correttamente e assegnare le unità alla seconda coppia di nuovi nodi (Node_A_2-IP e Node_B_2-IP).

1. Verificare che il tipo di configurazione MetroCluster sia IP-fabric: `metrocluster show`
2. Eseguire un controllo MetroCluster.
   a. Immettere il seguente comando: `metrocluster check run`
   b. Visualizzare i risultati del controllo MetroCluster: `metrocluster check show`
3. Verificare che il gruppo DR con i nodi IP MetroCluster sia configurato: `metrocluster node show`
4. Creare e eseguire il mirroring di aggregati di dati aggiuntivi per i controller Node_A_2-IP e Node_B_2-IP in ogni sito, in base alle necessità.

Installazione delle licenze per il nuovo modulo controller

È necessario aggiungere le licenze per il nuovo modulo controller per tutti i servizi ONTAP che richiedono licenze standard (con blocco a nodo). Per le funzionalità con licenze standard, ogni nodo del cluster deve disporre di una propria chiave per la funzionalità.

Per informazioni dettagliate sulle licenze, consultare l'articolo della Knowledge base 3013749: Panoramica e riferimenti sulle licenze di Data ONTAP 8.2 sul sito di supporto NetApp e il documento *riferimento per l'amministrazione del sistema*.

1. Se necessario, procurarsi le chiavi di licenza per il nuovo nodo sul sito di supporto NetApp nella sezione My Support (supporto personale) sotto Software licenss (licenze software).

   Per ulteriori informazioni sulle sostituzioni delle licenze, consultare l'articolo della Knowledge base "Processo di sostituzione della scheda madre per aggiornare le licenze su un sistema AFF/FAS."

2. Immettere il seguente comando per installare ogni chiave di licenza: `system license add -license -code license_key`

   License_key ha una lunghezza di 28 cifre.

   Ripetere questo passaggio per ogni licenza standard richiesta (bloccata da nodo).

Completamento della configurazione dei nodi

Prima di completare le procedure, è possibile eseguire varie fasi di configurazione. Alcuni di questi passaggi sono facoltativi.

1. Configurare il processore di servizio: `system service-processor network modify`
2. Impostare AutoSupport sui nuovi nodi: `system node autosupport modify`
3. I controller possono essere rinominati come parte della transizione. Il seguente comando viene utilizzato per rinominare un controller: `system node rename -node <old-name> -newname <new-name>`

   Il completamento dell'operazione di ridenominazione può richiedere alcuni minuti. Verificare che le modifiche al nome siano state propagate a ciascun nodo prima di continuare con altre operazioni utilizzando il comando di sistema show -fields node.

4. Configurare un servizio di monitoraggio come desiderato.

   "Considerazioni per Mediator"

   xref:../transition/../install-ip/concept_mediator_requirements.html

   "Installazione e configurazione del software Tiebreaker"

Invio di un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completata la transizione, devi inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.
   a. Immettere il seguente comando: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Ripetere il comando sul cluster partner.

Transizione senza interruzioni da MetroCluster FC a MetroCluster IP quando si ritirano gli shelf di storage (ONTAP 9.8 e versioni successive)

A partire da ONTAP 9.8, è possibile passare in modo disgregante da una configurazione MetroCluster FC a due nodi a una configurazione MetroCluster IP a quattro nodi e dismettere gli shelf di storage esistenti. La procedura include passaggi per spostare i dati dagli shelf di dischi esistenti alla nuova configurazione e poi ritirare i vecchi shelf.

- Questa procedura viene utilizzata quando si prevede di dismettere gli shelf di storage esistenti e spostare tutti i dati nei nuovi shelf nella configurazione IP di MetroCluster.
- I modelli di shelf di storage esistenti devono essere supportati dai nuovi nodi IP MetroCluster.
- Questa procedura è supportata nei sistemi che eseguono ONTAP 9.8 e versioni successive.
- Questa procedura ha un'interruzione.

- Questa procedura si applica solo a una configurazione MetroCluster FC a due nodi.

  Se si dispone di una configurazione MetroCluster FC a quattro nodi, vedere "Scelta della procedura di transizione".

- È necessario soddisfare tutti i requisiti e seguire tutte le fasi della procedura.

Requisiti per la transizione quando si ritirano i vecchi shelf

Prima di iniziare il processo di transizione, è necessario assicurarsi che la configurazione MetroCluster FC esistente soddisfi i requisiti.

- Deve essere una configurazione Fabric-Attached a due nodi o Stretch MetroCluster e tutti i nodi devono eseguire ONTAP 9.8 o versione successiva.

  I nuovi moduli controller IP MetroCluster devono eseguire la stessa versione di ONTAP 9.8.

- Le piattaforme esistenti e nuove devono essere una combinazione supportata per la transizione.

  "Piattaforme supportate per una transizione senza interruzioni"

- Deve soddisfare tutti i requisiti e i cavi descritti nelle *Guide di installazione e configurazione di MetroCluster*.

  "Installazione e configurazione di Fabric-Attached MetroCluster"

La nuova configurazione deve inoltre soddisfare i seguenti requisiti:

- I nuovi modelli di piattaforma MetroCluster IP devono supportare i vecchi modelli di shelf storage.

  "NetApp Hardware Universe"

- A seconda dei dischi spare disponibili negli shelf esistenti, è necessario aggiungere ulteriori dischi.

  Questo potrebbe richiedere ulteriori shelf di dischi.

  È necessario disporre di ulteriori 14 - 18 unità per ciascun controller:

  - Tre dischi pool 0
  - Tre dischi pool 1
  - Due dischi di riserva
  - Da sei a dieci dischi per il volume di sistema

- È necessario assicurarsi che la configurazione, inclusi i nuovi nodi, non superi i limiti della piattaforma per la configurazione, inclusi il numero di dischi, la capacità delle dimensioni dell'aggregato root e così via

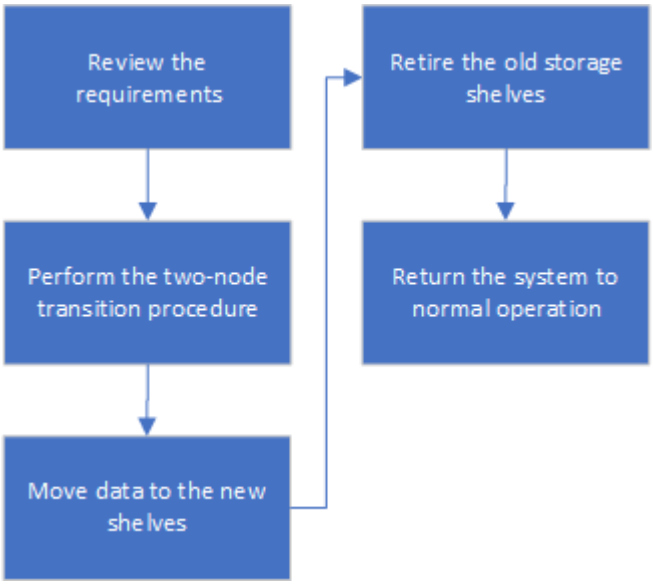
  Queste informazioni sono disponibili per ciascun modello di piattaforma all'indirizzo "NetApp Hardware Universe"

È necessario disporre dell'accesso remoto alla console per tutti e sei i nodi dal sito MetroCluster o pianificare il trasferimento tra i siti come richiesto dalla procedura.

Workflow per una transizione senza interruzioni durante lo spostamento dei dati e il ritiro dei vecchi shelf di storage

Devi seguire il workflow specifico per garantire una transizione di successo.

Mentre ti prepari per la transizione, pianifica i viaggi tra i siti. Tenere presente che, dopo aver eseguito il racking e il cablaggio dei nodi remoti, è necessario accedere al terminale seriale per i nodi. L'accesso al Service Processor non sarà disponibile fino a quando i nodi non saranno configurati.



Transizione della configurazione

Seguire la procedura di transizione dettagliata.

A proposito di questa attività

Nelle fasi seguenti, si viene indirizzati ad altre procedure. È necessario eseguire i passaggi di ciascuna procedura di riferimento nell'ordine indicato.

Fasi

1. Pianificare la mappatura delle porte utilizzando i passaggi descritti in "Mappatura delle porte dai nodi FC MetroCluster ai nodi IP MetroCluster".
2. Preparare i controller IP MetroCluster seguendo la procedura descritta in "Preparazione dei controller IP MetroCluster".
3. Verificare lo stato della configurazione MetroCluster FC.

   Eseguire le operazioni descritte in "Verifica dello stato della configurazione MetroCluster FC".

4. Raccogliere informazioni dalla configurazione MetroCluster FC.

   Eseguire le operazioni descritte in "Raccolta di informazioni dai moduli controller esistenti prima della transizione".

5. Rimuovere il monitoraggio di spareggio, se necessario.

   Eseguire le operazioni descritte in "Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio".

6. Preparare e rimuovere i nodi FC MetroCluster esistenti.

   Eseguire le operazioni descritte in "Transizione dei nodi FC MetroCluster".

7. Collegare i nuovi nodi IP MetroCluster.

   Eseguire le operazioni descritte in "Collegamento dei moduli del controller IP MetroCluster".

8. Configurare i nuovi nodi IP MetroCluster e completare la transizione.

   Eseguire le operazioni descritte in "Configurazione dei nuovi nodi e completamento della transizione".

Migrazione degli aggregati root

Una volta completata la transizione, migrare gli aggregati root esistenti rimanenti dalla configurazione MetroCluster FC ai nuovi shelf nella configurazione MetroCluster IP.

A proposito di questa attività

Questa attività sposta gli aggregati root per Node_A_1-FC e Node_B_1-FC negli shelf di dischi di proprietà dei nuovi controller IP MetroCluster:

Fasi

1. Assegnare il pool di dischi 0 sul nuovo shelf di storage locale al controller che ha la radice migrata (ad esempio, se la radice del nodo_A_1-FC viene migrata, assegnare il pool di dischi 0 sul nuovo shelf al nodo_A_1-IP)

   Si noti che la migrazione *rimuove e non crea di nuovo il mirror root*, pertanto non è necessario assegnare i dischi del pool 1 prima di inviare il comando di migrazione

2. Impostare la modalità dei privilegi su Advanced (avanzata):

   ```
   set priv advanced
   ```

3. Migrare l'aggregato root:

   ```
   system node migrate-root -node node-name -disklist disk-id1,disk-id2,diskn
   -raid-type raid-type
   ```

   - Il nome del nodo è il nodo in cui viene migrato l'aggregato root.
   - L'id disco identifica il pool 0 dischi sul nuovo shelf.
   - il tipo raid è normalmente lo stesso del tipo raid dell'aggregato root esistente.
   - È possibile utilizzare il comando `job show -idjob-id-instance` per controllare lo stato della migrazione, dove id lavoro è il valore fornito quando viene emesso il comando migrate-root.

     Ad esempio, se l'aggregato root per Node_A_1-FC consisteva in tre dischi con raid_dp, per migrare root in un nuovo shelf 11 viene utilizzato il seguente comando:

   ```
   system node migrate-root -node node_A_1-IP -disklist
   3.11.0,3.11.1,3.11.2 -raid-type raid_dp
   ```

4. Attendere il completamento dell'operazione di migrazione e il riavvio automatico del nodo.
5. Assegnare i dischi del pool 1 per l'aggregato root su un nuovo shelf direttamente connesso al cluster remoto.
6. Eseguire il mirroring dell'aggregato root migrato.
7. Attendere che l'aggregato root completi la risincronizzazione.

   È possibile utilizzare il comando show dell'aggregato di storage per controllare lo stato di sincronizzazione degli aggregati.

8. Ripetere questi passaggi per l'altro aggregato root.

Migrazione degli aggregati di dati

Crea aggregati di dati sui nuovi shelf e utilizza lo spostamento dei volumi per trasferire i volumi di dati dai vecchi shelf agli aggregati dei nuovi shelf.

1. Spostare i volumi di dati in aggregati sui nuovi controller, un volume alla volta.

   "Creazione di un aggregato e spostamento dei volumi nei nuovi nodi"

Shelf ritirati spostati da Node_A_1-FC e Node_A_2-FC

I vecchi shelf di storage vengono ritirati dalla configurazione FC originale di MetroCluster. Questi shelf erano originariamente di proprietà di Node_A_1-FC e Node_A_2-FC.

1. Identificare gli aggregati sui vecchi shelf sul cluster_B che devono essere cancellati.

   In questo esempio, i seguenti aggregati di dati sono ospitati dal cluster MetroCluster FC_B e devono essere cancellati: aggr_data_a1 e aggr_data_a2.

   > È necessario eseguire i passaggi per identificare, offline ed eliminare gli aggregati di dati sugli shelf. L'esempio riguarda un solo cluster.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-IP
raid_dp,

mirrored,

normal
aggr0_node_A_2-IP
           349.0GB   16.83GB   95% online       1 node_A_2-IP
raid_dp,

mirrored,

normal
...
8 entries were displayed.

cluster_B::>
```

2. Controllare se gli aggregati di dati hanno volumi MDV_aud ed eliminarli prima di eliminare gli aggregati.

   È necessario eliminare i volumi MDV_aud in quanto non possono essere spostati.

3. Portare tutti gli aggregati offline, quindi eliminarli:

   a. Portare l'aggregato offline:

      ```
      storage aggregate offline -aggregate aggregate-name
      ```

      L'esempio seguente mostra che il nodo aggregato_B_1_aggr0 è stato portato offline:

      ```
      cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

      Aggregate offline successful on aggregate: node_B_1_aggr0
      ```

   b. Eliminare l'aggregato:

      ```
      storage aggregate delete -aggregate aggregate-name
      ```

      Quando richiesto, è possibile distruggere il plex.

Nell'esempio seguente viene illustrato il nodo aggregato B_1_aggr0 che viene cancellato.

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. Dopo aver eliminato tutti gli aggregati, spegnere, scollegare e rimuovere gli shelf.
5. Ripetere i passaggi precedenti per dismettere gli shelf cluster_A.

Completamento della transizione

Dopo aver rimosso i vecchi moduli controller, è possibile completare il processo di transizione.

Fase

1. Completare il processo di transizione.

   Eseguire le operazioni descritte in "Ripristino del normale funzionamento del sistema".

Transizione disgregativa quando gli shelf esistenti non sono supportati sui nuovi controller (ONTAP 9.8 e versioni successive)

A partire da ONTAP 9.8, è possibile eseguire la transizione di una configurazione MetroCluster FC a due nodi e spostare i dati dagli shelf di dischi esistenti anche se gli shelf di storage esistenti non sono supportati dai nuovi nodi MetroCluster IP.

- Questa procedura deve essere utilizzata solo se i modelli di shelf di storage esistenti non sono supportati dai nuovi modelli di piattaforma IP di MetroCluster.
- Questa procedura è supportata nei sistemi che eseguono ONTAP 9.8 e versioni successive.
- Questa procedura ha un'interruzione.
- Questa procedura si applica solo a una configurazione MetroCluster FC a due nodi.

  Se si dispone di una configurazione MetroCluster FC a quattro nodi, vedere "Scelta della procedura di transizione".

- È necessario soddisfare tutti i requisiti e seguire tutte le fasi della procedura.

Requisiti per la transizione quando gli shelf non sono supportati sui nuovi nodi

Prima di avviare il processo di transizione, è necessario assicurarsi che la configurazione soddisfi i requisiti.

Prima di iniziare

- La configurazione esistente deve essere una configurazione Fabric-Attached a due nodi o Stretch MetroCluster e tutti i nodi devono eseguire ONTAP 9.8 o versione successiva.

I nuovi moduli controller IP MetroCluster devono eseguire la stessa versione di ONTAP 9.8.

- Le piattaforme esistenti e nuove devono essere una combinazione supportata per la transizione.

  "Piattaforme supportate per una transizione senza interruzioni"

- Deve soddisfare tutti i requisiti e i cavi descritti in "Installazione e configurazione di Fabric-Attached MetroCluster".
- I nuovi shelf di storage forniti con i nuovi controller (Node_A_1-IP, Node_A_2-IP, Node_B_1-IP e Node_B_2-IP) devono essere supportati dai vecchi controller (Node_A_1-FC e Node_B_1-FC).

  "NetApp Hardware Universe"

- I vecchi shelf di storage **non** sono supportati dai nuovi modelli di piattaforma IP di MetroCluster.

  "NetApp Hardware Universe"

- A seconda dei dischi spare disponibili negli shelf esistenti, è necessario aggiungere ulteriori dischi.

  Questo potrebbe richiedere ulteriori shelf di dischi.

  È necessario disporre di ulteriori 14 - 18 unità per ciascun controller:

  - Tre pool0 dischi
  - Tre unità pool1
  - Due dischi di riserva
  - Da sei a dieci dischi per il volume di sistema
- È necessario assicurarsi che la configurazione, inclusi i nuovi nodi, non superi i limiti della piattaforma per la configurazione, inclusi il numero di dischi, la capacità delle dimensioni dell'aggregato root e così via

  Queste informazioni sono disponibili per ciascun modello di piattaforma all'indirizzo *NetApp Hardware Universe*.

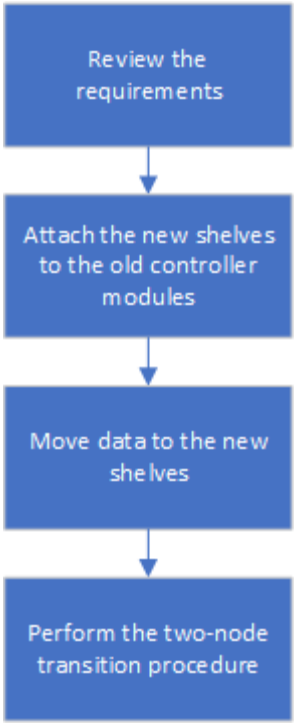
  "NetApp Hardware Universe"

- È necessario disporre dell'accesso remoto alla console per tutti e sei i nodi dal sito MetroCluster o pianificare il trasferimento tra i siti come richiesto dalla procedura.

Workflow per una transizione senza interruzioni quando gli shelf non sono supportati dai nuovi controller

Se i modelli di shelf esistenti non sono supportati dai nuovi modelli di piattaforma, è necessario collegare i nuovi shelf alla vecchia configurazione, spostare i dati sui nuovi shelf e passare alla nuova configurazione.

Mentre ti prepari per la transizione, pianifica i viaggi tra i siti. Tenere presente che, dopo aver eseguito il racking e il cablaggio dei nodi remoti, è necessario accedere al terminale seriale per i nodi. L'accesso al Service Processor non sarà disponibile fino a quando i nodi non saranno configurati.



Preparazione dei nuovi moduli controller

È necessario cancellare la configurazione e la proprietà del disco sui nuovi moduli controller e sui nuovi shelf di storage.

Fasi

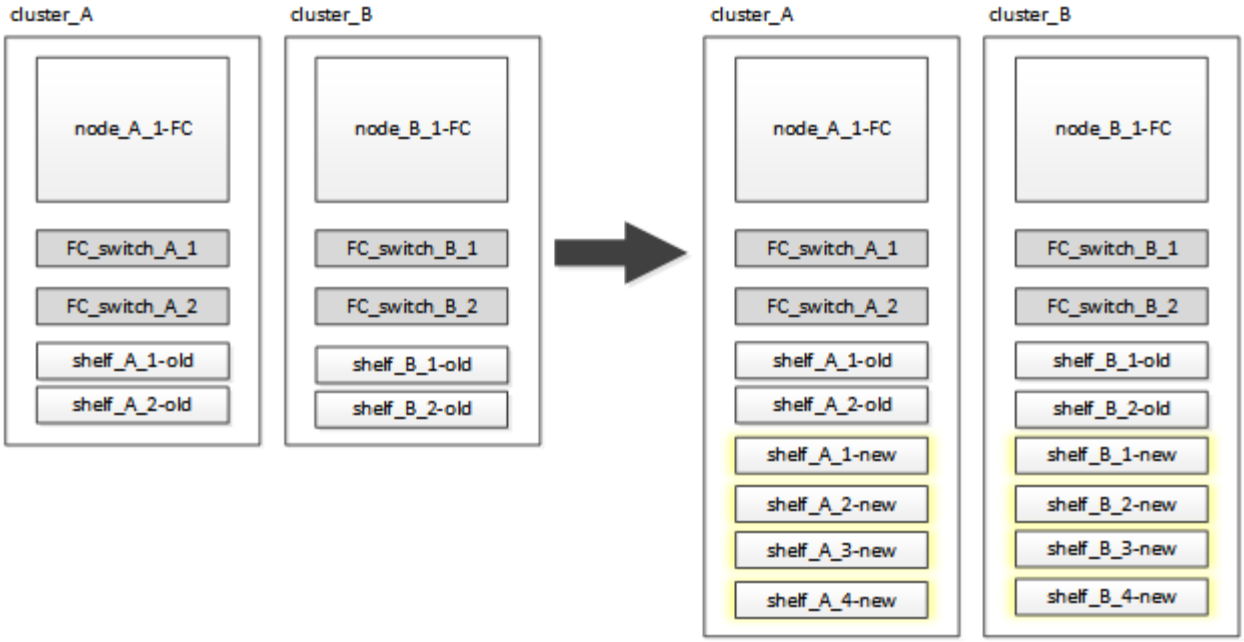
1. Con i nuovi shelf di storage collegati ai nuovi moduli controller IP MetroCluster, eseguire tutte le operazioni descritte in "Preparazione dei controller IP MetroCluster".
2. Scollegare i nuovi shelf di storage dai nuovi moduli controller IP MetroCluster.

Collegamento dei nuovi shelf di dischi ai controller FC MetroCluster esistenti

È necessario collegare i nuovi shelf di dischi ai moduli controller esistenti prima di passare a una configurazione MetroCluster IP.

A proposito di questa attività

La figura seguente mostra i nuovi shelf collegati alla configurazione MetroCluster FC.



Fasi

1. Disattiva l'assegnazione automatica dei dischi su Node_A_1-FC e Node_A_2-FC:

   ```
   disk option modify -node node-name -autoassign off
   ```

   Questo comando deve essere emesso su ciascun nodo.

   L'assegnazione automatica del disco è disattivata per evitare l'assegnazione degli shelf da aggiungere a Node_A_1-FC e Node_B_1-FC. Come parte della transizione, i dischi sono necessari per i nodi Node_A_1-IP e Node_B_2-IP e, se è consentita l'assegnazione automatica, la proprietà del disco deve essere rimossa in seguito prima che i dischi possano essere assegnati a Node_A_1-IP e Node_B_2-IP.

2. Collegare i nuovi shelf ai nodi FC MetroCluster esistenti, utilizzando bridge FC-SAS, se necessario.

   Consultare i requisiti e le procedure in "Aggiunta a caldo di storage a una configurazione MetroCluster FC"

Migrare gli aggregati root e spostare i dati nei nuovi shelf di dischi

È necessario spostare gli aggregati root dai vecchi shelf di dischi ai nuovi shelf di dischi che verranno utilizzati dai nodi IP di MetroCluster.

A proposito di questa attività

Questa attività viene eseguita prima della transizione sui nodi esistenti (Node_A_1-FC e Node_B_1-FC).

Fasi

1. Eseguire uno switchover negoziato dal nodo controller_B_1-FC:

   ```
   metrocluster switchover
   ```

2. Eseguire le operazioni di correzione degli aggregati e di correzione delle fasi principali del ripristino da Node_B_1-FC:

   ```
   metrocluster heal -phase aggregates
   ```

```
metrocluster heal -phase root-aggregates
```

3. Boot controller node_A_1-FC:

```
boot_ontap
```

4. Assegnare i dischi non proprietari sui nuovi shelf ai pool appropriati per il nodo controller_A_1-FC:

   a. Identificare i dischi sugli shelf:

   ```
   disk show -shelf pool_0_shelf -fields container-type,diskpathnames
   ```

   ```
   disk show -shelf pool_1_shelf -fields container-type,diskpathnames
   ```

   b. Accedere alla modalità locale in modo che i comandi vengano eseguiti sul nodo locale:

   ```
   run local
   ```

   c. Assegnare i dischi:

   ```
   disk assign disk1disk2disk3disk… -p 0
   ```

```
disk assign disk4disk5disk6disk… -p 1
```

   a. Uscire dalla modalità locale:

   ```
   exit
   ```

5. Creare un nuovo aggregato mirrorato per diventare il nuovo aggregato root per controller node_A_1-FC:

   a. Impostare la modalità dei privilegi su Advanced (avanzata):

   ```
   set priv advanced
   ```

   b. Creare l'aggregato:

   ```
   aggregate create -aggregate new_aggr -disklist disk1, disk2, disk3,… -mirror
   -disklist disk4disk5, disk6,… -raidtypesame-as-existing-root -force-small
   -aggregate true aggr show -aggregate new_aggr -fields percent-snapshot-space
   ```

   Se il valore percentuale-spazio-snapshot è inferiore al 5%, è necessario aumentarlo fino a un valore superiore al 5%:

```
aggr modify new_aggr -percent-snapshot-space 5
```

   a. Impostare nuovamente la modalità privilegio su admin:

   ```
   set priv admin
   ```

6. Verificare che il nuovo aggregato sia stato creato correttamente:

```
node run -node local sysconfig -r
```

7. Creare i backup della configurazione a livello di nodo e cluster:

> Quando i backup vengono creati durante lo switchover, il cluster è consapevole dello stato di switchover al momento del recovery. È necessario assicurarsi che il backup e il caricamento della configurazione di sistema siano riusciti, in quanto senza questo backup è **impossibile** riformare la configurazione MetroCluster tra i cluster.

a. Creare il backup del cluster:

```
system configuration backup create -node local -backup-type cluster -backup
-name cluster-backup-name
```

b. Controllare la creazione del backup del cluster

```
job show -id job-idstatus
```

c. Creare il backup del nodo:

```
system configuration backup create -node local -backup-type node -backup
-name node-backup-name
```

d. Verificare la presenza di backup di cluster e nodi:

```
system configuration backup show
```

È possibile ripetere il comando fino a quando entrambi i backup non vengono visualizzati nell'output.

8. Eseguire copie dei backup.

   I backup devono essere memorizzati in una posizione separata perché andranno persi localmente all'avvio del nuovo volume root.

   È possibile caricare i backup su un server FTP o HTTP oppure copiarli utilizzando `scp` comandi.

Processo	Fasi

Caricare il backup sul server FTP o HTTP	a. Caricare il backup del cluster:
	`system configuration backup upload -node local -backup cluster-backup-name -destination URL`
	b. Caricare il backup del nodo:
	`system configuration backup upload -node local -backup node-backup-name -destination URL`

Copiare i backup su un server remoto utilizzando una copia sicura	Dal server remoto utilizzare i seguenti comandi SCP:
	
	a. Copia del backup del cluster:
	
	`scp diagnode-mgmt-FC:/mroot/etc/backups/config/cluster-backup-name.7z .`
	
	b. Copia del backup del nodo:
	
	`scp diag@node-mgmt-FC:/mroot/etc/backups/config/node-backup-name.7z .`

9. Nodo di arresto_A_1-FC:

   ```
   halt -node local -ignore-quorum-warnings true
   ```

10. Nodo di boot_A_1-FC in modalità manutenzione:

    ```
    boot_ontap maint
    ```

11. Dalla modalità Maintenance (manutenzione), apportare le modifiche necessarie per impostare l'aggregato come root:

    a. Impostare il criterio ha su cfo:

    ```
    aggr options new_aggr ha_policy cfo
    ```

    Rispondere "yes" quando viene richiesto di procedere.

    ```
    Are you sure you want to proceed (y/n)?
    ```

    a. Impostare il nuovo aggregato come root:

    ```
    aggr options new_aggr root
    ```

    b. Arrestare il PROMPT DEL CARICATORE:

    ```
    halt
    ```

12. Avviare il controller ed eseguire il backup della configurazione di sistema.

    Il nodo viene avviato in modalità di ripristino quando viene rilevato il nuovo volume root

    a. Avviare il controller:

    ```
    boot_ontap
    ```

    b. Accedere ed eseguire il backup della configurazione.

    Quando si effettua l'accesso, viene visualizzato il seguente avviso:

```
Warning: The correct cluster system configuration backup must be
restored. If a backup
from another cluster or another system state is used then the root
volume will need to be
recreated and NGS engaged for recovery assistance.
```

a. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

b. Eseguire il backup della configurazione del cluster su un server:

```
system configuration backup download -node local -source URL of
server/cluster-backup-name.7z
```

c. Eseguire il backup della configurazione del nodo su un server:

```
system configuration backup download -node local -source URL of server/node-
backup-name.7z
```

d. Tornare alla modalità admin:

```
set -privilege admin
```

13. Controllare lo stato del cluster:
    a. Immettere il seguente comando:

    ```
    cluster show
    ```

    b. Impostare la modalità dei privilegi su Advanced (avanzata):

    ```
    set -privilege advanced
    ```

    c. Verificare i dettagli della configurazione del cluster:

    ```
    cluster ring show
    ```

    d. Tornare al livello di privilegio admin:

    ```
    set -privilege admin
    ```

14. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
    a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

    ```
    metrocluster show
    ```

    b. Verificare che siano visualizzati tutti i nodi previsti:

    ```
    metrocluster node show
    ```

c. Immettere il seguente comando:

```
metrocluster check run
```

d. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

15. Eseguire uno switchback dal nodo controller_B_1-FC:

```
metrocluster switchback
```

16. Verificare il funzionamento della configurazione MetroCluster:
    a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

    ```
    metrocluster show
    ```

    b. Eseguire un controllo MetroCluster:

    ```
    metrocluster check run
    ```

    c. Visualizzare i risultati del controllo MetroCluster:

    ```
    metrocluster check show
    ```

17. Aggiungere il nuovo volume root al database delle posizioni dei volumi.
    a. Impostare la modalità dei privilegi su Advanced (avanzata):

    ```
    set -privilege advanced
    ```

    b. Aggiungere il volume al nodo:

    ```
    volume add-other-volumes –node node_A_1-FC
    ```

    c. Tornare al livello di privilegio admin:

    ```
    set -privilege admin
    ```

18. Verificare che il volume sia visibile e che sia presente mroot.
    a. Visualizzare gli aggregati:

    ```
    storage aggregate show
    ```

    b. Verificare che il volume root disponga di mroot:

    ```
    storage aggregate show -fields has-mroot
    ```

    c. Visualizzare i volumi:

    ```
    volume show
    ```

19. Creare un nuovo certificato di sicurezza per riattivare l’accesso a System Manager:

```
security certificate create -common-name name -type server -size 2048
```

20. Ripetere i passaggi precedenti per migrare gli aggregati sugli shelf di proprietà di Node_A_1-FC.
21. Eseguire una pulizia.

    Per rimuovere il vecchio volume root e l'aggregato root, è necessario eseguire le seguenti operazioni sia su Node_A_1-FC che su Node_B_1-FC.

    a. Eliminare il vecchio volume root:

    ```
    run local

    vol offline old_vol0

    vol destroy old_vol0

    exit

    volume remove-other-volume -vserver node_name -volume old_vol0
    ```

    b. Eliminare l'aggregato root originale:

    ```
    aggr offline -aggregate old_aggr0_site
    ```

    ```
    aggr delete -aggregate old_aggr0_site
    ```

22. Migrare i volumi di dati in aggregati sui nuovi controller, un volume alla volta.

    Fare riferimento a. "Creazione di un aggregato e spostamento dei volumi nei nuovi nodi"

23. Dismettere i vecchi shelf eseguendo tutte le operazioni descritte in "Shelf ritirati spostati da Node_A_1-FC e Node_A_2-FC".

Transizione della configurazione

Seguire la procedura di transizione dettagliata.

A proposito di questa attività

Nei seguenti passaggi, viene descritto come affrontare altri argomenti. È necessario eseguire i passaggi di ciascun argomento nell'ordine indicato.

Fasi

1. Pianificare la mappatura delle porte.

   Eseguire tutte le operazioni descritte in "Mappatura delle porte dai nodi FC MetroCluster ai nodi IP MetroCluster".

2. Preparare i controller IP MetroCluster.

   Eseguire tutte le operazioni descritte in "Preparazione dei controller IP MetroCluster".

3. Verificare lo stato della configurazione MetroCluster.

   Eseguire tutte le operazioni descritte in "Verifica dello stato della configurazione MetroCluster FC".

4. Preparare e rimuovere i nodi FC MetroCluster esistenti.

   Eseguire tutte le operazioni descritte in "Transizione dei nodi FC MetroCluster".

5. Aggiungere i nuovi nodi IP MetroCluster.

   Eseguire tutte le operazioni descritte in "Collegamento dei moduli del controller IP MetroCluster".

6. Completare la transizione e la configurazione iniziale dei nuovi nodi IP MetroCluster.

   Eseguire tutte le operazioni descritte in "Configurazione dei nuovi nodi e completamento della transizione".

Spostamento di un carico di lavoro SAN FC da MetroCluster FC a nodi IP MetroCluster

Durante la transizione senza interruzioni da MetroCluster FC a nodi IP, è necessario spostare senza interruzioni gli oggetti host FC SAN da MetroCluster FC a nodi IP.

1. Impostare nuove interfacce FC (LIFS) sui nodi IP MetroCluster:
   a. Se necessario, sui nodi IP MetroCluster, modificare le porte FC da utilizzare per la connettività del client al linguaggio di destinazione FC.

      Potrebbe essere necessario riavviare i nodi.

   b. Creazione di interfacce FC LIFS/su nodi IP per tutte le SVM SAN. In alternativa, verificare che i WWPN delle LIF FC appena create siano registrati nello switch FC SAN
2. Aggiornare la configurazione dello zoning SAN per le nuove LIF FC aggiunte sui nodi IP MetroCluster.

   Per facilitare lo spostamento di volumi che contengono LUN che forniscono attivamente i dati ai client FC SAN, aggiornare le zone switch FC esistenti per consentire ai client FC SAN di accedere alle LUN sui nodi IP MetroCluster.

   a. Sullo switch FC SAN (Cisco o Brocade), aggiungere alla zona le WWPN delle nuove LIF FC SAN aggiunte.
   b. Aggiornare, salvare e confermare le modifiche di zoning.
   c. Dal client, verificare la presenza di accessi FC Initiator alle nuove LIF SAN sui nodi IP MetroCluster: `sanlun lun show -p`

      A questo punto, il client dovrebbe visualizzare ed essere connesso alle interfacce FC su entrambi i nodi MetroCluster FC e MetroCluster IP. LUN e volumi sono ancora fisicamente ospitati sui nodi FC MetroCluster.

      Poiché i LUN sono riportati solo sulle interfacce dei nodi FC MetroCluster, il client mostra solo i percorsi sui nodi FC. Ciò è visibile nell'output di `sanlun lun show -p` e. `multipath -ll -d` comandi.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

3. Modificare i nodi di reporting per aggiungere i nodi IP MetroCluster

   a. Elencare i nodi di reporting per LUN su SVM: `lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux`

      I nodi di reporting mostrati sono nodi locali in quanto i LUN sono fisicamente presenti sui nodi FC A_1 e A_2.

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                          igroup         reporting-nodes
-------  --------------------------- ------------
-------------------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol1/lun_linux_3 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol2/lun_linux_4 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol3/lun_linux_7 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_8 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_9 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_12 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_13 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol7/lun_linux_14 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol8/lun_linux_17 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_18 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_19 igroup_linux  A_1,A_2
12 entries were displayed.
```

b. Aggiungere nodi di reporting per includere nodi IP MetroCluster.

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes B_1,B_2 -igroup igroup_linux

12 entries were acted on.
```

c. Elencare i nodi di reporting e verificare la presenza dei nuovi nodi:

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                           igroup          reporting-nodes
------- ---------------------------    ------------
-----------------------------------------------------------------------
----------

vsa_1   /vol/vsa_1_vol1/lun_linux_2   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol1/lun_linux_3   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol2/lun_linux_4   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol3/lun_linux_7   igroup_linux    A_1,A_2,B_1,B_2
...

12 entries were displayed.
```

d. Verificare che il `sg3-utils` Il pacchetto è installato sull'host Linux. In questo modo si evita un `rescan-scsi-bus.sh utility not found` Errore quando si esegue nuovamente la scansione dell'host Linux per i LUN appena mappati utilizzando `rescan-scsi-bus` comando.

e. Eseguire nuovamente la scansione del bus SCSI sull'host per rilevare i percorsi appena aggiunti: `/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

f. Visualizzare i percorsi aggiunti di recente: `sanlun lun show -p`

   Ogni LUN avrà quattro percorsi.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a0980383046465 13f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

g. Sui controller, spostare i volumi contenenti LUN dal MetroCluster FC ai nodi MetroCluster IP.

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver    Volume    State    Move Phase   Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------   ----------------
----------------
vsa_1     vsa_1_vol1 healthy  initializing
 - -
```

h. Sul client FC SAN, visualizzare le informazioni del LUN: `sanlun lun show -p`

Le interfacce FC sui nodi IP MetroCluster in cui risiede il LUN vengono aggiornate come percorsi primari. Se il percorso primario non viene aggiornato dopo lo spostamento del volume, eseguire /usr/bin/rescan-scsi-bus.sh -a o semplicemente attendere che venga eseguita una nuova scansione su più percorsi.

Il percorso primario nell'esempio seguente è il LIF sul nodo IP MetroCluster.

```
[root@localhost ~]# sanlun lun show -p

                    ONTAP Path: vsa_1:/vol/vsa_1_vol1/lun_linux_2
                           LUN: 22
                      LUN Size: 2g
                       Product: cDOT
                   Host Device: 3600a098038302d324e5d50305063546e
              Multipath Policy: service-time 0
            Multipath Provider: Native
--------- ---------- ------- ------------
-----------------------------------------------
host      vserver
path      path       /dev/   host         vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------
-----------------------------------------------
up        primary    sddv    host6        fc_5
up        primary    sdjx    host7        fc_6
up        secondary  sdgv    host6        fc_8
up        secondary  sdkr    host7        fc_8
```

a. Ripetere i passaggi precedenti per tutti i volumi, le LUN e le interfacce FC appartenenti a un host FC SAN.

   Una volta completata l'operazione, tutte le LUN di un determinato host SVM e FC SAN devono trovarsi su nodi IP MetroCluster.

4. Rimuovere i nodi di reporting e i percorsi di nuova scansione dal client.

   a. Rimuovere i nodi di reporting remoti (i nodi FC MetroCluster) per le LUN linux: `lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igroup_linux -remote -nodes true`

      ```
      cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
      * -igroup igroup_linux -remote-nodes true
      12 entries were acted on.
      ```

   b. Controllare i nodi di reporting per le LUN: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
------- --------------------------- ------------
----------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol2/lun_linux_4 igroup_linux B_1,B_2
...

12 entries were displayed.
```

c. Eseguire nuovamente la scansione del bus SCSI sul client: `/usr/bin/rescan-scsi-bus.sh -r`

   I percorsi dai nodi MetroCluster FC vengono rimossi:

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
...
```

a. Verificare che dall'host siano visibili solo i percorsi dei nodi IP MetroCluster: `sanlun lun show -p`

b. Se necessario, rimuovere le LIF iSCSI dai nodi FC MetroCluster.

Questa operazione deve essere eseguita se non sono presenti altre LUN sui nodi mappati ad altri client.

Spostare gli host iSCSI Linux da MetroCluster FC ai nodi IP MetroCluster

Dopo aver eseguito la transizione dei nodi MetroCluster da FC a IP, potrebbe essere necessario spostare le connessioni host iSCSI nei nuovi nodi.

A proposito di questa attività

- Le interfacce IPv4 vengono create quando si configurano le nuove connessioni iSCSI.
- I comandi host e gli esempi sono specifici per i sistemi operativi Linux.
- I nodi FC di MetroCluster sono detti vecchi nodi, mentre i nodi IP di MetroCluster sono detti nuovi nodi.

Fase 1: Configurare nuove connessioni iSCSI

Per spostare le connessioni iSCSI, è necessario impostare nuove connessioni iSCSI nei nuovi nodi.

Fasi

1. Creare interfacce iSCSI sui nuovi nodi e verificare la connettività ping dagli host iSCSI alle nuove interfacce sui nuovi nodi.

   "Creare interfacce di rete"

   Tutte le interfacce iSCSI della SVM devono essere raggiungibili dall'host iSCSI.

2. Sull'host iSCSI, identificare le connessioni iSCSI esistenti dall'host al nodo precedente:

   ```
   iscsiadm -m session
   ```

   ```
   [root@scspr1789621001 ~]# iscsiadm -m session
   tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
   08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
   ```

3. Sul nuovo nodo, verificare le connessioni dal nuovo nodo:

   ```
   iscsi session show -vserver <svm-name>
   ```

```
node_A_1-new::*> iscsi session show -vserver vsa_1
 Tpgroup Initiator Initiator
Vserver Name TSIH Name ISID Alias
--------- ------- ---- ------------------------ ---------
---------------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
scspr1789621001.gdl.englab.netapp.com
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
scspr1789621001.gdl.englab.netapp.com
2 entries were displayed.
```

4. Nel nuovo nodo elenca le interfacce iSCSI in ONTAP per la SVM che contiene le interfacce:

```
iscsi interface show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1
 Logical Status Curr Curr
Vserver Interface  TPGT Admin/Oper IP Address Node Port Enabled
------- ---------- ---- ---------- --------------- ----------- ----
-------
vsa_1 iscsi_lf__n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
true
vsa_1 iscsi_lf__n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
htp-001 e0h true
vsa_1 iscsi_lf__n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
true
vsa_1 iscsi_lf__n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
htp-002 e0h true
vsa_1 iscsi_lf__n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
true
vsa_1 iscsi_lf__n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
true
6 entries were displayed.
```

5. Sull’host iSCSI, eseguire il rilevamento su uno qualsiasi degli indirizzi IP iSCSI sulla SVM per rilevare le nuove destinazioni:

```
iscsiadm -m discovery -t sendtargets -p iscsi-ip-address
```

Il rilevamento può essere eseguito su qualsiasi indirizzo IP della SVM, incluse le interfacce non iSCSI.

```
[root@scspr1789621001 ~]# iscsiadm -m discovery -t sendtargets -p
10.230.68.236:3260
10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.134:3260,1183 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. Sull'host iSCSI, accedere a tutti gli indirizzi rilevati:

```
iscsiadm -m node -L all -T node-address -p portal-address -l
```

```
[root@scspr1789621001 ~]# iscsiadm -m node -L all -T iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p
10.230.68.236:3260 -l
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] (multiple)
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] (multiple)
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] successful.
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] successful.
```

7. Sull'host iSCSI, verificare l'accesso e le connessioni:

```
iscsiadm -m session
```

```
[root@scspr1789621001 ~]# iscsiadm -m session
tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. Sul nuovo nodo, verificare l'accesso e la connessione con l'host:

```
iscsi initiator show -vserver <svm-name>
```

```
sti8200mcchtp001htp_siteA::*> iscsi initiator show -vserver vsa_1
 Tpgroup Initiator
Vserver Name             TSIH Name                  ISID
Igroup Name
------- --------         ---- --------------------- -----------------
-----------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf__n3_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf__n4_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux
4 entries were displayed.
```

Risultato

Al termine di questa attività, l'host è in grado di visualizzare tutte le interfacce iSCSI (sui nodi vecchi e nuovi) ed è connesso a tutte queste interfacce.

I LUN e i volumi sono ancora fisicamente ospitati nei vecchi nodi. Poiché i LUN sono riportati solo sulle vecchie interfacce di nodo, l'host mostrerà solo i percorsi sui vecchi nodi. Per vedere questo, eseguire `sanlun lun show -p` e. `multipath -ll -d` comandi sull'host ed esaminare gli output dei comandi.

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ -------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ -------------------
up        primary    sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

Passaggio 2: Aggiungere i nuovi nodi come nodi di reporting

Dopo aver impostato le connessioni ai nuovi nodi, aggiungere i nuovi nodi come nodi di reporting.

Fasi

1. Nel nuovo nodo, elenca i nodi di reporting per le LUN sulla SVM:

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   I seguenti nodi di reporting sono nodi locali, mentre i LUN si trovano fisicamente sui vecchi nodi node_A_1-old e node_A_2-old.

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux
vserver path                          igroup       reporting-nodes
------- ----------------------------- ------------
---------------------------
vsa_1   /vol/vsa_1_vol1/lun_linux_2  igroup_linux node_A_1-old,node_A_2-
old
.
.
.
vsa_1   /vol/vsa_1_vol9/lun_linux_19 igroup_linux node_A_1-old,node_A_2-
old
12 entries were displayed.
```

2. Nel nuovo nodo, aggiungere i nodi di reporting:

```
lun mapping add-reporting-nodes -vserver <svm-name> -path
/vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup <igroup_name>
```

```
node_A_1-new::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-new,node_A_2-new
-igroup igroup_linux
12 entries were acted on.
```

3. Sul nuovo nodo, verificare che siano presenti i nodi appena aggiunti:

```
lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
linux vserver path igroup reporting-nodes
```

```
node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igroup reporting-nodes
------- -------------------------- ------------
---------------------------------------------------------------------------
-------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux node_A_1-old,node_A_2-
old,node_A_1-new,node_A_2-new
.
.
.
12 entries were displayed.
```

4. Il `sg3-utils` Il pacchetto deve essere installato sull'host Linux. Questo impedisce un `rescan-scsi-bus.sh utility not found` Errore quando si esegue nuovamente la scansione dell'host Linux per i LUN appena mappati utilizzando `rescan-scsi-bus` comando.

   Sull'host, verificare che `sg3-utils` il pacchetto è installato:

   - Per una distribuzione basata su Debian:

     ```
     dpkg -l | grep sg3-utils
     ```

   - Per una distribuzione basata su Red Hat:

     ```
     rpm -qa | grep sg3-utils
     ```

   Se necessario, installare `sg3-utils` Pacchetto sull'host Linux:

   ```
   sudo apt-get install sg3-utils
   ```

5. Sull'host, eseguire nuovamente la scansione del bus SCSI sull'host e scoprire i nuovi percorsi aggiunti:

   ```
   /usr/bin/rescan-scsi-bus.sh -a
   ```

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

6. Sull'host iSCSI, elencare i percorsi appena aggiunti:

```
sanlun lun show -p
```

Per ogni LUN vengono visualizzati quattro percorsi.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
------- ---------- ------- ----------- ---------------------
host vserver
path path /dev/ host vserver
state   type       node    adapter     LIF
------  ---------- ------- ----------- ---------------------
up      primary    sdk      host3      iscsi_lf__n2_p1_
up      secondary  sdh     host2       iscsi_lf__n1_p1_
up      secondary  sdag    host4       iscsi_lf__n4_p1_
up      secondary  sdah    host5       iscsi_lf__n3_p1_
```

7. Nel nuovo nodo spostare il volume/i volumi contenenti LUN dai nodi vecchi ai nuovi nodi.

```
node_A_1-new::*> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_vol1" command to view the status of this operation.
node_A_1-new::*> vol move show
Vserver  Volume      State       Move       Phase            Percent-
Complete  Time-To-Complete
-------- ----------  --------    ---------- ----------------
----------------  ----------------
vsa_1    vsa_1_vol1  healthy                initializing     -
-
```

8. Una volta completato lo spostamento del volume nei nuovi nodi, verificare che sia online:

```
volume show -state
```

9. Le interfacce iSCSI sui nuovi nodi in cui risiede la LUN vengono aggiornate come percorsi primari. Se il percorso primario non viene aggiornato dopo lo spostamento del volume, eseguire `/usr/bin/rescan-scsi-bus.sh -a` e. `multipath -v3` sull'host o attendere semplicemente che venga eseguita la ripetizione della scansione multipath.

   Nell'esempio seguente, il percorso primario è una LIF nel nuovo nodo.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ -----------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------------
up        primary    sdag    host4        iscsi_lf__n4_p1_
up        secondary  sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
up        secondary  sdah    host5        iscsi_lf__n3_p1_
```

Passaggio 3: Rimuovere i nodi di reporting e ripetere la scansione dei percorsi

È necessario rimuovere i nodi di reporting e ripetere la scansione dei percorsi.

Fasi

1. Sul nuovo nodo, rimuovere i nodi di reporting remoti (i nuovi nodi) per le LUN Linux:

   ```
   lun mapping remove-reporting-nodes -vserver <svm-name> -path * -igroup
   <igroup_name> -remote-nodes true
   ```

   In questo caso, i nodi remoti sono vecchi.

   ```
   node_A_1-new::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
   * -igroup igroup_linux -remote-nodes true
   12 entries were acted on.
   ```

2. Sul nuovo nodo, controllare i nodi di reporting delle LUN:

   ```
   lun mapping show -vserver <svm-name> -fields reporting-nodes -ostype
   linux
   ```

   ```
   node_A_1-new::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
   -ostype linux
   vserver  path                          igroup        reporting-nodes
   -------  ---------------------------  ------------
   -------------------------
   vsa_1    /vol/vsa_1_vol1/lun_linux_2  igroup_linux  node_A_1-
   new,node_A_2-new
   vsa_1    /vol/vsa_1_vol1/lun_linux_3  igroup_linux  node_A_1-
   new,node_A_2-new
   vsa_1    /vol/vsa_1_vol2/lun_linux_4  group_linux   node_A_1-
   new,node_A_2-new
   .
   .
   .
   12 entries were displayed.
   ```

3. Il `sg3-utils` Il pacchetto deve essere installato sull'host Linux. Questo impedisce un `rescan-scsi-bus.sh utility not found` Errore quando si esegue nuovamente la scansione dell'host Linux per i LUN appena mappati utilizzando `rescan-scsi-bus` comando.

   Sull'host, verificare che `sg3-utils` il pacchetto è installato:

- Per una distribuzione basata su Debian:

```
dpkg -l | grep sg3-utils
```

- Per una distribuzione basata su Red Hat:

```
rpm -qa | grep sg3-utils
```

Se necessario, installare `sg3-utils` Pacchetto sull'host Linux:

```
sudo apt-get install sg3-utils
```

4. Sull'host iSCSI, eseguire nuovamente la scansione del bus SCSI:

```
/usr/bin/rescan-scsi-bus.sh -r
```

I percorsi rimossi sono i percorsi dei vecchi nodi.

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
.
.
.
```

5. Sull'host iSCSI, verificare che siano visibili solo i percorsi dai nuovi nodi:

```
sanlun lun show -p
```

```
multipath -ll -d
```

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto

"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Gestione di MetroCluster"	• Informazioni sulla configurazione di MetroCluster • Switchover, healing e switchback
"Disaster recovery"	• Disaster recovery • Switchover forzato • Ripristino da un errore di storage o multi-controller
"Manutenzione MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster FC • Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch • Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch • Sostituzione dell'hardware in un sito di emergenza in una configurazione FC MetroCluster Fabric-Attached o Stretch • Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.

"Upgrade ed espansione di MetroCluster"	• Aggiornamento o aggiornamento di una configurazione MetroCluster • Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi
"Transizione MetroCluster"	• Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP
"Upgrade, transizione ed espansione di MetroCluster"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
"Documentazione dei sistemi hardware ONTAP" **Nota:** le procedure standard di manutenzione dello shelf storage possono essere utilizzate con le configurazioni MetroCluster IP.	• Aggiunta a caldo di uno shelf di dischi • Rimozione a caldo di uno shelf di dischi
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster
"Concetti di ONTAP"	• Come funzionano gli aggregati mirrorati

Aggiornare, aggiornare o espandere la configurazione di MetroCluster

Inizia qui - scegli la procedura

Inizia qui: Scegli tra upgrade del controller, refresh del sistema o espansione

A seconda dell'ambito dell'aggiornamento dell'apparecchiatura, è possibile scegliere una procedura di aggiornamento del controller, una procedura di aggiornamento del sistema o una procedura di espansione.

- Le procedure di aggiornamento del controller si applicano solo ai moduli controller. I controller vengono sostituiti con un nuovo modello di controller.

  I modelli di shelf storage non vengono aggiornati.

  - Nelle procedure di switchover e switchback, l'operazione di switchover MetroCluster viene utilizzata per fornire un servizio senza interruzioni ai client mentre i moduli controller sul cluster partner vengono aggiornati.
  - In una procedura di upgrade del controller basata su ARL, le operazioni di trasferimento aggregato vengono utilizzate per spostare i dati senza interruzioni dalla vecchia configurazione alla nuova configurazione aggiornata.
- Le procedure di refresh si applicano ai controller e agli shelf di storage.

  Nelle procedure di refresh, nuovi controller e shelf vengono aggiunti alla configurazione di MetroCluster, creando un secondo gruppo di DR e quindi i dati vengono migrati senza interruzioni nei nuovi nodi.

  I controller originali vengono quindi ritirati.

- Le procedure di espansione aggiungono controller e shelf aggiuntivi alla configurazione MetroCluster senza rimuoverne nessuno.

  La procedura utilizzata dipende dal tipo di MetroCluster e dal numero di controller esistenti.

Tipo di upgrade	Vai a…
Upgrade del controller	"Scegliere una procedura di aggiornamento del controller"
Refresh del sistema	"Scegliere una procedura di aggiornamento del sistema"
Espansione	• "MetroCluster da due nodi a quattro" • "MetroCluster FC a quattro nodi fino a otto" • "IP MetroCluster a quattro nodi fino a otto"

Scegliere una procedura di aggiornamento del controller

La procedura di aggiornamento del controller utilizzata dipende dal modello di piattaforma

e dal tipo di configurazione MetroCluster.

In una procedura di aggiornamento, i controller vengono sostituiti con un nuovo modello di controller. I modelli di shelf storage non vengono aggiornati.

- Nelle procedure di switchover e switchback, l'operazione di switchover MetroCluster viene utilizzata per fornire un servizio senza interruzioni ai client mentre i moduli controller sul cluster partner vengono aggiornati.
- In una procedura di upgrade del controller basata su ARL, le operazioni di trasferimento aggregato vengono utilizzate per spostare i dati senza interruzioni dalla vecchia configurazione alla nuova configurazione aggiornata.

Scelta di una procedura che utilizzi il processo di switchover e switchback

Selezionare la piattaforma corrente dalla tabella FC o IP riportata di seguito. Se l'intersezione tra la riga della piattaforma corrente e la colonna della piattaforma di destinazione è vuota, l'aggiornamento non è supportato.

Aggiornamenti del controller IP MetroCluster supportati

Se la piattaforma non è elencata, non è disponibile alcuna combinazione di upgrade del controller supportata.

> Quando si esegue un aggiornamento del controller, il vecchio e il nuovo tipo di piattaforma **devono** corrispondere.
>
> - Puoi aggiornare un sistema FAS ad un sistema FAS o AFF A-Series ad un AFF a-Series.
> - Non è possibile aggiornare un sistema FAS ad un AFF A-Series o AFF A-Series a un AFF C-Series.
>
> Ad esempio, se la piattaforma che si desidera aggiornare è FAS8200, è possibile eseguire l'aggiornamento a FAS9000. Non è possibile aggiornare un sistema FAS8200 a un sistema AFF A700.

		Target MetroCluster IP platform									
		AFF A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150										
	FAS2750 AFF A220										
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250										
	FAS8200 AFF A300										Note 2
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										Note 2
	FAS8700										Note 2
	FAS9000 AFF A700										Note 1
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

- Nota 1: Per questo aggiornamento, utilizzare la procedura "Upgrade dei controller da AFF A700/FAS9000 a AFF A900/FAS9500 in una configurazione MetroCluster IP utilizzando switchover e switchback (ONTAP 9.10.1 o versione successiva)"
- Nota 2: Gli aggiornamenti dei controller sono supportati nei sistemi che eseguono ONTAP 9.13.1 o versioni successive.
- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, i nuovi controller devono eseguire la stessa versione di ONTAP dei vecchi controller.

Aggiornamenti del controller FC MetroCluster supportati

Se la piattaforma non è elencata, non è disponibile alcuna combinazione di upgrade del controller supportata.

> Quando si esegue un aggiornamento del controller, il vecchio e il nuovo tipo di piattaforma **devono** corrispondere.
>
> - Puoi aggiornare un sistema FAS ad un sistema FAS o AFF A-Series ad un AFF a-Series.
> - Non è possibile aggiornare un sistema FAS ad un AFF A-Series o AFF A-Series a un AFF C-Series.
>
> Ad esempio, se la piattaforma che si desidera aggiornare è FAS8200, è possibile eseguire l'aggiornamento a FAS9000. Non è possibile aggiornare un sistema FAS8200 a un sistema AFF A700.

		Target MetroCluster FC platform											
		FAS80x0	AFF80x0	FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8020	Note 1		Note 1		Note 1			Note 1				
	AFF8020		Note 1		Note 1		Note 1			Note 1			
	FAS8040 FAS8060 FAS8080												
	AFF8040 AFF8060 AFF8080												
	FAS8200					Note 2			Note 2		Note 4		
	AFF A300						Note 2			Note 2		Note 4	
	FAS8300										Note 4		
	AFF A400											Note 4	
	ASA A400												Note 5
	FAS9000										Note 3		
	AFF A700											Note 3	
	FAS9500												
	AFF A900												
	ASA A900												

- Nota 1: Per l'aggiornamento dei controller quando le connessioni FCVI su nodi FAS8020 o AFF8020 esistenti utilizzano le porte 1c e 1d, vedere quanto seguehttps://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/MetroCluster/Upgrading_controllers_when_FCVI_connections_on_existing_FAS8020_or_AFF8020_nodes_use_ports_1c_and_1d["Articolo della Knowledge base"^].
- Nota 2: Gli upgrade dei controller da piattaforme AFF A300 o FAS8200 utilizzando le porte integrate 0e e 0f come connessioni FC-VI sono supportati solo sui seguenti sistemi:
  - ONTAP 9.9.1 e versioni precedenti
  - ONTAP 9.10.1P9
  - ONTAP 9.11.1P5
  - ONTAP 9.12.1GA
  - ONTAP 9.13.1 e versioni successive

    Per ulteriori informazioni, consultare "Report pubblico".
- Nota 3: Per questo aggiornamento, fare riferimento a. "Upgrade dei controller da AFF A700/FAS9000 a AFF A900/FAS9500 in una configurazione MetroCluster FC utilizzando switchover e switchback (ONTAP 9.10.1 o versione successiva)"
- Nota 4: Gli upgrade dei controller sono supportati sui sistemi con ONTAP 9.13.1 o versione successiva.
- Nota 5: Gli upgrade dei controller sono supportati sui sistemi con ONTAP 9.14.1 o versione successiva.
- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, i nuovi controller devono eseguire la stessa versione di ONTAP dei vecchi controller.

Tipo di MetroCluster	Metodo di aggiornamento	Versione di ONTAP	Procedura
IP	Eseguire l'aggiornamento con i comandi "System controller replace"	9.13.1 e versioni successive	"Collegamento alla procedura"

FC	Eseguire l'aggiornamento con i comandi "System controller replace"	9.10.1 e versioni successive	"Collegamento alla procedura"
FC	Aggiornamento manuale con comandi CLI (solo da AFF A700/FAS9000 a AFF A900/FAS9500)	9.10.1 e versioni successive	"Collegamento alla procedura"
IP	Aggiornamento manuale con comandi CLI (solo da AFF A700/FAS9000 a AFF A900/FAS9500)	9.10.1 e versioni successive	"Collegamento alla procedura"
FC	Aggiornamento manuale con comandi CLI	9.8 e versioni successive	"Collegamento alla procedura"
IP	Aggiornamento manuale con comandi CLI	9.8 e versioni successive	"Collegamento alla procedura"

Scelta di una procedura che utilizzi il trasferimento di aggregati

In una procedura di upgrade del controller basata su ARL, le operazioni di trasferimento aggregato vengono utilizzate per spostare i dati senza interruzioni dalla vecchia configurazione alla nuova configurazione aggiornata.

Tipo di MetroCluster	Ricollocazione di aggregati	Versione di ONTAP	Procedura
FC	Utilizzo dei comandi "System controller replace" per aggiornare i modelli di controller nello stesso chassis	9.10.1 e versioni successive	"Collegamento alla procedura"
FC	Utilizzo di `system controller replace` comandi	9.8 e versioni successive	"Collegamento alla procedura"

Tipo di MetroCluster	Ricollocazione di aggregati	Versione di ONTAP	Procedura
FC	Utilizzo di `system controller replace` comandi	da 9.5 a 9.7	"Collegamento alla procedura"
FC	Utilizzo di comandi ARL manuali	9.8	"Collegamento alla procedura"
FC	Utilizzo di comandi ARL manuali	9.7 e versioni precedenti	"Collegamento alla procedura"

Scelta di un metodo di refresh del sistema

La procedura di refresh del sistema utilizzata dipende dal modello di piattaforma e dal tipo di configurazione MetroCluster. Le procedure di refresh si applicano ai controller e agli shelf di storage. Nelle procedure di refresh, nuovi controller e shelf vengono aggiunti alla configurazione di MetroCluster, creando un secondo gruppo di DR e quindi i dati vengono migrati senza interruzioni nei nuovi nodi. I controller originali vengono quindi ritirati.

Combinazioni di aggiornamento tecnico FC MetroCluster supportate

		Target MetroCluster FC platform									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
Source MetroCluster FC platform	FAS8200	■	■	■	■	■	■	■	■	■	■
	AFF A300	■	■	■	■	■	■	■	■	■	■
	FAS8300			■	■	■	■	■	■	■	■
	AFF A400			■	■	■	■	■	■	■	■
	ASA A400			■	■	■	■	■	■	■	■
	FAS9000						■	■	■	■	■
	AFF A700						■	■	■	■	■
	FAS9500								■	■	■
	AFF A900								■	■	■
	ASA A900								■	■	■

- È necessario completare la procedura di aggiornamento tecnico prima di aggiungere un nuovo carico.
- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, se si dispone di una configurazione a otto nodi, tutti e otto i nodi devono utilizzare la stessa versione di ONTAP.
- Non superare i limiti di oggetti della "parte inferiore" delle piattaforme nella combinazione. Applicare il limite inferiore di oggetti delle due piattaforme.
- Se i limiti della piattaforma di destinazione sono inferiori ai limiti MetroCluster, è necessario riconfigurare il MetroCluster in modo che sia pari o inferiore ai limiti della piattaforma di destinazione prima di aggiungere i nuovi nodi.
- Fare riferimento a. "Hardware Universe" per i limiti della piattaforma.

Combinazioni di aggiornamento tecnico MetroCluster IP supportate

		Target MetroCluster IP platform									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
Source MetroCluster IP platform	AFF A150 ASA A150	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS2750 AFF A220	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1	Note 1
	FAS8200 AFF A300										
	AFF A320										
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										
	FAS8700										
	FAS9000 AFF A700										
	AFF C800 ASA C800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

Nota 1: questa combinazione richiede ONTAP 9.13.1 o versione successiva.

- È necessario completare la procedura di aggiornamento tecnico prima di aggiungere un nuovo carico.
- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, se si dispone di una configurazione a otto nodi, tutti e otto i nodi devono utilizzare la stessa versione di ONTAP.
- Non superare i limiti di oggetti della "parte inferiore" delle piattaforme nella combinazione. Applicare il limite inferiore di oggetti delle due piattaforme.
- Se i limiti della piattaforma di destinazione sono inferiori ai limiti MetroCluster, è necessario riconfigurare il MetroCluster in modo che sia uguale o inferiore ai limiti della piattaforma di destinazione prima di aggiungere i nuovi nodi.
- Fare riferimento a. "Hardware Universe" per i limiti della piattaforma.

Metodo di refresh	Tipo di configurazione	Versione di ONTAP	Procedura
• Metodo: Espandere la configurazione MetroCluster e rimuovere i nodi precedenti	FC a quattro nodi	9.6 e versioni successive	"Collegamento alla procedura"
• Metodo: Espandere la configurazione MetroCluster e rimuovere i nodi precedenti	IP a quattro nodi	9.8 e versioni successive	"Collegamento alla procedura"

Scegliere una procedura di espansione

La procedura di espansione utilizzata dipende dal tipo di configurazione di MetroCluster e dalla versione di ONTAP.

Una procedura di espansione implica l'aggiunta di nuovi controller e storage alla configurazione MetroCluster.

L'espansione deve mantenere un numero pari di controller su ciascun sito e la procedura utilizzata dipende dal numero di nodi nella configurazione MetroCluster originale.

Metodo di espansione	Tipo di configurazione	Versione di ONTAP	Procedura
Metodo: Espandere un MetroCluster FC a due nodi a quattro	FC a due nodi	ONTAP 9 e versioni successive (le piattaforme devono essere supportate in ONTAP 9.2 e versioni successive)	"Collegamento alla procedura"
Metodo: Espandere un FC MetroCluster a quattro nodi a otto	FC a quattro nodi	ONTAP 9 o versione successiva	"Collegamento alla procedura"
Metodo: Espandere un IP MetroCluster a quattro nodi a otto	IP a quattro nodi	ONTAP 9.9.1 e versioni successive	"Collegamento alla procedura"

Aggiornare i controller in una configurazione MetroCluster IP a quattro nodi utilizzando lo switchover e lo switchback con i comandi "system controller replace" (ONTAP 9.13.1 e versioni successive)

È possibile utilizzare questa operazione di switchover MetroCluster automatizzato e guidato per eseguire un aggiornamento del controller senza interruzioni su una configurazione IP MetroCluster a quattro nodi. Altri componenti (ad esempio shelf di storage o switch) non possono essere aggiornati come parte di questa procedura.

Combinazioni di piattaforme supportate

Questa procedura supporta i seguenti upgrade dei controller su sistemi con ONTAP 9.13.1 e versioni successive.

Vecchio controller	Controller sostitutivo
AFF A300	AFF A900
FAS8200	FAS9500

È possibile eseguire gli aggiornamenti dei controller elencati nella tabella riportata sopra su sistemi che eseguono ONTAP 9.12.1 o 9.11.1 utilizzando la procedura di aggiornamento manuale descritta "qui".

Per ulteriori informazioni sulle combinazioni di upgrade della piattaforma, consultare la tabella di aggiornamento IP di MetroCluster in "Scegliere una procedura di aggiornamento del controller".

Fare riferimento a. "Scelta di un metodo di aggiornamento o refresh" per ulteriori procedure.

A proposito di questa attività

- Questa procedura può essere utilizzata solo per l'aggiornamento del controller.

  Gli altri componenti della configurazione, come gli shelf di storage o gli switch, non possono essere aggiornati contemporaneamente.

- Questa procedura si applica ai moduli controller in una configurazione MetroCluster IP a quattro nodi con ONTAP 9.13.1 o versione successiva.

  "NetApp Hardware Universe"

- I sistemi MetroCluster devono eseguire la stessa versione di ONTAP in entrambi i siti.
- È possibile utilizzare questa procedura per aggiornare i controller in una configurazione MetroCluster IP a quattro nodi utilizzando switchover e switchback automatici basati su NSO.

> L'esecuzione di un aggiornamento utilizzando il trasferimento aggregato (ARL) con i comandi "system controller replace" non è supportata per una configurazione MetroCluster IP a quattro nodi.

- È necessario utilizzare la procedura di aggiornamento automatico del controller NSO per aggiornare i controller in entrambi i siti in sequenza.
- Questa procedura di aggiornamento automatico del controller basata su NSO consente di avviare la sostituzione del controller in un sito di disaster recovery (DR) MetroCluster. È possibile avviare la sostituzione di un controller solo in un sito alla volta.
- Per avviare una sostituzione del controller nel sito A, eseguire il comando di avvio per la sostituzione del controller dal sito B. L'operazione consente di sostituire i controller di entrambi i nodi solo nel sito A. Per sostituire i controller nel sito B, eseguire il comando di avvio per la sostituzione dei controller dal sito A. Viene visualizzato un messaggio che identifica il sito in cui vengono sostituiti i controller.

In questa procedura vengono utilizzati i seguenti nomi di esempio:

- Sito_A.
  - Prima dell'aggiornamento:
    - Node_A_1-old
    - Node_A_2-old
  - Dopo l'aggiornamento:
    - Node_A_1-new
    - Node_A_2-new
- Sito_B
  - Prima dell'aggiornamento:
    - Node_B_1-old
    - Node_B_2-old

- Dopo l'aggiornamento:
  - Node_B_1-new
  - Node_B_2-new

Preparatevi per l'aggiornamento

Per prepararsi all'aggiornamento del controller, è necessario eseguire controlli preliminari del sistema e raccogliere le informazioni di configurazione.

Prima dell'avvio dei controlli preliminari, se ONTAP Mediator è installato, viene rilevato e rimosso automaticamente. Per confermare la rimozione, viene richiesto di inserire un nome utente e una password. Una volta completato l'aggiornamento, se i controlli preliminari non hanno esito positivo o se si sceglie di non procedere con l'aggiornamento, è necessario Riconfigurare manualmente il mediatore ONTAP.

Durante l'aggiornamento, è possibile eseguire il `system controller replace show` oppure `system controller replace show-details` Dal sito A per controllare lo stato. Se i comandi restituiscono un output vuoto, attendere alcuni minuti ed eseguire nuovamente il comando.

Fasi

1. Avviare la procedura di sostituzione automatica del controller dal sito A per sostituire i controller nel sito B:

   ```
   system controller replace start -nso true
   ```

   L'operazione automatica esegue i controlli preliminari. Se non vengono rilevati problemi, l'operazione viene interrotta in modo da poter raccogliere manualmente le informazioni relative alla configurazione.

- Se non si esegue `system controller replace start -nso true` La procedura di upgrade del controller sceglie lo switchover e lo switchback automatici basati su NSO come procedura predefinita sui sistemi MetroCluster IP.
- Vengono visualizzati il sistema di origine corrente e tutti i sistemi di destinazione compatibili. Se il controller di origine è stato sostituito con un controller con una versione ONTAP diversa o con una piattaforma non compatibile, l'operazione di automazione si interrompe e segnala un errore dopo l'avvio dei nuovi nodi. Per riportare il cluster a uno stato integro, è necessario seguire la procedura di ripristino manuale.

  Il `system controller replace start` il comando potrebbe segnalare il seguente errore di verifica preliminare:

```
Cluster-A::*>system controller replace show
Node        Status         Error-Action
----------- --------------
-------------------------------------
Node-A-1    Failed         MetroCluster check failed.
Reason : MCC check showed errors in component aggregates
```

  Controllare se si è verificato questo errore a causa di aggregati senza mirror o di un altro problema di aggregato. Verificare che tutti gli aggregati mirrorati siano integri e che non siano degradati o mirror-degradati. Se questo errore è dovuto solo agli aggregati senza mirror, è possibile ignorare questo errore selezionando `-skip-metrocluster-check true` sul `system controller replace start` comando. Se lo storage remoto è accessibile, gli aggregati senza mirror vengono online dopo lo switchover. Se il collegamento storage remoto non funziona, gli aggregati senza mirror non vengono collegati.

2. Raccogliere manualmente le informazioni di configurazione accedendo al sito B e seguendo i comandi elencati nel messaggio della console sotto `system controller replace show` oppure `system controller replace show-details` comando.

Raccolta di informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, se il volume root è crittografato, è necessario raccogliere la chiave di backup e altre informazioni per avviare i nuovi controller con i vecchi volumi root crittografati.

A proposito di questa attività

Questa attività viene eseguita sulla configurazione IP MetroCluster esistente.

Fasi

1. Etichettare i cavi per i controller esistenti, in modo da poter identificare facilmente i cavi durante la configurazione dei nuovi controller.
2. Visualizzare i comandi per acquisire la chiave di backup e altre informazioni:

   `system controller replace show`

   Eseguire i comandi elencati sotto `show` dal cluster partner.

Il `show` L'output del comando visualizza tre tabelle contenenti gli IP dell'interfaccia MetroCluster, gli ID di sistema e gli UID di sistema. Queste informazioni sono necessarie più avanti nella procedura per impostare i bootargs quando si avvia il nuovo nodo.

3. Raccogliere gli ID di sistema dei nodi nella configurazione MetroCluster:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Durante la procedura di aggiornamento, sostituisci questi vecchi ID di sistema con gli ID di sistema dei nuovi moduli controller.

   In questo esempio, per una configurazione IP MetroCluster a quattro nodi, vengono recuperati i seguenti vecchi ID di sistema:

   - Node_A_1-old: 4068741258
   - Node_A_2-old: 4068741260
   - Node_B_1-old: 4068741254
   - Node_B_2-old: 4068741256

   ```
   metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
   partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
   dr-group-id        cluster           node            node-systemid
   ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
   -----------        ---------------   ----------      -------------
   -------------------     -------------------    ---------------------
   1                    Cluster_A       Node_A_1-old    4068741258
   4068741260              4068741256             4068741256
   1                    Cluster_A       Node_A_2-old    4068741260
   4068741258              4068741254             4068741254
   1                    Cluster_B       Node_B_1-old    4068741254
   4068741256              4068741258             4068741260
   1                    Cluster_B       Node_B_2-old    4068741256
   4068741254              4068741260             4068741258
   4 entries were displayed.
   ```

   In questo esempio, per una configurazione MetroCluster IP a due nodi, vengono recuperati i seguenti vecchi ID di sistema:

   - Node_A_1: 4068741258
   - Node_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Raccogliere informazioni su porta e LIF per ciascun nodo precedente.

   Per ciascun nodo, è necessario raccogliere l'output dei seguenti comandi:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node` *`node-name`* `sysconfig -a`
5. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`
6. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

   ```
   security key-manager backup show
   ```

7. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

   Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

   a. Se Onboard Key Manager è configurato:

      ```
      security key-manager onboard show-backup
      ```

La passphrase sarà necessaria più avanti nella procedura di aggiornamento.

b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

```
security key-manager external show -instance
```

```
security key-manager key query
```

8. Al termine della raccolta delle informazioni di configurazione, riprendere l'operazione:

```
system controller replace resume
```

Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio, ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima di sostituire il vecchio controller.

Fasi

1. "Rimuovere la configurazione MetroCluster esistente" Dal software Tiebreaker.
2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Sostituzione dei vecchi controller e avvio dei nuovi controller

Una volta raccolte le informazioni e riavviata l'operazione, l'automazione procede con l'operazione di switchover.

A proposito di questa attività

L'operazione di automazione avvia le operazioni di switchover. Al termine di queste operazioni, l'operazione viene sospesa in **pausa per l'intervento dell'utente**, in modo da poter eseguire il rack e installare i controller, avviare i controller partner e riassegnare i dischi aggregati root al nuovo modulo controller dal backup flash utilizzando `sysids` raccolte in precedenza.

Prima di iniziare

Prima di iniziare lo switchover, l'operazione di automazione viene interrotta in modo da poter verificare manualmente che tutti i LIF siano "up" nel sito B. Se necessario, portare i LIF "dpropri" su "up" e riprendere l'operazione di automazione utilizzando `system controller replace resume` comando.

Preparazione della configurazione di rete dei vecchi controller

Per garantire che la rete riprenda correttamente sui nuovi controller, è necessario spostare i file LIF su una porta comune e rimuovere la configurazione di rete dei vecchi controller.

A proposito di questa attività

- Questa attività deve essere eseguita su ciascuno dei vecchi nodi.
- Verranno utilizzate le informazioni raccolte in Preparatevi per l'aggiornamento.

Fasi

1. Avviare i vecchi nodi e quindi accedere ai nodi:

   `boot_ontap`

2. Assegnare la porta home di tutti i file LIF di dati sul vecchio controller a una porta comune identica sia sul vecchio che sul nuovo modulo controller.

   a. Visualizzare le LIF:

      `network interface show`

      Tutti i dati LIFS, inclusi SAN e NAS, saranno admin “up” e operativi “down”, in quanto sono presenti nel sito di switchover (cluster_A).

   b. Esaminare l’output per trovare una porta di rete fisica comune che sia la stessa sui controller vecchi e nuovi che non sia utilizzata come porta del cluster.

      Ad esempio, “e0d” è una porta fisica sui vecchi controller ed è presente anche sui nuovi controller. “e0d” non viene utilizzato come porta del cluster o in altro modo sui nuovi controller.

      Per informazioni sull’utilizzo delle porte per i modelli di piattaforma, consultare "NetApp Hardware Universe"

   c. Modificare tutti i dati LIFS per utilizzare la porta comune come porta home:

      `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

      Nell’esempio seguente, si tratta di “e0d”.

      Ad esempio:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modificare i domini di broadcast per rimuovere la VLAN e le porte fisiche che devono essere eliminate:

   `broadcast-domain remove-ports -broadcast-domain` *`broadcast-domain-name`* `-ports` *`node-name:port-id`*

   Ripetere questo passaggio per tutte le porte VLAN e fisiche.

4. Rimuovere le porte VLAN utilizzando le porte del cluster come porte membro e gruppi di interfacce utilizzando le porte del cluster come porte membro.

   a. Elimina porte VLAN:

      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

      Ad esempio:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Rimuovere le porte fisiche dai gruppi di interfacce:

   `network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

   Ad esempio:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Rimuovere le porte della VLAN e del gruppo di interfacce dal dominio di broadcast:

   `network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modificare le porte del gruppo di interfacce per utilizzare altre porte fisiche come membro in base alle necessità.:

   `ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

5. Arrestare i nodi:

   `halt -inhibit-takeover true -node node-name`

   Questa operazione deve essere eseguita su entrambi i nodi.

Configurazione dei nuovi controller

I nuovi controller devono essere montati in rack e cablati.

Fasi

1. Pianificare il posizionamento dei nuovi moduli controller e degli shelf di storage in base alle necessità.

   Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di shelf di storage nella configurazione.

2. Mettere a terra l'utente.
3. Installare i moduli controller nel rack o nell'armadietto.

   "Documentazione dei sistemi hardware ONTAP"

4. Se i nuovi moduli controller non sono dotati di schede FC-VI e se le schede FC-VI dei vecchi controller sono compatibili con i nuovi controller, sostituire le schede FC-VI e installarle negli slot corretti.

   Vedere "NetApp Hardware Universe" Per informazioni sugli slot per schede FC-VI.

5. Collegare l'alimentazione, la console seriale e le connessioni di gestione dei controller come descritto nelle *Guide di installazione e configurazione di MetroCluster*.

   Non collegare altri cavi scollegati dai vecchi controller in questo momento.

   "Documentazione dei sistemi hardware ONTAP"

6. Accendere i nuovi nodi e premere Ctrl-C quando richiesto per visualizzare il prompt DEL CARICATORE.

Avvio in rete dei nuovi controller

Dopo aver installato i nuovi nodi, è necessario eseguire il netboot per assicurarsi che i nuovi nodi eseguano la stessa versione di ONTAP dei nodi originali. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

Questa attività viene eseguita su ciascuno dei nuovi moduli controller.

Fasi

1. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il file ontap-version_image.tgz in una directory accessibile dal Web.
3. Accedere alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

   L'elenco delle directory deve contenere una cartella netboot con un file del kernel: ontap-version_image.tgz

   Non è necessario estrarre il file ontap-version_image.tgz.

4. Al prompt DEL CARICATORE, configurare la connessione netboot per una LIF di gestione:
   - Se l'indirizzo IP è DHCP, configurare la connessione automatica:

     ```
     ifconfig e0M -auto
     ```

   - Se l'indirizzo IP è statico, configurare la connessione manuale:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Eseguire il netboot.
   - Se la piattaforma è un sistema della serie 80xx, utilizzare questo comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se la piattaforma è un altro sistema, utilizzare il seguente comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se viene richiesto di continuare la procedura, immettere `y`E quando
   viene richiesto il pacchetto, inserire l'URL del file immagine:
   `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

```
Enter username/password if applicable, or press Enter to continue.
```

7. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

```
Do you want to restore the backup configuration now? {y|n}
```

8. Riavviare immettendo `y` quando viene visualizzato un prompt simile a quanto segue:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   ```
   set-defaults
   ```

3. Salvare l'ambiente:

   ```
   saveenv
   ```

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

   ```
   boot_ontap menu
   ```

5. Al prompt del menu di avvio, cancellare la configurazione:

   ```
   wipeconfig
   ```

   Rispondere `yes` al prompt di conferma.

   Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Ripristino della configurazione HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:

   a. Verificare le impostazioni correnti delle porte: `ucadmin show`

   b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

2. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

3. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

   ```
   boot_ontap maint
   ```

4. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Impostare lo stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

```
ha-config show
```

Lo stato ha per tutti i componenti deve essere `mccip`.

2. Se lo stato di sistema visualizzato del controller o dello chassis non è corretto, impostare lo stato ha:

```
ha-config modify controller mccip
```

```
ha-config modify chassis mccip
```

3. Arrestare il nodo: `halt`

   Il nodo deve arrestarsi su `LOADER>` prompt.

4. Su ciascun nodo, controllare la data, l'ora e il fuso orario del sistema: `show date`
5. Se necessario, impostare la data in UTC o GMT: `set date <mm/dd/yyyy>`
6. Controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot: `show time`
7. Se necessario, impostare l'ora in UTC o GMT: `set time <hh:mm:ss>`
8. Salvare le impostazioni: `saveenv`
9. Raccogliere le variabili di ambiente: `printenv`

Aggiornare i file RCF dello switch per ospitare le nuove piattaforme

È necessario aggiornare gli switch a una configurazione che supporti i nuovi modelli di piattaforma.

A proposito di questa attività

Questa attività viene eseguita nel sito contenente i controller attualmente in fase di aggiornamento. Negli esempi illustrati in questa procedura, si esegue prima l'aggiornamento di Site_B.

Gli switch del sito_A verranno aggiornati quando i controller del sito_A verranno aggiornati.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire le istruzioni della sezione relativa al fornitore dello switch nella sezione *Installazione e configurazione IP MetroCluster*.

   "Installazione e configurazione di MetroCluster IP"

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"

2. Scaricare e installare i file RCF.

   Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP".

   - "Download e installazione dei file RCF Broadcom"
   - "Download e installazione dei file Cisco IP RCF"

Impostare le variabili di boot IP di MetroCluster

Alcuni valori di boot MetroCluster IP devono essere configurati sui nuovi moduli controller. I valori devono corrispondere a quelli configurati sui vecchi moduli controller.

A proposito di questa attività

In questa attività, verranno utilizzati gli UUID e gli ID di sistema identificati in precedenza nella procedura di aggiornamento in "Raccolta di informazioni prima dell'aggiornamento".

Fasi

1. Su `LOADER>` Prompt, impostare i seguenti bootargs sui nuovi nodi in Site_B:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   Nell'esempio seguente vengono impostati i valori per Node_B_1 utilizzando la VLAN 120 per la prima rete e la VLAN 130 per la seconda rete:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   Nell'esempio seguente vengono impostati i valori per Node_B_2 utilizzando la VLAN 120 per la prima rete e la VLAN 130 per la seconda rete:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
   ```

2. Ai nuovi nodi" `LOADER` Impostare gli UUID:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Impostare gli UUID su Node_B_1.

      L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_1:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Impostare gli UUID su Node_B_2:

L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_2:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Se i sistemi originali sono stati configurati per ADP, al prompt DEL CARICATORE di ciascun nodo sostitutivo, abilitare ADP:

```
setenv bootarg.mcc.adp_enabled true
```

4. Impostare le seguenti variabili:

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> Il `setenv bootarg.mcc.local_config_id` Variable deve essere impostato sul sys-id del modulo controller **original**, Node_B_1.

a. Impostare le variabili su Node_B_1.

L'esempio seguente mostra i comandi per impostare i valori su Node_B_1:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Impostare le variabili su Node_B_2.

L'esempio seguente mostra i comandi per impostare i valori su Node_B_2:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Se si utilizza la crittografia con il gestore delle chiavi esterno, impostare i bootargs richiesti:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Riassegnazione dei dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando `sysids` raccolte in precedenza

A proposito di questa attività

Questa attività viene eseguita in modalità manutenzione.

I vecchi ID di sistema sono stati identificati in "Raccolta di informazioni prima dell'aggiornamento".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Nodo	Vecchio ID di sistema	Nuovo ID di sistema
Node_B_1	4068741254	1574774970

Fasi

1. Collegare tutti gli altri collegamenti ai nuovi moduli controller (FC-VI, storage, interconnessione cluster, ecc.).
2. Arrestare il sistema e avviare la modalità di manutenzione dal prompt DEL CARICATORE:

   ```
   boot_ontap maint
   ```

3. Visualizzare i dischi di proprietà di Node_B_1-old:

   ```
   disk show -a
   ```

   L'output del comando mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi aggregati root sono ancora di proprietà del vecchio ID di sistema (4068741254). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Riassegnare i dischi aggregati root sugli shelf di dischi al nuovo controller:

   `disk reassign -s old-sysid -d new-sysid`

   > Se il sistema IP MetroCluster è configurato con la partizione avanzata dei dischi, è necessario includere l'id di sistema del partner DR eseguendo `disk reassign -s old-sysid -d new-sysid -r dr-partner-sysid` comando.

   L'esempio seguente mostra la riassegnazione dei dischi:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verificare che tutti i dischi siano riassegnati come previsto:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Visualizzare lo stato dell'aggregato:

   `aggr status`

   ```
   *> aggr status
              Aggr            State       Status           Options
   aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                              mirrored
   mirror_resync_priority=high(fixed)
                              fast zeroed
                              64-bit
   ```

7. Ripetere i passaggi precedenti sul nodo partner (Node_B_2-new).

Avviare i nuovi controller

Riavviare i controller dal menu di avvio per aggiornare l'immagine flash del controller. Se la crittografia è configurata, sono necessari ulteriori passaggi.

È possibile riconfigurare VLAN e gruppi di interfacce. Se necessario, modificare manualmente le porte per le LIF del cluster e i dettagli del dominio di trasmissione prima di riprendere l'operazione utilizzando `system controller replace resume` comando.

A proposito di questa attività

Questa attività deve essere eseguita su tutti i nuovi controller.

Fasi

1. Arrestare il nodo:

   `halt`

2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Visualizzare il menu di avvio:

   `boot_ontap menu`

4. Se viene utilizzata la crittografia root, selezionare l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…

Gestione delle chiavi integrata	Opzione “10” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione “11” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

5. Dal menu di boot, eseguire l’opzione “6”.

   L’opzione “6” riavvia il nodo due volte prima del completamento.

   Rispondere “y” alle richieste di modifica dell’id di sistema. Attendere i secondi messaggi di riavvio:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

   Durante uno dei riavvii dopo l’opzione “6”, viene visualizzato il prompt di conferma `Override system ID? {y|n}` viene visualizzato. Invio `y`.

6. Se viene utilizzata la crittografia root, selezionare nuovamente l’opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione “10” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione “11” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

   A seconda dell’impostazione del gestore delle chiavi, eseguire la procedura di ripristino selezionando l’opzione “10” o l’opzione “11”, quindi l’opzione “6” al primo prompt del menu di avvio. Per avviare completamente i nodi, potrebbe essere necessario ripetere la procedura di ripristino, continua con l’opzione “1” (boot normale).

7. Avviare i nodi:

```
boot_ontap
```

8. Attendere l'avvio dei nodi sostituiti.

   Se uno dei nodi è in modalità Takeover, eseguire un giveback utilizzando `storage failover giveback` comando.

9. Verificare che tutte le porte si trovino in un dominio di trasmissione:

   a. Visualizzare i domini di trasmissione:

      ```
      network port broadcast-domain show
      ```

   b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

      "Aggiunta o rimozione di porte da un dominio di broadcast"

   c. Aggiungere la porta fisica che ospiterà le LIF dell'intercluster al dominio di trasmissione corrispondente.
   d. Modificare le LIF dell'intercluster per utilizzare la nuova porta fisica come porta home.
   e. Dopo aver attivato le LIF dell'intercluster, controllare lo stato del peer del cluster e ristabilire il peering del cluster secondo necessità.

      Potrebbe essere necessario riconfigurare il peering del cluster.

      "Creazione di una relazione peer del cluster"

   f. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

      L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

      "Creazione di una VLAN"

   "Combinazione di porte fisiche per creare gruppi di interfacce"

   a. Verificare che il cluster partner sia raggiungibile e che la configurazione sia risincronizzata correttamente sul cluster partner:

      ```
      metrocluster switchback -simulate true
      ```

10. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

11. Prima di riprendere l'operazione, verificare che MetroCluster sia configurato correttamente. Controllare lo stato del nodo:

    ```
    metrocluster node show
    ```

    Verificare che i nuovi nodi (Site_B) si trovino nello stato **Waiting for switchback** from Site_A.

12. Riprendere l'operazione:

    ```
    system controller replace resume
    ```

Completamento dell'aggiornamento

L'operazione di automazione esegue controlli del sistema di verifica e quindi si ferma per verificare la raggiungibilità della rete. Dopo la verifica, viene avviata la fase di riconquista delle risorse e l'operazione di automazione esegue lo switchback nel sito A e si ferma ai controlli successivi all'aggiornamento. Dopo aver ripristinato l'operazione di automazione, esegue i controlli post-aggiornamento e, se non vengono rilevati errori, contrassegna l'aggiornamento come completo.

Fasi

1. Verificare la raggiungibilità della rete seguendo il messaggio della console.
2. Una volta completata la verifica, riprendere l'operazione:

    ```
    system controller replace resume
    ```

3. L'operazione di automazione viene eseguita `heal-aggregate`, `heal-root-aggregate`E le operazioni di switchback presso il sito A e i controlli successivi all'aggiornamento. Quando l'operazione viene interrotta, controllare manualmente lo stato LIF DELLA SAN e verificare la configurazione di rete seguendo il messaggio della console.
4. Una volta completata la verifica, riprendere l'operazione:

    ```
    system controller replace resume
    ```

5. Controllare lo stato dei controlli successivi all'aggiornamento:

    ```
    system controller replace show
    ```

    Se i controlli successivi all'aggiornamento non hanno segnalato errori, l'aggiornamento è completo.

6. Dopo aver completato l'aggiornamento del controller, accedere al sito B e verificare che i controller sostituiti siano configurati correttamente.

Riconfigurare il mediatore ONTAP

Configurare manualmente ONTAP Media, che è stato rimosso automaticamente prima di avviare l'aggiornamento.

1. Attenersi alla procedura descritta in "Configurare il servizio ONTAP Mediator da una configurazione IP MetroCluster".

Ripristino del monitoraggio di Tiebreaker

Se la configurazione MetroCluster è stata precedentemente configurata per il monitoraggio da parte del software Tiebreaker, è possibile ripristinare la connessione Tiebreaker.

1. Attenersi alla procedura descritta in "Aggiunta di configurazioni MetroCluster".

Aggiornamento dei controller in una configurazione MetroCluster FC mediante switchover e switchback

È possibile utilizzare l'operazione di switchover MetroCluster per fornire un servizio senza interruzioni ai client mentre i moduli controller sul cluster partner vengono aggiornati. Altri componenti (ad esempio shelf di storage o switch) non possono essere aggiornati come parte di questa procedura.

Combinazioni di piattaforme supportate

È possibile aggiornare alcune piattaforme utilizzando le operazioni di switchover e switchback in una configurazione MetroCluster FC.

Per informazioni sulle combinazioni di upgrade della piattaforma supportate, consultare la tabella di upgrade MetroCluster FC in "Scegliere una procedura di aggiornamento del controller".

Fare riferimento a. "Scelta di un metodo di aggiornamento o refresh" per ulteriori procedure.

A proposito di questa attività

- Questa procedura può essere utilizzata solo per l'aggiornamento del controller.

  Gli altri componenti della configurazione, come gli shelf di storage o gli switch, non possono essere aggiornati contemporaneamente.

- È possibile utilizzare questa procedura con alcune versioni di ONTAP:
  - Le configurazioni a due nodi sono supportate in ONTAP 9.3 e versioni successive.
  - Le configurazioni a quattro e otto nodi sono supportate in ONTAP 9.8 e versioni successive.

    Non utilizzare questa procedura su configurazioni a quattro o otto nodi con versioni di ONTAP precedenti alla 9.8.

- Le piattaforme originali e nuove devono essere compatibili e supportate.

  "NetApp Hardware Universe"

  > Se le piattaforme originali o nuove sono sistemi FAS8020 o AFF8020 che utilizzano le porte 1c e 1d in modalità FC-VI, consultare l'articolo della Knowledge base "Aggiornamento dei controller quando le connessioni FCVI su nodi FAS8020 o AFF8020 esistenti utilizzano le porte 1c e 1d."

- Le licenze di entrambi i siti devono corrispondere. È possibile ottenere nuove licenze da "Supporto NetApp".

- Questa procedura si applica ai moduli controller in una configurazione MetroCluster FC (Stretch MetroCluster a due nodi o una configurazione Fabric-Attached MetroCluster a due, quattro o otto nodi).
- Tutti i controller dello stesso gruppo di DR devono essere aggiornati durante lo stesso periodo di manutenzione.

  L'utilizzo della configurazione MetroCluster con diversi tipi di controller nello stesso gruppo DR non è supportato al di fuori di questa attività di manutenzione. Per le configurazioni MetroCluster a otto nodi, i controller all'interno di un gruppo DR devono essere gli stessi, ma entrambi i gruppi DR possono utilizzare diversi tipi di controller.

- Si consiglia di eseguire il mapping delle connessioni storage, FC ed Ethernet tra i nodi originali e i nuovi nodi in anticipo.
- Se la nuova piattaforma ha meno slot rispetto al sistema originale o se ha un numero inferiore o diversi tipi di porte, potrebbe essere necessario aggiungere un adattatore al nuovo sistema.

  Per ulteriori informazioni, consultare "NetApp Hardware Universe"

In questa procedura vengono utilizzati i seguenti nomi di esempio:

- Sito_A.
  - Prima dell'aggiornamento:
    - Node_A_1-old
    - Node_A_2-old
  - Dopo l'aggiornamento:
    - Node_A_1-new
    - Node_A_2-new
- Sito_B
  - Prima dell'aggiornamento:
    - Node_B_1-old
    - Node_B_2-old
  - Dopo l'aggiornamento:
    - Node_B_1-new
    - Node_B_2-new

Preparazione per l'aggiornamento

Prima di apportare modifiche alla configurazione MetroCluster esistente, è necessario controllare lo stato della configurazione, preparare le nuove piattaforme ed eseguire altre attività varie.

Verifica dello stato della configurazione MetroCluster

Prima di eseguire l'aggiornamento, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

a. Verificare che i nodi siano multipathing:
   `node run -node node-name sysconfig -a`

   Eseguire questo comando per ogni nodo della configurazione MetroCluster.

b. Verificare che non vi siano dischi rotti nella configurazione:

   `storage disk show -broken`

   Eseguire questo comando su ciascun nodo della configurazione MetroCluster.

c. Verificare la presenza di eventuali avvisi sullo stato di salute:

   `system health alert show`

   Eseguire questo comando su ciascun cluster.

d. Verificare le licenze sui cluster:

   `system license show`

   Eseguire questo comando su ciascun cluster.

e. Verificare i dispositivi collegati ai nodi:

   `network device-discovery show`

   Eseguire questo comando su ciascun cluster.

f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

   `cluster date show`

Eseguire questo comando su ciascun cluster. È possibile utilizzare `cluster date` comandi per configurare l'ora e il fuso orario.

2. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

   `storage switch show`

   Eseguire questo comando su ciascun cluster.

3. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
   a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      `metrocluster show`

   b. Verificare che siano visualizzati tutti i nodi previsti:

      `metrocluster node show`

   c. Immettere il seguente comando:

      `metrocluster check run`

d. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

4. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.
   a. Scaricare ed eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Mappatura delle porte dai vecchi nodi ai nuovi nodi

È necessario pianificare la mappatura delle LIF sulle porte fisiche dei vecchi nodi alle porte fisiche dei nuovi nodi.

A proposito di questa attività

Quando il nuovo nodo viene avviato per la prima volta durante il processo di aggiornamento, riproduce la configurazione più recente del vecchio nodo che sta sostituendo. Quando si avvia Node_A_1-new, ONTAP tenta di ospitare le LIF sulle stesse porte utilizzate su Node_A_1-old. Pertanto, come parte dell'aggiornamento, è necessario regolare la configurazione della porta e della LIF in modo che sia compatibile con quella del vecchio nodo. Durante la procedura di aggiornamento, verranno eseguiti i passaggi sul vecchio e sul nuovo nodo per garantire la corretta configurazione LIF di cluster, gestione e dati.

La seguente tabella mostra esempi di modifiche alla configurazione relative ai requisiti di porta dei nuovi nodi.

Porte fisiche di interconnessione cluster		
Vecchio controller	Nuovo controller	Azione richiesta
e0a, e0b	e3a, e3b	Nessuna porta corrispondente. Dopo l'aggiornamento, è necessario ricreare le porte del cluster."Preparazione delle porte del cluster su un modulo controller esistente"
e0c, e0d	e0a,e0b,e0c,e0d	e0c e e0d corrispondono alle porte. Non è necessario modificare la configurazione, ma dopo l'aggiornamento è possibile distribuire le LIF del cluster tra le porte del cluster disponibili.

Fasi

1. Determinare quali porte fisiche sono disponibili sui nuovi controller e quali LIF possono essere ospitate sulle porte.

   L'utilizzo della porta del controller dipende dal modulo della piattaforma e dagli switch che verranno utilizzati nella configurazione IP di MetroCluster. È possibile ottenere l'utilizzo delle porte delle nuove piattaforme da "NetApp Hardware Universe".

   Identificare anche l'utilizzo dello slot per schede FC-VI.

2. Pianificare l'utilizzo delle porte e, se necessario, compilare le seguenti tabelle come riferimento per ciascuno dei nuovi nodi.

   Durante l'esecuzione della procedura di aggiornamento, fare riferimento alla tabella.

	Node_A_1-old			Node_A_1-new		
LIF	Porte	IPspaces	Domini di broadcast	Porte	IPspaces	Domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						
Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

Raccolta di informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, è necessario raccogliere informazioni per ciascuno dei vecchi nodi e, se necessario, regolare i domini di broadcast di rete, rimuovere eventuali VLAN e gruppi di interfacce e raccogliere informazioni sulla crittografia.

A proposito di questa attività

Questa attività viene eseguita sulla configurazione MetroCluster FC esistente.

Fasi

1. Etichettare i cavi per i controller esistenti, per consentire una facile identificazione dei cavi durante la configurazione dei nuovi controller.
2. Raccogliere gli ID di sistema dei nodi nella configurazione MetroCluster:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

Durante la procedura di aggiornamento, sostituisci questi vecchi ID di sistema con gli ID di sistema dei nuovi moduli controller.

In questo esempio, per una configurazione MetroCluster FC a quattro nodi, vengono recuperati i seguenti vecchi ID di sistema:

- Node_A_1-old: 4068741258
- Node_A_2-old: 4068741260
- Node_B_1-old: 4068741254
- Node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                      node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------- ------------------
-------------                   -------------------
--------------------              ----------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                       4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                       4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                        4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                       4068741260
4068741258
4 entries were displayed.
```

In questo esempio, per una configurazione MetroCluster FC a due nodi, vengono recuperati i seguenti vecchi ID di sistema:

- Node_A_1: 4068741258
- Node_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Raccogliere informazioni su porta e LIF per ciascun nodo precedente.

   Per ciascun nodo, è necessario raccogliere l'output dei seguenti comandi:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node` *`node-name`* `sysconfig -a`
4. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`
5. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

   ```
   security key-manager backup show
   ```

6. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

   Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

   a. Se Onboard Key Manager è configurato:

      ```
      security key-manager onboard show-backup
      ```

La passphrase sarà necessaria più avanti nella procedura di aggiornamento.

b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

```
security key-manager external show -instance
```

```
security key-manager key query
```

Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima della transizione.

Fasi

1. Rimuovere la configurazione MetroCluster esistente dal software Tiebreaker.

   "Rimozione delle configurazioni MetroCluster"

2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è in corso.

   a. Immettere il seguente comando:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   `maintenance-window-in-hours` specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Ripetere il comando sul cluster partner.

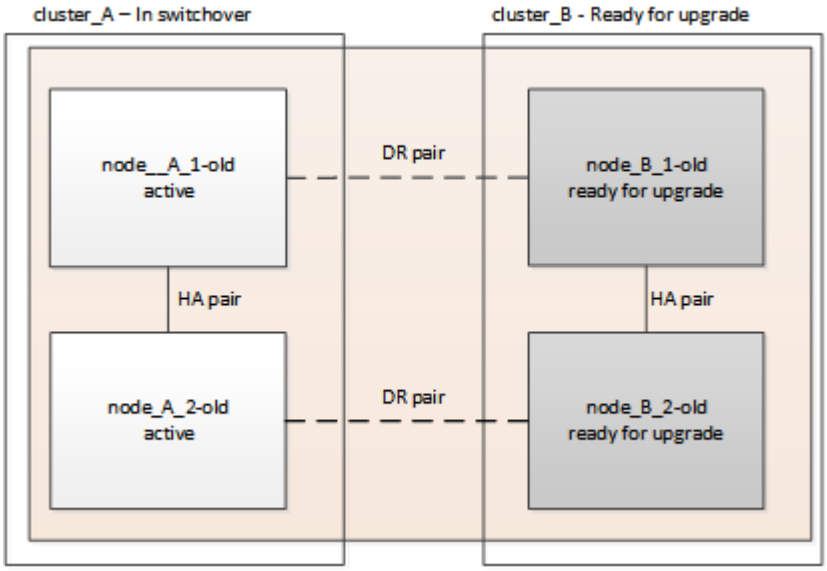
Passaggio alla configurazione MetroCluster

È necessario passare alla configurazione Site_A in modo che le piattaforme sul sito_B possano essere aggiornate.

A proposito di questa attività

Questa attività deve essere eseguita sul sito_A.

Al termine di questa attività, cluster_A è attivo e fornisce dati per entrambi i siti. Cluster_B è inattivo e pronto per iniziare il processo di aggiornamento, come mostrato nell'illustrazione seguente.



Fasi

1. Passare alla configurazione MetroCluster del sito_A in modo che i nodi del sito_B possano essere aggiornati:

   a. Selezionare l'opzione che corrisponde alla configurazione ed eseguire il comando corretto sul cluster_A:

   > **Opzione 1: Configurazione FC a quattro o otto nodi con ONTAP 9.8 o versione successiva**
   >
   > Eseguire il comando: `metrocluster switchover -controller-replacement true`
   >
   > **Opzione 2: Configurazione FC a due nodi con ONTAP 9.3 e versioni successive**
   >
   > Eseguire il comando: `metrocluster switchover`

   Il completamento dell'operazione può richiedere alcuni minuti.

   b. Monitorare il funzionamento dello switchover:

   ```
   metrocluster operation show
   ```

   c. Al termine dell'operazione, verificare che i nodi siano in stato di switchover:

   ```
   metrocluster show
   ```

d. Controllare lo stato dei nodi MetroCluster:

```
metrocluster node show
```

2. Riparare gli aggregati di dati.
   a. Riparare gli aggregati di dati:

```
metrocluster heal data-aggregates
```

   b. Verificare che l'operazione di riparazione sia completa eseguendo il `metrocluster operation show` comando sul cluster integro:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Riparare gli aggregati root.
   a. Riparare gli aggregati di dati:

```
metrocluster heal root-aggregates
```

   b. Verificare che l'operazione di riparazione sia completa eseguendo il `metrocluster operation show` comando sul cluster integro:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Preparazione della configurazione di rete dei vecchi controller

Per garantire che la rete riprenda correttamente sui nuovi controller, è necessario spostare i file LIF su una porta comune e rimuovere la configurazione di rete dei vecchi controller.

A proposito di questa attività

- Questa attività deve essere eseguita su ciascuno dei vecchi nodi.
- Verranno utilizzate le informazioni raccolte in "Mappatura delle porte dai vecchi nodi ai nuovi nodi".

Fasi

1. Avviare i vecchi nodi e quindi accedere ai nodi:

```
boot_ontap
```

2. Assegnare la porta home di tutti i file LIF di dati sul vecchio controller a una porta comune identica sia sul vecchio che sul nuovo modulo controller.

   a. Visualizzare le LIF:

      ```
      network interface show
      ```

      Tutti i dati LIFS, inclusi SAN e NAS, verranno gestiti e non verranno gestiti dal sistema operativo poiché sono attivi nel sito di switchover (cluster_A).

   b. Esaminare l'output per trovare una porta di rete fisica comune che sia la stessa sui controller vecchi e nuovi che non sia utilizzata come porta del cluster.

      Ad esempio, e0d è una porta fisica sui vecchi controller ed è presente anche sui nuovi controller. e0d non viene utilizzato come porta del cluster o in altro modo sui nuovi controller.

      Per informazioni sull'utilizzo delle porte per i modelli di piattaforma, consultare "NetApp Hardware Universe"

   c. Modificare tutti i dati LIFS per utilizzare la porta comune come porta home:

      network interface modify -vserver *svm-name* -lif *data-lif* -home-port *port-id*

      Nell'esempio seguente, questo è "e0d".

      Ad esempio:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modificare i domini di broadcast per rimuovere la vlan e le porte fisiche che devono essere eliminate:

   broadcast-domain remove-ports -broadcast-domain *broadcast-domain-name* -ports *node-name:port-id*

   Ripetere questo passaggio per tutte le porte VLAN e fisiche.

4. Rimuovere tutte le porte VLAN utilizzando le porte del cluster come porte membro e ifgrps utilizzando le porte del cluster come porte membro.

   a. Elimina porte VLAN:

      network port vlan delete -node *node-name* -vlan-name *portid-vlandid*

      Ad esempio:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

   b. Rimuovere le porte fisiche dai gruppi di interfacce:

```
network port ifgrp remove-port -node node-name -ifgrp interface-group-name
-port portid
```

Ad esempio:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Rimuovere le porte della VLAN e del gruppo di interfacce dal dominio di broadcast:

```
network port broadcast-domain remove-ports -ipspace ipspace -broadcast
-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..
```

b. Modificare le porte del gruppo di interfacce per utilizzare altre porte fisiche come membro in base alle necessità.:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Arrestare i nodi:

```
halt -inhibit-takeover true -node node-name
```

Questa operazione deve essere eseguita su entrambi i nodi.

Rimozione delle vecchie piattaforme

I vecchi controller devono essere rimossi dalla configurazione.

A proposito di questa attività

Questa attività viene eseguita sul sito_B.

Fasi

1. Connettersi alla console seriale dei vecchi controller (Node_B_1-old e Node_B_2-old) nel sito_B e verificare che venga visualizzato il prompt DEL CARICATORE.
2. Scollegare le connessioni di storage e di rete su Node_B_1-old e Node_B_2-old ed etichettare i cavi in modo che possano essere ricollegati ai nuovi nodi.
3. Scollegare i cavi di alimentazione da Node_B_1-old e Node_B_2-old.
4. Rimuovere i controller Node_B_1-old e Node_B_2-old dal rack.

Configurazione dei nuovi controller

È necessario eseguire il rack e installare i controller, eseguire la configurazione richiesta in modalità manutenzione, quindi avviare i controller e verificare la configurazione LIF sui controller.

Configurazione dei nuovi controller

I nuovi controller devono essere montati in rack e cablati.

Fasi

1. Pianificare il posizionamento dei nuovi moduli controller e degli shelf di storage in base alle necessità.

Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di shelf di storage nella configurazione.

2. Mettere a terra l'utente.
3. Installare i moduli controller nel rack o nell'armadietto.

   "Documentazione dei sistemi hardware ONTAP"

4. Se i nuovi moduli controller non sono dotati di schede FC-VI e se le schede FC-VI dei vecchi controller sono compatibili con i nuovi controller, sostituire le schede FC-VI e installarle negli slot corretti.

   Vedere "NetApp Hardware Universe" Per informazioni sugli slot per schede FC-VI.

5. Collegare l'alimentazione, la console seriale e le connessioni di gestione dei controller come descritto nelle *Guide di installazione e configurazione di MetroCluster*.

   Non collegare altri cavi scollegati dai vecchi controller in questo momento.

   "Documentazione dei sistemi hardware ONTAP"

6. Accendere i nuovi nodi e premere Ctrl-C quando richiesto per visualizzare il prompt DEL CARICATORE.

Avvio in rete dei nuovi controller

Dopo aver installato i nuovi nodi, è necessario eseguire il netboot per assicurarsi che i nuovi nodi eseguano la stessa versione di ONTAP dei nodi originali. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

Questa attività viene eseguita su ciascuno dei nuovi moduli controller.

Fasi

1. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il file ontap-version_image.tgz in una directory accessibile dal Web.
3. Accedere alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

Se il modello di piattaforma è…	Quindi…
Sistemi della serie FAS/AFF8000	Estrarre il contenuto del file ontap-version_image.tgznella directory di destinazione: Tar -zxvf ontap-version_image.tgz NOTA: Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine netboot. L'elenco delle directory deve contenere una cartella netboot con un file kernel:netboot/kernel
Tutti gli altri sistemi	L'elenco delle directory deve contenere una cartella netboot con un file del kernel: ontap-version_image.tgz non è necessario estrarre il file ontap-version_image.tgz.

4. Al prompt DEL CARICATORE, configurare la connessione netboot per una LIF di gestione:

- Se l'indirizzo IP è DHCP, configurare la connessione automatica:

  ```
  ifconfig e0M -auto
  ```

- Se l'indirizzo IP è statico, configurare la connessione manuale:

  ```
  ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
  ```

5. Eseguire il netboot.
   - Se la piattaforma è un sistema della serie 80xx, utilizzare questo comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se la piattaforma è un altro sistema, utilizzare il seguente comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se viene richiesto di continuare la procedura, immettere `y`E quando
   viene richiesto il pacchetto, inserire l'URL del file immagine:
   `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Riavviare immettendo `y` quando viene visualizzato un prompt simile a quanto segue:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è

necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   ```
   set-defaults
   ```

3. Salvare l'ambiente:

   ```
   saveenv
   ```

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

   ```
   boot_ontap menu
   ```

5. Al prompt del menu di avvio, cancellare la configurazione:

   ```
   wipeconfig
   ```

   Rispondere `yes` al prompt di conferma.

   Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Ripristino della configurazione HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:

   a. Verificare le impostazioni correnti delle porte: `ucadmin show`

   b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*

Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

2. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

3. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

   ```
   boot_ontap maint
   ```

4. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Impostazione dello stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Lo stato ha per tutti i componenti deve essere mcc.

Se la configurazione MetroCluster ha…	Lo stato ha deve essere…
Due nodi	mcc-2n
Quattro o otto nodi	mcc

2. Se lo stato di sistema visualizzato del controller non è corretto, impostare lo stato ha per il modulo controller e lo chassis:

Se la configurazione MetroCluster ha…	Eseguire questi comandi…

Due nodi	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Quattro o otto nodi	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Riassegnazione dei dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando i sistemi raccolti in precedenza

A proposito di questa attività

Questa attività viene eseguita in modalità manutenzione.

I vecchi ID di sistema sono stati identificati in "Raccolta di informazioni prima dell'aggiornamento".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Nodo	Vecchio ID di sistema	Nuovo ID di sistema
Node_B_1	4068741254	1574774970

Fasi

1. Collegare tutti gli altri collegamenti ai nuovi moduli controller (FC-VI, storage, interconnessione cluster, ecc.).
2. Arrestare il sistema e avviare la modalità di manutenzione dal prompt DEL CARICATORE:

   ```
   boot_ontap maint
   ```

3. Visualizzare i dischi di proprietà di Node_B_1-old:

   ```
   disk show -a
   ```

   L'output del comando mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi aggregati root sono ancora di proprietà del vecchio ID di sistema (4068741254). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Riassegnare i dischi aggregati root sugli shelf di dischi al nuovo controller:

   `disk reassign -s *old-sysid* -d *new-sysid*`

   L'esempio seguente mostra la riassegnazione dei dischi:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verificare che tutti i dischi siano riassegnati come previsto:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Visualizzare lo stato dell'aggregato:

   ```
   aggr status
   ```

   ```
   *> aggr status
              Aggr             State       Status           Options
   aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                            mirrored
   mirror_resync_priority=high(fixed)
                            fast zeroed
                            64-bit
   ```

7. Ripetere i passaggi precedenti sul nodo partner (Node_B_2-new).

Avviare i nuovi controller

Riavviare i controller dal menu di avvio per aggiornare l'immagine flash del controller. Se la crittografia è configurata, sono necessari ulteriori passaggi.

A proposito di questa attività

Questa attività deve essere eseguita su tutti i nuovi controller.

Fasi

1. Arrestare il nodo:

   ```
   halt
   ```

2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address

   setenv bootarg.kmip.init.interface interface-id
   ```

3. Visualizzare il menu di avvio:

   ```
   boot_ontap menu
   ```

4. Se viene utilizzata la crittografia root, a seconda della versione di ONTAP in uso, selezionare l'opzione del menu di avvio o immettere il comando del menu di avvio per la configurazione della gestione delle chiavi.

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, selezionare l'opzione del menu di avvio.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione "10" Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione "11" Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

ONTAP 9.7 e versioni precedenti

Per ONTAP 9.7 e versioni precedenti, eseguire il comando del menu di avvio.

Se si utilizza…	Eseguire questo comando al prompt del menu di avvio…
Gestione delle chiavi integrata	`recover_onboard_keymanager`
Gestione esterna delle chiavi	`recover_external_keymanager`

5. Se l'autoboot è attivato, interrompere l'autoboot premendo CTRL-C.
6. Dal menu di boot, eseguire l'opzione "6".

   L'opzione "6" riavvia il nodo due volte prima del completamento.

   Rispondere "y" alle richieste di modifica dell'id di sistema. Attendere i secondi messaggi di riavvio:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Verificare che il sistema partner sia corretto:

   ```
   printenv partner-sysid
   ```

   Se il partner-sysid non è corretto, impostarlo:

   ```
   setenv partner-sysid partner-sysID
   ```

8. Se viene utilizzata la crittografia root, a seconda della versione di ONTAP in uso, selezionare l'opzione del menu di avvio oppure eseguire nuovamente il comando del menu di avvio per la configurazione della gestione delle chiavi.

ONTAP 9.8 e versioni successive

A partire da ONTAP 9.8, selezionare l'opzione del menu di avvio.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione "10" Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione "11" Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

A seconda dell'impostazione del gestore delle chiavi, eseguire la procedura di ripristino selezionando l'opzione "10" o l'opzione "11", quindi l'opzione "6" al primo prompt del menu di avvio. Per avviare completamente i nodi, potrebbe essere necessario ripetere la procedura di ripristino, continua con l'opzione "1" (boot normale).

ONTAP 9.7 e versioni precedenti

Per ONTAP 9.7 e versioni precedenti, eseguire il comando del menu di avvio.

Se si utilizza…	Eseguire questo comando al prompt del menu di avvio…
Gestione delle chiavi integrata	`recover_onboard_keymanager`
Gestione esterna delle chiavi	`recover_external_keymanager`

Potrebbe essere necessario eseguire il `recover_xxxxxxxx_keymanager` al prompt del menu di boot più volte fino a quando i nodi non si avviano completamente.

9. Avviare i nodi:

```
boot_ontap
```

10. Attendere l'avvio dei nodi sostituiti.

    Se uno dei nodi è in modalità Takeover, eseguire un giveback:

```
storage failover giveback
```

11. Verificare che tutte le porte si trovino in un dominio di trasmissione:

    a. Visualizzare i domini di trasmissione:

    ```
    network port broadcast-domain show
    ```

    b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

    "Aggiunta o rimozione di porte da un dominio di broadcast"

    c. Aggiungere la porta fisica che ospiterà le LIF dell'intercluster al dominio Broadcast corrispondente.

    d. Modificare le LIF dell'intercluster per utilizzare la nuova porta fisica come porta home.

    e. Dopo aver attivato le LIF dell'intercluster, controllare lo stato del peer del cluster e ristabilire il peering del cluster secondo necessità.

    Potrebbe essere necessario riconfigurare il peering del cluster.

    "Creazione di una relazione peer del cluster"

    f. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

    L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

    "Creazione di una VLAN"

    "Combinazione di porte fisiche per creare gruppi di interfacce"

12. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Verifica della configurazione LIF in corso

Verificare che i file LIF siano ospitati su nodi/porte appropriati prima di passare al switchback. È necessario eseguire le seguenti operazioni

A proposito di questa attività

Questa attività viene eseguita sul sito_B, dove i nodi sono stati avviati con aggregati root.

Fasi

1. Verificare che i file LIF siano ospitati sul nodo e sulle porte appropriati prima di passare al switchback.

a. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

b. Eseguire l'override della configurazione della porta per garantire il corretto posizionamento di LIF:

```
vserver config override -command "network interface modify -vserver
vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
new_node_name"
```

Quando si accede a. `network interface modify` all'interno di `vserver config override` non è possibile utilizzare la funzione di completamento automatico della scheda. È possibile creare `network interface modify` utilizzando il completamento automatico e quindi racchiuderlo in `vserver config override` comando.

a. Tornare al livello di privilegio admin:
`set -privilege admin`

2. Ripristinare le interfacce nel nodo principale:

```
network interface revert * -vserver vserver-name
```

Eseguire questo passaggio su tutte le SVM secondo necessità.

Installare le nuove licenze

Prima dell'operazione di switchback, è necessario installare le licenze per i nuovi controller.

Fasi

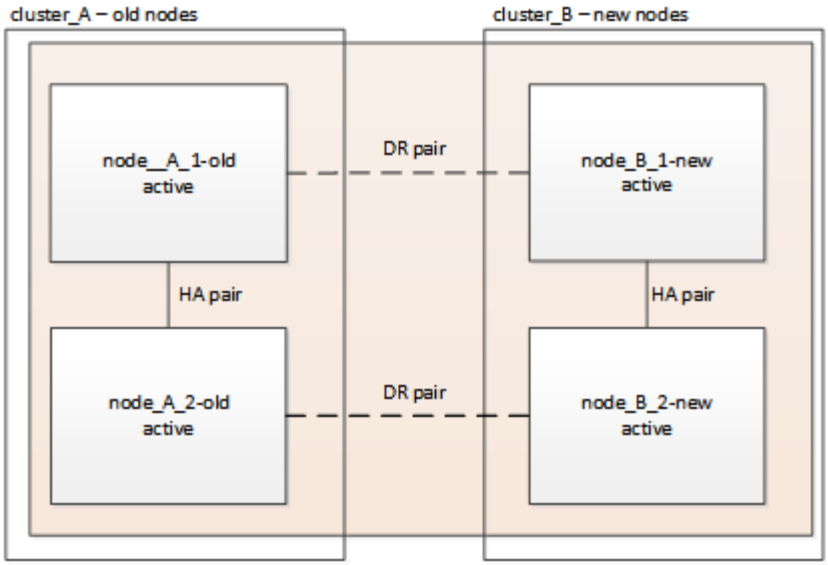
1. "Installazione delle licenze per il nuovo modulo controller"

Tornare indietro alla configurazione MetroCluster

Una volta configurati i nuovi controller, si torna alla configurazione MetroCluster per ripristinare il normale funzionamento della configurazione.

A proposito di questa attività

Questa attività consente di eseguire l'operazione di switchback, ripristinando il normale funzionamento della configurazione MetroCluster. I nodi sul sito_A sono ancora in attesa di aggiornamento.



Fasi

1. Eseguire il `metrocluster node show` Su Site_B e controllare l'output.
   a. Verificare che i nuovi nodi siano rappresentati correttamente.
   b. Verificare che i nuovi nodi siano nello stato "in attesa di switchback".
2. Switchback del cluster:

   ```
   metrocluster switchback
   ```

3. Controllare l'avanzamento dell'operazione di switchback:

   ```
   metrocluster show
   ```

   L'operazione di switchback è ancora in corso quando viene visualizzato l'output `waiting-for-switchback`:

   ```
   cluster_B::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_B         Configuration state configured
                             Mode                switchover
                             AUSO Failure Domain -
   Remote: cluster_A         Configuration state configured
                             Mode                waiting-for-switchback
                             AUSO Failure Domain -
   ```

   L'operazione di switchback viene completata quando viene visualizzato l'output `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando. Questo comando si trova al livello di privilegio avanzato.

Verifica dello stato della configurazione di MetroCluster

Dopo aver aggiornato i moduli controller, è necessario verificare lo stato della configurazione MetroCluster.

A proposito di questa attività

Questa attività può essere eseguita su qualsiasi nodo della configurazione MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster:

   a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

   `metrocluster show`

   b. Eseguire un controllo MetroCluster:

   `metrocluster check run`

   c. Visualizzare i risultati del controllo MetroCluster:

   `metrocluster check show`

   > Dopo aver eseguito `metrocluster check run` e. `metrocluster check show`viene visualizzato un messaggio di errore simile al seguente:

Esempio

```
Failed to validate the node and cluster components before the switchover
operation.
                  Cluster_A:: node_A_1 (non-overridable veto): DR
partner NVLog mirroring is not online. Make sure that the links between
the two sites are healthy and properly configured.
```

+ Si tratta di un comportamento previsto dovuto a una mancata corrispondenza del controller durante il

processo di aggiornamento e il messaggio di errore può essere ignorato in modo sicuro.

Aggiornamento dei nodi sul cluster_A.

È necessario ripetere le attività di aggiornamento su cluster_A.

Fase

1. Ripetere i passaggi per aggiornare i nodi sul cluster_A, iniziando da "Preparazione per l'aggiornamento".

   Durante l'esecuzione delle attività, tutti i riferimenti di esempio ai cluster e ai nodi vengono invertiti. Ad esempio, quando l'esempio viene dato allo switchover da cluster_A, si passa da cluster_B.

Invio di un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completato l'aggiornamento, inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

Fase

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.
   a. Immettere il seguente comando:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   b. Ripetere il comando sul cluster partner.

Ripristino del monitoraggio di Tiebreaker

Se la configurazione MetroCluster è stata precedentemente configurata per il monitoraggio da parte del software Tiebreaker, è possibile ripristinare la connessione Tiebreaker.

1. Attenersi alla procedura descritta in "Aggiunta di configurazioni MetroCluster" In *Installazione e configurazione di MetroCluster Tiebreaker*.

Upgrade dei controller da AFF A700/FAS9000 a AFF A900/FAS9500 in una configurazione MetroCluster FC utilizzando switchover e switchback (ONTAP 9.10.1 o versione successiva)

È possibile utilizzare l'operazione di switchover MetroCluster per fornire un servizio senza interruzioni ai client mentre i moduli controller sul cluster partner vengono aggiornati. Non è possibile aggiornare altri componenti (ad esempio shelf di storage o switch) come parte di questa procedura.

A proposito di questa attività

- Questa procedura può essere utilizzata solo per l'aggiornamento del controller.

  Non è possibile aggiornare contemporaneamente altri componenti della configurazione, ad esempio shelf di storage o switch.

- È possibile utilizzare questa procedura per aggiornare un AFF A700 a AFF A900 con ONTAP 9.10.1 e versioni successive.
- È possibile utilizzare questa procedura per aggiornare FAS9000 a FAS9500 con ONTAP 9.10.1P3 e versioni successive.
  - Le configurazioni a quattro e otto nodi sono supportate in ONTAP 9.10.1 e versioni successive.

    Il sistema AFF A900 è supportato solo in ONTAP 9.10.1 o versione successiva.

  "NetApp Hardware Universe"

- Tutti i controller della configurazione devono essere aggiornati durante lo stesso periodo di manutenzione.

  La tabella seguente mostra la matrice dei modelli supportata per l'aggiornamento del controller.

Vecchio modello di piattaforma	Nuovo modello di piattaforma
• AFF A700	• AFF A900
• FAS9000	• FAS9500

- Durante la procedura di aggiornamento, è necessario modificare il fabric MetroCluster, inclusi l'RCF e le modifiche fisiche del cablaggio. È possibile eseguire le modifiche RCF e cablaggio prima di eseguire l'aggiornamento del controller.
- Questa procedura di aggiornamento non richiede la modifica delle connessioni storage, FC ed Ethernet tra i nodi originali e i nuovi nodi.
- Durante la procedura di aggiornamento, non aggiungere o rimuovere altre schede dal sistema AFF A700 o FAS9000. Per ulteriori informazioni, consultare "NetApp Hardware Universe"

I seguenti nomi di esempio vengono utilizzati negli esempi e nella grafica di questa procedura:

- Sito_A.
  - Prima dell'aggiornamento:
    - Node_A_1-A700
    - Node_A_2-A700
  - Dopo l'aggiornamento:
    - Node_A_1-A900
    - Node_A_2-A900
- Sito_B
  - Prima dell'aggiornamento:
    - Node_B_1-A700
    - Node_B_2-A700
  - Dopo l'aggiornamento:
    - Node_B_1-A900
    - Node_B_2-A900

Preparatevi per l'aggiornamento

Prima di apportare modifiche alla configurazione MetroCluster esistente, è necessario verificare lo stato della configurazione, modificare i file RCF e il cablaggio in modo che corrispondano alla nuova topologia di connettività della porta richiesta per la configurazione AFF A900 o FAS9000 Fabric MetroCluster ed eseguire altre attività varie.

Liberare lo slot 7 sul controller AFF A700

La configurazione MetroCluster su AFF A900 o FAS9500 richiede 8 porte FC-VI su schede FC-VI negli slot 5 e 7. Prima di iniziare l'aggiornamento, se sono presenti schede nello slot 7 del sistema AFF A700 o FAS9000, è necessario spostarle in altri slot per tutti i nodi del cluster.

Verificare lo stato della configurazione MetroCluster

Prima di aggiornare i file RCF e il cablaggio per la configurazione AFF A900 o FAS9500 Fabric MetroCluster, è necessario verificare lo stato e la connettività della configurazione.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che i nodi siano multipathing:
   `node run -node node-name sysconfig -a`

      Eseguire questo comando per ogni nodo della configurazione MetroCluster.

   b. Verificare che non vi siano dischi rotti nella configurazione:

      ```
      storage disk show -broken
      ```

      Eseguire questo comando su ciascun nodo della configurazione MetroCluster.

   c. Verificare la presenza di eventuali avvisi sullo stato di salute:

      ```
      system health alert show
      ```

      Eseguire questo comando su ciascun cluster.

   d. Verificare le licenze sui cluster:

      ```
      system license show
      ```

      Eseguire questo comando su ciascun cluster.

   e. Verificare i dispositivi collegati ai nodi:

      ```
      network device-discovery show
      ```

      Eseguire questo comando su ciascun cluster.

   f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

      ```
      cluster date show
      ```

Eseguire questo comando su ciascun cluster. È possibile utilizzare `cluster date` comandi per configurare l'ora e il fuso orario.

2. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

   ```
   storage switch show
   ```

   Eseguire questo comando su ciascun cluster.

3. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
   a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      ```
      metrocluster show
      ```

   b. Verificare che siano visualizzati tutti i nodi previsti:

      ```
      metrocluster node show
      ```

   c. Immettere il seguente comando:

      ```
      metrocluster check run
      ```

   d. Visualizzare i risultati del controllo MetroCluster:

      ```
      metrocluster check show
      ```

4. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.
   a. Scaricare ed eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Aggiornare i file RCF dello switch fabric

Il fabric MetroCluster AFF A900 o FAS9500 richiede due adattatori FC-VI a quattro porte per nodo rispetto a un singolo adattatore FC-VI a quattro porte richiesto da un AFF A700. Prima di avviare l'aggiornamento del controller al controller AFF A900 o FAS9500, è necessario modificare i file RCF dello switch fabric per supportare la topologia di connessione AFF A900 o FAS9500.

1. Dal "Pagina di download del file MetroCluster RCF", Scaricare il file RCF corretto per un Fabric MetroCluster AFF A900 o FAS9500 e il modello di switch in uso nella configurazione AFF A700 o FAS9000.
2. aggiornare il file RCF sugli switch fabric A, sullo switch A1 e sullo switch B1 seguendo la procedura descritta in "Configurazione degli switch FC".

   > L'aggiornamento del file RCF per il supporto della configurazione AFF A900 o FAS9500 Fabric MetroCluster non influisce sulla porta e sulle connessioni utilizzate per la configurazione AFF A700 o FAS9000 Fabric MetroCluster.

3. Dopo aver aggiornato i file RCF sugli switch fabric A, tutte le connessioni storage e FC-VI dovrebbero essere online. Controllare le connessioni FC-VI:

```
metrocluster interconnect mirror show
```

   a. Verificare che i dischi del sito locale e remoto siano elencati nella `sysconfig` output.

4. è necessario verificare che MetroCluster sia in buono stato dopo l'aggiornamento del file RCF per gli switch fabric A.

   a. Controllare le connessioni del cluster della metropolitana: `metrocluster interconnect mirror show`

   b. Eseguire il controllo MetroCluster: `metrocluster check run`

   c. Vedere i risultati dell'esecuzione di MetroCluster al termine dell'esecuzione: `metrocluster check show`

5. Aggiornare gli switch fabric B (switch 2 e 4) ripetendo la procedura Fase 2 a. Fase 5.

Verificare lo stato della configurazione MetroCluster dopo l'aggiornamento del file RCF

Prima di eseguire l'aggiornamento, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che i nodi siano multipathing:
   `node run -node node-name sysconfig -a`

   Eseguire questo comando per ogni nodo della configurazione MetroCluster.

   b. Verificare che non vi siano dischi rotti nella configurazione:

   ```
   storage disk show -broken
   ```

   Eseguire questo comando su ciascun nodo della configurazione MetroCluster.

   c. Verificare la presenza di eventuali avvisi sullo stato di salute:

   ```
   system health alert show
   ```

   Eseguire questo comando su ciascun cluster.

   d. Verificare le licenze sui cluster:

   ```
   system license show
   ```

   Eseguire questo comando su ciascun cluster.

   e. Verificare i dispositivi collegati ai nodi:

   ```
   network device-discovery show
   ```

   Eseguire questo comando su ciascun cluster.

   f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

```
cluster date show
```

Eseguire questo comando su ciascun cluster. È possibile utilizzare `cluster date` comandi per configurare l'ora e il fuso orario.

2. Verificare la presenza di eventuali avvisi sullo stato di salute sugli switch (se presenti):

   ```
   storage switch show
   ```

   Eseguire questo comando su ciascun cluster.

3. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
   a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

      ```
      metrocluster show
      ```

   b. Verificare che siano visualizzati tutti i nodi previsti:

      ```
      metrocluster node show
      ```

   c. Immettere il seguente comando:

      ```
      metrocluster check run
      ```

   d. Visualizzare i risultati del controllo MetroCluster:

      ```
      metrocluster check show
      ```

4. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.
   a. Scaricare ed eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Mappare le porte dai nodi AFF A700 o FAS9000 ai nodi AFF A900 o FAS9500

Durante il processo di aggiornamento del controller, è necessario modificare solo le connessioni indicate in questa procedura.

Se i controller AFF A700 o FAS9000 dispongono di una scheda nello slot 7, spostarla in un altro slot prima di avviare la procedura di aggiornamento del controller. È necessario disporre dello slot 7 per aggiungere il secondo adattatore FC-VI necessario per il funzionamento di Fabric MetroCluster sui controller AFF A900 o FAS9500.

Raccogliere informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, è necessario raccogliere informazioni per ciascuno dei vecchi nodi e, se necessario, regolare i domini di broadcast di rete, rimuovere eventuali VLAN e gruppi di interfacce e raccogliere informazioni sulla crittografia.

A proposito di questa attività

Questa attività viene eseguita sulla configurazione MetroCluster FC esistente.

Fasi

1. Raccogliere gli ID di sistema del nodo di configurazione MetroCluster:

   `metrocluster node show -fields node-systemid,dr-partner-systemid`

   Durante la procedura di aggiornamento, sostituisci questi vecchi ID di sistema con gli ID di sistema dei moduli controller.

   In questo esempio, per una configurazione MetroCluster FC a quattro nodi, vengono recuperati i seguenti vecchi ID di sistema:

   - Node_A_1-A700: 537037649
   - Node_A_2-A700: 537407030
   - Node_B_1-A700: 0537407114
   - Node_B_2-A700: 537035354

   ```
   Cluster_A::*> metrocluster node show -fields node-systemid,ha-partner-
   systemid,dr-partner-systemid,dr-auxiliary-systemid
   dr-group-id cluster    node           node-systemid ha-partner-systemid
   dr-partner-systemid dr-auxiliary-systemid
   ----------- ------------------------- ------------- -------------------
   ------------------- ---------------------
   1           Cluster_A  nodeA_1-A700   537407114     537035354
   537411005           537410611
   1           Cluster_A  nodeA_2-A700   537035354     537407114
   537410611           537411005
   1           Cluster_B  nodeB_1-A700   537410611     537411005
   537035354           537407114
   1           Cluster_B  nodeB_2-A700   537411005

   4 entries were displayed.
   ```

2. Raccogliere informazioni su porta e LIF per ciascun nodo precedente.

   Per ciascun nodo, è necessario raccogliere l'output dei seguenti comandi:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`

- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

3. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

4. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

   ```
   security key-manager backup show
   ```

5. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

   Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

   a. Se Onboard Key Manager è configurato:

      ```
      security key-manager onboard show-backup
      ```

      La passphrase sarà necessaria più avanti nella procedura di aggiornamento.

   b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

      ```
      security key-manager external show -instance
      ```

   ```
   security key-manager key query
   ```

Rimuovere la configurazione esistente dallo spareggio o da un altro software di monitoraggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima della transizione.

Fasi

1. Rimuovere la configurazione MetroCluster esistente dal software Tiebreaker.

   "Rimozione delle configurazioni MetroCluster"

2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Inviare un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è in corso.

   a. Immettere il seguente comando:

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Ripetere il comando sul cluster partner.

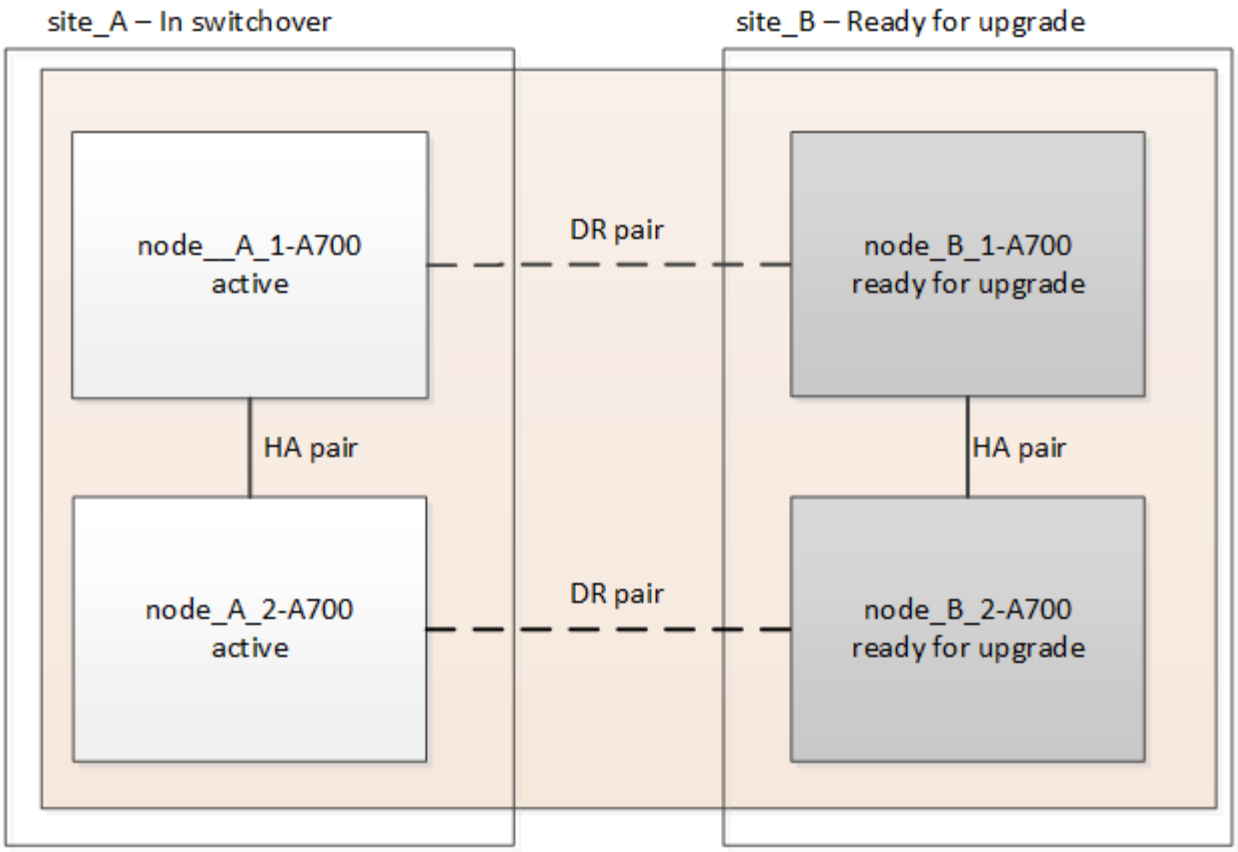
Passare alla configurazione MetroCluster

È necessario passare alla configurazione Site_A in modo che le piattaforme sul sito_B possano essere aggiornate.

A proposito di questa attività

Questa attività deve essere eseguita sul sito_A.

Dopo aver completato questa attività, Site_A è attivo e fornisce dati per entrambi i siti. Site_B è inattivo e pronto per iniziare il processo di aggiornamento, come mostrato nell'illustrazione seguente. (Questa illustrazione si applica anche all'aggiornamento di un controller FAS9000 a un controller FAS9500).



Fasi

1. Passare alla configurazione MetroCluster del sito_A in modo che i nodi del sito_B possano essere aggiornati:

   a. Eseguire il seguente comando sul sito_A:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Il completamento dell'operazione può richiedere alcuni minuti.

   a. Monitorare il funzionamento dello switchover:

   ```
   metrocluster operation show
   ```

   b. Al termine dell'operazione, verificare che i nodi siano in stato di switchover:

   ```
   metrocluster show
   ```

   c. Controllare lo stato dei nodi MetroCluster:

   ```
   metrocluster node show
   ```

2. Riparare gli aggregati di dati.

   a. Riparare gli aggregati di dati:

   ```
   metrocluster heal data-aggregates
   ```

b. Verificare che l'operazione di riparazione sia completa eseguendo il `metrocluster operation show` comando sul cluster integro:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Riparare gli aggregati root.

   a. Riparare gli aggregati di dati:

   ```
   metrocluster heal root-aggregates
   ```

   b. Verificare che l'operazione di riparazione sia completa eseguendo il `metrocluster operation show` comando sul cluster integro:

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2020 20:58:41
      End Time: 7/29/2020 20:59:42
        Errors: -
   ```

Rimuovere il modulo controller AFF A700 o FAS9000 e il modulo NVS sul sito_B.

È necessario rimuovere i vecchi controller dalla configurazione.

Questa attività viene eseguita sul sito_B.

Prima di iniziare

Se non si è già collegati a terra, mettere a terra l'utente.

Fasi

1. Connettersi alla console seriale dei vecchi controller (Node_B_1-700 e Node_B_2-700) nel sito_B e verificare che venga visualizzato `LOADER` prompt.
2. Raccogliere i valori di bootarg da entrambi i nodi nel sito_B: `printenv`
3. Spegnere lo chassis sul sito_B.

Rimuovere il modulo controller e NVS da entrambi i nodi in Site_B.

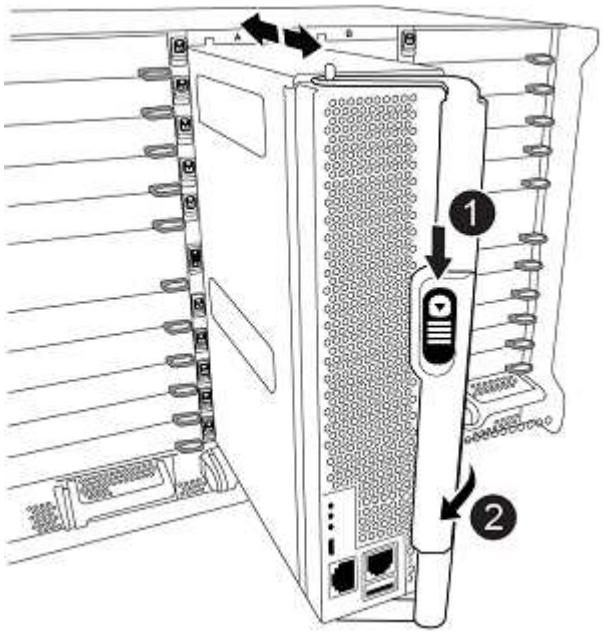
Rimuovere il modulo del controller AFF A700 o FAS9000

Utilizzare la seguente procedura per rimuovere il modulo controller AFF A700 o FAS9000.

Fasi

1. Scollegare il cavo della console, se presente, e il cavo di gestione dal modulo controller prima di rimuovere il modulo controller.
2. Sbloccare e rimuovere il modulo controller dal telaio.

   a. Far scorrere il pulsante arancione sulla maniglia della camma verso il basso fino a sbloccarla.



1	Pulsante di rilascio della maniglia della camma
2	Maniglia CAM

   a. Ruotare la maniglia della camma in modo da disimpegnare completamente il modulo controller dal telaio, quindi estrarre il modulo controller dal telaio. Assicurarsi di sostenere la parte inferiore del modulo controller mentre lo si sposta fuori dallo chassis.

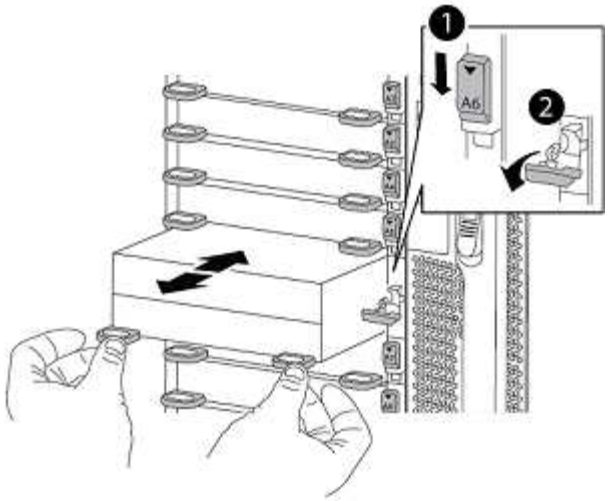
Rimuovere il modulo NVS AFF A700 o FAS9000

Per rimuovere il modulo NVS AFF A700 o FAS9000, attenersi alla seguente procedura.

> Il modulo NVS AFF A700 o FAS9000 si trova nello slot 6 e presenta un'altezza doppia rispetto agli altri moduli del sistema.

1. Sbloccare e rimuovere l'NVS dallo slot 6.

   a. Premere il tasto contrassegnato e numerato CAM. Il pulsante CAM si allontana dal telaio.
   b. Ruotare il fermo della camma verso il basso fino a portarlo in posizione orizzontale. Il sistema NVS si disinnesta dal telaio e si sposta di pochi centimetri.
   c. Rimuovere l'NVS dal telaio tirando le linguette di estrazione ai lati della superficie del modulo.



	Latch i/o Cam intestato e numerato
	Fermo i/o completamente sbloccato

- Non trasferire moduli aggiuntivi utilizzati come dispositivi di coredump sul modulo di storage non volatile AFF A700 nello slot 6 al modulo AFF A900 NVS. Non trasferire alcuna parte dal controller AFF A700 e dai moduli NVS al modulo controller AFF A900.
- Per gli aggiornamenti da FAS9000 a FAS9500, è necessario trasferire solo i moduli Flash cache sul modulo FAS9000 NVS al modulo FAS9500 NVS. Non trasferire altre parti dal controller FAS9000 e dai moduli NVS al modulo controller FAS9500.

Installare il modulo NVS e controller AFF A900 o FAS9500

È necessario installare il modulo NVS e controller AFF A900 o FAS9500 dal kit di aggiornamento su entrambi i nodi nel sito_B. Non spostare il dispositivo di coredump dal modulo NVS AFF A700 o FAS9000 al modulo NVS AFF A900 o FAS9500.

Prima di iniziare

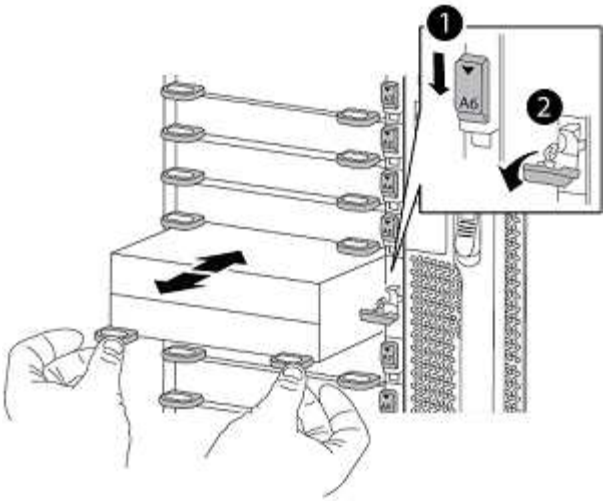
Se non si è già collegati a terra, mettere a terra l'utente.

Installare AFF A900 o FAS9500 NVS

Utilizzare la seguente procedura per installare AFF A900 o FAS9500 NVS nello slot 6 di entrambi i nodi nel sito_B.

Fasi

1. Allineare l'NVS con i bordi dell'apertura dello chassis nello slot 6.
2. Far scorrere delicatamente l'NVS nello slot fino a quando il dispositivo di chiusura della camma i/o con lettere e numeri non inizia a impegnarsi con il perno della camma i/o, quindi spingere il dispositivo di chiusura della camma i/o fino in fondo per bloccare l'NVS in posizione.



	Latch i/o Cam intestato e numerato
	Fermo i/o completamente sbloccato

Installare il modulo controller AFF A900 o FAS9500

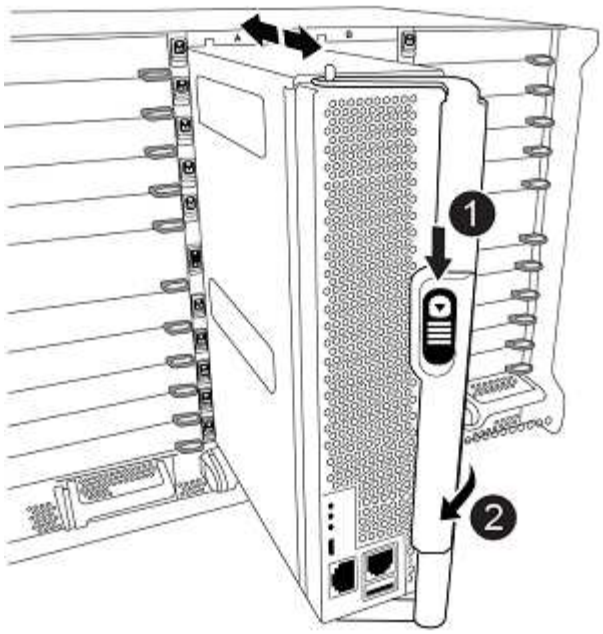
Utilizzare la seguente procedura per installare il modulo controller AFF A900 o FAS9500.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
2. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito.

   Non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio per evitare di danneggiare i connettori.

3. Collegare le porte di gestione e console al modulo controller.



	Pulsante di rilascio della maniglia della camma
	Maniglia CAM

4. Installare la seconda scheda X91129A nello slot 7 di ciascun nodo.
   a. Collegare le porte FC-VI dallo slot 7 agli switch. Fare riferimento a. "Installazione e configurazione fabric-attached" Documentazione e consultare i requisiti di connessione AFF A900 o FAS9500 Fabric MetroCluster per il tipo di switch nell'ambiente in uso.
5. Accendere lo chassis e collegarlo alla console seriale.
6. Dopo l'inizializzazione del BIOS, se il nodo inizia a eseguire l'autoboot, interrompere L'AUTOBOOT premendo Control-C.
7. Dopo aver interrotto l'autoboot, i nodi si fermano al prompt DEL CARICATORE. Se non si interrompe l'avvio automatico in tempo e node1 inizia l'avvio, attendere che venga visualizzato il prompt Control-C per accedere al menu di avvio. Dopo che il nodo si è arrestato nel menu di boot, usare l'opzione 8 per riavviare il nodo e interrompere l'autoboot durante il riavvio.
8. Su `LOADER` prompt, impostare le variabili di ambiente predefinite: `set-defaults`
9. Salvare le impostazioni predefinite delle variabili di ambiente: `saveenv`

NetBoot dei nodi nel sito_B.

Dopo aver scambiato il modulo controller AFF A900 o FAS9500 e NVS, è necessario eseguire il netboot dei nodi AFF A900 o FAS9500 e installare la stessa versione e lo stesso livello di patch ONTAP in esecuzione sul cluster. Il termine `netboot` Indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per `netboot`, È necessario aggiungere una copia dell'immagine di avvio di ONTAP 9 su un server Web a cui il sistema può accedere.

Non è possibile controllare la versione di ONTAP installata sul supporto di avvio di un modulo controller AFF A900 o FAS9500, a meno che non sia installato in uno chassis e acceso. La versione di ONTAP sul supporto di avvio di AFF A900 o FAS9500 deve essere uguale alla versione di ONTAP in esecuzione sul sistema AFF

A700 o FAS9000 in fase di aggiornamento e le immagini di avvio primaria e di backup devono corrispondere. È possibile configurare le immagini eseguendo una `netboot` seguito da `wipeconfig` dal menu di boot. Se il modulo controller è stato utilizzato in precedenza in un altro cluster, il `wipeconfig` il comando cancella qualsiasi configurazione residua sul supporto di avvio.

Prima di iniziare

- Verificare che sia possibile accedere a un server HTTP con il sistema.
- È necessario scaricare i file di sistema necessari per il sistema e la versione corretta di ONTAP da "Supporto NetApp" sito. A proposito di questa attività è necessario `netboot` I nuovi controller, se la versione di ONTAP installata non è la stessa installata sui controller originali. Dopo aver installato ciascun nuovo controller, avviare il sistema dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avvii del sistema.

Fasi

1. Accesso "Supporto NetApp" per scaricare i file necessari per eseguire un netboot di sistema utilizzato per eseguire il netboot del sistema.
2. Scarica il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizza il `<ontap_version>_image.tgz` file in una directory accessibile dal web.
3. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili. L'elenco delle directory deve contenere `<ontap_version>_image.tgz`.
4. Configurare `netboot` connessione scegliendo una delle seguenti azioni. Nota: Utilizzare la porta di gestione e l'IP come `netboot` connessione. Non utilizzare un IP LIF dei dati, altrimenti potrebbe verificarsi un'interruzione dei dati durante l'aggiornamento.

Se DHCP (Dynamic host Configuration Protocol) è…	Quindi…
In esecuzione	Configurare la connessione automaticamente utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -auto`
Non in esecuzione	Configurare manualmente la connessione utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` È l'indirizzo IP del sistema di storage. `<netmask>` è la maschera di rete del sistema di storage. `<gateway>` è il gateway per il sistema storage. `<dns_addr>` È l'indirizzo IP di un name server sulla rete. Questo parametro è facoltativo. `<dns_domain>` È il nome di dominio DNS (Domain Name Service). Questo parametro è facoltativo. NOTA: Per l'interfaccia potrebbero essere necessari altri parametri. Per ulteriori informazioni, immettere help ifconfig al prompt del firmware.

5. Eseguire `netboot` sul nodo 1: `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`Il `<path_to_the_web-

`accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>_image.tgz` poll Fase 2.

> Non interrompere l'avvio.

6. Attendere che il nodo 1 in esecuzione sul modulo controller AFF A900 o FAS9500 si avvii e visualizzare le opzioni del menu di avvio come mostrato di seguito:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

7. Dal menu di avvio, selezionare opzione `(7) Install new software first`. Questa opzione di menu consente di scaricare e installare la nuova immagine ONTAP sul dispositivo di avvio.

> Ignorare il seguente messaggio: `This procedure is not supported for Non-Disruptive Upgrade on an HA pair`. Questa nota si applica agli aggiornamenti software ONTAP senza interruzioni e non agli aggiornamenti del controller. Utilizzare sempre netboot per aggiornare il nuovo nodo all'immagine desiderata. Se si utilizza un altro metodo per installare l'immagine sul nuovo controller, potrebbe essere installata un'immagine errata. Questo problema riguarda tutte le versioni di ONTAP.

8. Se viene richiesto di continuare la procedura, immettere `y`E quando viene richiesto il pacchetto, immettere l'URL:

   `http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`

9. Completare i seguenti passaggi secondari per riavviare il modulo controller:

   a. Invio `n` per ignorare il ripristino del backup quando viene visualizzato il seguente prompt: `Do you want to restore the backup configuration now? {y|n}`

   b. Invio `y` per riavviare quando viene visualizzato il seguente prompt: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`

      Il modulo controller si riavvia ma si arresta al menu di avvio perché il dispositivo di avvio è stato riformattato e i dati di configurazione devono essere ripristinati.

10. Quando richiesto, eseguire `wipeconfig` comando per cancellare qualsiasi configurazione precedente sul supporto di avvio:
    a. Quando viene visualizzato il messaggio riportato di seguito, rispondere `yes`: `This will delete 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?:`
    b. Il nodo viene riavviato per terminare `wipeconfig` e poi si ferma al menu di boot.
11. Selezionare l'opzione `5` per passare alla modalità di manutenzione dal menu di avvio. Risposta `yes` al prompt finché il nodo non si arresta in modalità di manutenzione e al prompt dei comandi `*>`.

Ripristinare la configurazione dell'HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:
    a. Verificare le impostazioni correnti delle porte: `ucadmin show`
    b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

Impostare lo stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

    ```
    ha-config show
    ```

    Lo stato ha per tutti i componenti deve essere mcc.

2. Se lo stato di sistema visualizzato del controller o dello chassis non è corretto, impostare lo stato ha:

```
ha-config modify controller mcc
```

```
ha-config modify chassis mcc
```

3. Arrestare il nodo: `halt`Il nodo deve arrestarsi su `LOADER>` prompt.
4. Su ciascun nodo, controllare la data, l'ora e il fuso orario del sistema: `Show date`
5. Se necessario, impostare la data in UTC o ora di Greenwich (GMT): `set date <mm/dd/yyyy>`
6. Controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot: `show time`
7. Se necessario, impostare l'ora in UTC o GMT: `set time <hh:mm:ss>`
8. Salvare le impostazioni: `saveenv`
9. Raccogliere le variabili di ambiente: `printenv`
10. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione: `boot_ontap maint`
11. Verificare che le modifiche apportate siano effettive e che ucadmin mostri le porte initiator FC in linea.

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

12. Verificare la modalità ha-config: `ha-config show`
    a. Verificare di disporre dei seguenti risultati:

```
*> ha-config show
Chassis HA configuration: mcc
Controller HA configuration: mcc
```

Impostare lo stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

```
ha-config show
```

Lo stato ha per tutti i componenti deve essere mcc.

Se la configurazione MetroCluster ha…	Lo stato ha deve essere…
Due nodi	mcc-2n

Quattro o otto nodi	mcc

2. Se lo stato di sistema visualizzato del controller non è corretto, impostare lo stato ha per il modulo controller e lo chassis:

Se la configurazione MetroCluster ha…	Eseguire questi comandi…

Due nodi	`ha-config modify controller mcc-2n`
	
	`ha-config modify chassis mcc-2n`

Quattro o otto nodi	`ha-config modify controller mcc`
	
	`ha-config modify chassis mcc`

Riassegnare i dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando i sistemi raccolti in precedenza

A proposito di questa attività

Questa attività viene eseguita in modalità manutenzione.

I vecchi ID di sistema sono stati identificati in "Raccolta di informazioni prima dell'aggiornamento".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Nodo	Vecchio ID di sistema	Nuovo ID di sistema
Node_B_1	4068741254	1574774970

Fasi

1. Collegare tutti gli altri collegamenti ai nuovi moduli controller (FC-VI, storage, interconnessione cluster, ecc.).
2. Arrestare il sistema e avviare la modalità di manutenzione dal `LOADER` prompt (prompt):

   ```
   boot_ontap maint
   ```

3. Visualizzare i dischi di proprietà di Node_B_1-A700:

   ```
   disk show -a
   ```

   L'output di esempio mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi aggregati root sono ancora di proprietà del vecchio ID di sistema (4068741254). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-A700(4068741254)   Pool1  PZHYN0MD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L49 node_B_1-A700(4068741254)   Pool1  PPG3J5HA
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L21 node_B_1-A700(4068741254)   Pool1  PZHTDSZD
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L2  node_B_1-A700(4068741254)   Pool0  S0M1J2CF
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:8.126L3  node_B_1-A700(4068741254)   Pool0  S0M0CQM5
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
rr18:9.126L27 node_B_1-A700(4068741254)   Pool0  S0M1PSDW
node_B_1-A700(4068741254)  node_B_1-A700(4068741254)
...
```

4. Riassegnare i dischi aggregati root sugli shelf di dischi al nuovo controller:

   `disk reassign -s old-sysid -d new-sysid`

   L'esempio seguente mostra la riassegnazione dei dischi:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verificare che tutti i dischi siano riassegnati come previsto: `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-A900(1574774970)   Pool1  PZHYN0MD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L49 node_B_1-A900(1574774970)   Pool1  PPG3J5HA
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L21 node_B_1-A900(1574774970)   Pool1  PZHTDSZD
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L2  node_B_1-A900(1574774970)   Pool0  S0M1J2CF
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:9.126L29 node_B_1-A900(1574774970)   Pool0  S0M0CQM5
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
rr18:8.126L1  node_B_1-A900(1574774970)   Pool0  S0M1PSDW
node_B_1-A900(1574774970)  node_B_1-A900(1574774970)
*>
```

6. Visualizzare lo stato dell'aggregato: `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Ripetere i passaggi precedenti sul nodo partner (Node_B_2-A900).

Avviare i nuovi controller

Riavviare i controller dal menu di avvio per aggiornare l'immagine flash del controller. Se la crittografia è configurata, sono necessari ulteriori passaggi.

A proposito di questa attività

Questa attività deve essere eseguita su tutti i nuovi controller.

Fasi

1. Arrestare il nodo: `halt`
2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Visualizzare il menu di avvio: `boot_ontap menu`
4. Se viene utilizzata la crittografia root, immettere il comando del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione 10 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi
Gestione esterna delle chiavi	Opzione 11 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi

5. Se l'autoboot è attivato, interrompere l'autoboot premendo Ctrl-C.
6. Dal menu di boot, eseguire l'opzione (6).

L'opzione 6 riavvia il nodo due volte prima del completamento.

Rispondere `y` alle richieste di modifica dell'id di sistema. Attendere i secondi messaggi di riavvio:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Verificare che il sistema partner sia corretto: `printenv partner-sysid`

   Se il partner-sysid non è corretto, impostarlo: `setenv partner-sysid` *`partner-sysID`*

8. Se viene utilizzata la crittografia root, eseguire nuovamente il comando del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione 10 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi
Gestione esterna delle chiavi	Opzione 11 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi

   Potrebbe essere necessario eseguire il `recover_xxxxxxxx_keymanager` al prompt del menu di boot più volte fino a quando i nodi non si avviano completamente.

9. Avviare i nodi: `boot_ontap`
10. Attendere l'avvio dei nodi sostituiti.

    Se uno dei nodi è in modalità Takeover, eseguire un giveback utilizzando `storage failover giveback` comando.

11. Verificare che tutte le porte si trovino in un dominio di trasmissione:

    a. Visualizzare i domini di trasmissione:

       `network port broadcast-domain show`

    b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

       "Aggiungere o rimuovere porte da un dominio di broadcast"

    c. Aggiungere la porta fisica che ospiterà le LIF dell'intercluster al dominio Broadcast corrispondente.
    d. Modificare le LIF dell'intercluster per utilizzare la nuova porta fisica come porta home.
    e. Dopo aver attivato le LIF dell'intercluster, controllare lo stato del peer del cluster e ristabilire il peering del cluster secondo necessità.

Potrebbe essere necessario riconfigurare il peering del cluster.

"Creazione di una relazione peer del cluster"

f. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

"Creazione di una VLAN"

"Combinazione di porte fisiche per creare gruppi di interfacce"

12. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

Verificare la configurazione LIF

Verificare che i file LIF siano ospitati su nodi/porte appropriati prima di passare al switchback. È necessario eseguire le seguenti operazioni

A proposito di questa attività

Questa attività viene eseguita sul sito_B, dove i nodi sono stati avviati con aggregati root.

Fasi

1. Verificare che i file LIF siano ospitati sul nodo e sulle porte appropriati prima di passare al switchback.

   a. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

   b. Eseguire l'override della configurazione della porta per garantire il corretto posizionamento di LIF:

   ```
   vserver config override -command "network interface modify" -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Quando si accede a. `network interface modify` all'interno di `vserver config override` non è possibile utilizzare la funzione di completamento automatico della scheda. È possibile creare `network interface modify` utilizzando il completamento automatico e quindi racchiuderlo in `vserver config override` comando.

a. Tornare al livello di privilegio admin:
   `set -privilege admin`

2. Ripristinare le interfacce nel nodo principale:

   `network interface revert * -vserver vserver-name`

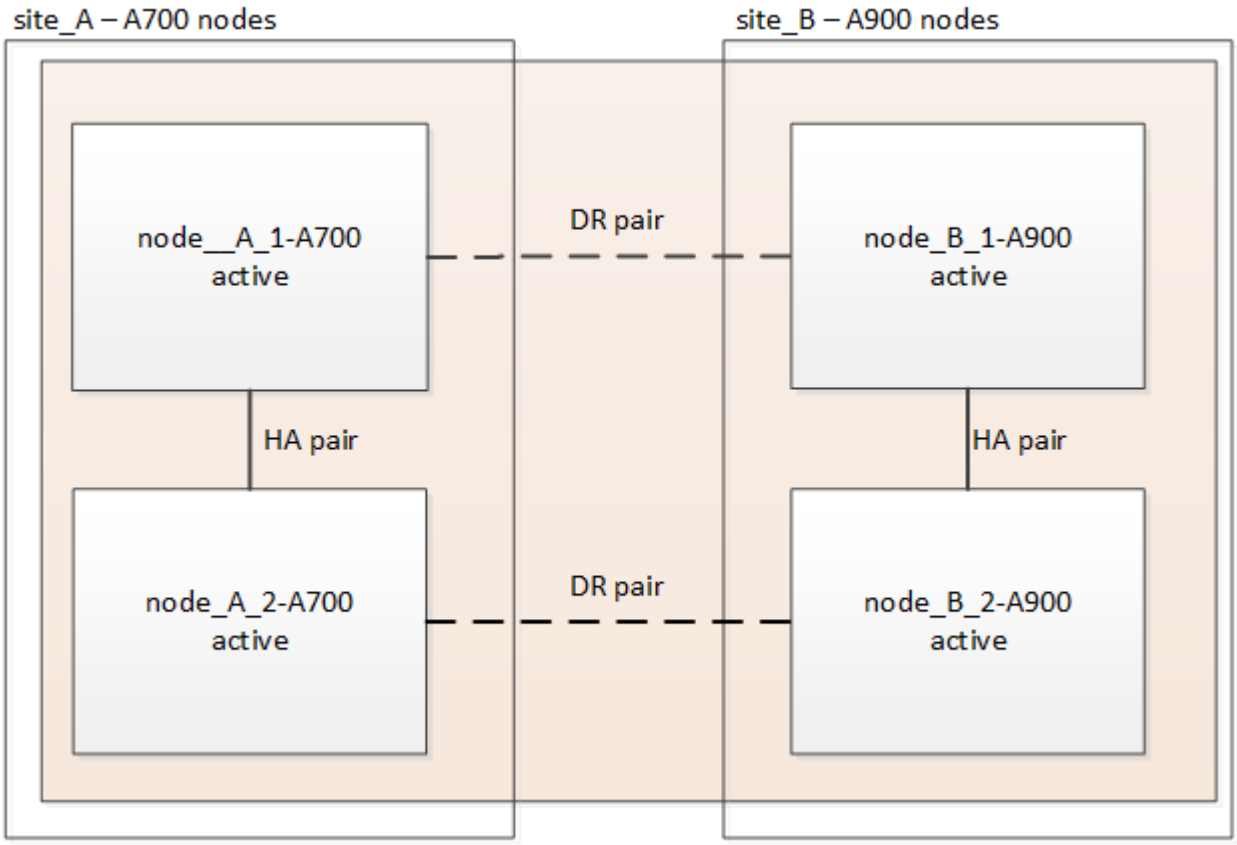
   Eseguire questo passaggio su tutte le SVM secondo necessità.

Ripristinare la configurazione MetroCluster

Una volta configurati i nuovi controller, si torna alla configurazione MetroCluster per ripristinare il normale funzionamento della configurazione.

A proposito di questa attività

Questa attività consente di eseguire l'operazione di switchback, ripristinando il normale funzionamento della configurazione MetroCluster. I nodi sul sito_A sono ancora in attesa di aggiornamento, come illustrato nella seguente illustrazione. (Questa illustrazione si applica anche all'aggiornamento di un controller FAS9000 a un controller FAS9500).



Fasi

1. Eseguire il `metrocluster node show` Su Site_B e controllare l'output.
   a. Verificare che i nuovi nodi siano rappresentati correttamente.
   b. Verificare che i nuovi nodi siano nello stato "in attesa di switchback".
2. Switchback del cluster:

```
metrocluster switchback
```

3. Controllare l'avanzamento dell'operazione di switchback:

```
metrocluster show
```

L'operazione di switchback è ancora in corso quando viene visualizzato l'output `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'operazione di switchback viene completata quando viene visualizzato l'output `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando. Questo comando si trova al livello di privilegio avanzato.

Controllare lo stato della configurazione MetroCluster

Dopo aver aggiornato i moduli controller, è necessario verificare lo stato della configurazione MetroCluster.

A proposito di questa attività

Questa attività può essere eseguita su qualsiasi nodo della configurazione MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster:

   a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

```
metrocluster show
```

b. Eseguire un controllo MetroCluster:

```
metrocluster check run
```

c. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

Dopo aver eseguito `metrocluster check run` e. `metrocluster check show` potrebbe essere visualizzato un errore simile al seguente esempio:

```
Cluster_A:: node_A_1 (non-overridable veto): DR partner NVLog mirroring
is not online. Make sure that the links between the two sites are
healthy and properly configured.
```

+ Questo errore si verifica a causa di una mancata corrispondenza del controller durante il processo di aggiornamento. È possibile ignorare l'errore e procedere all'aggiornamento dei nodi sul sito_A.

Aggiornare i nodi sul sito_A.

È necessario ripetere le attività di aggiornamento sul sito_A.

Fase

1. Ripetere i passaggi per aggiornare i nodi sul sito_A, iniziando con "Preparatevi per l'aggiornamento".

   Durante l'esecuzione delle attività, tutti i riferimenti di esempio ai siti e ai nodi vengono invertiti. Ad esempio, quando l'esempio viene fornito per lo switchover da Site_A, si passa da Site_B.

Inviare un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completato l'aggiornamento, inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

Fase

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.

   a. Immettere il seguente comando:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

   b. Ripetere il comando sul cluster partner.

Ripristinare il monitoraggio di Tiebreaker

Se la configurazione MetroCluster è stata precedentemente configurata per il monitoraggio da parte del software Tiebreaker, è possibile ripristinare la connessione Tiebreaker.

1. Attenersi alla procedura descritta in: "Aggiunta di configurazioni MetroCluster" Nella sezione *Installazione e*

configurazione di MetroCluster Tiebreaker.

Aggiornamento dei controller in una configurazione MetroCluster FC a quattro nodi mediante switchover e switchback con comandi "system controller replace" (ONTAP 9.10.1 e versioni successive)

È possibile utilizzare questa operazione di switchover MetroCluster automatizzato e guidato per eseguire un aggiornamento del controller senza interruzioni su una configurazione FC MetroCluster a quattro nodi. Altri componenti (ad esempio shelf di storage o switch) non possono essere aggiornati come parte di questa procedura.

Combinazioni di piattaforme supportate

- Per informazioni sulle combinazioni di upgrade della piattaforma supportate, consultare la tabella di aggiornamento MetroCluster FC in "Scegliere una procedura di aggiornamento del controller".

Fare riferimento a. "Scelta di un metodo di aggiornamento o refresh" per ulteriori procedure.

A proposito di questa attività

- Questa procedura può essere utilizzata solo per l'aggiornamento del controller.

  Gli altri componenti della configurazione, come gli shelf di storage o gli switch, non possono essere aggiornati contemporaneamente.

- Questa procedura si applica ai moduli controller in una configurazione MetroCluster FC a quattro nodi.
- Sulle piattaforme deve essere in esecuzione ONTAP 9.10.1 o versione successiva.

  "NetApp Hardware Universe"

- È possibile utilizzare questa procedura per aggiornare i controller in una configurazione MetroCluster FC a quattro nodi utilizzando switchover e switchback automatici basati su NSO. Se si desidera eseguire un aggiornamento del controller utilizzando il trasferimento aggregato (ARL), fare riferimento a. "Utilizzare i comandi "System controller replace" per aggiornare l'hardware del controller con ONTAP 9.8 o versione successiva". Si consiglia di utilizzare la procedura automatica basata su NSO.
- Se i siti MetroCluster si trovano fisicamente in due posizioni diverse, è necessario utilizzare la procedura di aggiornamento automatico del controller NSO per aggiornare i controller di entrambi i siti in sequenza.
- Questa procedura di aggiornamento automatico del controller basata su NSO consente di avviare la sostituzione del controller in un sito di disaster recovery (DR) MetroCluster. È possibile avviare la sostituzione di un controller solo in un sito alla volta.
- Per avviare una sostituzione del controller nel sito A, eseguire il comando di avvio per la sostituzione del controller dal sito B. L'operazione consente di sostituire i controller di entrambi i nodi solo nel sito A. Per sostituire i controller nel sito B, eseguire il comando di avvio per la sostituzione dei controller dal sito A. Viene visualizzato un messaggio che identifica il sito in cui vengono sostituiti i controller.

In questa procedura vengono utilizzati i seguenti nomi di esempio:

- Sito_A.

    - Prima dell'aggiornamento:
        - Node_A_1-old
        - Node_A_2-old
    - Dopo l'aggiornamento:
        - Node_A_1-new
        - Node_A_2-new
- Sito_B
    - Prima dell'aggiornamento:
        - Node_B_1-old
        - Node_B_2-old
    - Dopo l'aggiornamento:
        - Node_B_1-new
        - Node_B_2-new

Preparazione per l'aggiornamento

Per prepararsi all'aggiornamento del controller, è necessario eseguire controlli preliminari del sistema e raccogliere le informazioni di configurazione.

Durante l'aggiornamento, è possibile eseguire il `system controller replace show` oppure `system controller replace show-details` Dal sito A per controllare lo stato. Se i comandi restituiscono un output vuoto, attendere alcuni minuti ed eseguire nuovamente il comando.

Fasi

1. Avviare la procedura di sostituzione automatica del controller dal sito A per sostituire i controller nel sito B:

   `system controller replace start`

   L'operazione automatica esegue i controlli preliminari. Se non vengono rilevati problemi, l'operazione viene interrotta in modo da poter raccogliere manualmente le informazioni relative alla configurazione.

   > Vengono visualizzati il sistema di origine corrente e tutti i sistemi di destinazione compatibili. Se il controller di origine è stato sostituito con un controller con una versione ONTAP diversa o con una piattaforma non compatibile, l'operazione di automazione si interrompe e segnala un errore dopo l'avvio dei nuovi nodi. Per riportare il cluster a uno stato integro, è necessario seguire la procedura di ripristino manuale.

   Il `system controller replace start` il comando potrebbe segnalare il seguente errore di verifica preliminare:

   ```
   Cluster-A::*>system controller replace show
   Node        Status         Error-Action
   ----------- -------------- ------------------------------------
   Node-A-1    Failed         MetroCluster check failed. Reason : MCC check
   showed errors in component aggregates
   ```

Controllare se si è verificato questo errore a causa di aggregati senza mirror o di un altro problema di aggregato. Verificare che tutti gli aggregati mirrorati siano integri e che non siano degradati o mirror-degradati. Se questo errore è dovuto solo agli aggregati senza mirror, è possibile ignorare questo errore selezionando `-skip-metrocluster-check true` sul `system controller replace start` comando. Se lo storage remoto è accessibile, gli aggregati senza mirror vengono online dopo lo switchover. Se il collegamento storage remoto non funziona, gli aggregati senza mirror non vengono collegati.

2. Raccogliere manualmente le informazioni di configurazione accedendo al sito B e seguendo i comandi elencati nel messaggio della console sotto `system controller replace show` oppure `system controller replace show-details` comando.

Raccolta di informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, se il volume root è crittografato, è necessario raccogliere la chiave di backup e altre informazioni per avviare i nuovi controller con i vecchi volumi root crittografati.

A proposito di questa attività

Questa attività viene eseguita sulla configurazione MetroCluster FC esistente.

Fasi

1. Etichettare i cavi per i controller esistenti, in modo da poter identificare facilmente i cavi durante la configurazione dei nuovi controller.
2. Visualizzare i comandi per acquisire la chiave di backup e altre informazioni:

   ```
   system controller replace show
   ```

   Eseguire i comandi elencati sotto `show` dal cluster partner.

3. Raccogliere gli ID di sistema dei nodi nella configurazione MetroCluster:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   Durante la procedura di aggiornamento, sostituisci questi vecchi ID di sistema con gli ID di sistema dei nuovi moduli controller.

   In questo esempio, per una configurazione MetroCluster FC a quattro nodi, vengono recuperati i seguenti vecchi ID di sistema:

   - Node_A_1-old: 4068741258
   - Node_A_2-old: 4068741260
   - Node_B_1-old: 4068741254
   - Node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-systemid,ha-
partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
dr-group-id        cluster           node            node-systemid
ha-partner-systemid     dr-partner-systemid    dr-auxiliary-systemid
-----------        ---------------   ----------      -------------
-------------------     -------------------    ---------------------
1                    Cluster_A       Node_A_1-old    4068741258
4068741260              4068741256             4068741256
1                    Cluster_A       Node_A_2-old    4068741260
4068741258              4068741254             4068741254
1                    Cluster_B       Node_B_1-old    4068741254
4068741256              4068741258             4068741260
1                    Cluster_B       Node_B_2-old    4068741256
4068741254              4068741260             4068741258
4 entries were displayed.
```

In questo esempio, per una configurazione MetroCluster FC a due nodi, vengono recuperati i seguenti vecchi ID di sistema:

- Node_A_1: 4068741258
- Node_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node          node-systemid dr-partner-systemid
----------- ---------- --------      ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

4. Raccogliere informazioni su porta e LIF per ciascun nodo precedente.

   Per ciascun nodo, è necessario raccogliere l'output dei seguenti comandi:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`

- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

5. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

6. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

   ```
   security key-manager backup show
   ```

7. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

   Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

   a. Se Onboard Key Manager è configurato:

      ```
      security key-manager onboard show-backup
      ```

      La passphrase sarà necessaria più avanti nella procedura di aggiornamento.

   b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

      ```
      security key-manager external show -instance
      ```

   ```
   security key-manager key query
   ```

8. Al termine della raccolta delle informazioni di configurazione, riprendere l'operazione:

   ```
   system controller replace resume
   ```

Rimozione della configurazione esistente dal software di monitoraggio o dallo spareggio

Se la configurazione esistente viene monitorata con la configurazione di MetroCluster Tiebreaker o altre applicazioni di terze parti (ad esempio, ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal Tiebreaker o da un altro software prima di sostituire il vecchio controller.

Fasi

1. "Rimuovere la configurazione MetroCluster esistente" Dal software Tiebreaker.
2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Sostituzione dei vecchi controller e avvio dei nuovi controller

Una volta raccolte le informazioni e riavviata l'operazione, l'automazione procede con l'operazione di switchover.

A proposito di questa attività

L'operazione di automazione avvia lo switchover, `heal-aggregates`, e. `heal root-aggregates` operazioni. Al termine di queste operazioni, l'operazione viene sospesa in **pausa per l'intervento dell'utente**, in modo da poter eseguire il rack e installare i controller, avviare i controller partner e riassegnare i dischi aggregati root al nuovo modulo controller dal backup flash utilizzando `sysids` raccolte in precedenza.

Prima di iniziare

Prima di iniziare lo switchover, l'operazione di automazione viene interrotta in modo da poter verificare manualmente che tutti i LIF siano "up" nel sito B. Se necessario, portare i LIF "dpropri" su "up" e riprendere l'operazione di automazione utilizzando `system controller replace resume` comando.

Preparazione della configurazione di rete dei vecchi controller

Per garantire che la rete riprenda correttamente sui nuovi controller, è necessario spostare i file LIF su una porta comune e rimuovere la configurazione di rete dei vecchi controller.

A proposito di questa attività

- Questa attività deve essere eseguita su ciascuno dei vecchi nodi.
- Verranno utilizzate le informazioni raccolte in Preparazione per l'aggiornamento.

Fasi

1. Avviare i vecchi nodi e quindi accedere ai nodi:

   ```
   boot_ontap
   ```

2. Assegnare la porta home di tutti i file LIF di dati sul vecchio controller a una porta comune identica sia sul vecchio che sul nuovo modulo controller.

   a. Visualizzare le LIF:

      ```
      network interface show
      ```

      Tutti i dati LIFS, inclusi SAN e NAS, saranno admin "up" e operativi "down", in quanto sono presenti nel sito di switchover (cluster_A).

   b. Esaminare l'output per trovare una porta di rete fisica comune che sia la stessa sui controller vecchi e nuovi che non sia utilizzata come porta del cluster.

      Ad esempio, "e0d" è una porta fisica sui vecchi controller ed è presente anche sui nuovi controller. "e0d" non viene utilizzato come porta del cluster o in altro modo sui nuovi controller.

      Per informazioni sull'utilizzo delle porte per i modelli di piattaforma, consultare "NetApp Hardware Universe"

   c. Modificare tutti i dati LIFS per utilizzare la porta comune come porta home:

      ```
      network interface modify -vserver svm-name -lif data-lif -home-port port-id
      ```

Nell'esempio seguente, si tratta di "e0d".

Ad esempio:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modificare i domini di broadcast per rimuovere la VLAN e le porte fisiche che devono essere eliminate:

   `broadcast-domain remove-ports -broadcast-domain broadcast-domain-name -ports node-name:port-id`

   Ripetere questo passaggio per tutte le porte VLAN e fisiche.

4. Rimuovere le porte VLAN utilizzando le porte del cluster come porte membro e gruppi di interfacce utilizzando le porte del cluster come porte membro.

   a. Elimina porte VLAN:

      `network port vlan delete -node node-name -vlan-name portid-vlandid`

      Ad esempio:

      ```
      network port vlan delete -node node1 -vlan-name e1c-80
      ```

   b. Rimuovere le porte fisiche dai gruppi di interfacce:

      `network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

      Ad esempio:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

   a. Rimuovere le porte della VLAN e del gruppo di interfacce dal dominio di broadcast:

      `network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

   b. Modificare le porte del gruppo di interfacce per utilizzare altre porte fisiche come membro in base alle necessità.:

      `ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

5. Arrestare i nodi:

   `halt -inhibit-takeover true -node node-name`

   Questa operazione deve essere eseguita su entrambi i nodi.

Configurazione dei nuovi controller

I nuovi controller devono essere montati in rack e cablati.

Fasi

1. Pianificare il posizionamento dei nuovi moduli controller e degli shelf di storage in base alle necessità.

   Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di shelf di storage nella configurazione.

2. Mettere a terra l'utente.
3. Installare i moduli controller nel rack o nell'armadietto.

   "Documentazione dei sistemi hardware ONTAP"

4. Se i nuovi moduli controller non sono dotati di schede FC-VI e se le schede FC-VI dei vecchi controller sono compatibili con i nuovi controller, sostituire le schede FC-VI e installarle negli slot corretti.

   Vedere "NetApp Hardware Universe" Per informazioni sugli slot per schede FC-VI.

5. Collegare l'alimentazione, la console seriale e le connessioni di gestione dei controller come descritto nelle *Guide di installazione e configurazione di MetroCluster*.

   Non collegare altri cavi scollegati dai vecchi controller in questo momento.

   "Documentazione dei sistemi hardware ONTAP"

6. Accendere i nuovi nodi e premere Ctrl-C quando richiesto per visualizzare il prompt DEL CARICATORE.

Avvio in rete dei nuovi controller

Dopo aver installato i nuovi nodi, è necessario eseguire il netboot per assicurarsi che i nuovi nodi eseguano la stessa versione di ONTAP dei nodi originali. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

Questa attività viene eseguita su ciascuno dei nuovi moduli controller.

Fasi

1. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il file ontap-version_image.tgz in una directory accessibile dal Web.
3. Accedere alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

Se il modello di piattaforma è…	Quindi…
Sistemi della serie FAS/AFF8000	Estrarre il contenuto del file ontap-version_image.tgznella directory di destinazione: Tar -zxvf ontap-version_image.tgz NOTA: Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine netboot. L'elenco delle directory deve contenere una cartella netboot con un file kernel:netboot/kernel

Tutti gli altri sistemi	L'elenco delle directory deve contenere una cartella netboot con un file del kernel: ontap-version_image.tgz non è necessario estrarre il file ontap-version_image.tgz.

4. Al prompt DEL CARICATORE, configurare la connessione netboot per una LIF di gestione:
   - Se l'indirizzo IP è DHCP, configurare la connessione automatica:

     ```
     ifconfig e0M -auto
     ```

   - Se l'indirizzo IP è statico, configurare la connessione manuale:

     ```
     ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
     ```

5. Eseguire il netboot.
   - Se la piattaforma è un sistema della serie 80xx, utilizzare questo comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se la piattaforma è un altro sistema, utilizzare il seguente comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se viene richiesto di continuare la procedura, immettere `y`E quando
   viene richiesto il pacchetto, inserire l'URL del file immagine:
   `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Riavviare immettendo `y` quando viene visualizzato un prompt simile a quanto segue:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   `halt`

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   `set-defaults`

3. Salvare l'ambiente:

   `saveenv`

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

   `boot_ontap menu`

5. Al prompt del menu di avvio, cancellare la configurazione:

   `wipeconfig`

   Rispondere `yes` al prompt di conferma.

   Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Ripristino della configurazione HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:

   a. Verificare le impostazioni correnti delle porte: `ucadmin show`

   b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…

FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

2. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

3. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

   ```
   boot_ontap maint
   ```

4. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Riassegnazione dei dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando `sysids` raccolte in precedenza

A proposito di questa attività

Questa attività viene eseguita in modalità manutenzione.

I vecchi ID di sistema sono stati identificati in "Raccolta di informazioni prima dell'aggiornamento".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Nodo	Vecchio ID di sistema	Nuovo ID di sistema
Node_B_1	4068741254	1574774970

Fasi

1. Collegare tutti gli altri collegamenti ai nuovi moduli controller (FC-VI, storage, interconnessione cluster, ecc.).
2. Arrestare il sistema e avviare la modalità di manutenzione dal prompt DEL CARICATORE:

```
boot_ontap maint
```

3. Visualizzare i dischi di proprietà di Node_B_1-old:

```
disk show -a
```

L'output del comando mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi aggregati root sono ancora di proprietà del vecchio ID di sistema (4068741254). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Riassegnare i dischi aggregati root sugli shelf di dischi al nuovo controller:

```
disk reassign -s old-sysid -d new-sysid
```

L'esempio seguente mostra la riassegnazione dei dischi:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Verificare che tutti i dischi siano riassegnati come previsto:

```
disk show
```

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                      POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------              -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Visualizzare lo stato dell'aggregato:

   `aggr status`

   ```
   *> aggr status
              Aggr            State       Status           Options
   aggr0_node_b_1-root        online      raid_dp, aggr    root, nosnap=on,
                              mirrored
   mirror_resync_priority=high(fixed)
                              fast zeroed
                              64-bit
   ```

7. Ripetere i passaggi precedenti sul nodo partner (Node_B_2-new).

Avviare i nuovi controller

Riavviare i controller dal menu di avvio per aggiornare l'immagine flash del controller. Se la crittografia è configurata, sono necessari ulteriori passaggi.

È possibile riconfigurare VLAN e gruppi di interfacce. Se necessario, modificare manualmente le porte per le LIF del cluster e i dettagli del dominio di trasmissione prima di riprendere l'operazione utilizzando `system controller replace resume` comando.

A proposito di questa attività

Questa attività deve essere eseguita su tutti i nuovi controller.

Fasi

1. Arrestare il nodo:

   `halt`

2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Visualizzare il menu di avvio:

   `boot_ontap menu`

4. Se viene utilizzata la crittografia root, selezionare l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…

Gestione delle chiavi integrata	Opzione “10” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione “11” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

5. Se l’autoboot è attivato, interrompere l’autoboot premendo Ctrl-C.
6. Dal menu di boot, eseguire l’opzione “6”.

   L’opzione “6” riavvia il nodo due volte prima del completamento.

   Rispondere “y” alle richieste di modifica dell’id di sistema. Attendere i secondi messaggi di riavvio:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Verificare che il sistema partner sia corretto:

   ```
   printenv partner-sysid
   ```

   Se il partner-sysid non è corretto, impostarlo:

   ```
   setenv partner-sysid partner-sysID
   ```

8. Se viene utilizzata la crittografia root, selezionare nuovamente l’opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione “10” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione “11” Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

A seconda dell’impostazione del gestore delle chiavi, eseguire la procedura di ripristino selezionando

l'opzione "10" o l'opzione "11", quindi l'opzione "6" al primo prompt del menu di avvio. Per avviare completamente i nodi, potrebbe essere necessario ripetere la procedura di ripristino, continua con l'opzione "1" (boot normale).

9. Avviare i nodi:

   ```
   boot_ontap
   ```

10. Attendere l'avvio dei nodi sostituiti.

    Se uno dei nodi è in modalità Takeover, eseguire un giveback utilizzando `storage failover giveback` comando.

11. Verificare che tutte le porte si trovino in un dominio di trasmissione:

    a. Visualizzare i domini di trasmissione:

       ```
       network port broadcast-domain show
       ```

    b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

       "Aggiunta o rimozione di porte da un dominio di broadcast"

    c. Aggiungere la porta fisica che ospiterà le LIF dell'intercluster al dominio di trasmissione corrispondente.
    d. Modificare le LIF dell'intercluster per utilizzare la nuova porta fisica come porta home.
    e. Dopo aver attivato le LIF dell'intercluster, controllare lo stato del peer del cluster e ristabilire il peering del cluster secondo necessità.

       Potrebbe essere necessario riconfigurare il peering del cluster.

       "Creazione di una relazione peer del cluster"

    f. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

       L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

       "Creazione di una VLAN"

    "Combinazione di porte fisiche per creare gruppi di interfacce"

    a. Verificare che il cluster partner sia raggiungibile e che la configurazione sia risincronizzata correttamente sul cluster partner:

       ```
       metrocluster switchback -simulate true
       ```

12. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…

Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

13. Prima di riprendere l'operazione, verificare che MetroCluster sia configurato correttamente. Controllare lo stato del nodo:

    ```
    metrocluster node show
    ```

    Verificare che i nuovi nodi (Site_B) si trovino nello stato **Waiting for switchback** from Site_A.

14. Riprendere l'operazione:

    ```
    system controller replace resume
    ```

Completamento dell'aggiornamento

L'operazione di automazione esegue controlli del sistema di verifica e quindi si ferma per verificare la raggiungibilità della rete. Dopo la verifica, viene avviata la fase di riconquista delle risorse e l'operazione di automazione esegue lo switchback nel sito A e si ferma ai controlli successivi all'aggiornamento. Dopo aver ripristinato l'operazione di automazione, esegue i controlli post-aggiornamento e, se non vengono rilevati errori, contrassegna l'aggiornamento come completo.

Fasi

1. Verificare la raggiungibilità della rete seguendo il messaggio della console.
2. Una volta completata la verifica, riprendere l'operazione:

    ```
    system controller replace resume
    ```

3. L'operazione di automazione esegue lo switchback presso il sito A e i controlli successivi all'aggiornamento. Quando l'operazione viene interrotta, controllare manualmente lo stato LIF DELLA SAN e verificare la configurazione di rete seguendo il messaggio della console.
4. Una volta completata la verifica, riprendere l'operazione:

    ```
    system controller replace resume
    ```

5. Controllare lo stato dei controlli successivi all'aggiornamento:

    ```
    system controller replace show
    ```

    Se i controlli successivi all'aggiornamento non hanno segnalato errori, l'aggiornamento è completo.

6. Dopo aver completato l'aggiornamento del controller, accedere al sito B e verificare che i controller sostituiti siano configurati correttamente.

Ripristino del monitoraggio di Tiebreaker

Se la configurazione MetroCluster è stata precedentemente configurata per il monitoraggio da parte del software Tiebreaker, è possibile ripristinare la connessione Tiebreaker.

1. Attenersi alla procedura descritta in "Aggiunta di configurazioni MetroCluster".

Aggiornamento dei controller in una configurazione MetroCluster IP mediante switchover e switchback (ONTAP 9.8 e versioni successive)

A partire da ONTAP 9.8, è possibile utilizzare l'operazione di switchover MetroCluster per fornire un servizio senza interruzioni ai client mentre i moduli controller del cluster partner vengono aggiornati. Altri componenti (ad esempio shelf di storage o switch) non possono essere aggiornati come parte di questa procedura.

Piattaforme supportate da questa procedura

- Sulle piattaforme deve essere in esecuzione ONTAP 9.8 o versione successiva.
- La piattaforma di destinazione (nuova) deve essere un modello diverso rispetto alla piattaforma originale.
- I modelli di piattaforma con shelf interni non sono supportati.
- È possibile aggiornare solo modelli di piattaforma specifici utilizzando questa procedura in una configurazione MetroCluster IP.
  - Per informazioni sulle combinazioni di upgrade della piattaforma supportate, consultare la tabella di aggiornamento IP di MetroCluster in "Scegliere una procedura di aggiornamento del controller".

    Fare riferimento a. "Scelta di un metodo di aggiornamento o refresh" per ulteriori procedure.

A proposito di questa attività

- Questa procedura si applica ai moduli controller in una configurazione MetroCluster IP.
- Tutti i controller della configurazione devono essere aggiornati durante lo stesso periodo di manutenzione.

  L'utilizzo della configurazione MetroCluster con diversi tipi di controller non è supportato al di fuori di questa attività di manutenzione.

- Gli switch IP devono disporre di una versione firmware supportata.
- Se la nuova piattaforma ha meno slot rispetto al sistema originale o se ha un numero inferiore o diversi tipi di porte, potrebbe essere necessario aggiungere un adattatore al nuovo sistema.

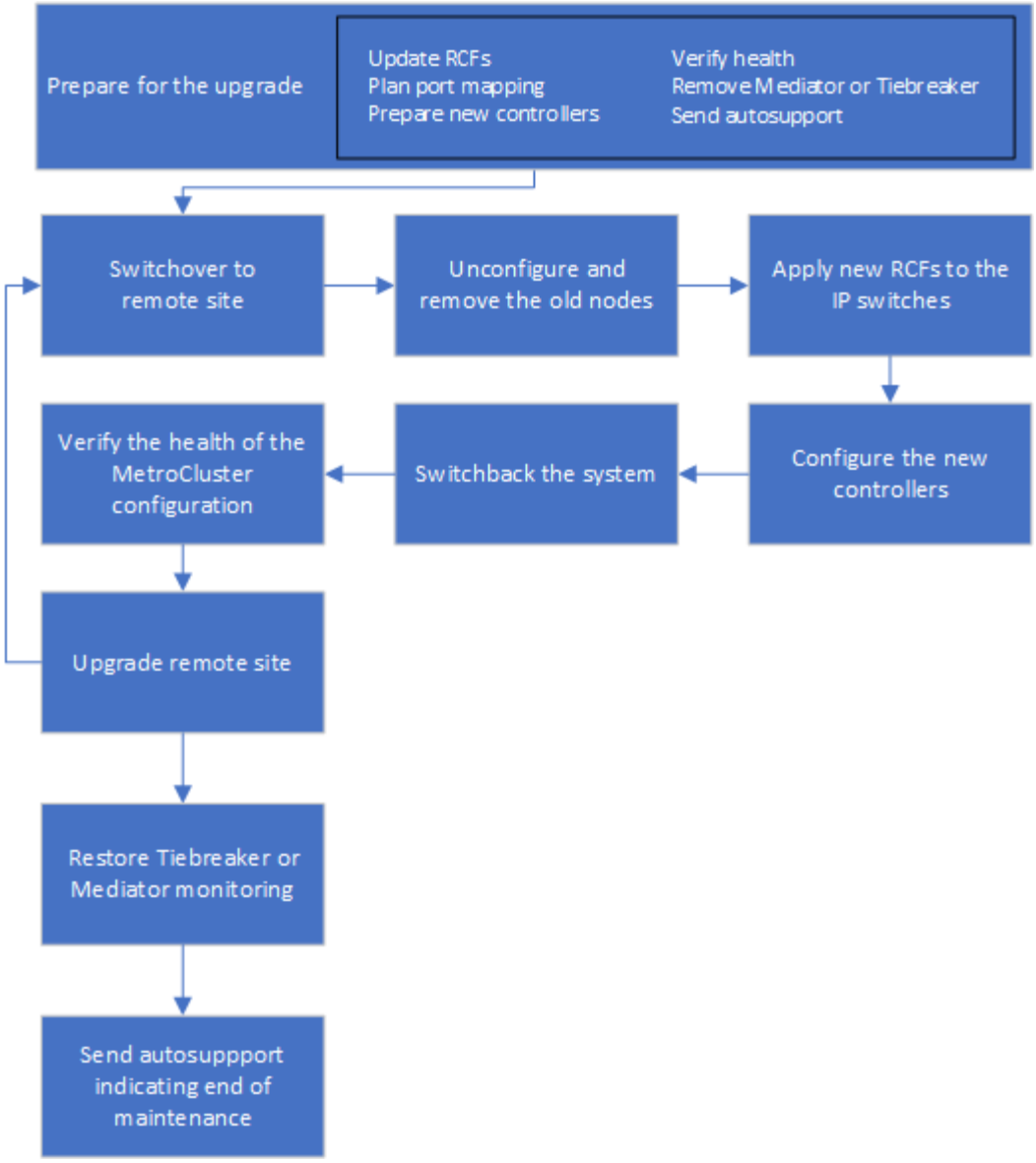
  Per ulteriori informazioni, consultare "NetApp Hardware Universe".

- Gli indirizzi IP, le netmask e i gateway delle piattaforme originali verranno riutilizzati sulle nuove piattaforme.
- In questa procedura vengono utilizzati i seguenti nomi di esempio:
  - Sito_A.
    - Prima dell'aggiornamento:

        - Node_A_1-old
        - Node_A_2-old
    - Dopo l’aggiornamento:
        - Node_A_1-new
        - Node_A_2-new
  - Sito_B
    - Prima dell’aggiornamento:
        - Node_B_1-old
        - Node_B_2-old
    - Dopo l’aggiornamento:
        - Node_B_1-new
        - Node_B_2-new

Workflow per l’aggiornamento dei controller in una configurazione MetroCluster IP

È possibile utilizzare il diagramma del flusso di lavoro per pianificare le attività di aggiornamento.



Preparazione per l'aggiornamento

Prima di apportare modifiche alla configurazione MetroCluster esistente, è necessario controllare lo stato della configurazione, preparare le nuove piattaforme ed eseguire altre attività varie.

Aggiornamento dei file RCF dello switch MetroCluster prima dell'aggiornamento dei controller

A seconda dei vecchi modelli di piattaforma, se la configurazione dello switch non è sulla versione minima o se si desidera modificare gli ID VLAN utilizzati dalle connessioni MetroCluster back-end, è necessario aggiornare i file RCF dello switch prima di iniziare la procedura di aggiornamento della piattaforma.

A proposito di questa attività

È necessario aggiornare il file RCF nei seguenti scenari:

- Per alcuni modelli di piattaforma, gli switch devono utilizzare un ID VLAN supportato per le connessioni IP MetroCluster back-end. Se i modelli di piattaforma vecchi o nuovi sono riportati nella tabella seguente, **e non** utilizzando un ID VLAN supportato, è necessario aggiornare i file RCF dello switch.

Le connessioni del cluster locale possono utilizzare qualsiasi VLAN, non devono necessariamente trovarsi nell'intervallo specificato.

Modello di piattaforma (vecchio o nuovo)	ID VLAN supportati
• AFF A400	• 10 • 20 • Qualsiasi valore compreso tra 101 e 4096 inclusi.

- La configurazione dello switch non è stata configurata con la versione RCF minima supportata:

Modello di switch	Versione del file RCF richiesta
Cisco 3132Q-V.	1.7 o versione successiva
Cisco 3232C	1.7 o versione successiva
Broadcom BES-53248	1.3 o versione successiva

- Si desidera modificare la configurazione della VLAN.

  L'intervallo di ID VLAN è compreso tra 101 e 4096.

Gli switch del sito_A verranno aggiornati quando i controller del sito_A verranno aggiornati.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP".

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"
2. Scaricare e installare i file RCF.

   Seguire la procedura descritta in "Installazione e configurazione di MetroCluster IP".

   - "Download e installazione dei file RCF Broadcom"
   - "Download e installazione dei file Cisco IP RCF"

Mappatura delle porte dai vecchi nodi ai nuovi nodi

È necessario verificare che le porte fisiche sul nodo_A_1-old si mappino correttamente alle porte fisiche sul nodo_A_1-new, che consentirà al nodo_A_1-new di comunicare con altri nodi nel cluster e con la rete dopo l'aggiornamento.

A proposito di questa attività

Quando il nuovo nodo viene avviato per la prima volta durante il processo di aggiornamento, riproduce la

configurazione più recente del vecchio nodo che sta sostituendo. Quando si avvia Node_A_1-new, ONTAP tenta di ospitare le LIF sulle stesse porte utilizzate su Node_A_1-old. Pertanto, come parte dell'aggiornamento, è necessario regolare la configurazione della porta e della LIF in modo che sia compatibile con quella del vecchio nodo. Durante la procedura di aggiornamento, verranno eseguiti i passaggi sul vecchio e sul nuovo nodo per garantire la corretta configurazione LIF di cluster, gestione e dati.

La seguente tabella mostra esempi di modifiche alla configurazione relative ai requisiti di porta dei nuovi nodi.

Porte fisiche di interconnessione cluster		
Vecchio controller	Nuovo controller	Azione richiesta
e0a, e0b	e3a, e3b	Nessuna porta corrispondente. Dopo l'aggiornamento, è necessario ricreare le porte del cluster.
e0c, e0d	e0a,e0b,e0c,e0d	e0c e e0d corrispondono alle porte. Non è necessario modificare la configurazione, ma dopo l'aggiornamento è possibile distribuire le LIF del cluster tra le porte del cluster disponibili.

Fasi

1. Determinare quali porte fisiche sono disponibili sui nuovi controller e quali LIF possono essere ospitate sulle porte.

   L'utilizzo della porta del controller dipende dal modulo della piattaforma e dagli switch che verranno utilizzati nella configurazione IP di MetroCluster. È possibile ottenere l'utilizzo delle porte delle nuove piattaforme da "NetApp Hardware Universe".

2. Pianificare l'utilizzo delle porte e compilare le seguenti tabelle come riferimento per ciascuno dei nuovi nodi.

   Durante l'esecuzione della procedura di aggiornamento, fare riferimento alla tabella.

	Node_A_1-old			Node_A_1-new		
LIF	Porte	IPspaces	Domini di broadcast	Porte	IPspaces	Domini di broadcast
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Gestione dei nodi						

Gestione del cluster						
Dati 1						
Dati 2						
Dati 3						
Dati 4						
SAN						
Porta intercluster						

Avvio in rete dei nuovi controller

Dopo aver installato i nuovi nodi, è necessario eseguire il netboot per assicurarsi che i nuovi nodi eseguano la stessa versione di ONTAP dei nodi originali. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario inserire una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere.

Fasi

1. NetBoot i nuovi controller:

    a. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.

    b. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il `ontap-version_image.tgz` file in una directory accessibile dal web.

    c. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

Se il modello di piattaforma è…	Quindi…

sistemi della serie 8000	Estrarre il contenuto di `ontap-version_image.tgz` file nella directory di destinazione:
	
	`tar -zxvf ontap-version_image.tgz`
	
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot. L'elenco delle directory deve contenere una cartella netboot con un file kernel:netboot/kernel
	
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	
	`netboot/kernel`

Tutti gli altri sistemi	L'elenco delle directory deve contenere una cartella netboot con un file kernel: `_ontap-version_image.tgz` Non è necessario estrarre `_ontap-version_image.tgz` file.

d. Al prompt DEL CARICATORE, configurare la connessione netboot per una LIF di gestione:

Se l'indirizzo IP è…	Quindi…
DHCP	Configurare la connessione automatica: `ifconfig e0M -auto`
Statico	Configurare la connessione manuale: `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

e. Eseguire il netboot.

Se il modello di piattaforma è…	Quindi…
Sistemi della serie FAS/AFF8000	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Tutti gli altri sistemi	`netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

f. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

   Ignorare il seguente messaggio:

`"This procedure is not supported for Non-Disruptive Upgrade on an HA pair"`. Si applica agli aggiornamenti software senza interruzioni e non agli aggiornamenti dei controller.

a. Se viene richiesto di continuare la procedura, immettere `y`E quando viene richiesto il pacchetto, inserire l'URL del file immagine:

   `http://`*`web_server_ip/path_to_web-accessible_directory/ontap-version`*`_image.tgz`

b. Immettere il nome utente e la password, se applicabile, oppure premere Invio per continuare.

c. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

```
Do you want to restore the backup configuration now? {y|n} **n**
```

d. Riavviare immettendo **`y`** quando viene visualizzato un prompt simile a quanto segue:

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
```

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   `halt`

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   `set-defaults`

3. Salvare l'ambiente:

   `saveenv`

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

   `boot_ontap menu`

5. Al prompt del menu di avvio, cancellare la configurazione:

`wipeconfig`

Rispondere `yes` al prompt di conferma.

Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Verifica dello stato di salute di MetroCluster prima dell'aggiornamento del sito

Prima di eseguire l'aggiornamento, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che i nodi siano multipathing:
   `node run -node node-name sysconfig -a`

   Eseguire questo comando per ogni nodo della configurazione MetroCluster.

   b. Verificare che non vi siano dischi rotti nella configurazione:
   `storage disk show -broken`

   Eseguire questo comando su ciascun nodo della configurazione MetroCluster.

   c. Verificare la presenza di eventuali avvisi sullo stato di salute:

   ```
   system health alert show
   ```

   Eseguire questo comando su ciascun cluster.

   d. Verificare le licenze sui cluster:

   ```
   system license show
   ```

   Eseguire questo comando su ciascun cluster.

   e. Verificare i dispositivi collegati ai nodi:

   ```
   network device-discovery show
   ```

   Eseguire questo comando su ciascun cluster.

   f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

   ```
   cluster date show
   ```

   Eseguire questo comando su ciascun cluster. È possibile utilizzare `cluster date` comandi per configurare l'ora e il fuso orario.

2. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
   a. Confermare la configurazione MetroCluster e che la modalità operativa è `normal`:
      `metrocluster show`
   b. Verificare che siano visualizzati tutti i nodi previsti:
      `metrocluster node show`
   c. Immettere il seguente comando:

      ```
      metrocluster check run
      ```

   d. Visualizzare i risultati del controllo MetroCluster:

      ```
      metrocluster check show
      ```

3. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.
   a. Scaricare ed eseguire Config Advisor.

      "Download NetApp: Config Advisor"

   b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Raccolta di informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, è necessario raccogliere informazioni per ciascuno dei nodi e, se necessario, regolare i domini di broadcast di rete, rimuovere eventuali VLAN e gruppi di interfacce e raccogliere informazioni sulla crittografia.

Fasi

1. Registrare il cablaggio fisico di ciascun nodo, etichettando i cavi secondo necessità per consentire il cablaggio corretto dei nuovi nodi.
2. Raccogliere informazioni su interconnessione, porta e LIF per ciascun nodo.

   Per ciascun nodo, è necessario raccogliere l'output dei seguenti comandi:

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`

- `system node run -node node-name sysconfig -a`
- `vserver fcp initiator show`
- `storage disk show`
- `metrocluster configuration-settings interface show`

3. Raccogliere gli UUID per il sito_B (il sito le cui piattaforme sono attualmente in fase di aggiornamento):

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Questi valori devono essere configurati con precisione sui nuovi moduli controller Site_B per garantire un aggiornamento corretto. Copiare i valori in un file in modo da poterli copiare nei comandi appropriati in un secondo momento del processo di aggiornamento.

   L'esempio seguente mostra l'output del comando con gli UUID:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

   Si consiglia di registrare gli UUID in una tabella simile alla seguente.

Cluster o nodo	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A.	ee7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039

Node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi:

   ```
   security key-manager backup show
   ```

6. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle chiavi e alle passphrase.

   Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

   a. Se Onboard Key Manager è configurato:
      `security key-manager onboard show-backup`

      La passphrase sarà necessaria più avanti nella procedura di aggiornamento.

   b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

      `security key-manager external show -instance security key-manager key query`

7. Raccogliere gli ID di sistema dei nodi esistenti:

   ```
   metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid
   ```

   Il seguente output mostra i dischi riassegnati.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Rimozione del monitoraggio di Mediator o Tiebreaker

Prima di aggiornare le piattaforme, è necessario rimuovere il monitoraggio se la configurazione MetroCluster viene monitorata con l'utility Tiebreaker o Mediator.

Fasi

1. Raccogliere l'output per il seguente comando:

   ```
   storage iscsi-initiator show
   ```

2. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza…	Utilizzare questa procedura…
Spareggio	"Rimozione delle configurazioni MetroCluster"
Mediatore	Immettere il seguente comando dal prompt di ONTAP: `metrocluster configuration-settings mediator remove`
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Il `maintenance-window-in-hours` parametro specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Ripetere questi passaggi sul sito del partner.

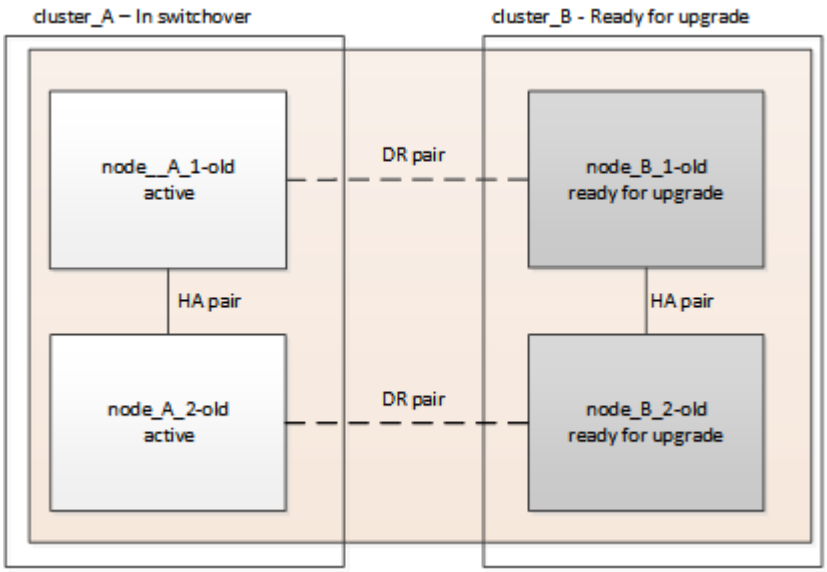
Passaggio alla configurazione MetroCluster

È necessario passare alla configurazione Site_A in modo che le piattaforme sul sito_B possano essere aggiornate.

A proposito di questa attività

Questa attività deve essere eseguita sul sito_A.

Al termine di questa attività, cluster_A è attivo e fornisce dati per entrambi i siti. Cluster_B è inattivo e pronto per iniziare il processo di aggiornamento.



Fasi

1. Passare alla configurazione MetroCluster del sito_A in modo che i nodi del sito_B possano essere aggiornati:

   a. Eseguire il seguente comando sul cluster_A:

```
metrocluster switchover -controller-replacement true
```

Il completamento dell'operazione può richiedere alcuni minuti.

b. Monitorare il funzionamento dello switchover:

```
metrocluster operation show
```

c. Al termine dell'operazione, verificare che i nodi siano in stato di switchover:

```
metrocluster show
```

d. Controllare lo stato dei nodi MetroCluster:

```
metrocluster node show
```

La riparazione automatica degli aggregati dopo lo switchover negoziato viene disattivata durante l'aggiornamento del controller.

Rimozione delle configurazioni dell'interfaccia e disinstallazione dei vecchi controller

È necessario spostare i file LIF dei dati su una porta comune, rimuovere le VLAN e i gruppi di interfacce sui vecchi controller, quindi disinstallare fisicamente i controller.

A proposito di questa attività

- Questi passaggi vengono eseguiti sui vecchi controller (node_B_1-old, node_B_2-old).
- Consultare le informazioni raccolte in "Mappatura delle porte dai vecchi nodi ai nuovi nodi".

Fasi

1. Avviare i vecchi nodi e accedere ai nodi:

```
boot_ontap
```

2. Assegnare la porta home di tutti i file LIF di dati sul vecchio controller a una porta comune identica sia sul vecchio che sul nuovo modulo controller.

   a. Visualizzare le LIF:

```
network interface show
```

   Tutti i dati LIFS, inclusi SAN e NAS, verranno gestiti e non verranno gestiti dal sistema operativo poiché sono attivi nel sito di switchover (cluster_A).

   b. Esaminare l'output per trovare una porta di rete fisica comune che sia la stessa sui controller vecchi e nuovi che non sia utilizzata come porta del cluster.

   Ad esempio, e0d è una porta fisica sui vecchi controller ed è presente anche sui nuovi controller. e0d non viene utilizzato come porta del cluster o in altro modo sui nuovi controller.

   Per informazioni sull'utilizzo delle porte per i modelli di piattaforma, consultare "NetApp Hardware Universe"

c. Modificare tutti i dati LIFS per utilizzare la porta comune come porta home:
`network interface modify -vserver svm-name -lif data-lif -home-port port-id`

Nell'esempio seguente, questo è "e0d".

Ad esempio:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Rimuovere tutte le porte VLAN utilizzando le porte del cluster come porte membro e ifgrps utilizzando le porte del cluster come porte membro.

a. Eliminare le porte VLAN:
`network port vlan delete -node node-name -vlan-name portid-vlandid`

Ad esempio:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Rimuovere le porte fisiche dai gruppi di interfacce:

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

Ad esempio:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Rimuovere le porte della VLAN e del gruppo di interfacce dal dominio di broadcast:

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

b. Modificare le porte del gruppo di interfacce per utilizzare altre porte fisiche come membro in base alle necessità.:

`ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id`

4. Arrestare i nodi al prompt DEL CARICATORE:

`halt -inhibit-takeover true`

5. Connettersi alla console seriale dei vecchi controller (Node_B_1-old e Node_B_2-old) nel sito_B e verificare che venga visualizzato il prompt DEL CARICATORE.
6. Raccogliere i valori di bootarg:

`printenv`

7. Scollegare le connessioni di storage e di rete su Node_B_1-old e Node_B_2-old ed etichettare i cavi in modo che possano essere ricollegati ai nuovi nodi.
8. Scollegare i cavi di alimentazione da Node_B_1-old e Node_B_2-old.
9. Rimuovere i controller Node_B_1-old e Node_B_2-old dal rack.

Aggiornamento degli RCF dello switch per adattarsi alle nuove piattaforme

È necessario aggiornare gli switch a una configurazione che supporti i nuovi modelli di piattaforma.

A proposito di questa attività

Questa attività viene eseguita nel sito contenente i controller attualmente in fase di aggiornamento. Negli esempi illustrati in questa procedura, si esegue prima l'aggiornamento di Site_B.

Gli switch del sito_A verranno aggiornati quando i controller del sito_A verranno aggiornati.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire i passaggi della procedura per il fornitore dello switch:

   "Installazione e configurazione di MetroCluster IP"

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"
2. Scaricare e installare i file RCF.

   Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP".

   - "Download e installazione dei file RCF Broadcom"
   - "Download e installazione dei file Cisco IP RCF"

Configurazione dei nuovi controller

È necessario eseguire il rack e installare i controller, eseguire la configurazione richiesta in modalità manutenzione, quindi avviare i controller e verificare la configurazione LIF sui controller.

Configurazione dei nuovi controller

I nuovi controller devono essere montati in rack e cablati.

Fasi

1. Pianificare il posizionamento dei nuovi moduli controller e degli shelf di storage in base alle necessità.

   Lo spazio rack dipende dal modello di piattaforma dei moduli controller, dai tipi di switch e dal numero di shelf di storage nella configurazione.

2. Mettere a terra l'utente.
3. Installare i moduli controller nel rack o nell'armadietto.

   "Documentazione dei sistemi hardware ONTAP"

4. Collegare i controller agli switch IP come descritto in "Installazione e configurazione di MetroCluster IP".
    - "Cablaggio degli switch IP"
5. Accendere i nuovi nodi e avviarli in modalità manutenzione.

Ripristino della configurazione HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:

    a. Verificare le impostazioni correnti delle porte:

    ```
    ucadmin show
    ```

    b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*
Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

2. Uscire dalla modalità di manutenzione:

    ```
    halt
    ```

    Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

3. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

    ```
    boot_ontap maint
    ```

4. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Impostazione dello stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Lo stato ha per tutti i componenti deve essere “mccip”.

2. Se lo stato di sistema visualizzato del controller o dello chassis non è corretto, impostare lo stato ha:

   ```
   ha-config modify controller mccip
   ```

   ```
   ha-config modify chassis mccip
   ```

Impostazione delle variabili di boot MetroCluster IP

Alcuni valori di boot MetroCluster IP devono essere configurati sui nuovi moduli controller. I valori devono corrispondere a quelli configurati sui vecchi moduli controller.

A proposito di questa attività

In questa attività, verranno utilizzati gli UUID e gli ID di sistema identificati in precedenza nella procedura di aggiornamento in "Raccolta di informazioni prima dell’aggiornamento".

Fasi

1. Se i nodi da aggiornare sono i modelli AFF A400, FAS8300 o FAS8700, impostare i seguenti bootargs al prompt DEL CARICATORE:

   ```
   setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
   partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
   ```

   ```
   setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
   partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
   ```

   > Se le interfacce utilizzano le VLAN predefinite, l’id vlan non è necessario.

   I seguenti comandi impostano i valori per Node_B_1-New utilizzando VLAN 120 per la prima rete e VLAN 130 per la seconda rete:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

   I seguenti comandi impostano i valori per Node_B_2-New utilizzando VLAN 120 per la prima rete e VLAN 130 per la seconda rete:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

L'esempio seguente mostra i comandi per node_B_1-new quando viene utilizzata la VLAN predefinita:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

L'esempio seguente mostra i comandi per node_B_2-new quando viene utilizzata la VLAN predefinita:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. Se i nodi da aggiornare non sono sistemi elencati nella fase precedente, al prompt DEL CARICATORE per ciascuno dei nodi sopravvissuti, impostare i seguenti bootargs con local_IP/mask:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   I seguenti comandi impostano i valori per node_B_1-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

   I seguenti comandi impostano i valori per node_B_2-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

3. Al prompt DEL CARICATORE dei nuovi nodi, impostare gli UUID:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Impostare gli UUID su Node_B_1-New.

      L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_1-New:

      ```
      setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
      setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
      00a098ca379f
      setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
      00a098908039
      ```

   b. Impostare gli UUID su Node_B_2-New:

      L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_2-New:

   ```
   setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
   setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
   00a098c9e55d
   setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
   setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
   setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
   ```

4. Se i sistemi originali sono stati configurati per ADP, al prompt DEL CARICATORE di ciascun nodo sostitutivo, abilitare ADP:

   `setenv bootarg.mcc.adp_enabled true`

5. Impostare le seguenti variabili:

   `setenv bootarg.mcc.local_config_id` *`original-sys-id`*

   `setenv bootarg.mcc.dr_partner` *`dr-partner-sys-id`*

> Il `setenv bootarg.mcc.local_config_id` Variable deve essere impostato sul sys-id del modulo controller **original**, node_B_1-old.

a. Impostare le variabili su Node_B_1-New.

   L'esempio seguente mostra i comandi per impostare i valori su Node_B_1-New:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Impostare le variabili su Node_B_2-new.

   L'esempio seguente mostra i comandi per impostare i valori su Node_B_2-New:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

6. Se si utilizza la crittografia con il gestore delle chiavi esterno, impostare i bootargs richiesti:

```
setenv bootarg.kmip.init.ipaddr

setenv bootarg.kmip.kmip.init.netmask

setenv bootarg.kmip.kmip.init.gateway

setenv bootarg.kmip.kmip.init.interface
```

Riassegnazione dei dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando i sistemi raccolti in precedenza.

A proposito di questa attività

Questi passaggi vengono eseguiti in modalità manutenzione.

> I dischi aggregati root sono gli unici dischi che devono essere riassegnati durante il processo di upgrade dei controller. La proprietà del disco degli aggregati di dati viene gestita come parte dell'operazione di switchover/switchback.

Fasi

1. Avviare il sistema in modalità di manutenzione:

```
boot_ontap maint
```

2. Visualizzare i dischi su Node_B_1-New dal prompt della modalità di manutenzione:

```
disk show -a
```

   L'output del comando mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi

aggregati root sono ancora di proprietà del vecchio ID di sistema (537403322). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.
```

3. Riassegnare i dischi aggregati root sugli shelf di dischi ai nuovi controller.

Se si utilizza ADP…	Quindi utilizzare questo comando…
Sì	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
No	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Riassegnare i dischi aggregati root sugli shelf di dischi ai nuovi controller:

   `disk reassign -s old-sysid -d new-sysid`

   L'esempio seguente mostra la riassegnazione dei dischi in una configurazione non ADP:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verificare che i dischi dell'aggregato root siano riassegnati correttamente in modalità vecchia rimozione:

   ```
   disk show
   ```

   ```
   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                     DR HOME
------------             -------------            -----  -------------
-------------            -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Avviare i nuovi controller

È necessario avviare i nuovi controller, assicurandosi che le variabili di boot siano corrette e, se necessario, eseguire le operazioni di ripristino della crittografia.

Fasi

1. Arrestare i nuovi nodi:

   ```
   halt
   ```

2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Verificare se il sistema partner è quello corrente:

   ```
   printenv partner-sysid
   ```

   Se il partner-sysid non è corretto, impostarlo:

   ```
   setenv partner-sysid partner-sysID
   ```

4. Visualizzare il menu di avvio di ONTAP:

   ```
   boot_ontap menu
   ```

5. Se viene utilizzata la crittografia root, selezionare l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione `10` Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione `11` Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

6. Dal menu di avvio, selezionare "(6) Update flash from backup config".

   > L'opzione 6 riavvia il nodo due volte prima del completamento.

   Rispondere "y" alle richieste di modifica dell'id di sistema. Attendere i secondi messaggi di riavvio:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Sul CARICATORE, controllare due volte i valori di bootarg e aggiornarli secondo necessità.

   Attenersi alla procedura descritta in "Impostazione delle variabili di boot MetroCluster IP".

8. Verificare che il sistema partner sia corretto:

   ```
   printenv partner-sysid
   ```

   Se il partner-sysid non è corretto, impostarlo:

```
setenv partner-sysid partner-sysID
```

9. Se viene utilizzata la crittografia root, selezionare nuovamente l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione `10` Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.
Gestione esterna delle chiavi	Opzione "11" Seguire le istruzioni per fornire gli input necessari per ripristinare la configurazione di gestione delle chiavi.

A seconda dell'impostazione del gestore delle chiavi, eseguire la procedura di ripristino selezionando l'opzione "10" o l'opzione "11", quindi l'opzione `6` al primo prompt del menu di avvio. Per avviare completamente i nodi, potrebbe essere necessario ripetere la procedura di ripristino, continua con l'opzione "1" (boot normale).

10. Attendere l'avvio dei nodi sostituiti.

    Se uno dei nodi è in modalità Takeover, eseguire un giveback utilizzando `storage failover giveback` comando.

11. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Verificare che tutte le porte si trovino in un dominio di trasmissione:

    a. Visualizzare i domini di trasmissione:

    ```
    network port broadcast-domain show
    ```

    b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

    "Aggiunta o rimozione di porte da un dominio di broadcast"

c. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

   L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

   "Creazione di una VLAN"

"Combinazione di porte fisiche per creare gruppi di interfacce"

Verifica e ripristino della configurazione LIF

Verificare che i file LIF siano ospitati su nodi e porte appropriati, come mappati all'inizio della procedura di aggiornamento.

A proposito di questo tsak

- Questa attività viene eseguita sul sito_B.
- Vedere il piano di mappatura delle porte creato in "Mappatura delle porte dai vecchi nodi ai nuovi nodi".

Fasi

1. Verificare che i file LIF siano ospitati sul nodo e sulle porte appropriati prima di passare al switchback.

   a. Passare al livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

   b. Eseguire l'override della configurazione della porta per garantire il corretto posizionamento di LIF:

      ```
      vserver config override -command "network interface modify -vserver
      vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
      new_node_name"
      ```

   Quando si immette il comando di modifica dell'interfaccia di rete in `vserver config override` non è possibile utilizzare la funzione di completamento automatico della scheda. È possibile creare la rete `interface modify` utilizzando il completamento automatico e quindi racchiuderlo in `vserver config override` comando.

   a. Tornare al livello di privilegio admin:

      ```
      set -privilege admin
      ```

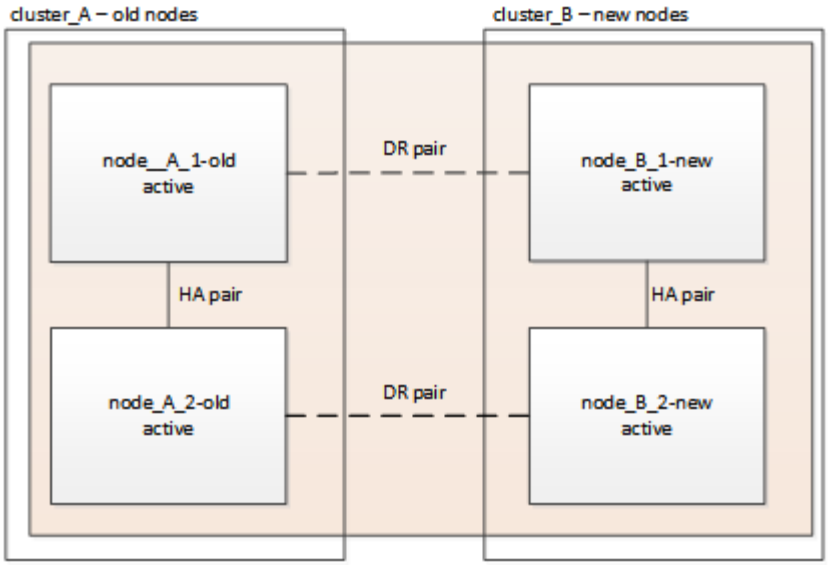
2. Ripristinare le interfacce nel nodo principale:

   ```
   network interface revert * -vserver vserver-name
   ```

   Eseguire questo passaggio su tutte le SVM secondo necessità.

Tornare indietro alla configurazione MetroCluster

In questa attività, viene eseguita l'operazione di switchback e la configurazione MetroCluster torna al funzionamento normale. I nodi sul sito_A sono ancora in attesa di aggiornamento.



Fasi

1. Eseguire il `metrocluster node show` Su Site_B e controllare l'output.
   a. Verificare che i nuovi nodi siano rappresentati correttamente.
   b. Verificare che i nuovi nodi siano nello stato "in attesa di switchback".
2. Eseguire la riparazione e lo switchback eseguendo i comandi richiesti da qualsiasi nodo del cluster attivo (il cluster che non è in fase di aggiornamento).
   a. Riparare gli aggregati di dati:
      `metrocluster heal aggregates`
   b. Riparare gli aggregati root:

      `metrocluster heal root`

   c. Switchback del cluster:

      `metrocluster switchback`

3. Controllare l'avanzamento dell'operazione di switchback:

   `metrocluster show`

   L'operazione di switchback è ancora in corso quando viene visualizzato l'output `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'operazione di switchback è completa quando l'output visualizza normale:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando. Questo comando si trova al livello di privilegio avanzato.

Verifica dello stato della configurazione di MetroCluster

Dopo aver aggiornato i moduli controller, è necessario verificare lo stato della configurazione MetroCluster.

A proposito di questa attività

Questa attività può essere eseguita su qualsiasi nodo della configurazione MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster:
   a. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale: `metrocluster show`
   b. Eseguire un controllo MetroCluster: `metrocluster check run`
   c. Visualizzare i risultati del controllo MetroCluster:

      `metrocluster check show`

2. Verificare lo stato e la connettività MetroCluster.

a. Verificare le connessioni IP MetroCluster:

```
storage iscsi-initiator show
```

b. Verificare che i nodi funzionino:

```
metrocluster node show
```

c. Verificare che le interfacce IP di MetroCluster siano disponibili:

```
metrocluster configuration-settings interface show
```

d. Verificare che il failover locale sia attivato:

```
storage failover show
```

Aggiornamento dei nodi sul cluster_A.

È necessario ripetere le attività di aggiornamento su cluster_A.

Fasi

1. Ripetere i passaggi per aggiornare i nodi sul cluster_A, iniziando da "Preparazione per l'aggiornamento".

   Durante l'esecuzione delle attività, tutti i riferimenti di esempio ai cluster e ai nodi vengono invertiti. Ad esempio, quando l'esempio viene dato allo switchover da cluster_A, si passa da cluster_B.

Ripristino del monitoraggio di Tiebreaker o Mediator

Dopo aver completato l'aggiornamento della configurazione MetroCluster, è possibile riprendere il monitoraggio con l'utility Tiebreaker o Mediator.

Fasi

1. Ripristinare il monitoraggio, se necessario, utilizzando la procedura per la configurazione.

Se si utilizza…	Utilizzare questa procedura
Spareggio	"Aggiunta di configurazioni MetroCluster".
Mediatore	Link:../install-ip/concept_mediator_requirements.html [Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster].
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Invio di un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completato l'aggiornamento, inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

Fasi

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.
   a. Eseguire il seguente comando:
      `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Ripetere il comando sul cluster partner.

Upgrade dei controller da AFF A700/FAS9000 a AFF A900/FAS9500 in una configurazione MetroCluster IP utilizzando switchover e switchback (ONTAP 9.10.1 o versione successiva)

È possibile utilizzare l'operazione di switchover MetroCluster per fornire un servizio senza interruzioni ai client mentre i moduli controller sul cluster partner vengono aggiornati. Altri componenti (ad esempio shelf di storage o switch) non possono essere aggiornati come parte di questa procedura.

A proposito di questa attività

- Per aggiornare i moduli controller AFF A700 a AFF A900, i controller devono eseguire ONTAP 9.10.1 o versione successiva.
- Per aggiornare i moduli controller FAS9000 a FAS9500, i controller devono eseguire ONTAP 9.10.1P3 o versione successiva.
- Tutti i controller della configurazione devono essere aggiornati durante lo stesso periodo di manutenzione.

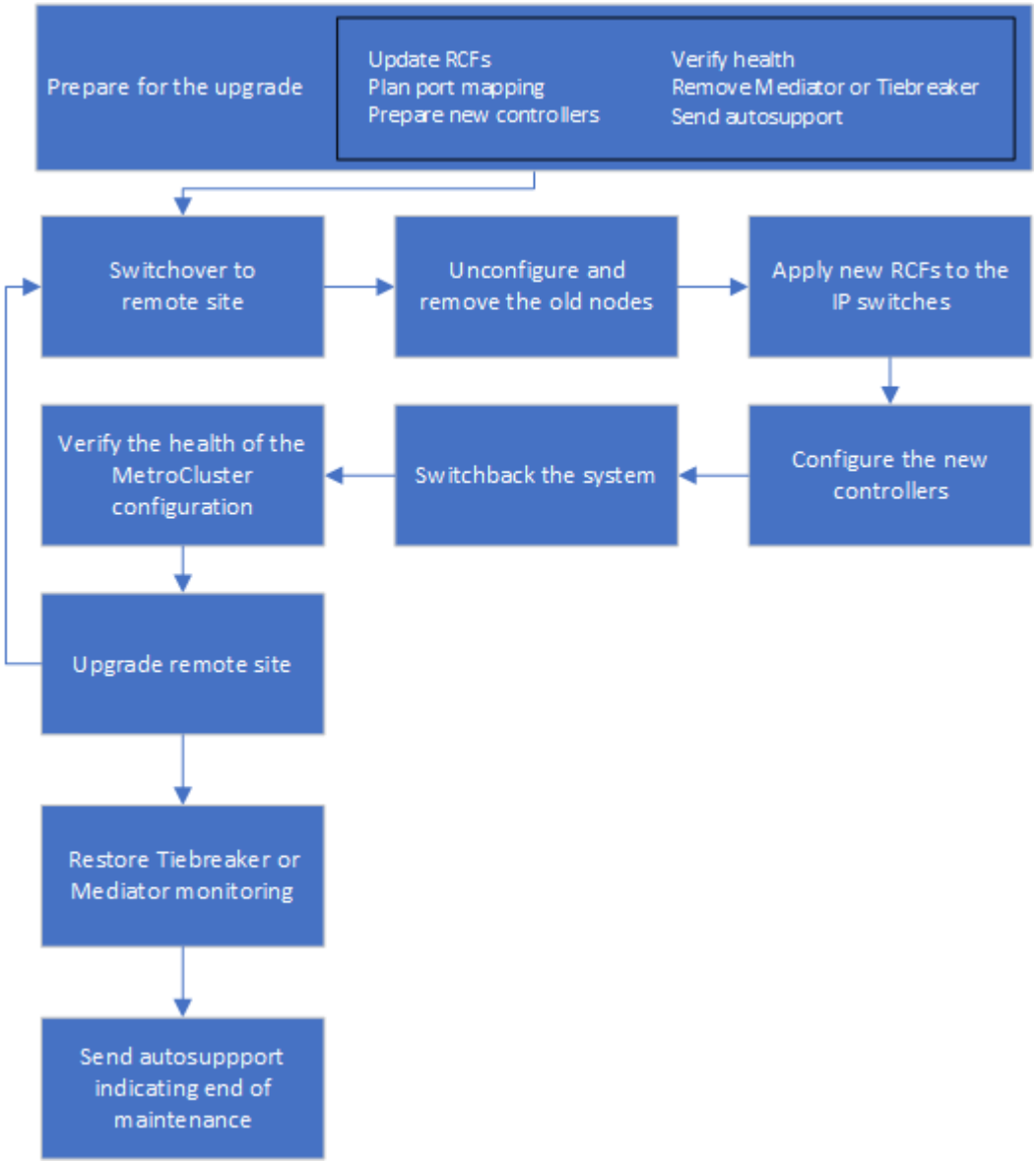
  L'utilizzo della configurazione MetroCluster con un AFF A700 e un AFF A900 o con un FAS9000 e un controller FAS9500 non è supportato al di fuori di questa attività di manutenzione.

- Gli switch IP devono disporre di una versione firmware supportata.
- Gli indirizzi IP, le netmask e i gateway delle piattaforme originali verranno riutilizzati sulle nuove piattaforme.
- In questa procedura vengono utilizzati i seguenti nomi di esempio, sia negli esempi che nella grafica:
  - Sito_A.
    - Prima dell'aggiornamento:
      - Node_A_1-A700
      - Node_A_2-A700
    - Dopo l'aggiornamento:
      - Node_A_1-A900
      - Node_A_2-A900
  - Sito_B
    - Prima dell'aggiornamento:
      - Node_B_1-A700
      - Node_B_2-A700

- Dopo l'aggiornamento:
  - Node_B_1-A900
  - Node_B_2-A900

Workflow per l'aggiornamento dei controller in una configurazione MetroCluster IP

È possibile utilizzare il diagramma del flusso di lavoro per pianificare le attività di aggiornamento.



Preparatevi per l'aggiornamento

Prima di apportare modifiche alla configurazione MetroCluster esistente, è necessario controllare lo stato della configurazione, preparare le nuove piattaforme ed eseguire altre attività varie.

Liberare lo slot 7 del controller AFF A700 o FAS9000

La configurazione MetroCluster su un sistema AFF A900 o FAS9500 utilizza una delle porte delle schede DR situate negli slot 5 e 7. Prima di iniziare l'aggiornamento, se sono presenti schede nello slot 7 del sistema AFF A700 o FAS9000, è necessario spostarle in altri slot per tutti i nodi del cluster.

Aggiornare i file RCF dello switch MetroCluster prima di aggiornare i controller

Quando si esegue questo aggiornamento, è necessario aggiornare i file RCF sugli switch MetroCluster. La seguente tabella fornisce gli intervalli di VLAN supportati per le configurazioni IP MetroCluster AFF A900/FAS9500.

Modello di piattaforma	ID VLAN supportati
• AFF A900 o FAS9500	• 10 • 20 • Qualsiasi valore compreso tra 101 e 4096 inclusi.

- Se lo switch non è configurato con la versione minima supportata del file RCF, è necessario aggiornare il file RCF. Per la versione del file RCF corretta per il modello di switch in uso, fare riferimento a. "Tool RcfFileGenerator". La procedura seguente riguarda l'applicazione file RCF.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP" contenuto.

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"

2. Scaricare e installare i file RCF.

   Seguire la procedura descritta in "Installazione e configurazione di MetroCluster IP" contenuto.

   - "Download e installazione dei file RCF Broadcom"
   - "Download e installazione dei file Cisco IP RCF"

Mappare le porte dai vecchi nodi ai nuovi nodi

Quando si esegue l'aggiornamento da AFF A700 a AFF A900 o da FAS9000 a FAS9500, non è necessario modificare le porte della rete dati, dell'adattatore SAN FCP e delle porte di storage SAS e NVMe. Le LIF dei dati rimangono dove si trovano durante e dopo l'aggiornamento. Pertanto, non è necessario mappare le porte di rete dai vecchi nodi ai nuovi nodi.

Verificare lo stato di salute di MetroCluster prima dell'aggiornamento del sito

Prima di eseguire l'aggiornamento, è necessario verificare lo stato e la connettività della configurazione di MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che i nodi siano multipathing:
   `node run -node node-name sysconfig -a`

      Eseguire questo comando per ogni nodo della configurazione MetroCluster.

b. Verificare che non vi siano dischi rotti nella configurazione:
`storage disk show -broken`

Eseguire questo comando su ciascun nodo della configurazione MetroCluster.

c. Verificare la presenza di eventuali avvisi sullo stato di salute:

```
system health alert show
```

Eseguire questo comando su ciascun cluster.

d. Verificare le licenze sui cluster:

```
system license show
```

Eseguire questo comando su ciascun cluster.

e. Verificare i dispositivi collegati ai nodi:

```
network device-discovery show
```

Eseguire questo comando su ciascun cluster.

f. Verificare che il fuso orario e l'ora siano impostati correttamente su entrambi i siti:

```
cluster date show
```

Eseguire questo comando su ciascun cluster. È possibile utilizzare `cluster date` per configurare l'ora e il fuso orario.

2. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.

a. Confermare la configurazione MetroCluster e che la modalità operativa è `normal`:
`metrocluster show`

b. Verificare che siano visualizzati tutti i nodi previsti:
`metrocluster node show`

c. Immettere il seguente comando:

```
metrocluster check run
```

d. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

3. Controllare il cablaggio MetroCluster con lo strumento Config Advisor.

a. Scaricare ed eseguire Config Advisor.

"Download NetApp: Config Advisor"

b. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

Raccogliere informazioni prima dell'aggiornamento

Prima di eseguire l'aggiornamento, è necessario raccogliere informazioni per ciascuno dei nodi e, se necessario, regolare i domini di broadcast di rete, rimuovere eventuali VLAN e gruppi di interfacce e raccogliere informazioni sulla crittografia.

Fasi

1. Registrare il cablaggio fisico di ciascun nodo, etichettando i cavi secondo necessità per consentire il cablaggio corretto dei nuovi nodi.
2. Raccogliere l'output dei seguenti comandi per ciascun nodo:
   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node node-name`
   - `network port ifgrp show -node node_name -instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`
   - `storage aggregate show`
   - `system node run -node node-name sysconfig -a`
   - `vserver fcp initiator show`
   - `storage disk show`
   - `metrocluster configuration-settings interface show`
3. Raccogliere gli UUID per il sito_B (il sito le cui piattaforme sono attualmente in fase di aggiornamento): `metrocluster node show -fields node-cluster-uuid, node-uuid`

   Questi valori devono essere configurati con precisione sui nuovi moduli controller Site_B per garantire un aggiornamento corretto. Copiare i valori in un file in modo da poterli copiare nei comandi appropriati in un secondo momento del processo di aggiornamento. + l'esempio seguente mostra l'output del comando con gli UUID:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
   (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1-A700 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2-A700 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1-A700 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2-A700 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

Si consiglia di registrare gli UUID in una tabella simile alla seguente.

Cluster o nodo	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1-A700	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2-A700	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A.	ee7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1-A700	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2-A700	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. Se i nodi MetroCluster si trovano in una configurazione SAN, raccogliere le informazioni pertinenti.

   Si dovrebbe ottenere l'output dei seguenti comandi:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`
5. Se il volume root è crittografato, raccogliere e salvare la passphrase utilizzata per il gestore delle chiavi: `security key-manager backup show`
6. Se i nodi MetroCluster utilizzano la crittografia per volumi o aggregati, copiare le informazioni relative alle

chiavi e alle passphrase. Per ulteriori informazioni, vedere "Backup manuale delle informazioni di gestione delle chiavi integrate".

a. Se Onboard Key Manager è configurato: `security key-manager onboard show-backup`+ la passphrase sarà necessaria più avanti nella procedura di aggiornamento.

b. Se la gestione delle chiavi aziendali (KMIP) è configurata, eseguire i seguenti comandi:

```
security key-manager external show -instance
security key-manager key query
```

7. Raccogliere gli ID di sistema dei nodi esistenti: `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   Il seguente output mostra i dischi riassegnati.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1-A700   537403324     537403323
537403321           537403322
1           cluster_A node_A_2-A700   537403323     537403324
537403322           537403321
1           cluster_B node_B_1-A700   537403322     537403321
537403323           537403324
1           cluster_B node_B_2-A700   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Rimuovere il monitoraggio di Mediator o Tiebreaker

Prima di aggiornare le piattaforme, è necessario rimuovere il monitoraggio se la configurazione MetroCluster viene monitorata con l'utility Tiebreaker o Mediator.

Fasi

1. Raccogliere l'output per il seguente comando:

   ```
   storage iscsi-initiator show
   ```

2. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza…	Utilizzare questa procedura…

Spareggio	"Rimozione delle configurazioni MetroCluster" Nel *contenuto di installazione e configurazione di MetroCluster Tiebreaker*
Mediatore	Immettere il seguente comando dal prompt di ONTAP: `metrocluster configuration-settings mediator remove`
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Inviare un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, è necessario inviare un messaggio AutoSupport per informare il supporto tecnico che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Il `maintenance-window-in-hours` parametro specifica la lunghezza della finestra di manutenzione, con un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Ripetere questi passaggi sul sito del partner.

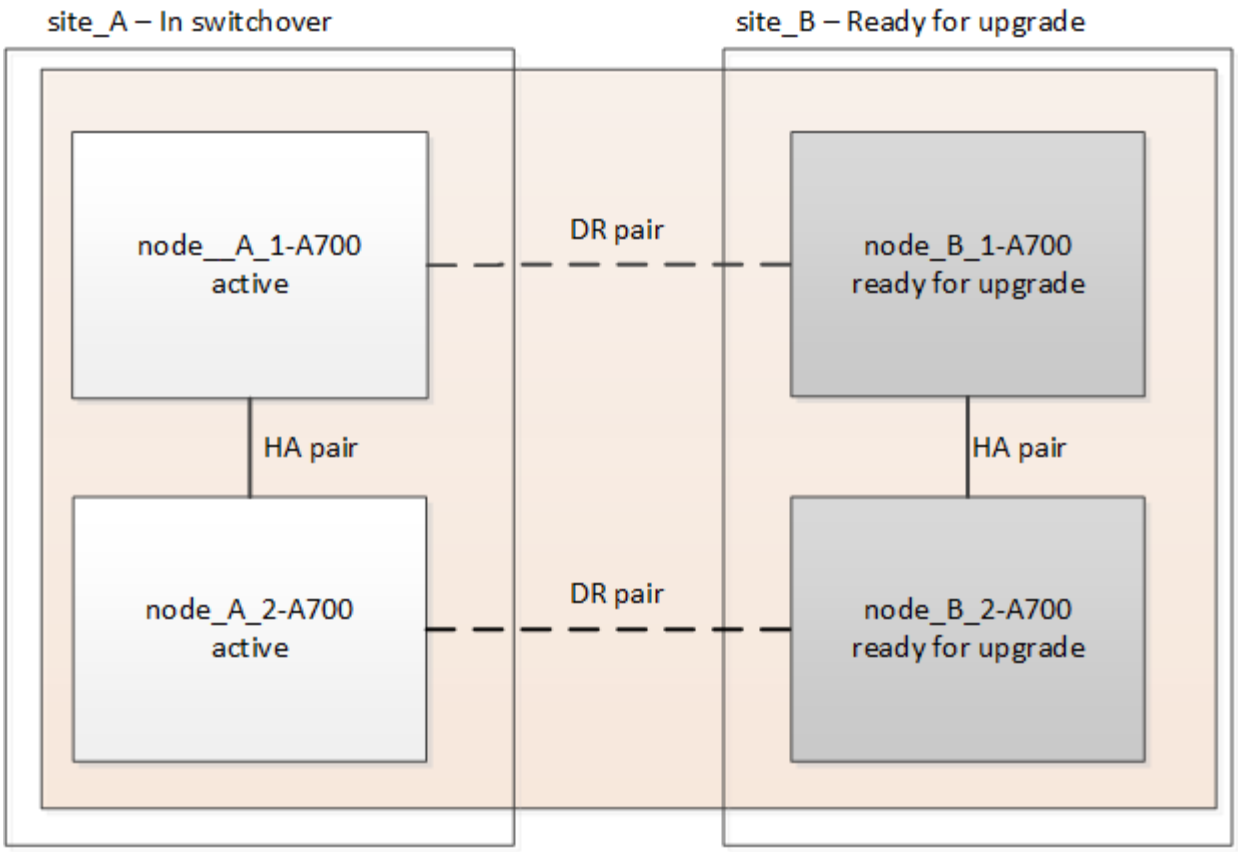
Passare alla configurazione MetroCluster

È necessario passare alla configurazione Site_A in modo che le piattaforme sul sito_B possano essere aggiornate.

A proposito di questa attività

Questa attività deve essere eseguita sul sito_A.

Dopo aver completato questa attività, Site_A è attivo e fornisce dati per entrambi i siti. Site_B è inattivo e pronto per iniziare il processo di aggiornamento.



Fasi

1. Passare alla configurazione MetroCluster del sito_A in modo che i nodi del sito_B possano essere aggiornati:

   a. Eseguire il seguente comando sul sito_A:

   ```
   metrocluster switchover -controller-replacement true
   ```

   Il completamento dell'operazione può richiedere alcuni minuti.

   b. Monitorare il funzionamento dello switchover:

   ```
   metrocluster operation show
   ```

   c. Al termine dell'operazione, verificare che i nodi siano in stato di switchover:

   ```
   metrocluster show
   ```

   d. Controllare lo stato dei nodi MetroCluster:

   ```
   metrocluster node show
   ```

   La riparazione automatica degli aggregati dopo lo switchover negoziato viene disattivata durante l'aggiornamento del controller. I nodi nel sito_B vengono arrestati e arrestati nel `LOADER` prompt.

Rimuovere il modulo controller della piattaforma AFF A700 o FAS9000 e il modulo NVS

A proposito di questa attività

Se non si è già collegati a terra, mettere a terra l'utente.

Fasi

1. Raccogliere i valori di bootarg da entrambi i nodi nel sito_B: `printenv`
2. Spegnere lo chassis sul sito_B.

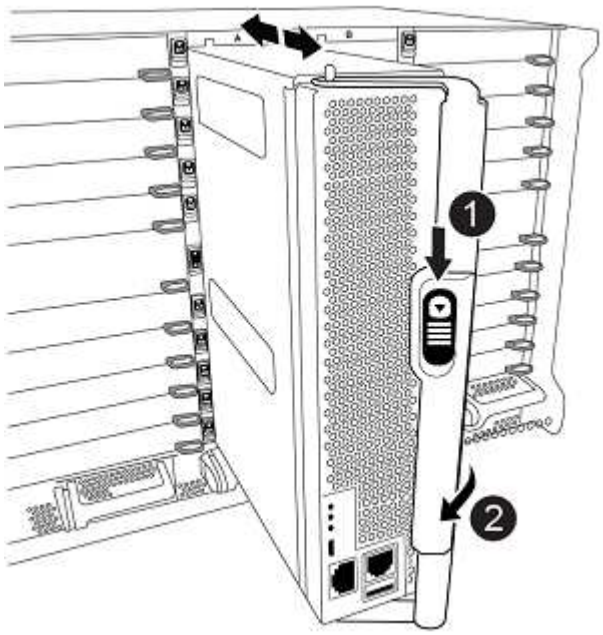
Rimuovere il modulo del controller AFF A700 o FAS9000

Utilizzare la seguente procedura per rimuovere il modulo controller AFF A700 o FAS9000

Fasi

1. Scollegare il cavo della console, se presente, e il cavo di gestione dal modulo controller prima di rimuovere il modulo controller.
2. Sbloccare e rimuovere il modulo controller dal telaio.

   a. Far scorrere il pulsante arancione sulla maniglia della camma verso il basso fino a sbloccarla.



1	Pulsante di rilascio della maniglia della camma
2	Maniglia CAM

   a. Ruotare la maniglia della camma in modo da disimpegnare completamente il modulo controller dal telaio, quindi estrarre il modulo controller dal telaio. Assicurarsi di sostenere la parte inferiore del modulo controller mentre lo si sposta fuori dallo chassis.

Rimuovere il modulo NVS AFF A700 o FAS9000

Per rimuovere il modulo NVS AFF A700 o FAS9000, attenersi alla seguente procedura.

Nota: Il modulo NVS si trova nello slot 6 e presenta un'altezza doppia rispetto agli altri moduli del sistema.

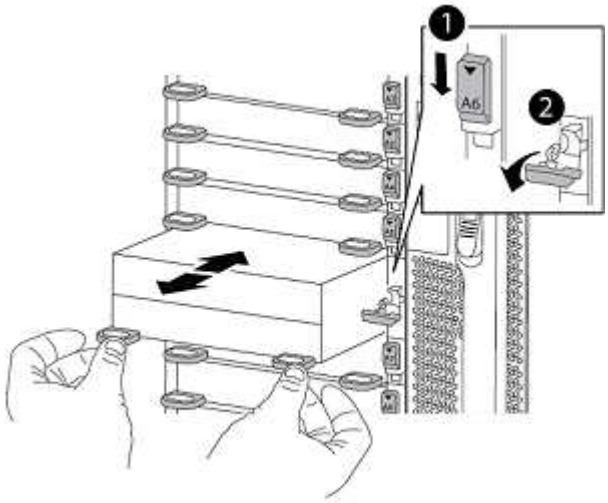
Fasi

1. Sbloccare e rimuovere l'NVS dallo slot 6.

   a. Premere il tasto 'Cam' con lettere e numeri. Il pulsante CAM si allontana dal telaio.

   b. Ruotare il fermo della camma verso il basso fino a portarlo in posizione orizzontale. Il sistema NVS si disinnesta dal telaio e si sposta di pochi centimetri.

   c. Rimuovere l'NVS dal telaio tirando le linguette di estrazione ai lati della superficie del modulo.



	Latch i/o Cam intestato e numerato
	Fermo i/o completamente sbloccato

2. Se si utilizzano moduli aggiuntivi utilizzati come dispositivi di coredump su AFF A700 o FAS9000 NVS, non trasferirli su AFF A900 o FAS9500 NVS. Non trasferire alcuna parte dal modulo controller AFF A700 o FAS9000 e NVS al modulo AFF A900 o FAS9500.

Installare i moduli NVS e controller AFF A900 o FAS9500

È necessario installare il modulo NVS e controller AFF A900 o FAS9500 ricevuto nel kit di aggiornamento su entrambi i nodi presso il sito_B. Non spostare il dispositivo di coredump dal modulo NVS AFF A700 o FAS9000 al modulo NVS AFF A900 o FAS9500.

A proposito di questa attività

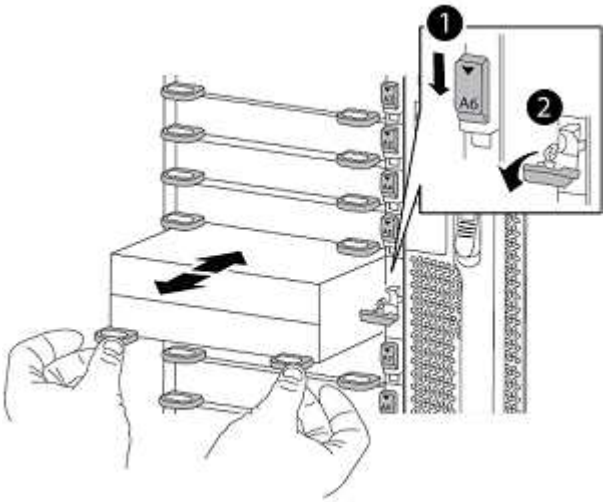
Se non si è già collegati a terra, mettere a terra l'utente.

Installare AFF A900 o FAS9500 NVS

Utilizzare la seguente procedura per installare AFF A900 o FAS9500 NVS nello slot 6 di entrambi i nodi nel sito_B.

Fasi

1. Allineare l'NVS con i bordi dell'apertura dello chassis nello slot 6.
2. Far scorrere delicatamente l'NVS nello slot fino a quando il dispositivo di chiusura della camma i/o con lettere e numeri non inizia a impegnarsi con il perno della camma i/o, quindi spingere il dispositivo di chiusura della camma i/o fino in fondo per bloccare l'NVS in posizione.



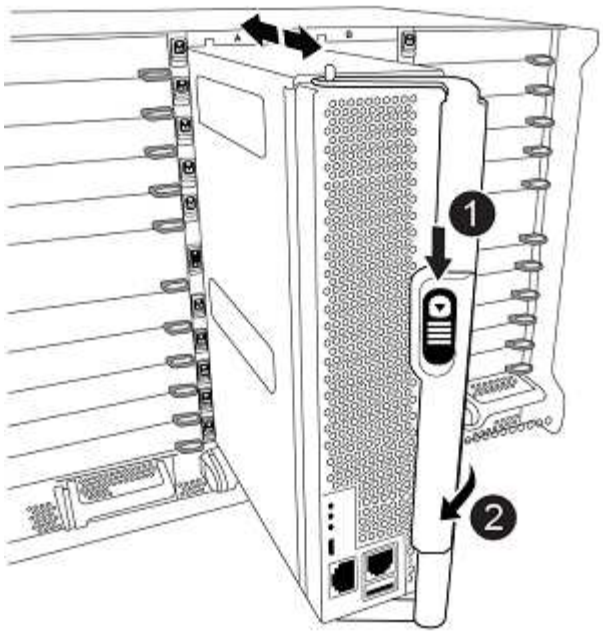
	Latch i/o Cam intestato e numerato
	Fermo i/o completamente sbloccato

Installare il modulo controller AFF A900 o FAS9500.

Utilizzare la seguente procedura per installare il modulo controller AFF A900 o FAS9500.

Fasi

1. Allineare l'estremità del modulo controller con l'apertura dello chassis, quindi spingere delicatamente il modulo controller a metà nel sistema.
2. Spingere con decisione il modulo controller nello chassis fino a quando non raggiunge la scheda intermedia e non è completamente inserito. Il dispositivo di chiusura si solleva quando il modulo controller è completamente inserito. Attenzione: Per evitare di danneggiare i connettori, non esercitare una forza eccessiva quando si fa scorrere il modulo controller nel telaio.
3. Collegare le porte di gestione e console al modulo controller.



1	Pulsante di rilascio della maniglia della camma
2	Maniglia CAM

4. Installare la seconda scheda X91146A nello slot 7 di ciascun nodo.
   a. Spostare la connessione e5b su e7b.
   b. Spostare la connessione e5a su e5b.

> Lo slot 7 su tutti i nodi del cluster deve essere vuoto, come indicato nella Mappare le porte dai vecchi nodi ai nuovi nodi sezione.

5. Accendere lo chassis e collegarlo alla console seriale.
6. Dopo l'inizializzazione del BIOS, se il nodo avvia l'autoboot, interrompere L'AUTOBOOT premendo Control-C.
7. Dopo l'interruzione dell'autoboot, i nodi si fermano al prompt DEL CARICATORE. Se non si interrompe l'autoboot in tempo e node1 inizia l'avvio, attendere che il prompt premi Ctrl-C per accedere al menu di boot. Dopo che il nodo si è arrestato nel menu di boot, usare l'opzione 8 per riavviare il nodo e interrompere l'autoboot durante il riavvio.
8. Al prompt DEL CARICATORE, impostare le variabili di ambiente predefinite: Set-defaults
9. Salvare le impostazioni predefinite delle variabili di ambiente: `saveenv`

Nodi NetBoot nel sito_B.

Dopo aver scambiato il modulo controller AFF A900 o FAS9500 e NVS, è necessario eseguire il netboot dei nodi AFF A900 o FAS9500 e installare la stessa versione e lo stesso livello di patch ONTAP in esecuzione sul cluster. Il termine netboot indica che si sta eseguendo l'avvio da un'immagine ONTAP memorizzata su un server remoto. Durante la preparazione per il netboot, è necessario aggiungere una copia dell'immagine di boot di ONTAP 9 su un server Web a cui il sistema può accedere. Non è possibile controllare la versione di ONTAP installata sul supporto di avvio di un modulo controller AFF A900 o FAS9500, a meno che non sia

installato in uno chassis e acceso. La versione di ONTAP sul supporto di avvio di AFF A900 o FAS9500 deve essere la stessa della versione di ONTAP in esecuzione sul sistema AFF A700 o FAS9000 in fase di aggiornamento e le immagini di avvio primaria e di backup devono corrispondere. È possibile configurare le immagini eseguendo un netboot seguito da `wipeconfig` dal menu di boot. Se il modulo controller è stato utilizzato in precedenza in un altro cluster, il `wipeconfig` il comando cancella qualsiasi configurazione residua sul supporto di avvio.

Prima di iniziare

- Verificare che sia possibile accedere a un server HTTP con il sistema.
- È necessario scaricare i file di sistema necessari per il sistema e la versione corretta di ONTAP dal sito del supporto NetApp.

A proposito di questa attività

Se la versione di ONTAP installata non corrisponde a quella installata sui controller originali, è necessario eseguire il netboot dei nuovi controller. Dopo aver installato ciascun nuovo controller, avviare il sistema dall'immagine di ONTAP 9 memorizzata sul server Web. È quindi possibile scaricare i file corretti sul dispositivo di avvio per i successivi avvii del sistema.

Fasi

1. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scarica il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizza il `ontap-version_image.tgz` file in una directory accessibile dal web.
3. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili.
4. L'elenco delle directory deve contenere ontap_version_image.tgz.
5. Configurare la connessione di netboot scegliendo una delle seguenti operazioni.

> Utilizzare la porta di gestione e l'IP come connessione di netboot. Non utilizzare un IP LIF dei dati, altrimenti potrebbe verificarsi un'interruzione dei dati durante l'aggiornamento.

Se il protocollo DCHP (Dynamic host Configuration Protocol) è…	Quindi…
In esecuzione	Configurare la connessione automaticamente utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -auto`

Non in esecuzione	Configurare manualmente la connessione utilizzando il seguente comando al prompt dell'ambiente di boot: `ifconfig e0M -addr=<filer_addr> -mask=<netmask> -gw=<gateway> - dns=<dns_addr> domain=<dns_domain>` `<filer_addr>` È l'indirizzo IP del sistema di storage. `<netmask>` è la maschera di rete del sistema di storage. `<gateway>` è il gateway per il sistema storage. `<dns_addr>` È l'indirizzo IP di un name server sulla rete. Questo parametro è facoltativo. `<dns_domain>` È il nome di dominio DNS (Domain Name Service). Questo parametro è facoltativo. NOTA: Per l'interfaccia potrebbero essere necessari altri parametri. Invio `help ifconfig` al prompt del firmware per ulteriori informazioni.

6. Eseguire il netboot su Node_B_1: `netboot http://<web_server_ip/path_to_web_accessible_directory>/netboot/kernel`

   Il `<path_to_the_web-accessible_directory>` dovrebbe portare alla posizione in cui è stato scaricato `<ontap_version>\_image.tgz` poll Fase 2.

   > Non interrompere l'avvio.

7. Attendere l'avvio del Node_B_1 sul modulo controller AFF A900 o FAS9500 e visualizzare le opzioni del menu di avvio come mostrato di seguito:

```
Please choose one of the following:

(1)  Normal Boot.
(2)  Boot without /etc/rc.
(3)  Change password.
(4)  Clean configuration and initialize all disks.
(5)  Maintenance mode boot.
(6)  Update flash from backup config.
(7)  Install new software first.
(8)  Reboot node.
(9)  Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

8. Dal menu di avvio, selezionare opzione `(7) Install new software first`.Questa opzione di menu consente di scaricare e installare la nuova immagine ONTAP sul dispositivo di avvio. NOTA: Ignorare il seguente messaggio: `This procedure is not supported for Non-Disruptive Upgrade on`

`an HA pair.` Questa nota si applica agli aggiornamenti software ONTAP senza interruzioni e non agli aggiornamenti del controller.

Utilizzare sempre netboot per aggiornare il nuovo nodo all'immagine desiderata. Se si utilizza un altro metodo per installare l'immagine sul nuovo controller, l'immagine potrebbe non essere corretta. Questo problema riguarda tutte le versioni di ONTAP.

9. Se viene richiesto di continuare la procedura, immettere `y`E quando viene richiesto il pacchetto, immettere l'URL: `\http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>\_image.tgz`
10. Completare i seguenti passaggi secondari per riavviare il modulo controller:
    a. Invio `n` per ignorare il ripristino del backup quando viene visualizzato il seguente prompt: `Do you want to restore the backup configuration now? {y|n}`
    b. Invio `y to reboot when you see the following prompt: `The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}`Il modulo controller si riavvia ma si arresta al menu di avvio perché il dispositivo di avvio è stato riformattato e i dati di configurazione devono essere ripristinati.
11. Quando richiesto, eseguire `wipeconfig` comando per cancellare qualsiasi configurazione precedente sul supporto di avvio:
    a. Quando viene visualizzato il seguente messaggio, rispondere `yes`: `This will delete 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?:`
    b. Il nodo viene riavviato per terminare `wipeconfig` e poi si ferma al menu di boot.
12. Selezionare l'opzione `5` per passare alla modalità di manutenzione dal menu di avvio. Risposta `yes` ai prompt fino all'arresto del nodo in modalità di manutenzione e al prompt dei comandi.
13. Ripetere questa procedura per netboot Node_B_2.

Ripristinare la configurazione dell'HBA

A seconda della presenza e della configurazione delle schede HBA nel modulo controller, è necessario configurarle correttamente per l'utilizzo da parte del sito.

Fasi

1. In modalità Maintenance (manutenzione), configurare le impostazioni per gli HBA presenti nel sistema:
    a. Verificare le impostazioni correnti delle porte:

    ```
    ucadmin show
    ```

    b. Aggiornare le impostazioni della porta secondo necessità.

Se si dispone di questo tipo di HBA e della modalità desiderata…	Utilizzare questo comando…
FC CNA	`ucadmin modify -m fc -t initiator` *`adapter-name`*

Ethernet CNA	`ucadmin modify -mode cna` *`adapter-name`*
Destinazione FC	`fcadmin config -t target` *`adapter-name`*
Iniziatore FC	`fcadmin config -t initiator` *`adapter-name`*

2. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver eseguito il comando, attendere che il nodo si arresti al prompt DEL CARICATORE.

3. Riavviare il nodo in modalità Maintenance per rendere effettive le modifiche di configurazione:

   ```
   boot_ontap maint
   ```

4. Verificare le modifiche apportate:

Se si dispone di questo tipo di HBA…	Utilizzare questo comando…
CNA	`ucadmin show`
FC	`fcadmin show`

Impostare lo stato ha sui nuovi controller e chassis

È necessario verificare lo stato ha dei controller e dello chassis e, se necessario, aggiornarlo in modo che corrisponda alla configurazione del sistema.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Lo stato ha per tutti i componenti deve essere `mccip`.

2. Se lo stato di sistema visualizzato del controller o dello chassis non è corretto, impostare lo stato ha:

   ```
   ha-config modify controller mccip
   ```

   ```
   ha-config modify chassis mccip
   ```

3. Arrestare il nodo: `halt`

   Il nodo deve arrestarsi su `LOADER>` prompt.

4. Su ciascun nodo, controllare la data, l'ora e il fuso orario del sistema: `show date`

5. Se necessario, impostare la data in UTC o GMT: `set date <mm/dd/yyyy>`
6. Controllare l'ora utilizzando il seguente comando al prompt dell'ambiente di boot: `show time`
7. Se necessario, impostare l'ora in UTC o GMT: `set time <hh:mm:ss>`
8. Salvare le impostazioni: `saveenv`
9. Raccogliere le variabili di ambiente: `printenv`

Aggiornare i file RCF dello switch per ospitare le nuove piattaforme

È necessario aggiornare gli switch a una configurazione che supporti i nuovi modelli di piattaforma.

A proposito di questa attività

Questa attività viene eseguita nel sito contenente i controller attualmente in fase di aggiornamento. Negli esempi illustrati in questa procedura, si esegue prima l'aggiornamento di Site_B.

Gli switch del sito_A verranno aggiornati quando i controller del sito_A verranno aggiornati.

Fasi

1. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

   Seguire le istruzioni della sezione relativa al fornitore dello switch nella sezione *Installazione e configurazione IP MetroCluster*.

   "Installazione e configurazione di MetroCluster IP"

   - "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
   - "Ripristino delle impostazioni predefinite dello switch IP Cisco"
2. Scaricare e installare i file RCF.

   Seguire i passaggi descritti nella sezione relativa al fornitore dello switch di "Installazione e configurazione di MetroCluster IP".

   - "Download e installazione dei file RCF Broadcom"
   - "Download e installazione dei file Cisco IP RCF"

Configurare i nuovi controller

A questo punto, i nuovi controller devono essere pronti e cablati.

Impostare le variabili di boot IP di MetroCluster

Alcuni valori di boot MetroCluster IP devono essere configurati sui nuovi moduli controller. I valori devono corrispondere a quelli configurati sui vecchi moduli controller.

A proposito di questa attività

In questa attività, verranno utilizzati gli UUID e gli ID di sistema identificati in precedenza nella procedura di aggiornamento in "Raccolta di informazioni prima dell'aggiornamento".

Fasi

1. Su `LOADER>` Prompt, impostare i seguenti bootargs sui nuovi nodi in Site_B:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id
```

Nell'esempio seguente vengono impostati i valori per Node_B_1-A900 utilizzando VLAN 120 per la prima rete e VLAN 130 per la seconda rete:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

Nell'esempio seguente vengono impostati i valori per Node_B_2-A900 utilizzando VLAN 120 per la prima rete e VLAN 130 per la seconda rete:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

2. Ai nuovi nodi" `LOADER` Impostare gli UUID:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID
```

   a. Impostare gli UUID su Node_B_1-A900.

      L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_1-A900:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f
setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Impostare gli UUID su Node_B_2-A900:

L'esempio seguente mostra i comandi per impostare gli UUID su Node_B_2-A900:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d
setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d
setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

3. Se i sistemi originali sono stati configurati per ADP, al prompt DEL CARICATORE di ciascun nodo sostitutivo, abilitare ADP:

```
setenv bootarg.mcc.adp_enabled true
```

4. Impostare le seguenti variabili:

```
setenv bootarg.mcc.local_config_id original-sys-id
```

```
setenv bootarg.mcc.dr_partner dr-partner-sys-id
```

> Il `setenv bootarg.mcc.local_config_id` Variable deve essere impostato sul sys-id del modulo controller **original**, Node_B_1-A700.

a. Impostare le variabili su Node_B_1-A900.

L'esempio seguente mostra i comandi per impostare i valori su Node_B_1-A900:

```
setenv bootarg.mcc.local_config_id 537403322
setenv bootarg.mcc.dr_partner 537403324
```

b. Impostare le variabili su Node_B_2-A900.

L'esempio seguente mostra i comandi per impostare i valori su Node_B_2-A900:

```
setenv bootarg.mcc.local_config_id 537403321
setenv bootarg.mcc.dr_partner 537403323
```

5. Se si utilizza la crittografia con il gestore delle chiavi esterno, impostare i bootargs richiesti:

   ```
   setenv bootarg.kmip.init.ipaddr

   setenv bootarg.kmip.kmip.init.netmask

   setenv bootarg.kmip.kmip.init.gateway

   setenv bootarg.kmip.kmip.init.interface
   ```

Riassegnare i dischi aggregati root

Riassegnare i dischi aggregati root al nuovo modulo controller, utilizzando i sistemi raccolti in precedenza.

A proposito di questa attività

Questi passaggi vengono eseguiti in modalità manutenzione.

Fasi

1. Avviare il sistema in modalità di manutenzione:

   ```
   boot_ontap maint
   ```

2. Visualizzare i dischi su Node_B_1-A900 dal prompt della modalità di manutenzione:

   ```
   disk show -a
   ```

   L'output del comando mostra l'ID di sistema del nuovo modulo controller (1574774970). Tuttavia, i dischi aggregati root sono ancora di proprietà del vecchio ID di sistema (537403322). Questo esempio non mostra i dischi di proprietà di altri nodi nella configurazione MetroCluster.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-A700(537403322)  Pool1  PZHYN0MD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod4-rk18:9.126L49  node_B_1-A700(537403322)  Pool1  PPG3J5HA
node_B_1-A700(537403322)  node_B_1-700(537403322)
prod4-rk18:8.126L21   node_B_1-A700(537403322)  Pool1  PZHTDSZD
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L2    node_B_1-A700(537403322)  Pool0  S0M1J2CF
node_B_1-(537403322)  node_B_1-A700(537403322)
prod2-rk18:8.126L3    node_B_1-A700(537403322)  Pool0  S0M0CQM5
node_B_1-A700(537403322)  node_B_1-A700(537403322)
prod1-rk18:9.126L27   node_B_1-A700(537403322)  Pool0  S0M1PSDW
node_B_1-A700(537403322)  node_B_1-A700(537403322)
.
.
.
```

3. Riassegnare i dischi aggregati root sugli shelf di dischi ai nuovi controller.

Se si utilizza ADP…	Quindi utilizzare questo comando…
Sì	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
No	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Riassegnare i dischi aggregati root sugli shelf di dischi ai nuovi controller:

   `disk reassign -s old-sysid -d new-sysid`

   L'esempio seguente mostra la riassegnazione dei dischi in una configurazione non ADP:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verificare che i dischi dell'aggregato root siano riassegnati correttamente, rimuovere i dischi:

   ```
   disk show
   ```

   ```
   storage aggr status
   ```

```
*> disk show
Local System ID: 537097247

  DISK                     OWNER                     POOL   SERIAL NUMBER
HOME                      DR HOME
------------              -------------             -----  -------------
-------------             -------------
prod03-rk18:8.126L18 node_B_1-A900(537097247)  Pool1  PZHYN0MD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:9.126L49 node_B_1-A900(537097247)  Pool1  PPG3J5HA
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod04-rk18:8.126L21 node_B_1-A900(537097247)  Pool1  PZHTDSZD
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:8.126L2  node_B_1-A900(537097247)  Pool0  S0M1J2CF
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod02-rk18:9.126L29 node_B_1-A900(537097247)  Pool0  S0M0CQM5
node_B_1-A900(537097247)   node_B_1-A900(537097247)
prod01-rk18:8.126L1  node_B_1-A900(537097247)  Pool0  S0M1PSDW
node_B_1-A900(537097247)   node_B_1-A900(537097247)
::>
::> aggr status
           Aggr          State           Status                Options
aggr0_node_B_1           online          raid_dp, aggr         root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Avviare i nuovi controller

È necessario avviare i nuovi controller, assicurandosi che le variabili di boot siano corrette e, se necessario, eseguire le operazioni di ripristino della crittografia.

Fasi

1. Arrestare i nuovi nodi:

   ```
   halt
   ```

2. Se è configurato un gestore di chiavi esterno, impostare i relativi bootargs:

   ```
   setenv bootarg.kmip.init.ipaddr ip-address

   setenv bootarg.kmip.init.netmask netmask

   setenv bootarg.kmip.init.gateway gateway-address
   ```

```
setenv bootarg.kmip.init.interface interface-id
```

3. Verificare se il sistema partner è quello corrente:

```
printenv partner-sysid
```

Se il partner-sysid non è corretto, impostarlo:

```
setenv partner-sysid partner-sysID
```

4. Visualizzare il menu di avvio di ONTAP:

```
boot_ontap menu
```

5. Se viene utilizzata la crittografia root, selezionare l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione 10 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi
Gestione esterna delle chiavi	Opzione 11 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi

6. Dal menu di avvio, selezionare `(6) Update flash from backup config`.

> L'opzione 6 riavvia il nodo due volte prima del completamento.

Rispondere `y` alle richieste di modifica dell'id di sistema. Attendere i secondi messaggi di riavvio:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. Interrompere L'AUTOBOOT per arrestare i controller al CARICATORE.

> Su ogni nodo, controllare i bootargs impostati in "Impostazione delle variabili di boot MetroCluster IP" e correggere eventuali valori errati. Passare alla fase successiva solo dopo aver controllato i valori di boot.

8. Verificare che il sistema partner sia corretto:

```
printenv partner-sysid
```

Se il partner-sysid non è corretto, impostarlo:

```
setenv partner-sysid partner-sysID
```

9. Se viene utilizzata la crittografia root, selezionare l'opzione del menu di avvio per la configurazione della gestione delle chiavi.

Se si utilizza…	Selezionare questa opzione del menu di avvio…
Gestione delle chiavi integrata	Opzione 10 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi
Gestione esterna delle chiavi	Opzione 11 e seguire le istruzioni per fornire gli input necessari per ripristinare o ripristinare la configurazione del gestore delle chiavi

È necessario eseguire la procedura di ripristino selezionando l'opzione 10 o l'opzione 11 a seconda dell'impostazione del gestore delle chiavi e l'opzione 6 al prompt del menu di avvio. Per avviare completamente i nodi, potrebbe essere necessario eseguire la procedura di ripristino, continua con l'opzione 1 (avvio normale).

10. Attendere l'avvio dei nuovi nodi Node_B_1-A900 e Node_B_2-A900.

    Se uno dei nodi è in modalità Takeover, eseguire un giveback utilizzando `storage failover giveback` comando.

11. Se viene utilizzata la crittografia, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".
Gestione esterna delle chiavi	`security key-manager external restore -vserver *SVM* -node *node* -key-server _host_name

12. Verificare che tutte le porte si trovino in un dominio di trasmissione:

    a. Visualizzare i domini di trasmissione:

    ```
    network port broadcast-domain show
    ```

    b. Aggiungere eventuali porte a un dominio di broadcast in base alle esigenze.

    "Aggiunta o rimozione di porte da un dominio di broadcast"

    c. Ricreare VLAN e gruppi di interfacce in base alle esigenze.

    L'appartenenza alla VLAN e al gruppo di interfacce potrebbe essere diversa da quella del nodo precedente.

"Creazione di una VLAN"

"Combinazione di porte fisiche per creare gruppi di interfacce"

Verificare e ripristinare la configurazione LIF

Verificare che i file LIF siano ospitati su nodi e porte appropriati, come mappati all'inizio della procedura di aggiornamento.

A proposito di questa attività

- Questa attività viene eseguita sul sito_B.
- Vedere il piano di mappatura delle porte creato in "Mappatura delle porte dai vecchi nodi ai nuovi nodi".

Fasi

1. Verificare che i file LIF siano ospitati sul nodo e sulle porte appropriati prima di passare al switchback.

   a. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

   b. Eseguire l'override della configurazione della porta per garantire il corretto posizionamento di LIF:

   ```
   vserver config override -command "network interface modify -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   new_node_name"
   ```

   Quando si immette il comando di modifica dell'interfaccia di rete in `vserver config override` non è possibile utilizzare la funzione di completamento automatico della scheda. È possibile creare la rete `interface modify` utilizzando il completamento automatico e quindi racchiuderlo in `vserver config override` comando.

   a. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

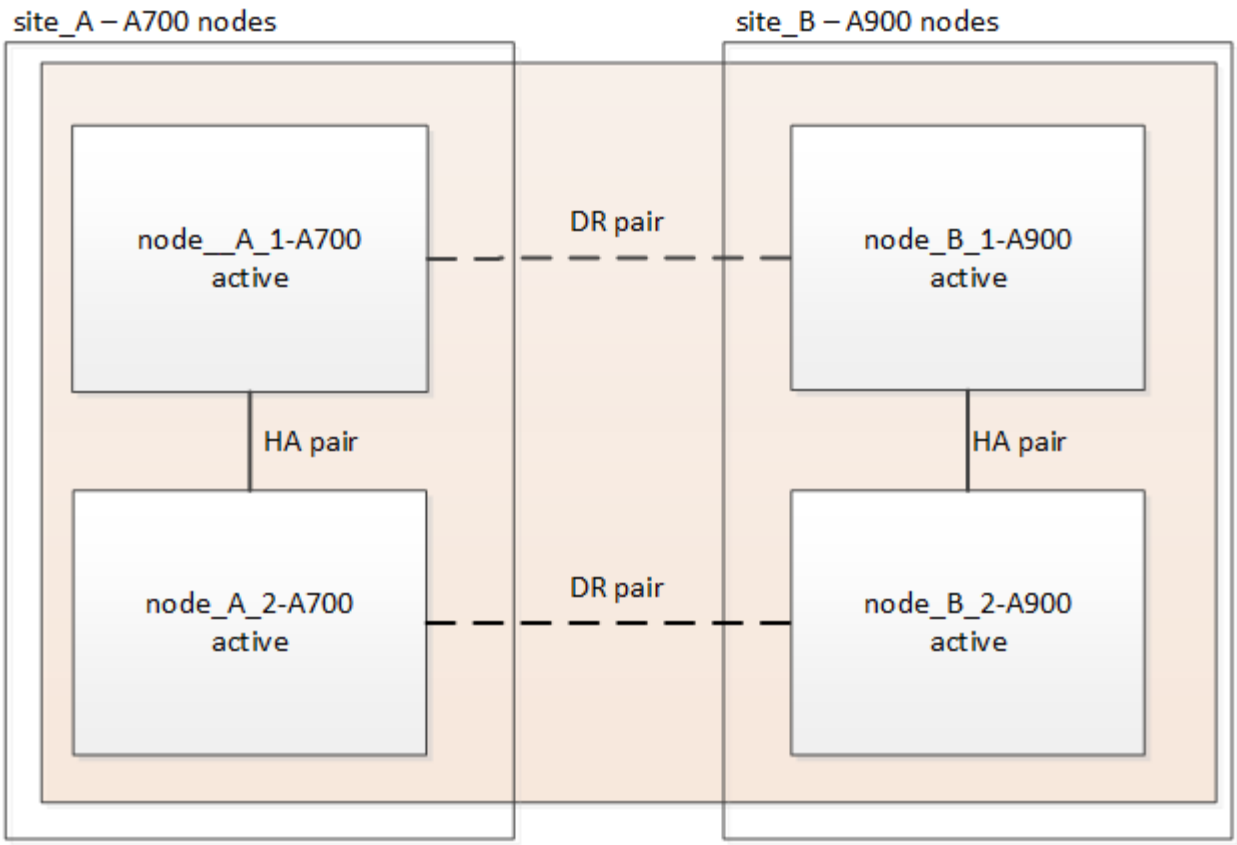
2. Ripristinare le interfacce nel nodo principale:

   ```
   network interface revert * -vserver vserver-name
   ```

   Eseguire questo passaggio su tutte le SVM secondo necessità.

Ripristinare la configurazione MetroCluster

In questa attività, viene eseguita l'operazione di switchback e la configurazione MetroCluster torna al funzionamento normale. I nodi sul sito_A sono ancora in attesa di aggiornamento.



Fasi

1. Eseguire il `metrocluster node show` Dal sito_B e controllare l'output.
   a. Verificare che i nuovi nodi siano rappresentati correttamente.
   b. Verificare che i nuovi nodi siano nello stato "in attesa di switchback".
2. Eseguire la riparazione e lo switchback eseguendo i comandi richiesti da qualsiasi nodo del cluster attivo (il cluster che non è in fase di aggiornamento).
   a. Riparare gli aggregati di dati:
      `metrocluster heal aggregates`
   b. Riparare gli aggregati root:

      ```
      metrocluster heal root
      ```

   c. Switchback del cluster:

      ```
      metrocluster switchback
      ```

3. Controllare l'avanzamento dell'operazione di switchback:

   ```
   metrocluster show
   ```

   L'operazione di switchback è ancora in corso quando viene visualizzato l'output `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'operazione di switchback è completa quando l'output visualizza normale:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando `metrocluster config-replication resync-status show` comando. Questo comando si trova al livello di privilegio avanzato.

Controllare lo stato della configurazione MetroCluster

Dopo aver aggiornato i moduli controller, è necessario verificare lo stato della configurazione MetroCluster.

A proposito di questa attività

Questa attività può essere eseguita su qualsiasi nodo della configurazione MetroCluster.

Fasi

1. Verificare il funzionamento della configurazione MetroCluster:
   a. Confermare la configurazione MetroCluster e verificare che la modalità operativa sia normale: `metrocluster show`
   b. Eseguire un controllo MetroCluster: `metrocluster check run`
   c. Visualizzare i risultati del controllo MetroCluster:

      `metrocluster check show`

2. Verificare lo stato e la connettività MetroCluster.

a. Verificare le connessioni IP MetroCluster:

```
storage iscsi-initiator show
```

b. Verificare che i nodi funzionino:

```
metrocluster node show
```

c. Verificare che le interfacce IP di MetroCluster siano disponibili:

```
metrocluster configuration-settings interface show
```

d. Verificare che il failover locale sia attivato:

```
storage failover show
```

Aggiornare i nodi sul sito_A.

È necessario ripetere le attività di aggiornamento sul sito_A.

Fasi

1. Ripetere i passaggi per aggiornare i nodi sul sito_A, iniziando con "Preparatevi per l'aggiornamento".

   Durante l'esecuzione delle attività, tutti i riferimenti di esempio ai siti e ai nodi vengono invertiti. Ad esempio, quando l'esempio viene fornito per lo switchover da Site_A, si passa da Site_B.

Ripristinare il monitoraggio di Tiebreaker o Mediator

Dopo aver completato l'aggiornamento della configurazione MetroCluster, è possibile riprendere il monitoraggio con l'utility Tiebreaker o Mediator.

Fasi

1. Ripristinare il monitoraggio, se necessario, utilizzando la procedura per la configurazione.

Se si utilizza…	Utilizzare questa procedura
Spareggio	"Aggiunta di configurazioni MetroCluster" Nella sezione *Installazione e configurazione di MetroCluster Tiebreaker*.
Mediatore	"Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster" Nella sezione *Installazione e configurazione IP MetroCluster*.
Applicazioni di terze parti	Consultare la documentazione del prodotto.

Inviare un messaggio AutoSupport personalizzato dopo la manutenzione

Una volta completato l'aggiornamento, inviare un messaggio AutoSupport che indica la fine della manutenzione, in modo da poter riprendere la creazione automatica del caso.

Fasi

1. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.

   a. Eseguire il seguente comando:
   `system node autosupport invoke -node * -type all -message MAINT=end`

   b. Ripetere il comando sul cluster partner.

Aggiornamento di una configurazione MetroCluster FC a quattro nodi

È possibile aggiornare i controller e lo storage in una configurazione MetroCluster a quattro nodi espandendo la configurazione fino a diventare una configurazione a otto nodi e rimuovendo quindi il vecchio gruppo di disaster recovery (DR).

A proposito di questa attività

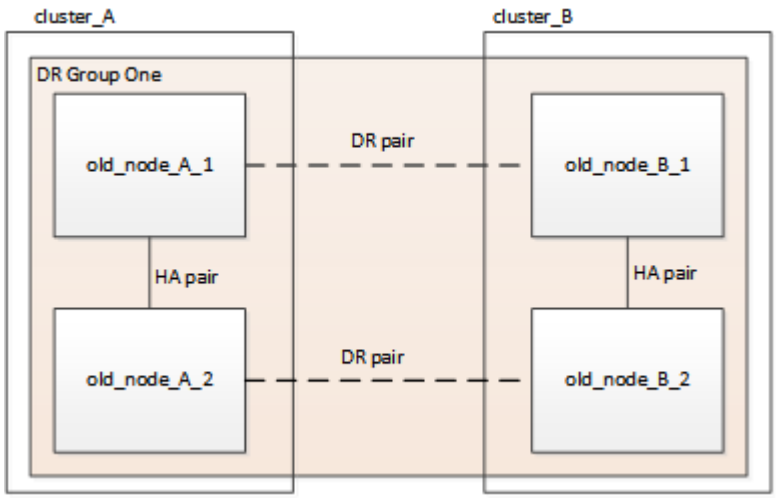
I riferimenti ai "vecchi nodi" indicano i nodi che si intende sostituire.

- È possibile aggiornare solo modelli di piattaforma specifici utilizzando questa procedura in una configurazione MetroCluster FC.
  - Per informazioni sulle combinazioni di upgrade della piattaforma supportate, consultare la tabella di refresh MetroCluster FC in "Scelta di un metodo di refresh del sistema".

Fasi

1. Raccogliere informazioni dai vecchi nodi.

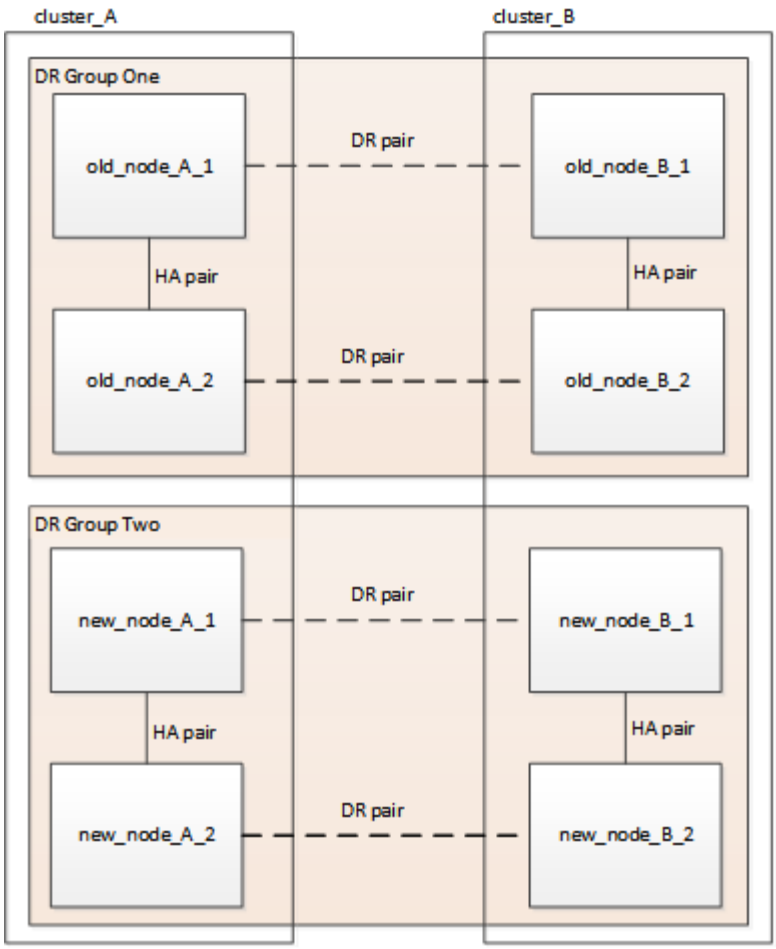
   A questo punto, la configurazione a quattro nodi viene visualizzata come mostrato nell'immagine seguente:



2. Eseguire tutti i passaggi della procedura di espansione a quattro nodi per il tipo di MetroCluster in uso.

   "Espansione di una configurazione MetroCluster FC a quattro nodi in una configurazione a otto nodi"

   Al termine della procedura di espansione, la configurazione viene visualizzata come mostrato nell'immagine seguente:



3. Spostare i volumi CRS.

   Eseguire le operazioni descritte in "Spostare un volume di metadati nelle configurazioni MetroCluster".

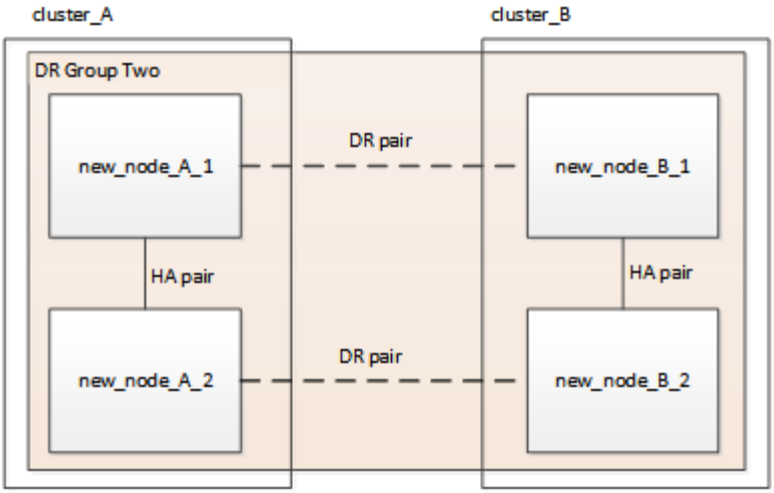
4. Spostare i dati dai vecchi nodi ai nuovi nodi utilizzando le seguenti procedure:
   a. Eseguire tutte le operazioni descritte in "Creazione di un aggregato e spostamento dei volumi nei nuovi nodi".

      È possibile scegliere di eseguire il mirroring dell'aggregato quando o dopo la sua creazione.

   b. Eseguire tutte le operazioni descritte in "Spostare le LIF di dati non SAN e le LIF di gestione del cluster nei nuovi nodi".
   c. Eseguire tutte le operazioni descritte in "Eliminare le LIF SAN non più richieste dai nodi originali".
5. Seguire i passi della procedura per rimuovere il vecchio gruppo DR.

   "Rimozione di un gruppo di disaster recovery"

   Dopo aver rimosso il vecchio gruppo DR (gruppo DR uno), la configurazione viene visualizzata come mostrato nell'immagine seguente:



Aggiornamento di una configurazione MetroCluster IP a quattro o otto nodi (ONTAP 9.8 e versioni successive)

È possibile utilizzare questa procedura per aggiornare controller e storage in configurazioni a quattro o otto nodi.

A partire da ONTAP 9.13.1, è possibile aggiornare i controller e lo storage in una configurazione MetroCluster IP a otto nodi espandendo la configurazione fino a diventare una configurazione temporanea a dodici nodi e rimuovendo i vecchi gruppi di disaster recovery (DR).

A partire da ONTAP 9.8, è possibile aggiornare i controller e lo storage in una configurazione MetroCluster IP a quattro nodi espandendo la configurazione fino a diventare una configurazione temporanea a otto nodi e rimuovendo quindi il vecchio gruppo di DR.

A proposito di questa attività

- Se si dispone di una configurazione a otto nodi, il sistema deve eseguire ONTAP 9.13.1 o versione successiva.
- Se si dispone di una configurazione a quattro nodi, il sistema deve eseguire ONTAP 9.8 o versione successiva.
- Se si stanno aggiornando anche gli switch IP, è necessario aggiornarli prima di eseguire questa procedura di aggiornamento.
- Questa procedura descrive i passaggi necessari per aggiornare un gruppo DR a quattro nodi. Se si dispone di una configurazione a otto nodi (due gruppi DR), è possibile aggiornare uno o entrambi i gruppi DR.

  Se si aggiornano entrambi i gruppi di DR, è necessario aggiornare un gruppo di DR alla volta.

- I riferimenti ai "vecchi nodi" indicano i nodi che si intende sostituire.
- Per le configurazioni a otto nodi, è necessario supportare la combinazione di piattaforme MetroCluster a otto nodi di origine e destinazione.

> Se si aggiornano entrambi i gruppi di DR, la combinazione di piattaforme potrebbe non essere supportata dopo l'aggiornamento del primo gruppo di DR. È necessario aggiornare entrambi i gruppi di DR per ottenere una configurazione a otto nodi supportata.

- È possibile aggiornare solo modelli di piattaforma specifici utilizzando questa procedura in una configurazione MetroCluster IP.
  - Per informazioni sulle combinazioni di upgrade della piattaforma supportate, consultare la tabella di aggiornamento dell'IP MetroCluster in "Scelta di un metodo di refresh del sistema".
- Si applicano i limiti inferiori delle piattaforme di origine e di destinazione. Se si passa a una piattaforma superiore, i limiti della nuova piattaforma si applicano solo dopo il completamento dell'aggiornamento tecnico di tutti i gruppi di DR.
- Se si esegue un aggiornamento tecnico su una piattaforma con limiti inferiori rispetto alla piattaforma di origine, è necessario regolare e ridurre i limiti in modo che siano pari o inferiori ai limiti della piattaforma di destinazione prima di eseguire questa procedura.

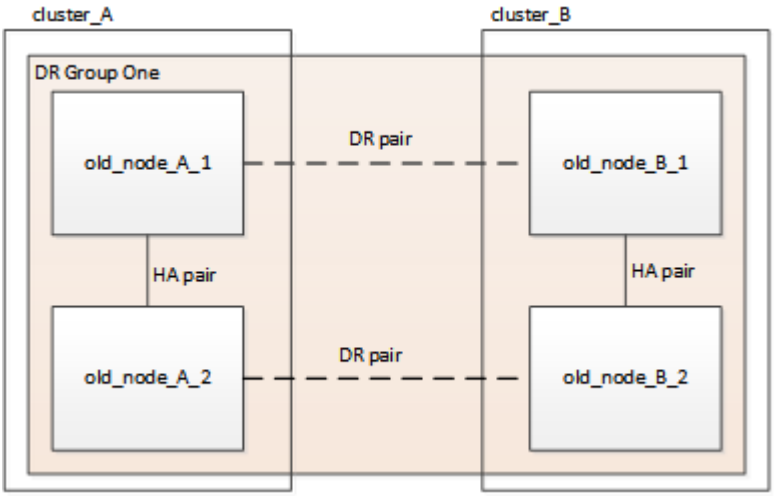
Fasi

1. Verificare di disporre di un dominio di broadcast predefinito creato sui vecchi nodi.

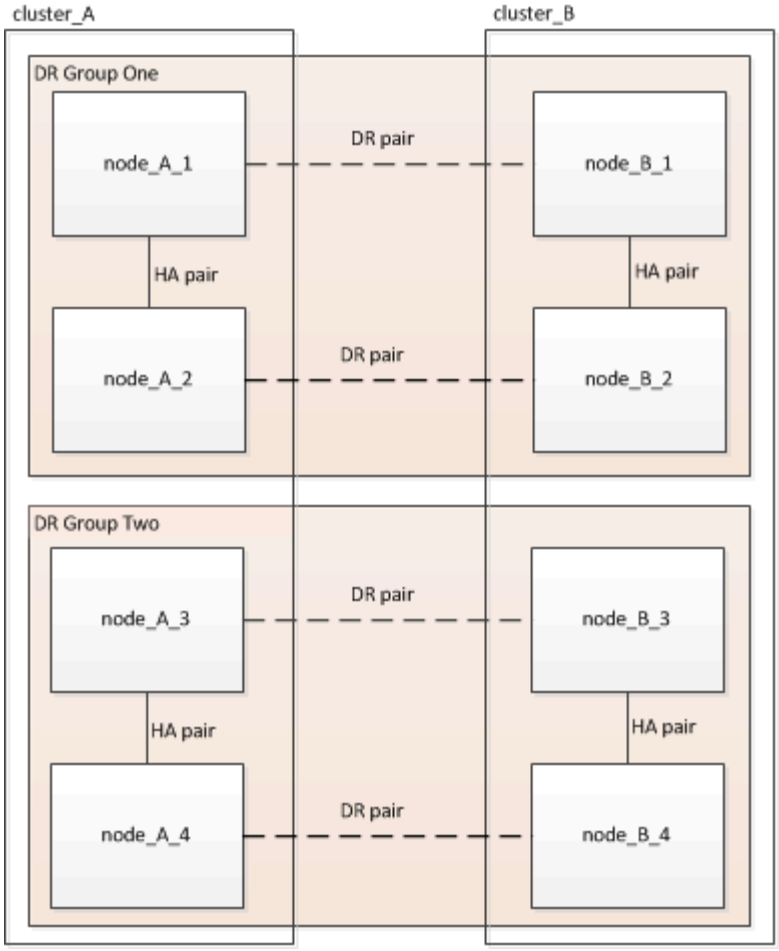
   Quando si aggiungono nuovi nodi a un cluster esistente senza un dominio di broadcast predefinito, le LIF di gestione nodi vengono create per i nuovi nodi utilizzando gli UUID (Universal Unique Identifier) e non i nomi previsti. Per ulteriori informazioni, consultare l'articolo della Knowledge base "LIF di gestione nodi su nodi appena aggiunti generati con nomi UUID".

2. Raccogliere informazioni dai vecchi nodi.

   A questo punto, la configurazione a quattro nodi viene visualizzata come mostrato nell'immagine seguente:



   La configurazione a otto nodi viene visualizzata come mostrato nell'immagine seguente:



3. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che l'aggiornamento è in corso.

   a. Eseguire il seguente comando:
   `system node autosupport invoke -node * -type all -message "MAINT=10h Upgrading old-model to new-model"`

   Nell'esempio seguente viene specificata una finestra di manutenzione di 10 ore. A seconda del piano, potrebbe essere necessario dedicare più tempo.

   Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Ripetere il comando sul cluster partner.

4. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza…	Utilizzare questa procedura…

Spareggio	a. Utilizzare l'interfaccia CLI di tiebreaker `monitor remove` Comando per rimuovere la configurazione MetroCluster.
	
	Nell'esempio seguente, "cluster_A" viene rimosso dal software:
	
	`NetApp MetroCluster Tiebreaker :> monitor remove -monitor -name cluster_A Successfully removed monitor from NetApp MetroCluster Tiebreaker software.`
	
	b. Verificare che la configurazione MetroCluster sia stata rimossa correttamente utilizzando l'interfaccia CLI di tiebreaker `monitor show -status` comando.
	
	`NetApp MetroCluster Tiebreaker :> monitor show -status`

Mediatore	Immettere il seguente comando dal prompt di ONTAP: `metrocluster configuration-settings mediator remove`
Applicazioni di terze parti	Consultare la documentazione del prodotto.

5. Eseguire tutte le operazioni descritte in "Espansione di una configurazione IP MetroCluster" per aggiungere i nuovi nodi e lo storage alla configurazione.

   Al termine della procedura di espansione, la configurazione temporanea viene visualizzata come mostrato nelle seguenti immagini:

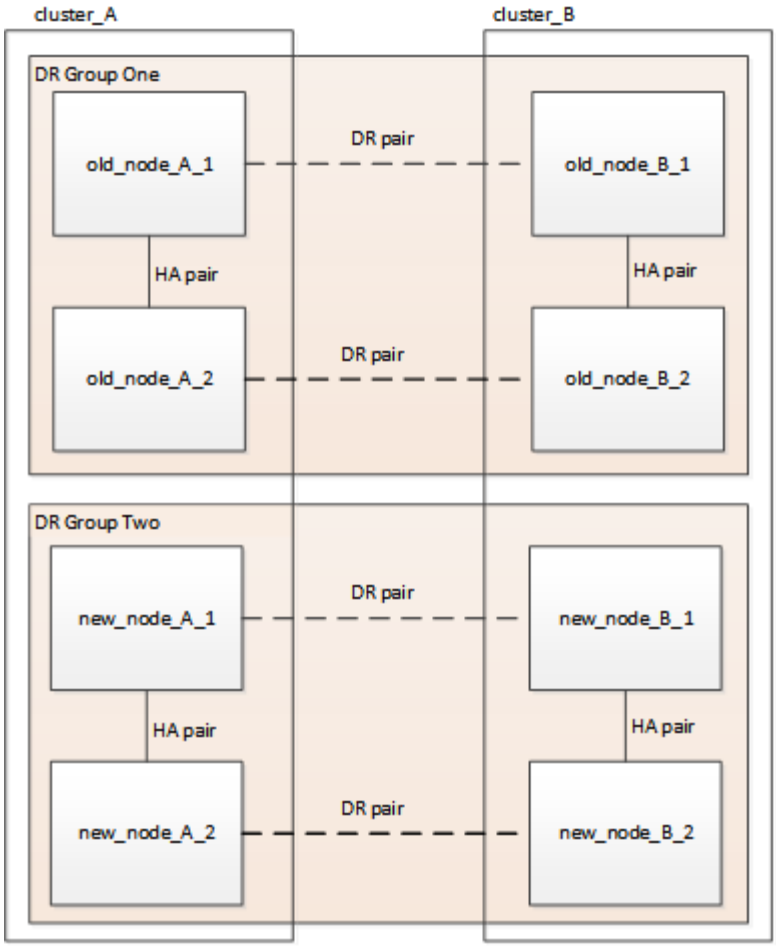


Figura 1. Configurazione temporanea a otto nodi

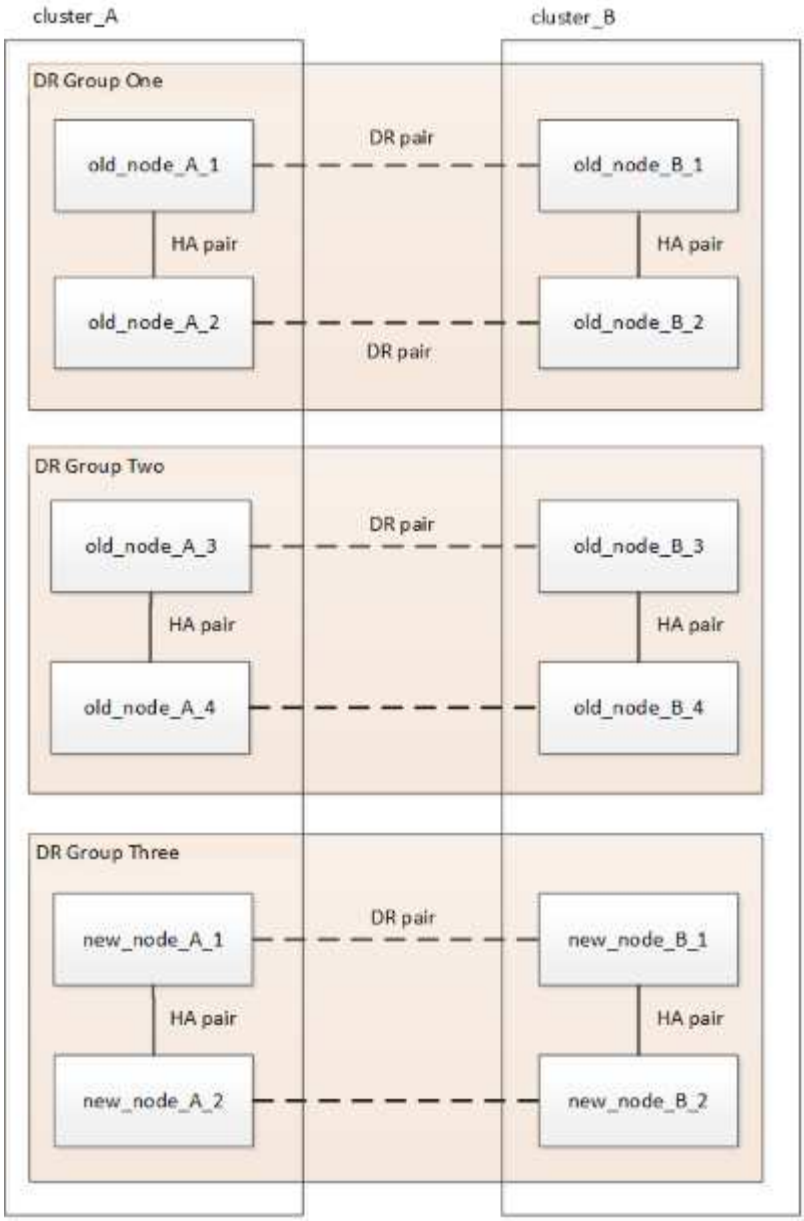


Figura 2. Configurazione temporanea a dodici nodi

6. Verificare che sia possibile il Takeover e che i nodi siano connessi eseguendo il seguente comando su entrambi i cluster:

   `storage failover show`

```
cluster_A::> storage failover show
                                      Takeover
Node           Partner                Possible    State Description
-------------- --------------------- ---------   ------------------
Node_FC_1      Node_FC_2                true      Connected to Node_FC_2
Node_FC_2      Node_FC_1                true      Connected to Node_FC_1
Node_IP_1      Node_IP_2                true      Connected to Node_IP_2
Node_IP_2      Node_IP_1                true      Connected to Node_IP_1
```

7. Spostare i volumi CRS.

   Eseguire le operazioni descritte in "Spostamento di un volume di metadati nelle configurazioni MetroCluster".

8. Spostare i dati dai vecchi nodi ai nuovi nodi seguendo le seguenti procedure:
   a. Eseguire tutte le operazioni descritte in "Creare un aggregato e spostare i volumi nei nuovi nodi".

      È possibile scegliere di eseguire il mirroring dell'aggregato quando o dopo la sua creazione.

   b. Eseguire tutte le operazioni descritte in "Spostamento delle LIF dati non SAN e delle LIF di gestione cluster nei nuovi nodi".

9. Modificare l'indirizzo IP per il peer del cluster dei nodi in transizione per ciascun cluster:

   a. Identificare il peer cluster_A utilizzando `cluster peer show` comando:

```
cluster_A::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B         1-80-000011           Unavailable    absent
```

      i. Modificare l'indirizzo IP del peer cluster_A:

```
cluster peer modify -cluster cluster_A -peer-addrs node_A_3_IP -address
-family ipv4
```

   b. Identificare il peer cluster_B utilizzando `cluster peer show` comando:

```
cluster_B::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A         1-80-000011           Unavailable    absent
```

      i. Modificare l'indirizzo IP del peer cluster_B:

```
cluster peer modify -cluster cluster_B -peer-addrs node_B_3_IP -address
-family ipv4
```

   c. Verificare che l'indirizzo IP del peer del cluster sia aggiornato per ciascun cluster:

      i. Verificare che l'indirizzo IP sia aggiornato per ciascun cluster utilizzando `cluster peer show -instance` comando.

Il `Remote Intercluster Addresses` Nei seguenti esempi viene visualizzato l'indirizzo IP aggiornato.

Esempio per cluster_A:

```
cluster_A::> cluster peer show -instance

Peer Cluster Name: cluster_B
           Remote Intercluster Addresses: 172.21.178.204,
172.21.178.212
      Availability of the Remote Cluster: Available
                      Remote Cluster Name: cluster_B
                      Active IP Addresses: 172.21.178.212,
172.21.178.204
                    Cluster Serial Number: 1-80-000011
                     Remote Cluster Nodes: node_B_3-IP,
                                           node_B_4-IP
                    Remote Cluster Health: true
                  Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_A::>
```

+ Esempio per cluster_B.

```
cluster_B::> cluster peer show -instance

                      Peer Cluster Name: cluster_A
           Remote Intercluster Addresses: 172.21.178.188, 172.21.178.196
<<<<<<<< Should reflect the modified address
      Availability of the Remote Cluster: Available
                     Remote Cluster Name: cluster_A
                     Active IP Addresses: 172.21.178.196, 172.21.178.188
                   Cluster Serial Number: 1-80-000011
                    Remote Cluster Nodes: node_A_3-IP,
                                          node_A_4-IP
                   Remote Cluster Health: true
                 Unreachable Local Nodes: -
          Address Family of Relationship: ipv4
    Authentication Status Administrative: use-authentication
       Authentication Status Operational: ok
                         Last Update Time: 4/20/2023 18:23:53
            IPspace for the Relationship: Default
Proposed Setting for Encryption of Inter-Cluster Communication: -
Encryption Protocol For Inter-Cluster Communication: tls-psk
  Algorithm By Which the PSK Was Derived: jpake

cluster_B::>
```

10. Seguire la procedura descritta in "Rimozione di un gruppo di disaster recovery" Per rimuovere il vecchio gruppo DR.
11. Se si desidera aggiornare entrambi i gruppi di DR in una configurazione a otto nodi, è necessario ripetere l'intera procedura per ciascun gruppo di DR.

    Dopo aver rimosso il vecchio gruppo DR, la configurazione viene visualizzata come mostrato nelle seguenti immagini:

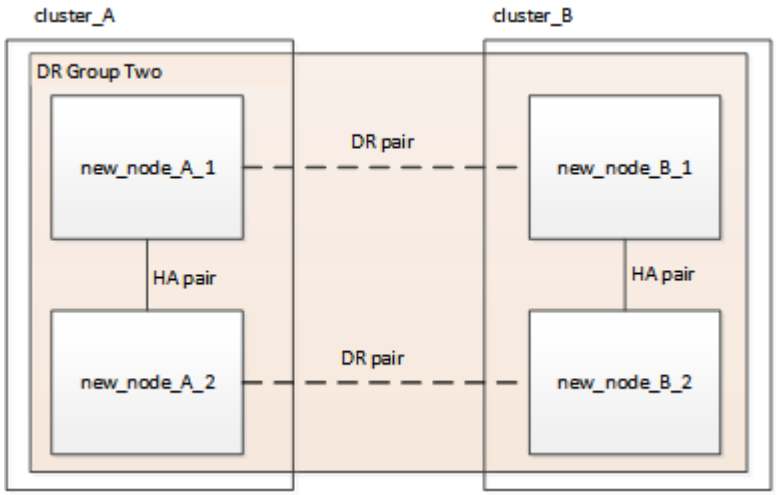


Figura 3. Configurazione a quattro nodi

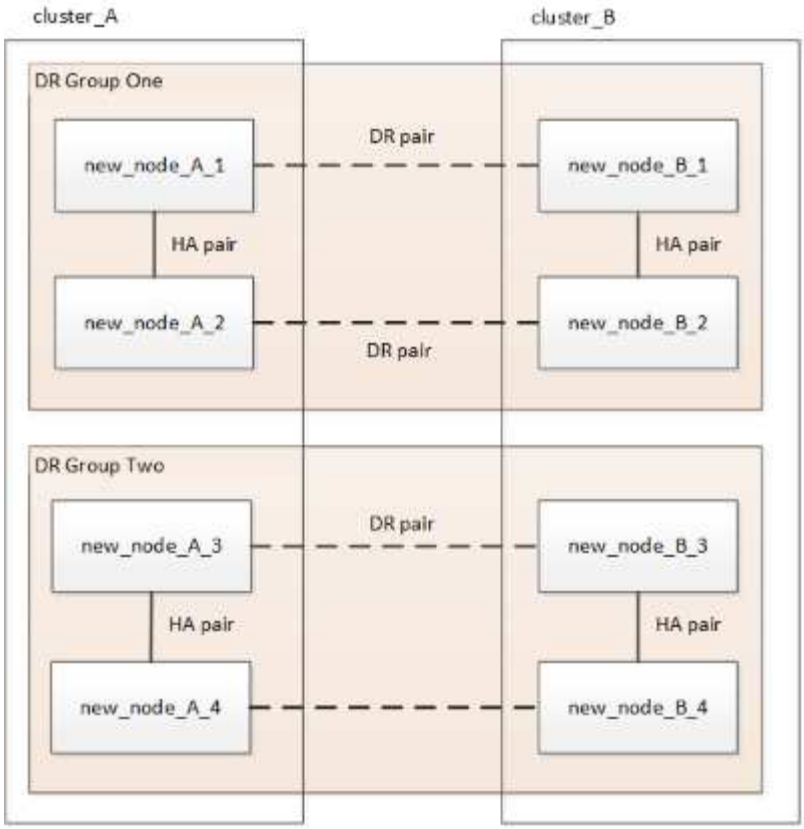


Figura 4. Configurazione a otto nodi

12. Confermare la modalità operativa della configurazione MetroCluster ed eseguire un controllo MetroCluster.
    a. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

    ```
    metrocluster show
    ```

    b. Verificare che siano visualizzati tutti i nodi previsti:

    ```
    metrocluster node show
    ```

    c. Immettere il seguente comando:

    ```
    metrocluster check run
    ```

    d. Visualizzare i risultati del controllo MetroCluster:

    ```
    metrocluster check show
    ```

13. Ripristinare il monitoraggio, se necessario, utilizzando la procedura per la configurazione.

Se si utilizza…	Utilizzare questa procedura
Spareggio	"Aggiunta di configurazioni MetroCluster" Nella sezione *Installazione e configurazione di MetroCluster Tiebreaker*.

Mediatore	"Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster" In *Installazione e configurazione IP MetroCluster*.
Applicazioni di terze parti	Consultare la documentazione del prodotto.

14. Per riprendere la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che la manutenzione è stata completata.
    a. Immettere il seguente comando:

    ```
    system node autosupport invoke -node * -type all -message MAINT=end
    ```

    b. Ripetere il comando sul cluster partner.

Espandere una configurazione MetroCluster FC a due nodi in una configurazione a quattro nodi

Espansione di una configurazione MetroCluster FC a due nodi in una configurazione a quattro nodi

L'espansione di una configurazione MetroCluster FC a due nodi in una configurazione MetroCluster FC a quattro nodi comporta l'aggiunta di un controller a ciascun cluster per formare una coppia ha in ogni sito MetroCluster e l'aggiornamento della configurazione MetroCluster FC.

Prima di iniziare

- I nodi devono eseguire ONTAP 9 o versione successiva in una configurazione MetroCluster FC.

  Questa procedura non è supportata nelle versioni precedenti di ONTAP o nelle configurazioni MetroCluster IP.

- Se le piattaforme nella configurazione a due nodi non sono supportate in ONTAP 9.2 e si prevede di eseguire l'aggiornamento alle piattaforme supportate in ONTAP 9.2 *e* espandersi in un cluster a quattro nodi, è necessario aggiornare le piattaforme nella configurazione a due nodi *prima di* espandere la configurazione MetroCluster FC.
- La configurazione MetroCluster FC esistente deve essere in buone condizioni.
- L'apparecchiatura che si sta aggiungendo deve essere supportata e soddisfare tutti i requisiti descritti nelle seguenti procedure:

  "Installazione e configurazione di Fabric-Attached MetroCluster"

  "Estensione dell'installazione e della configurazione di MetroCluster"

- È necessario disporre di porte switch FC disponibili per ospitare i nuovi controller e i nuovi bridge.
- Verificare di disporre di un dominio di broadcast predefinito creato sui vecchi nodi.

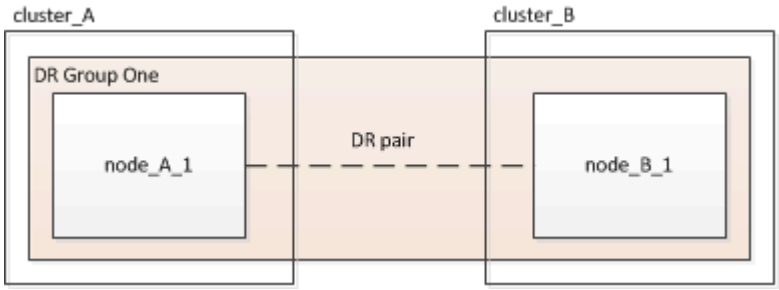
  Quando si aggiungono nuovi nodi a un cluster esistente senza un dominio di broadcast predefinito, le LIF di gestione nodi vengono create per i nuovi nodi utilizzando gli UUID (Universal Unique Identifier) e non i

nomi previsti. Per ulteriori informazioni, consultare l'articolo della Knowledge base "LIF di gestione nodi su nodi appena aggiunti generati con nomi UUID".

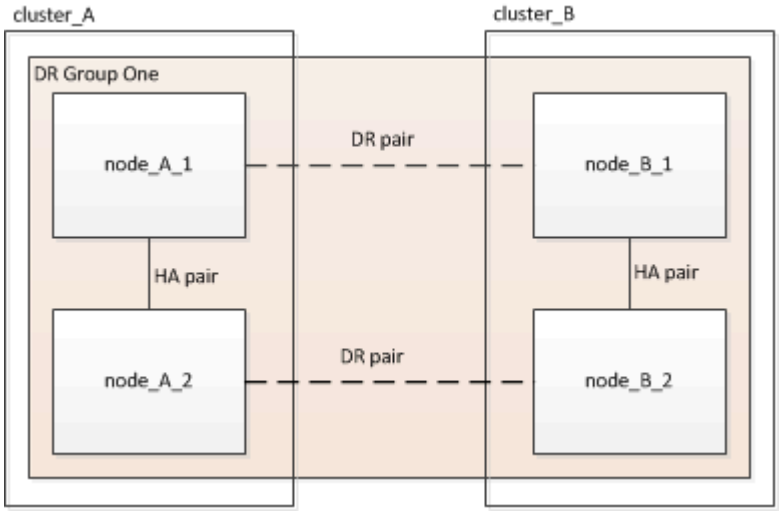
- È necessaria la password admin e l'accesso a un server FTP o SCP.

A proposito di questa attività

- Questa procedura si applica solo alle configurazioni MetroCluster FC.
- Questa procedura è un'interruzione e richiede circa quattro ore per essere completata.
- Prima di eseguire questa procedura, la configurazione MetroCluster FC è costituita da due cluster a nodo singolo:



  Al termine di questa procedura, la configurazione MetroCluster FC è costituita da due coppie ha, una per ciascun sito:



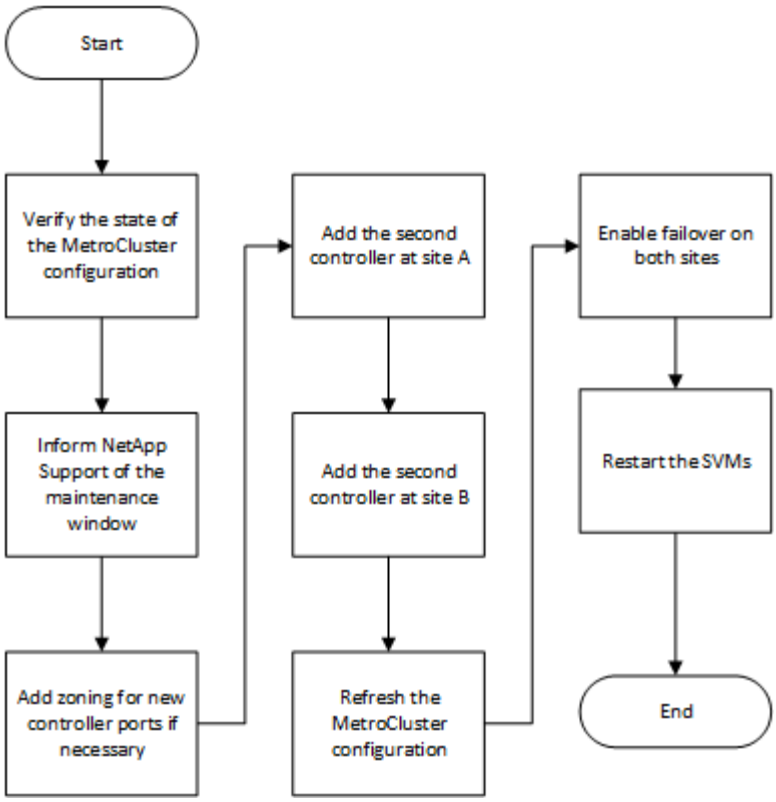
- Entrambi i siti devono essere espansi in modo uguale.

  Una configurazione MetroCluster non può essere costituita da un numero di nodi non uniforme.

- Questa procedura può richiedere più di un'ora per sito, con un tempo aggiuntivo per attività come l'inizializzazione dei dischi e l'avvio in rete dei nuovi nodi.

  Il tempo di inizializzazione dei dischi dipende dalle dimensioni dei dischi.

- Questa procedura utilizza il seguente flusso di lavoro:



Verifica dello stato della configurazione MetroCluster

È necessario identificare i controller esistenti e confermare le relazioni di disaster recovery (DR) tra di essi, che i controller sono in modalità normale e che gli aggregati sono sottoposti a mirroring.

Fasi

1. Visualizzare i dettagli dei nodi nella configurazione MetroCluster da qualsiasi nodo della configurazione:

   ```
   metrocluster node show -fields node,dr-partner,dr-partner-systemid
   ```

   Il seguente output mostra che questa configurazione MetroCluster ha un singolo gruppo DR e un nodo in ciascun cluster.

   ```
   cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
   systemid

   dr-group-id  cluster         node            dr-partner      dr-partner-
   systemid
   -----------  -------------   -------         ----------
   -------------------
   1            cluster_A       controller_A_1  controller_B_1  536946192
   1            cluster_B       controller_B_1  controller_A_1  536946165
   2 entries were displayed.
   ```

2. Visualizzare lo stato della configurazione MetroCluster:

```
metrocluster show
```

Il seguente output mostra che i nodi esistenti nella configurazione MetroCluster sono in modalità normale:

```
cluster_A::> metrocluster show

Configuration: two-node-fabric

Cluster                         Entry Name             State
------------------------------- ----------------------
---------------------
Local: cluster_A                Configuration State    configured
                                Mode                   normal
                                AUSO Failure Domain    auso-on-cluster-
disaster
Remote: controller_B_1_siteB
                                Configuration State    configured
                                Mode                   normal
                                AUSO Failure Domain    auso-on-cluster-
disaster
```

3. Controllare lo stato degli aggregati su ciascun nodo nella configurazione MetroCluster:

```
storage aggregate show
```

Il seguente output mostra che gli aggregati su cluster_A sono online e mirrorati:

```
cluster_A::> storage aggregate show


Aggregate                Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

Invio di un messaggio AutoSupport personalizzato prima dell'aggiunta di nodi alla configurazione MetroCluster

Devi inviare un messaggio AutoSupport per informare il supporto tecnico di NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster dal sito_A.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Il `maintenance-window-in-hours` il parametro specifica la lunghezza della finestra di manutenzione e può essere un massimo di 72 ore. Se si completa la manutenzione prima che sia trascorso il tempo, è possibile eseguire il seguente comando per indicare che il periodo di manutenzione è terminato:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Ripetere questo passaggio sul sito del partner.

Zoning per le nuove porte del controller quando si aggiunge un modulo controller in una configurazione Fabric-Attached MetroCluster

Lo zoning dello switch FC deve ospitare le connessioni del nuovo controller. Se per configurare gli switch sono stati utilizzati i file di configurazione di riferimento (RCF) forniti da NetApp, lo zoning è preconfigurato e non è necessario apportare modifiche.

Se gli switch FC sono stati configurati manualmente, assicurarsi che la zoning sia corretta per le connessioni dell'iniziatore dai nuovi moduli controller. Vedere le sezioni relative allo zoning in "Installazione e configurazione di Fabric-Attached MetroCluster".

Aggiungere un nuovo modulo controller a ciascun cluster

Aggiunta di un nuovo modulo controller a ciascun cluster

È necessario aggiungere un nuovo modulo controller a ciascun sito, creando una coppia ha in ciascun sito. Si tratta di un processo a più fasi che prevede modifiche hardware e software che devono essere eseguite nell'ordine corretto in ogni sito.

A proposito di questa attività

- Il nuovo modulo controller deve essere ricevuto da NetApp come parte del kit di aggiornamento.

  Verificare che le schede PCIe nel nuovo modulo controller siano compatibili e supportate dal nuovo modulo controller.

"NetApp Hardware Universe"

- Il sistema deve disporre di uno slot vuoto per il nuovo modulo controller quando si esegue l'aggiornamento a una coppia ha a chassis singolo (una coppia ha in cui entrambi i moduli controller risiedono nello stesso chassis).

  > Questa configurazione non è supportata su tutti i sistemi. Le piattaforme con configurazioni a chassis singolo supportate in ONTAP 9 sono AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080 E FAS9000.

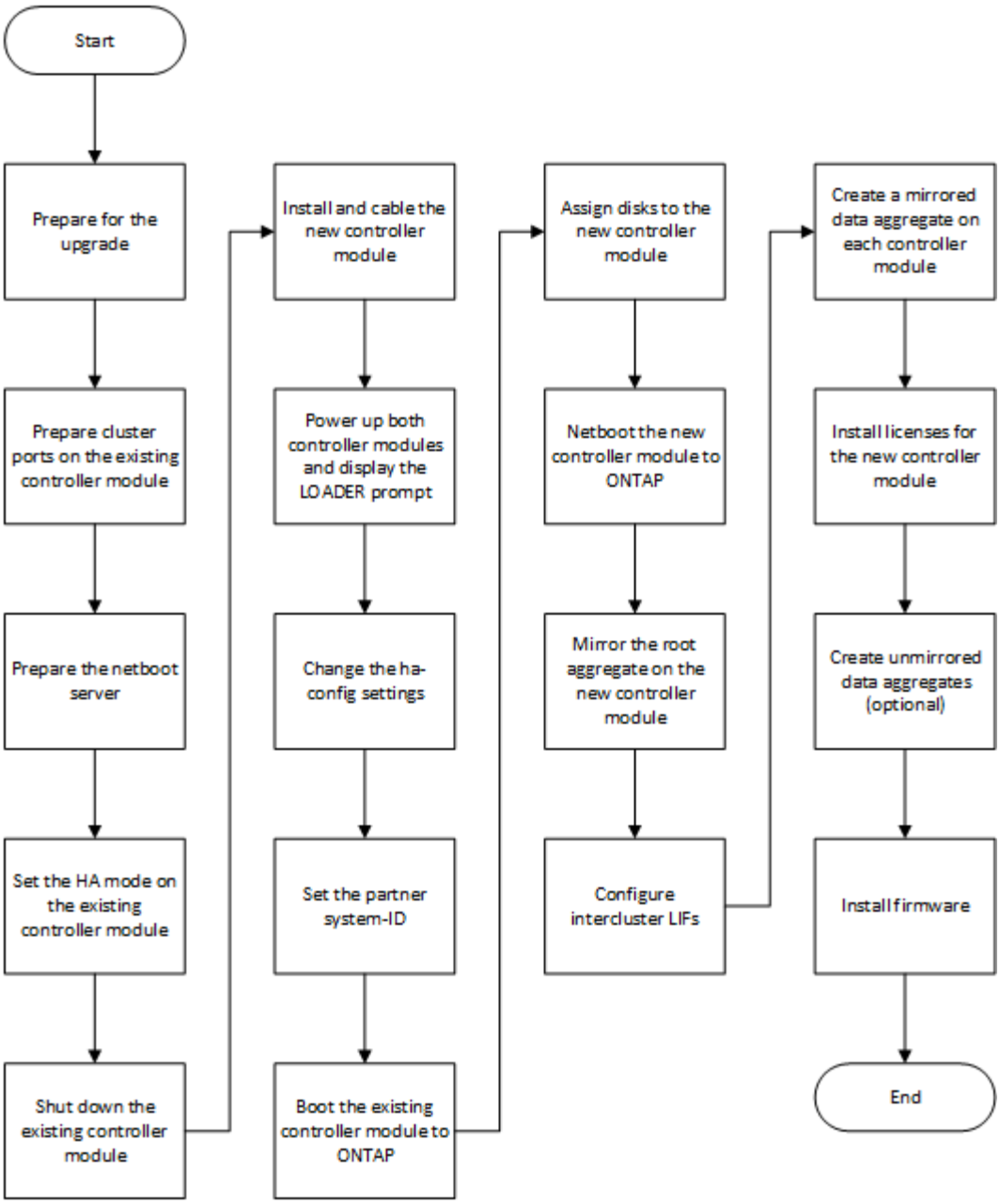
- È necessario disporre di spazio rack e cavi per il nuovo modulo controller quando si esegue l'aggiornamento a una coppia ha a doppio chassis (una coppia ha in cui i moduli controller risiedono in uno chassis separato).

  > Questa configurazione non è supportata su tutti i sistemi.

- È necessario collegare ciascun modulo controller alla rete di gestione tramite la relativa porta e0a oppure, se il sistema ne dispone, è possibile connettersi alla porta e0M come porta di gestione.
- Queste attività devono essere ripetute in ogni sito.
- I moduli controller preesistenti sono indicati come moduli controller *esistenti*.

  Gli esempi di questa procedura presentano il prompt della console `existing_ctlr>`.

- I moduli controller aggiunti sono denominati *nuovi* moduli controller; gli esempi di questa procedura hanno il prompt della console `new_ctlr>`.
- Questa attività utilizza il seguente flusso di lavoro:



Preparazione per l'aggiornamento

Prima di eseguire l'aggiornamento a una coppia ha, è necessario verificare che il sistema soddisfi tutti i requisiti e disporre di tutte le informazioni necessarie.

Fasi

1. Identificare i dischi non assegnati o i dischi spare che è possibile assegnare al nuovo modulo controller utilizzando i seguenti comandi:
   - `storage disk show -container-type spare`
   - `storage disk show -container-type unassigned`
2. Completare i seguenti passaggi secondari:
   a. Determinare dove si trovano gli aggregati per il nodo esistente:

```
storage aggregate show
```

b. Se l'assegnazione automatica della proprietà del disco è attivata, disattivarla:

```
storage disk option modify -node node_name -autoassign off
```

c. Rimuovere la proprietà sui dischi che non dispongono di aggregati:

```
storage disk removeowner disk_name
```

d. Ripetere il passaggio precedente per tutti i dischi necessari per il nuovo nodo.

3. Verificare che i cavi siano pronti per le seguenti connessioni:
   - Connessioni cluster

     Se si crea un cluster senza switch a due nodi, sono necessari due cavi per collegare i moduli controller. In caso contrario, sono necessari almeno quattro cavi, due per ogni connessione del modulo controller allo switch cluster-network. Gli altri sistemi (come la serie 80xx) dispongono di quattro o sei connessioni cluster predefinite.

   - Connessioni di interconnessione HA, se il sistema si trova in una coppia ha a doppio chassis
4. Verificare di disporre di una console con porta seriale per i moduli controller.
5. Verificare che l'ambiente soddisfi i requisiti di sito e di sistema.

   "NetApp Hardware Universe"

6. Raccogliere tutti gli indirizzi IP e gli altri parametri di rete per il nuovo modulo controller.

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   ```
   set-defaults
   ```

3. Salvare l'ambiente:

   ```
   saveenv
   ```

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

   ```
   boot_ontap menu
   ```

5. Al prompt del menu di avvio, cancellare la configurazione:

   ```
   wipeconfig
   ```

Rispondere `yes` al prompt di conferma.

Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Preparazione delle porte del cluster su un modulo controller esistente

Prima di installare un nuovo modulo controller, è necessario configurare le porte del cluster sul modulo controller esistente in modo che le porte del cluster possano fornire la comunicazione del cluster con il nuovo modulo controller.

A proposito di questa attività

Se si crea un cluster senza switch a due nodi (senza switch di rete del cluster), è necessario attivare la modalità di rete del cluster senza switch.

Per informazioni dettagliate sulla configurazione di porta, LIF e rete in ONTAP, vedere "Gestione della rete".

Fasi

1. Determinare quali porte devono essere utilizzate come porte del cluster del nodo.

   Per un elenco dei ruoli porta predefiniti per la piattaforma, vedere "Hardware Universe"

   Le *istruzioni per l'installazione e la configurazione* della piattaforma sul sito di supporto NetApp contengono informazioni sulle porte per le connessioni di rete cluster.

2. Per ciascuna porta del cluster, identificare i ruoli delle porte:

   ```
   network port show
   ```

   Nell'esempio seguente, le porte "e0a", "e0b", "e0c" e "e0d" devono essere modificate in porte cluster:

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. Per qualsiasi LIF di dati che utilizza una porta cluster come porta home o porta corrente, modificare LIF per utilizzare una porta dati come porta home:

   `network interface modify`

   Nell'esempio seguente viene modificata la porta home di una LIF dati in una porta dati:

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. Per ogni LIF modificato, ripristinare la LIF alla nuova porta home:

   `network interface revert`

   Nell'esempio riportato di seguito, LIF "datalif1" torna alla nuova porta home "e1b":

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Rimuovere tutte le porte VLAN utilizzando le porte del cluster come porte membro e ifgrps utilizzando le porte del cluster come porte membro.

   a. Eliminare le porte VLAN:
      `network port vlan delete -node *node-name* -vlan-name *portid-vlandid*`

Ad esempio:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Rimuovere le porte fisiche dai gruppi di interfacce:

   `network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

   Ad esempio:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

a. Rimuovere le porte della VLAN e del gruppo di interfacce dal dominio di broadcast:

   `network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname,..`*

b. Modificare le porte del gruppo di interfacce per utilizzare altre porte fisiche come membro in base alle necessità.:
   `ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

6. Verificare che i ruoli delle porte siano stati modificati:

   `network port show`

   L'esempio seguente mostra che le porte "e0a", "e0b", "e0c" e "e0d" sono ora porte cluster:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Aggiungere le porte al dominio di trasmissione del cluster:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id`*, *`port-id`*, *`port-id`*…

   Ad esempio:

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. Se il sistema fa parte di un cluster con switch, creare le LIF del cluster sulle porte del cluster: `network interface create`

   Nell'esempio seguente viene creata una LIF del cluster su una delle porte del cluster del nodo. Il `-auto` Parameter (parametro): Configura la LIF in modo che utilizzi un indirizzo IP link-local.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. Se si crea un cluster senza switch a due nodi, attivare la modalità di rete senza switch del cluster:

   a. Passare al livello di privilegio avanzato da uno dei nodi:

      `set -privilege advanced`

Puoi rispondere `y` quando viene richiesto se si desidera continuare in modalità avanzata. Viene visualizzato il prompt della modalità avanzata (`*>`).

a. Attivare la modalità di rete senza switch del cluster:

```
network options switchless-cluster modify -enabled true
```

b. Tornare al livello di privilegio admin:

```
set -privilege admin
```

> La creazione dell'interfaccia del cluster per il nodo esistente in un sistema cluster senza switch a due nodi viene completata dopo il completamento dell'installazione del cluster attraverso un netboot sul nuovo modulo controller.

Preparazione del server netboot per il download dell'immagine

Quando si è pronti per preparare il server netboot, è necessario scaricare l'immagine di netboot ONTAP corretta dal sito del supporto NetApp sul server netboot e annotare l'indirizzo IP.

A proposito di questa attività

- È necessario poter accedere a un server HTTP dal sistema prima e dopo aver aggiunto il nuovo modulo controller.
- Per scaricare i file di sistema necessari per la piattaforma e la versione di ONTAP in uso, è necessario accedere al sito del supporto NetApp.

  "Sito di supporto NetApp"

- Entrambi i moduli controller della coppia ha devono eseguire la stessa versione di ONTAP.

Fasi

1. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il `<ontap_version>_image.tgz` file in una directory accessibile dal web.

   Il `<ontap_version>_image.tgz` file viene utilizzato per eseguire un netboot del sistema.

2. Passare alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

Per…	Quindi…

SISTEMI DELLE SERIE FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	Estrarre il contenuto del file ontap_version_image.tgz nella directory di destinazione:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine di netboot.
	
	L'elenco delle directory deve contenere una cartella netboot con un file kernel:
	
	`netboot/kernel`

Tutti gli altri sistemi	L'elenco delle directory deve contenere il seguente file: `<ontap_version>_image.tgz` Non è necessario estrarre il contenuto del file.

3. Determinare l'indirizzo IP del modulo controller esistente.

   Questo indirizzo viene indicato più avanti in questa procedura come *ip-address-of-existing controller*.

4. Ping *ip-address-of-existing controller* Per verificare che l'indirizzo IP sia raggiungibile.

Impostazione della modalità ha sul modulo controller esistente

È necessario utilizzare il comando di modifica del failover dello storage per impostare la modalità sul modulo controller esistente. Il valore della modalità viene attivato in seguito, dopo il riavvio del modulo controller.

Fasi

1. Impostare la modalità su ha:

   `storage failover modify -mode ha -node existing_node_name`

Arresto del modulo controller esistente

Per verificare che tutti i dati siano stati scritti su disco, è necessario eseguire un arresto completo del modulo controller esistente. È inoltre necessario scollegare gli alimentatori.

A proposito di questa attività

Prima di sostituire i componenti del sistema, è necessario eseguire un arresto pulito del sistema per evitare la perdita di dati non scritti nella NVRAM o NVMEM.

Fasi

1. Arrestare il nodo dal prompt del modulo controller esistente:

   ```
   halt local -inhibit-takeover true
   ```

   Se viene richiesto di continuare la procedura di interruzione, immettere `y` Quando richiesto, quindi attendere che il sistema si arresti al prompt DEL CARICATORE.

   In un sistema 80xx, il LED NVRAM si trova sul modulo controller a destra delle porte di rete, contrassegnato dal simbolo della batteria.

   Questo LED lampeggia se nella NVRAM sono presenti dati non scritti. Se questo LED lampeggia in ambra dopo aver immesso il comando halt, riavviare il sistema e provare a interromperlo di nuovo.

2. Se non si è già collegati a terra, mettere a terra l'utente.
3. Spegnere gli alimentatori e scollegare l'alimentazione, utilizzando il metodo corretto per il sistema e il tipo di alimentatore in uso:

Se il sistema utilizza…	Quindi…
Alimentatori CA	Scollegare i cavi di alimentazione dalla fonte di alimentazione, quindi rimuovere i cavi di alimentazione.
Alimentatori CC	Scollegare l'alimentazione dalla fonte CC, quindi rimuovere i cavi CC, se necessario.

Installare e cablare il nuovo modulo controller

Installazione e cablaggio del nuovo modulo controller

È necessario installare fisicamente il nuovo modulo controller nello chassis e collegarlo via cavo.

Fasi

1. Se si dispone di un modulo di espansione i/o (IOXM) nel sistema e si sta creando una coppia ha a chassis singolo, è necessario scollegare e rimuovere IOXM.

   È quindi possibile utilizzare l'alloggiamento vuoto per il nuovo modulo controller. Tuttavia, la nuova configurazione non avrà l'i/o extra fornito da IOXM.

2. Installare fisicamente il nuovo modulo controller e, se necessario, installare ventole aggiuntive:

Se si aggiunge un modulo controller…	Quindi, eseguire questa procedura…

A un alloggiamento vuoto per creare una coppia ha a chassis singolo e il sistema appartiene a una delle seguenti piattaforme:	a. Rimuovere la piastra vuota nella parte posteriore dello chassis che copre l'alloggiamento vuoto che contiene il nuovo modulo controller. b. Spingere delicatamente il modulo controller a metà nel telaio. Per evitare che il modulo controller si avvii automaticamente, non inserirlo completamente nel telaio fino a quando non viene eseguita questa procedura.
In uno chassis separato dal partner ha per creare una coppia ha a doppio chassis quando la configurazione esistente si trova in una configurazione controller-modulo IOX. • FAS8200 • 80xx	Installare il nuovo sistema nel rack o nell'armadietto del sistema.

3. Cablare le connessioni di rete del cluster, se necessario:

   a. Identificare le porte sul modulo controller per le connessioni del cluster.

      "Sistemi AFF A320: Installazione e configurazione"

      "Istruzioni per l'installazione e la configurazione dei sistemi AFF A220/FAS2700"

      "Istruzioni per l'installazione e la configurazione dei sistemi AFF A800"

      "Istruzioni per l'installazione e la configurazione dei sistemi AFF A300"

      "Istruzioni per l'installazione e la configurazione dei sistemi FAS8200"

   b. Se si configura un cluster con switch, identificare le porte che verranno utilizzate sugli switch di rete del cluster.

      Vedere "Guida alla configurazione degli switch Clustered Data ONTAP per gli switch Cisco", "^Guida all'installazione dello switch in modalità cluster ^NetApp 10G" oppure "Guida all'installazione dello switch in modalità cluster NetApp 1G", a seconda degli interruttori utilizzati.

   c. Collegare i cavi alle porte del cluster:

Se il cluster è…	Quindi…
Un cluster senza switch a due nodi	Collegare direttamente le porte del cluster sul modulo controller esistente alle porte del cluster corrispondenti sul nuovo modulo controller.

Un cluster con switch	Collegare le porte del cluster di ciascun controller alle porte degli switch di rete del cluster identificati nel passo b.

Collegamento delle porte FC-VI e HBA del nuovo modulo controller agli switch FC

Le porte FC-VI e gli HBA (host bus adapter) del nuovo modulo controller devono essere cablati agli switch FC del sito.

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 i sistemi che utilizzano due porte initiator"

Cablaggio delle connessioni di peering del nuovo modulo controller

È necessario collegare il nuovo modulo controller alla rete di peering del cluster in modo che sia connesso al cluster sul sito del partner.

A proposito di questa attività

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.

Fasi

1. Identificare e collegare almeno due porte per il peering del cluster e verificare che dispongano di connettività di rete con il cluster partner.

Accendere entrambi i moduli controller e visualizzare il prompt DEL CARICATORE

Accendere il modulo controller esistente e il nuovo modulo controller per visualizzare il prompt DEL CARICATORE.

Fasi

Accendere i moduli controller e interrompere il processo di avvio, seguendo la procedura per la configurazione:

Se i moduli controller sono…	Quindi…

Nello stesso chassis	1. Verificare che il nuovo modulo controller sia **non** completamente inserito nell'alloggiamento. Il modulo controller esistente deve essere inserito completamente nell'alloggiamento perché non è mai stato rimosso dallo chassis, ma il nuovo modulo controller non dovrebbe esserlo. 2. Collegare l'alimentazione e accendere gli alimentatori in modo che il modulo controller esistente riceva alimentazione. 3. Interrompere il processo di avvio sul modulo controller esistente premendo Ctrl-C. 4. Inserire saldamente il nuovo modulo controller nell'alloggiamento. Una volta inserito completamente, il nuovo modulo controller riceve alimentazione e si avvia automaticamente. 5. Interrompere il processo di avvio premendo Ctrl-C. 6. Serrare la vite a testa zigrinata sull'impugnatura della camma, se presente. 7. Installare il dispositivo di gestione dei cavi, se presente. 8. Collegare i cavi al dispositivo di gestione dei cavi con il gancio e la fascetta.
In uno chassis separato	1. Accendere gli alimentatori del modulo controller esistente. 2. Interrompere il processo di avvio premendo Ctrl-C. 3. Ripetere questa procedura per il nuovo modulo controller

Ogni modulo controller dovrebbe visualizzare il prompt DEL CARICATORE (`LOADER>`, `LOADER-A>`, o. `LOADER-B>`).

> Se non viene visualizzato alcun prompt DEL CARICATORE, annotare il messaggio di errore. Se il sistema visualizza il menu di avvio, riavviare e tentare di interrompere nuovamente il processo di avvio.

Modifica dell'impostazione ha-config sui moduli controller esistenti e nuovi

Quando si espande una configurazione MetroCluster, è necessario aggiornare l'impostazione ha-config del modulo controller esistente e del nuovo modulo controller. È inoltre necessario determinare l'ID di sistema del nuovo modulo controller.

A proposito di questa attività

Questa attività viene eseguita in modalità di manutenzione sui moduli controller esistenti e nuovi.

Fasi

1. Modificare l'impostazione ha-config del modulo controller esistente:

   a. Visualizzare l'impostazione ha-config del modulo controller e dello chassis esistenti:

   ```
   ha-config show
   ```

L'impostazione ha-config è "mcc-2n" per tutti i componenti perché il modulo controller era in una configurazione MetroCluster a due nodi.

b. Modificare l'impostazione ha-config del modulo controller esistente in "mcc":
```
ha-config modify controller mcc
```
c. Modificare l'impostazione ha-config dello chassis esistente in "mcc":

```
ha-config modify chassis mcc
```

d. Recuperare l'ID di sistema per il modulo controller esistente:

```
sysconfig
```

Annotare l'ID del sistema. È necessario quando si imposta l'ID partner sul nuovo modulo controller.

a. Uscire dalla modalità di manutenzione per tornare al prompt DEL CARICATORE:

```
halt
```

2. Modificare l'impostazione ha-config e recuperare l'ID di sistema del nuovo modulo controller:

a. Se il nuovo modulo controller non è già in modalità di manutenzione, avviarlo in modalità di manutenzione:

```
boot_ontap maint
```

b. Modificare l'impostazione ha-config del nuovo modulo controller in "mcc":

```
ha-config modify controller mcc
```

c. Modificare l'impostazione ha-config del nuovo chassis in mcc:

```
ha-config modify chassis mcc
```

d. Recuperare l'ID di sistema per il nuovo modulo controller:

```
sysconfig
```

Annotare l'ID del sistema. È necessario quando si imposta l'ID partner e si assegnano i dischi al nuovo modulo controller.

a. Uscire dalla modalità di manutenzione per tornare al prompt DEL CARICATORE:

```
halt
```

Impostazione dell'ID del sistema partner per entrambi i moduli controller

È necessario impostare l'ID del sistema partner su entrambi i moduli controller in modo che possano formare una coppia ha.

A proposito di questa attività

Questa attività viene eseguita con entrambi i moduli controller al prompt DEL CARICATORE.

Fasi

1. Sul modulo controller esistente, impostare l'ID del sistema partner su quello del nuovo modulo controller:

   ```
   setenv partner-sysid sysID_of_new_controller
   ```

2. Sul nuovo modulo controller, impostare l'ID del sistema partner su quello del modulo controller esistente:

   ```
   setenv partner-sysid sysID_of_existing_controller
   ```

Avvio del modulo controller esistente

È necessario avviare il modulo controller esistente in ONTAP.

Fasi

1. Al prompt DEL CARICATORE, avviare il modulo controller esistente in ONTAP:

   ```
   boot_ontap
   ```

Assegnazione di dischi al nuovo modulo controller

Prima di completare la configurazione del nuovo modulo controller tramite netboot, è necessario assegnarvi i dischi.

A proposito di questa attività

È necessario assicurarsi che vi siano abbastanza spare, dischi non assegnati o dischi assegnati che non fanno parte di un aggregato esistente.

"Preparazione per l'aggiornamento"

Questi passaggi vengono eseguiti sul modulo controller esistente.

Fasi

1. Assegnare il disco root al nuovo modulo controller:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

   Se il modello di piattaforma utilizza la funzione Advanced Drive Partitioning (ADP), è necessario includere il parametro -root true:

   ```
   storage disk assign -disk disk_name -root true -sysid new_controller_sysID
   -force true
   ```

2. Assegnare i dischi rimanenti richiesti al nuovo modulo controller immettendo il seguente comando per ciascun disco:

   ```
   storage disk assign -disk disk_name -sysid new_controller_sysID -force true
   ```

3. Verificare che le assegnazioni dei dischi siano corrette:

   ```
   storage disk show -partitionownership*
   ```

Assicurarsi di aver assegnato tutti i dischi che si desidera assegnare al nuovo nodo.

Avvio in rete e configurazione di ONTAP sul nuovo modulo controller

Quando si aggiungono moduli controller a una configurazione MetroCluster esistente, è necessario eseguire una sequenza specifica di passaggi per eseguire il netboot e installare il sistema operativo ONTAP sul nuovo modulo controller.

A proposito di questa attività

- Questa attività inizia dal prompt DEL CARICATORE del nuovo modulo controller.
- Questa attività include l'inizializzazione dei dischi.

  Il tempo necessario per inizializzare i dischi dipende dalle dimensioni dei dischi.

- Il sistema assegna automaticamente due dischi al nuovo modulo controller.

  "Gestione di dischi e aggregati"

Fasi

1. Al prompt DEL CARICATORE, configurare l'indirizzo IP del nuovo modulo controller in base alla disponibilità DHCP:

Se DHCP è…	Quindi immettere il seguente comando…
Disponibile	**`ifconfig e0M -auto`**
Non disponibile	`ifconfig e0M -addr=`*`filer_addr`* `-mask=`*`netmask`* `-gw=`*`gateway`* `-dns=`*`dns_addr`* `-domain=`*`dns_domain`* *`filer_addr`* È l'indirizzo IP del sistema di storage. *`netmask`* è la maschera di rete del sistema di storage. *`gateway`* è il gateway per il sistema storage. *`dns_addr`* È l'indirizzo IP di un name server sulla rete. *`dns_domain`* È il nome di dominio DNS (Domain Name System). Se si utilizza questo parametro opzionale, non è necessario un nome di dominio completo nell'URL del server netboot; è necessario solo il nome host del server. Potrebbero essere necessari altri parametri per l'interfaccia. Per ulteriori informazioni, utilizzare `help ifconfig` Al prompt DEL CARICATORE.

2. Al prompt DEL CARICATORE, eseguire il netboot del nuovo nodo:

Per…	Eseguire questo comando…

SISTEMI DELLE SERIE FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
Tutti gli altri sistemi	`netboot \http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

Il *`path_to_the_web-accessible_directory`* è la posizione del scaricato `<ontap_version>_image.tgz` file.

3. Selezionare l'opzione **Installa prima il nuovo software** dal menu visualizzato.

   Questa opzione di menu consente di scaricare e installare la nuova immagine ONTAP sul dispositivo di avvio.

   - Inserire "y" quando viene visualizzato il messaggio che indica che questa procedura non è supportata per l'aggiornamento senza interruzioni su una coppia ha.
   - Inserire "y" quando viene visualizzato un messaggio che indica che questo processo sostituisce il software ONTAP esistente con un nuovo software.
   - Quando viene richiesto l'URL del file image.tgz, inserire il percorso nel modo seguente:

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Inserire "y" quando richiesto in relazione all'aggiornamento o alla sostituzione del software senza interruzioni.
5. Inserire il percorso del file image.tgz quando viene richiesto l'URL del pacchetto.

   ```
   What is the URL for the package? `http://path_to_web-accessible_directory/image.tgz`
   ```

6. Immettere "n" per ignorare il ripristino del backup quando viene richiesto di ripristinare la configurazione del backup.

```
*************************************************************
*             Restore Backup Configuration                  *
*  This procedure only applies to storage controllers that  *
*  are configured as an HA pair.                            *
*                                                           *
*  Choose Yes to restore the "varfs" backup configuration   *
*  from the SSH server.  Refer to the Boot Device Replacement *
*  guide for more details.                                  *
*  Choose No to skip the backup recovery and return to the  *
*  boot menu.                                               *
*************************************************************

Do you want to restore the backup configuration
now? {y|n} `n`
```

7. Immettere “y” quando viene richiesto di riavviare ora.

```
The node must be rebooted to start using the newly installed software.
Do you want to
reboot now? {y|n} `y`
```

8. Se necessario, selezionare l’opzione **clean Configuration and initialize all disks** after the node has boot (pulizia configurazione e inizializzazione di tutti i dischi* dopo l’avvio del nodo).

   Poiché si sta configurando un nuovo modulo controller e i dischi del nuovo modulo controller sono vuoti, è possibile rispondere “y” quando il sistema avverte che verranno cancellati tutti i dischi.

   > Il tempo necessario per inizializzare i dischi dipende dalle dimensioni dei dischi e dalla configurazione.

9. Una volta inizializzati i dischi e avviata l’installazione guidata del cluster, impostare il nodo:

   Inserire le informazioni LIF di gestione dei nodi nella console.

10. Accedere al nodo e immettere `cluster setup` quindi, digitare “join” quando viene richiesto di unirsi al cluster.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}: `join`
```

11. Rispondere alle richieste rimanenti in base alle esigenze del sito.

    Il "Setup ONTAP (Configurazione guidata)" Per la versione di ONTAP in uso sono disponibili ulteriori dettagli.

12. Se il sistema si trova in una configurazione cluster senza switch a due nodi, creare le interfacce del cluster

sul nodo esistente utilizzando il comando di creazione dell'interfaccia di rete per creare le LIF del cluster sulle porte del cluster.

Di seguito viene riportato un comando di esempio per la creazione di una LIF del cluster su una delle porte del cluster del nodo. Il parametro -auto configura la LIF in modo che utilizzi un indirizzo IP link-local.

```
cluster_A::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node_A_1 -home-port e1a -auto true
```

13. Una volta completata l'installazione, verificare che il nodo sia integro e idoneo a partecipare al cluster:

    ```
    cluster show
    ```

    L'esempio seguente mostra un cluster dopo l'Unione del secondo nodo (cluster1-02):

    ```
    cluster_A::> cluster show
    Node                  Health  Eligibility
    --------------------- ------- ------------
    node_A_1              true    true
    node_A_2              true    true
    ```

    È possibile accedere alla configurazione guidata del cluster per modificare i valori immessi per la macchina virtuale di storage amministrativa (SVM) o il nodo SVM utilizzando il comando di installazione del cluster.

14. Verificare che siano configurate quattro porte come interconnessioni cluster:

    ```
    network port show
    ```

    L'esempio seguente mostra l'output per due moduli controller in cluster_A:

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_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
node_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.
```

Mirroring dell'aggregato root sul nuovo controller

È necessario eseguire il mirroring dell'aggregato root per fornire la protezione dei dati quando si aggiunge un controller a una configurazione MetroCluster.

Questa attività deve essere eseguita sul nuovo modulo controller.

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.

Configurare le LIF tra cluster

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 nel cluster01:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

   ```
   network interface show -fields home-port,curr-port
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra che alle porte "e0e" e "e0f" non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Creare un gruppo di failover per le porte dedicate:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Nell'esempio seguente vengono assegnate le porte "e0e" e "e0f" al gruppo di failover "cluster01" sul sistema SVM "cluster01":

```
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
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Versione di ONTAP	Comando
9.6 e versioni successive	`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`
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:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verificare che le LIF dell'intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta 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
```

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
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Creazione di LIF intercluster sulla SVM di sistema:

In 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`*
In 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`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e. `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che i LIF 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
```

Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

A proposito di questa attività

- Devi sapere quali dischi verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come assicurarsi di selezionare il tipo di disco corretto.
- I dischi sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi in tale aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale per quell'aggregato.

  Nei sistemi che utilizzano ADP, gli aggregati vengono creati utilizzando partizioni in cui ciascun disco viene partizionato nelle partizioni P1, P2 e P3.

- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.

  "Gestione di dischi e aggregati"

> 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.

Fasi

1. Visualizzare un elenco delle parti di ricambio disponibili:

   ```
   storage disk show -spare -owner node_name
   ```

2. Creare l'aggregato:

   `storage aggregate create -mirror true`

   Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su qualsiasi nodo del cluster. Per assicurarsi che l'aggregato venga creato su un nodo specifico, utilizzare `-node` o specificare i dischi di proprietà di quel nodo.

   È possibile specificare le seguenti opzioni:

   - Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
   - Elenco dei dischi specifici da aggiungere all'aggregato
   - Numero di dischi da includere

     > Nella configurazione minima supportata, in cui è disponibile un numero limitato di dischi, è necessario utilizzare l'opzione force-Small-aggregate per consentire la creazione di un aggregato RAID-DP a tre dischi.

   - Stile checksum da utilizzare per l'aggregato
   - Tipo di dischi da utilizzare
   - Dimensioni delle unità da utilizzare
   - Velocità del disco da utilizzare
   - Tipo RAID per i gruppi RAID sull'aggregato
   - Numero massimo di dischi che possono essere inclusi in un gruppo RAID
   - Se sono consentiti dischi con diversi RPM

     Per ulteriori informazioni su queste opzioni, 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`*

Installazione delle licenze per il nuovo modulo controller

È necessario aggiungere le licenze per il nuovo modulo controller per tutti i servizi ONTAP che richiedono licenze standard (con blocco a nodo). Per le funzionalità con licenze standard, ogni nodo del cluster deve disporre di una propria chiave per la

funzionalità.

Per informazioni dettagliate sulle licenze, consultare l'articolo della Knowledge base 3013749: Panoramica e riferimenti sulle licenze di Data ONTAP 8.2 sul sito di supporto NetApp e il documento *riferimento per l'amministrazione del sistema*.

Fasi

1. Se necessario, procurarsi le chiavi di licenza per il nuovo nodo sul sito di supporto NetApp nella sezione My Support (supporto personale) sotto Software licenss (licenze software).

   Per ulteriori informazioni sulle sostituzioni delle licenze, consultare l'articolo della Knowledge base "Processo di sostituzione della scheda madre per aggiornare le licenze su un sistema AFF/FAS."

2. Immettere il seguente comando per installare ogni chiave di licenza:

   ```
   system license add -license-code license_key
   ```

   Il *license_key* lunghezza: 28 cifre.

3. Ripetere questo passaggio per ogni licenza standard richiesta (bloccata da nodo).

Creazione di aggregati di dati senza mirror

È possibile creare aggregati di dati senza mirroring per i dati che non richiedono il mirroring ridondante fornito dalle configurazioni MetroCluster.

A proposito di questa attività

- È necessario sapere quali dischi o LUN di array verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come verificare che sia selezionato il tipo di disco corretto.

> Nelle configurazioni MetroCluster IP, gli aggregati remoti senza mirror non sono accessibili dopo uno switchover

> Gli aggregati senza mirror devono essere locali rispetto al nodo che li possiede.

- I dischi e le LUN degli array sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi dell'aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale dell'aggregato.
- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.
- *Gestione di dischi e aggregati* contiene ulteriori informazioni sugli aggregati di mirroring.

Fasi

1. Installare e cablare gli shelf di dischi che conterranno gli aggregati senza mirror.

   È possibile utilizzare le procedure descritte nella documentazione di *installazione e configurazione* per la piattaforma e gli shelf di dischi.

   "Documentazione dei sistemi hardware ONTAP"

2. Assegnare manualmente tutti i dischi sul nuovo shelf al nodo appropriato:

   `disk assign -disk disk-id -owner owner-node-name`

3. 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 inoltre necessario assicurarsi di includere nell'aggregato solo i dischi sullo shelf senza mirror.

   È possibile specificare le seguenti opzioni:

   - Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
   - Elenco di unità o LUN di array specifici da aggiungere all'aggregato
   - Numero di dischi da includere
   - Stile checksum da utilizzare per l'aggregato
   - Tipo di dischi da utilizzare
   - Dimensioni delle unità da utilizzare
   - Velocità del disco da utilizzare
   - Tipo RAID per i gruppi RAID sull'aggregato
   - Numero massimo di unità o LUN di array che possono essere inclusi in un gruppo RAID
   - Se sono consentiti dischi con diversi RPM

     Per ulteriori informazioni su queste opzioni, consultare `storage aggregate create` pagina man.

     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
```

4. Verificare il gruppo RAID e i dischi del nuovo aggregato:

   `storage aggregate show-status -aggregate aggregate-name`

Informazioni correlate

"Gestione di dischi e aggregati"

Installazione del firmware dopo l'aggiunta di un modulo controller

Dopo aver aggiunto il modulo controller, è necessario installare il firmware più recente sul nuovo modulo controller in modo che il modulo controller funzioni correttamente con ONTAP.

Fasi

1. Scaricare la versione più recente del firmware per il sistema e seguire le istruzioni per scaricare e installare il nuovo firmware.

   "Download NetApp: Firmware di sistema e diagnostica"

Aggiornamento della configurazione MetroCluster con nuovi controller

È necessario aggiornare la configurazione MetroCluster quando si espande da una configurazione a due nodi a una a quattro nodi.

Fasi

1. Aggiornare la configurazione MetroCluster:

   a. Accedere alla modalità avanzata dei privilegi:
   `set -privilege advanced`

   b. Aggiornare la configurazione MetroCluster:
   `metrocluster configure -refresh true -allow-with-one-aggregate true`

   Il seguente comando aggiorna la configurazione MetroCluster su tutti i nodi del gruppo DR che contiene controller_A_1:

```
controller_A_1::*> metrocluster configure -refresh true -allow-with-one
-aggregate true

[Job 726] Job succeeded: Configure is successful.
```

   a. Tornare alla modalità privilegi di amministratore:

   `set -privilege admin`

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
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    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
```

c. Verificare che le relazioni di DR siano state create correttamente:

   `metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner`

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner   dr-
auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Attivazione del failover dello storage su entrambi i moduli controller e attivazione del cluster ha

Dopo aver aggiunto nuovi moduli controller alla configurazione MetroCluster, è necessario abilitare il failover dello storage su entrambi i moduli controller e abilitare separatamente il cluster ha.

Prima di iniziare

La configurazione di MetroCluster deve essere stata aggiornata in precedenza utilizzando `metrocluster configure -refresh true` comando.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Abilitare il failover dello storage:

   `storage failover modify -enabled true -node existing-node-name`

   Il singolo comando consente il failover dello storage su entrambi i moduli controller.

2. Verificare che il failover dello storage sia attivato:

   `storage failover show`

   L'output dovrebbe essere simile a quanto segue:

   ```
   Node           Partner        Possible State Description
   -------------- -------------- -------- ----------------------
   old-ctlr        new-ctlr      true      Connected to new-ctlr
   new-ctlr        old-ctlr      true      Connected to old-ctlr
   2 entries were displayed.
   ```

3. Attiva cluster ha:

   `cluster ha modify -configured true`

   La disponibilità elevata del cluster (ha) deve essere configurata in un cluster se contiene solo due nodi e differisce dall'ha fornito dal failover dello storage.

Riavviare le SVM

Dopo aver espanso la configurazione MetroCluster, è necessario riavviare le SVM.

Fasi

1. Identificare le SVM che devono essere riavviate:

   `metrocluster vserver show`

   Questo comando mostra le SVM su entrambi i cluster MetroCluster.

2. Riavviare le SVM sul primo cluster:

   a. Accedere alla modalità avanzata dei privilegi, premendo **y** quando richiesto:

      `set -privilege advanced`

   b. Riavviare le SVM:

      `vserver start -vserver SVM_name -force true`

   c. Tornare alla modalità privilegi di amministratore:

```
set -privilege admin
```

3. Ripetere il passaggio precedente sul cluster partner.
4. Verificare che le SVM siano in buono stato:

```
metrocluster vserver show
```

Espandere una configurazione MetroCluster FC a quattro nodi in una configurazione a otto nodi

Espansione di una configurazione MetroCluster FC a quattro nodi in una configurazione a otto nodi

L'espansione di una configurazione MetroCluster FC a quattro nodi in una configurazione MetroCluster FC a otto nodi comporta l'aggiunta di due controller a ciascun cluster per formare una seconda coppia ha in ogni sito MetroCluster e quindi l'esecuzione dell'operazione di configurazione MetroCluster FC.

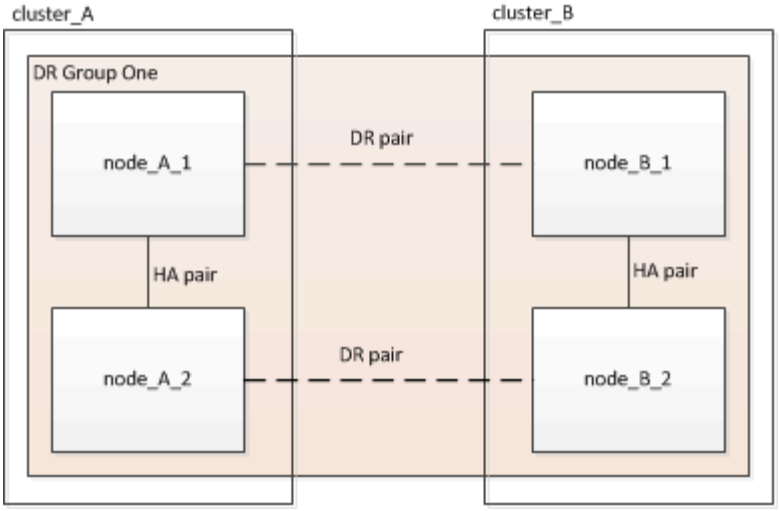
A proposito di questa attività

- I nodi devono eseguire ONTAP 9 in una configurazione MetroCluster FC.

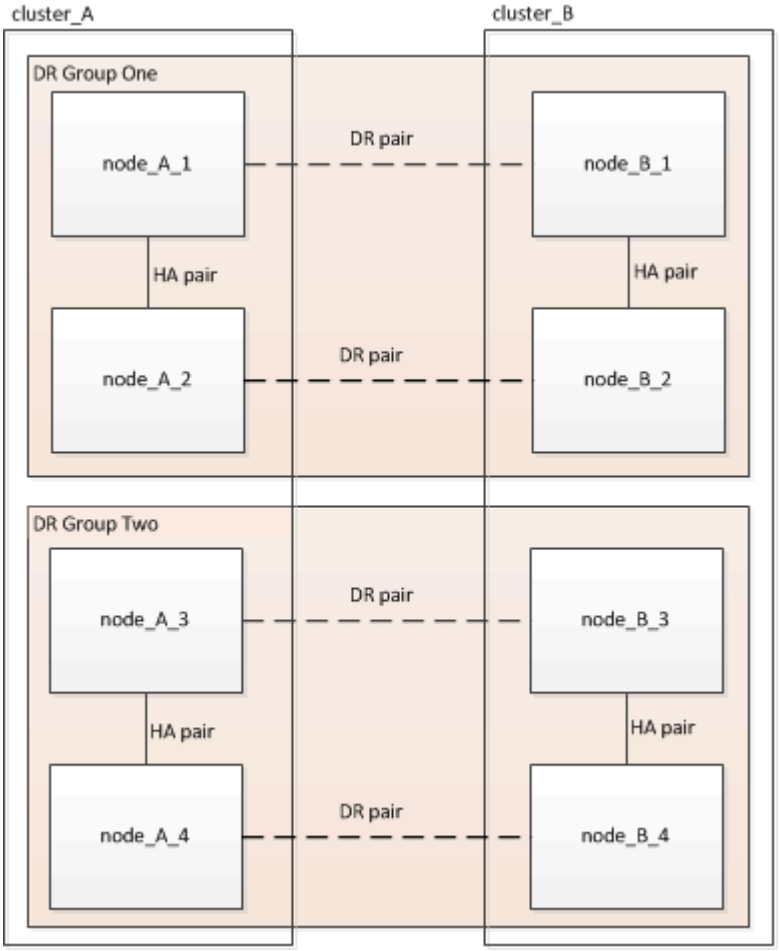
  Questa procedura non è supportata nelle versioni precedenti di ONTAP o nelle configurazioni MetroCluster IP.

- La configurazione MetroCluster FC esistente deve essere in buone condizioni.
- L'apparecchiatura che si sta aggiungendo deve essere supportata e soddisfare tutti i requisiti descritti in "Installazione e configurazione di Fabric-Attached MetroCluster"
- È necessario disporre di porte switch FC disponibili per ospitare i nuovi controller e i nuovi bridge.
- È necessaria la password admin e l'accesso a un server FTP o SCP.
- Questa procedura si applica solo alle configurazioni MetroCluster FC.
- Questa procedura è senza interruzioni e richiede circa un giorno per il completamento (ad esclusione di rack e stack) quando i dischi vengono azzerati.

Prima di eseguire questa procedura, la configurazione MetroCluster FC è costituita da quattro nodi, con una coppia ha in ogni sito:



Al termine di questa procedura, la configurazione MetroCluster FC è costituita da due coppie ha in ogni sito:



Entrambi i siti devono essere espansi in modo uguale. Una configurazione MetroCluster FC non può essere costituita da un numero di nodi non uniforme.

Combinazioni di piattaforme supportate quando si aggiunge un secondo gruppo DR

La seguente tabella mostra le combinazioni di piattaforme supportate per le configurazioni FC MetroCluster a otto nodi.

- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, se si dispone di una configurazione a otto nodi, tutti e otto i nodi devono utilizzare la stessa versione di ONTAP.
- Le combinazioni di questa tabella si applicano solo alle configurazioni a otto nodi regolari o permanenti.
- Le combinazioni di piattaforme in questa tabella **non** si applicano se si utilizzano le procedure di transizione o aggiornamento.
- Tutti i nodi di un gruppo di DR devono essere dello stesso tipo e configurazione.

		8Node DrGroup 2									
		FAS8200	AFF A300	FAS8300	AFF A400	ASA A400	FAS9000	AFF A700	FAS9500	AFF A900	ASA A900
8Node DrGroup 1	FAS8200										
	AFF A300										
	FAS8300										
	AFF A400										
	ASA A400										
	FAS9000										
	AFF A700										
	FAS9500										
	AFF A900										
	ASA A900										

Determinazione del nuovo layout di cablaggio

È necessario determinare il cablaggio dei nuovi moduli controller e dei nuovi shelf di dischi per gli switch FC esistenti.

A proposito di questa attività

Questa attività deve essere eseguita in ogni sito MetroCluster.

Fasi

1. Seguire la procedura descritta in "Installazione e configurazione di Fabric-Attached MetroCluster" Per creare un layout di cablaggio per il proprio tipo di switch, utilizzando l'utilizzo della porta per una configurazione MetroCluster a otto nodi.

   L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo descritto nella procedura per poter utilizzare i file di configurazione di riferimento (RCF).

   Se non è possibile cablare l'ambiente in modo da poter utilizzare i file RCF, è necessario configurare manualmente il sistema in base alle istruzioni riportate nella "Installazione e configurazione di Fabric-Attached MetroCluster". Non utilizzare questa procedura se il cablaggio non utilizza file RCF.

Scaffalatura delle nuove apparecchiature

È necessario eseguire il rack dell'apparecchiatura per i nuovi nodi.

Fasi

1. Seguire la procedura descritta in "Installazione e configurazione di Fabric-Attached MetroCluster" Per il rack di nuovi sistemi storage, shelf di dischi e bridge FC-SAS.

Verifica dello stato della configurazione MetroCluster

Verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Verificare che il mirroring sia attivato su ciascun nodo:

   ```
   metrocluster node show
   ```

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Verificare che i componenti di MetroCluster siano in buone condizioni:

   ```
   metrocluster check run
   ```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Verificare che non siano presenti avvisi sullo stato di salute:

   `system health alert show`

5. Simulare un'operazione di switchover:
   a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:
      `set -privilege advanced`

      Devi rispondere con **`y`** quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

   b. Eseguire l'operazione di switchover con il parametro -simulate:
      `metrocluster switchover -simulate`
   c. Tornare al livello di privilegio admin:
      `set -privilege admin`

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.

Invio di un messaggio AutoSupport personalizzato prima dell'aggiunta di nodi alla configurazione MetroCluster

Devi inviare un messaggio AutoSupport per informare il supporto tecnico di NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster dal sito_A.
2. Richiamare un messaggio AutoSupport che indica l'inizio della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours
   ```

   Il `maintenance-window-in-hours` il parametro specifica la lunghezza della finestra di manutenzione e può essere un massimo di 72 ore. Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile inviare il seguente comando per indicare che il periodo di manutenzione è terminato:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Ripetere questo passaggio sul sito del partner.

Ricable e zone a fabric di switch per i nuovi nodi

Disconnessione del gruppo DR esistente dal fabric

È necessario scollegare i moduli controller esistenti dagli switch FC nel fabric.

A proposito di questa attività

Questa attività deve essere eseguita in ogni sito MetroCluster.

Fasi

1. Disattivare le porte HBA che collegano i moduli controller esistenti al fabric switch in fase di manutenzione:

   ```
   storage port disable -node node-name -port port-number
   ```

2. Sugli switch FC locali, rimuovere i cavi dalle porte dei bridge HBA, FC-VI e ATTO del modulo controller esistente.

   I cavi devono essere etichettati per facilitarne l'identificazione quando vengono riccavi. Solo le porte ISL

devono rimanere cablate.

È possibile riconfigurare e riconfigurare gli switch

È necessario applicare i file RCF per riconfigurare lo zoning in modo da ospitare i nuovi nodi.

Se non è possibile utilizzare i file RCF per configurare gli switch, è necessario configurarli manualmente. Vedere:

- "Configurare manualmente gli switch Brocade FC"
- "Configurare manualmente gli switch Cisco FC"

Fasi

1. Individuare i file RCF per la configurazione.

   È necessario utilizzare i file RCF per una configurazione a otto nodi che corrisponda al modello di switch in uso.

2. Applicare i file RCF seguendo le istruzioni riportate nella pagina di download, regolando le impostazioni ISL in base alle necessità.
3. Assicurarsi che la configurazione dello switch sia salvata.
4. Riavviare gli switch FC.
5. Collegare i bridge FC-SAS preesistenti e nuovi agli switch FC, utilizzando il layout di cablaggio creato in precedenza.

   L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo di otto nodi MetroCluster descritto in "Installazione e configurazione di Fabric-Attached MetroCluster" In modo da poter utilizzare i file di configurazione di riferimento (RCF).

6. Verificare che le porte siano in linea utilizzando il comando corretto per lo switch.

Vendor di switch	Comando
Brocade	switchshow
Cisco	mostra il brief dell'interfaccia

7. Seguire la procedura descritta in "Installazione e configurazione di Fabric-Attached MetroCluster" Per collegare le porte FC-VI dai controller esistenti e nuovi, utilizzando il layout di cablaggio creato in precedenza.

   L'utilizzo della porta dello switch FC deve corrispondere all'utilizzo di otto nodi MetroCluster descritto in "Installazione e configurazione di Fabric-Attached MetroCluster" In modo da poter utilizzare i file di configurazione di riferimento (RCF).

8. Dai nodi esistenti, verificare che le porte FC-VI siano in linea:

   ```
   metrocluster interconnect adapter show
   ```

   ```
   metrocluster interconnect mirror show
   ```

9. Collegare le porte HBA ai controller attuali e nuovi.
10. Sui moduli controller esistenti, abilitare e-abilitare le porte collegate allo switch fabric in fase di manutenzione:

    ```
    storage port enable -node node-name -port port-ID
    ```

11. Avviare i nuovi controller e avviarli in modalità di manutenzione:

    ```
    boot_ontap maint
    ```

12. Verificare che solo lo storage che verrà utilizzato dal nuovo gruppo DR sia visibile ai nuovi moduli controller.

    Nessuno dello storage utilizzato dall'altro gruppo di DR deve essere visibile.

13. Tornare all'inizio di questa procedura per ricollegare il secondo fabric dello switch.

Configurare ONTAP sui nuovi controller

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

    ```
    halt
    ```

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

    ```
    set-defaults
    ```

3. Salvare l'ambiente:

    ```
    saveenv
    ```

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

    ```
    boot_ontap menu
    ```

5. Al prompt del menu di avvio, cancellare la configurazione:

    ```
    wipeconfig
    ```

    Rispondere `yes` al prompt di conferma.

    Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

    Rispondere `yes` al prompt di conferma.

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.

A proposito di questa attività

I controller dello storage devono essere in modalità Maintenance (manutenzione).

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, mentre il Pool 1 contiene sempre i dischi che sono remoti al sistema di storage che li possiede.

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 del partner ha 0:
   `disk assign -disk disk-name -p pool -n number-of-disks`

      Se lo storage controller 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 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.

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.

A proposito di questa attività

I controller dello storage devono essere in modalità Maintenance (manutenzione).

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-nameshelf-name -p pool
```

Se lo storage 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.

Verifica dello stato ha-config dei componenti

In una configurazione MetroCluster, lo stato ha-config del modulo controller e dei componenti dello chassis deve essere impostato su **mcc** per consentire il corretto avvio.

A proposito di questa attività

- Il sistema deve essere in modalità di manutenzione.
- Questa attività deve essere eseguita su ogni nuovo modulo controller.

Fasi

1. In modalità Maintenance (manutenzione), visualizzare lo stato ha del modulo controller e dello chassis:

   ```
   ha-config show
   ```

   Lo stato ha per tutti i componenti deve essere "mcc".

2. Se lo stato di sistema visualizzato del controller non è corretto, impostare lo stato ha per il modulo controller:

   ```
   ha-config modify controller mcc
   ```

3. Se lo stato di sistema visualizzato dello chassis non è corretto, impostare lo stato ha per lo chassis:

   ```
   ha-config modify chassis mcc
   ```

4. Ripetere questi passaggi sull'altro nodo sostitutivo.

Avviare i nuovi controller e unirli al cluster

Per unire i nuovi controller al cluster, è necessario avviare ciascun nuovo modulo controller e utilizzare la procedura guidata di configurazione del cluster ONTAP per identificare l'Unione del cluster.

Prima di iniziare

La configurazione MetroCluster deve essere cablata.

Non è necessario aver configurato il Service Processor prima di eseguire questa attività.

A proposito di questa attività

Questa attività deve essere eseguita su ciascuno dei nuovi controller in entrambi i cluster nella configurazione MetroCluster.

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 `halt` Per uscire dalla modalità di manutenzione, quindi immettere il seguente comando dal prompt DEL CARICATORE:

   ```
   boot_ontap
   ```

   Il modulo controller accede alla procedura guidata di configurazione dei nodi.

   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, quindi 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 si esegue il `metrocluster configure` comando più avanti nel processo di configurazione.

5. Verificare che siano configurate quattro porte come interconnessioni cluster:

   `network port show`

   L'esempio seguente mostra l'output per due controller in cluster_A. Se si tratta di una configurazione MetroCluster a due nodi, l'output mostra solo un nodo.

```
cluster_A::> network port show
                                                                  Speed
(Mbps)
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. Poiché si sta utilizzando la CLI per configurare il cluster, uscire dalla procedura guidata Node Setup:

   ```
   exit
   ```

7. Accedere all'account admin utilizzando `admin` nome utente.
8. Avviare l'installazione guidata del cluster, quindi unirsi al cluster esistente:

   ```
   cluster setup
   ```

```
::> cluster setup

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.


Do you want to create a new cluster or join an existing cluster?
{create, join}:`join`
```

9. Una volta completata la procedura guidata **Cluster Setup** e chiusa, verificare che il cluster sia attivo e che il nodo funzioni correttamente:

   `cluster show`

   L'esempio seguente mostra un cluster in cui il primo nodo (cluster1-01) è integro e idoneo a partecipare:

```
cluster_A::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node_A_1              true    true
node_A_2              true    true
node_A_3              true    true
```

   Se è necessario modificare una delle impostazioni immesse per l'SVM amministrativa o il nodo SVM, è possibile accedere alla procedura guidata **Cluster Setup** utilizzando `cluster setup command`.

Configurare i cluster in una configurazione MetroCluster

Configurare le LIF tra cluster

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 nel cluster01:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

```
network interface show -fields home-port,curr-port
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che alle porte "e0e" e "e0f" non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Creare un gruppo di failover per le porte dedicate:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical_or_logical_ports`*

   Nell'esempio seguente vengono assegnate le porte "e0e" e "e0f" al gruppo di failover "cluster01" sul sistema SVM "cluster01":

```
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
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Versione di ONTAP	Comando
9.6 e versioni successive	`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`
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:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verificare che le LIF dell'intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster "cluster01_icl01" e "cluster01_icl02" sulla porta 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
```

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
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Creazione di LIF intercluster sulla SVM di sistema:

In 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`*
In 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`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e. `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

In ONTAP 9.6 e versioni successive:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

In ONTAP 9.6 e versioni successive:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:
`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che i LIF 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
```

Mirroring degli aggregati root

È necessario eseguire il mirroring degli aggregati root per garantire la protezione dei dati.

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.

Implementazione della configurazione MetroCluster

È necessario eseguire `metrocluster configure -refresh true` Per avviare la

protezione dei dati sui nodi aggiunti a una configurazione MetroCluster.

A proposito di questa attività

Si emette il `metrocluster configure -refresh true` Una volta, su uno dei nodi appena aggiunti, per aggiornare la configurazione MetroCluster. Non è necessario eseguire il comando su ciascuno dei siti o nodi.

Il `metrocluster configure -refresh true` 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.

Fasi

1. Aggiornare la configurazione MetroCluster:

   a. Accedere alla modalità avanzata dei privilegi:

      ```
      set -privilege advanced
      ```

   b. Aggiornare la configurazione MetroCluster su uno dei nuovi nodi:
      `metrocluster configure -refresh true`

      L'esempio seguente mostra la configurazione MetroCluster aggiornata su entrambi i gruppi di DR:

   ```
   controller_A_2::*> metrocluster configure -refresh true

   [Job 726] Job succeeded: Configure is successful.
   ```

   +

   ```
   controller_A_4::*> metrocluster configure -refresh true

   [Job 740] Job succeeded: Configure is successful.
   ```

   a. Tornare alla modalità privilegi di amministratore:

      ```
      set -privilege admin
      ```

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
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verificare la configurazione MetroCluster da entrambi i siti nella configurazione MetroCluster:

   a. Verificare la configurazione dal sito A:

   ```
   metrocluster show
   ```

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

   a. Verificare la configurazione dal sito B:
   ```
   metrocluster show
   ```

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

Creazione di un aggregato di dati mirrorato su ciascun nodo

È necessario creare un aggregato di dati mirrorato su ciascun nodo del gruppo DR.

A proposito di questa attività

- Devi sapere quali dischi verranno utilizzati nel nuovo aggregato.
- Se nel sistema sono presenti più tipi di dischi (storage eterogeneo), è necessario comprendere come assicurarsi di selezionare il tipo di disco corretto.
- I dischi sono di proprietà di un nodo specifico; quando si crea un aggregato, tutti i dischi in tale aggregato devono essere di proprietà dello stesso nodo, che diventa il nodo principale per quell'aggregato.

  Nei sistemi che utilizzano ADP, gli aggregati vengono creati utilizzando partizioni in cui ciascun disco viene partizionato nelle partizioni P1, P2 e P3.

- I nomi degli aggregati devono essere conformi allo schema di denominazione stabilito al momento della pianificazione della configurazione MetroCluster.

  "Gestione di dischi e aggregati"

> 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.

Fasi

1. Visualizzare un elenco delle parti di ricambio disponibili:

   `storage disk show -spare -owner node_name`

2. Creare l'aggregato:

   `storage aggregate create -mirror true`

   Se si è connessi al cluster nell'interfaccia di gestione del cluster, è possibile creare un aggregato su

qualsiasi nodo del cluster. Per assicurarsi che l'aggregato venga creato su un nodo specifico, utilizzare `-node` o specificare i dischi di proprietà di quel nodo.

È possibile specificare le seguenti opzioni:

- Nodo principale dell'aggregato (ovvero, il nodo proprietario dell'aggregato durante il normale funzionamento)
- Elenco dei dischi specifici da aggiungere all'aggregato
- Numero di dischi da includere

> Nella configurazione minima supportata, in cui è disponibile un numero limitato di dischi, è necessario utilizzare l'opzione force-Small-aggregate per consentire la creazione di un aggregato RAID-DP a tre dischi.

- Stile checksum da utilizzare per l'aggregato
- Tipo di dischi da utilizzare
- Dimensioni delle unità da utilizzare
- Velocità del disco da utilizzare
- Tipo RAID per i gruppi RAID sull'aggregato
- Numero massimo di dischi che possono essere inclusi in un gruppo RAID
- Se sono consentiti dischi con diversi RPM

  Per ulteriori informazioni su queste opzioni, 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`*

Configurazione di bridge FC-SAS per il monitoraggio dello stato di salute

Scoprite come configurare i bridge FC-to-SAS per il monitoraggio dello stato di salute.

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.

Fase

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	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*
9.4 e versioni precedenti	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

   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              Symbolic Name Is Monitored  Monitor Status  Vendor
Model                Bridge WWN
------------------  ------------- ------------  --------------  ------
-----------------    ----------
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::>
```

È possibile spostare un volume di metadati da un aggregato a un altro in una configurazione MetroCluster. È possibile spostare un volume di metadati quando l'aggregato di origine viene decommissionato o non viene eseguito il mirroring o per altri motivi che rendono l'aggregato non idoneo.

A proposito di questa attività

- Per eseguire questa attività, è necessario disporre dei privilegi di amministratore del cluster.
- L'aggregato di destinazione deve essere mirrorato e non deve trovarsi nello stato degradato.
- Lo spazio disponibile nell'aggregato di destinazione deve essere maggiore del volume di metadati che si sta spostando.

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

   ```
   set -privilege advanced
   ```

2. Identificare il volume di metadati da spostare:

   ```
   volume show MDV_CRS*
   ```

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identificare un aggregato di destinazione idoneo:

   `metrocluster check config-replication show-aggregate-eligibility`

   Il seguente comando identifica gli aggregati in cluster_A idonei per ospitare i volumi di metadati:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

Nell'esempio precedente, Node_A_1_aggr2 e Node_A_2_aggr2 sono idonei.

4. Avviare l'operazione di spostamento del volume:

   `volume move start -vserver` *`svm_name`* `-volume` *`metadata_volume_name`* `-destination -aggregate` *`destination_aggregate_name`*`*`

   Il seguente comando sposta il volume di metadati "MDV_CRS_14c00d4ac9f311e7922800a0984395f1" da "aggregate Node_A_1_aggr1" a "aggregate Node_A_1_aggr2":

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verificare lo stato dell'operazione di spostamento del volume:

```
volume move show -volume vol_constituent_name
```

6. Tornare al livello di privilegio admin:

```
set -privilege admin
```

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` i comandi non mostrano l'output previsto.

Fasi

1. Controllare la configurazione:

   ```
   metrocluster check run
   ```

   Il comando viene eseguito come processo in background e potrebbe non essere completato immediatamente.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait
   for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command,
   "metrocluster operation history show -job-id 2245"
   ```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. 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                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
```

```
                      controller_A_1_aggr1
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_1_aggr2
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok


controller_A_2        controller_A_2_aggr0
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_2_aggr1
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      ownership-state
ok
                      controller_A_2_aggr2
                                                      mirroring-status
ok
                                                      disk-pool-allocation
ok
                                                      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.
```

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.

Invio di un messaggio AutoSupport personalizzato dopo l'aggiunta di nodi alla configurazione MetroCluster

Devi inviare un messaggio AutoSupport per informare il supporto tecnico di NetApp che la manutenzione è stata completata.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Accedere al cluster dal sito_A.
2. Richiamare un messaggio AutoSupport che indica la fine della manutenzione:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Ripetere questo passaggio sul sito del partner.

Verifica dello switchover, della riparazione e dello switchback

Verificare le operazioni di switchover, riparazione e switchback della configurazione MetroCluster.

Fasi

1. Utilizzare le procedure per lo switchover negoziato, la riparazione e lo switchback in "Gestione MetroCluster e disaster recovery".

Espansione di una configurazione IP MetroCluster

A seconda della versione di ONTAP, è possibile espandere la configurazione IP di MetroCluster aggiungendo quattro nuovi nodi come nuovo gruppo di DR.

A partire da ONTAP 9.13.1, puoi espandere temporaneamente una configurazione MetroCluster a otto nodi per fare un refresh dei controller e dello storage. Vedere "Aggiornamento di una configurazione MetroCluster IP a quattro o otto nodi (ONTAP 9.8 e versioni successive)" per ulteriori informazioni.

A partire da ONTAP 9.9.1, è possibile aggiungere quattro nuovi nodi alla configurazione IP di MetroCluster come secondo gruppo di DR. In questo modo viene creata una configurazione MetroCluster a otto nodi.

Prima di iniziare

- I nodi vecchi e nuovi devono eseguire la stessa versione di ONTAP.
- Questa procedura descrive i passaggi necessari per aggiungere un gruppo DR a quattro nodi a una configurazione IP MetroCluster esistente. Se si aggiorna una configurazione a otto nodi, è necessario ripetere l'intera procedura per ciascun gruppo di DR, aggiungendone uno alla volta.
- Verificare che i modelli di piattaforma vecchi e nuovi siano supportati per la combinazione di piattaforme.

  "NetApp Hardware Universe"

- Verificare che i modelli di piattaforma vecchi e nuovi siano entrambi supportati dagli switch IP.

  "NetApp Hardware Universe"

- Se lo sei "Aggiornamento di una configurazione IP MetroCluster a quattro o otto nodi", i nuovi nodi devono disporre di spazio di archiviazione sufficiente per ospitare i dati dei vecchi nodi, insieme a dischi adeguati per gli aggregati root e i dischi di riserva.
- Verificare di disporre di un dominio di broadcast predefinito creato sui vecchi nodi.

  Quando si aggiungono nuovi nodi a un cluster esistente senza un dominio di broadcast predefinito, le LIF di gestione nodi vengono create per i nuovi nodi utilizzando gli UUID (Universal Unique Identifier) e non i nomi previsti. Per ulteriori informazioni, consultare l'articolo della Knowledge base "LIF di gestione nodi su nodi appena aggiunti generati con nomi UUID".

Esempio di denominazione in questa procedura

Questa procedura utilizza nomi di esempio per identificare i gruppi DR, i nodi e gli switch coinvolti.

Gruppi DR	Cluster_A presso il sito_A.	Cluster_B nel sito_B.
dr_group_1-old	• Node_A_1-old • Node_A_2-old	• Node_B_1-old • Node_B_2-old
dr_group_2-new	• Node_A_3-new • Node_A_4-new	• Node_B_3-new • Node_B_4-new

Combinazioni di piattaforme supportate quando si aggiunge un secondo gruppo DR

La seguente tabella mostra le combinazioni di piattaforme supportate per le configurazioni IP a otto nodi.

- Tutti i nodi della configurazione MetroCluster devono utilizzare la stessa versione di ONTAP. Ad esempio, se si dispone di una configurazione a otto nodi, tutti e otto i nodi devono utilizzare la stessa versione di ONTAP.
- Le combinazioni di questa tabella si applicano solo alle configurazioni a 8 nodi regolari o permanenti.
- Le combinazioni di piattaforme mostrate in questa tabella **non** si applicano se si utilizzano le procedure di transizione o aggiornamento.
- Tutti i nodi di un gruppo di DR devono essere dello stesso tipo e configurazione.

		8Node DrGroup 2									
		AFF A150 ASA A150	FAS2750 AFF A220	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	FAS8200 AFF A300	AFF A320	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	FAS8700	FAS9000 AFF A700	AFF C800 ASA C800 AFF A800 ASA A800	FAS9500 AFF A900 ASA A900
8Node DrGroup 1	AFF A150 ASA A150	Note 2									
	FAS2750 AFF A220										
	FAS500f AFF C250 ASA C250 AFF A250 ASA A250										
	FAS8200 AFF A300				Note 1						
	AFF A320					Note 1					
	FAS8300 AFF C400 ASA C400 AFF A400 ASA A400										
	FAS8700										
	FAS9000 AFF A700								Note 1		
	AFF C800 ASA A800 AFF A800 ASA A800										
	FAS9500 AFF A900 ASA A900										

- **Nota 1**: Per queste combinazioni è necessario ONTAP 9.9.1 o versione successiva (o la versione minima di ONTAP supportata dalla piattaforma).

- **Nota 2**: Per queste combinazioni è necessario ONTAP 9.13.1 o versione successiva (o la versione minima di ONTAP supportata dalla piattaforma).

Invio di un messaggio AutoSupport personalizzato prima della manutenzione

Prima di eseguire la manutenzione, devi inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la manutenzione è in corso. Informare il supporto tecnico che la manutenzione è in corso impedisce loro di aprire un caso partendo dal presupposto che si sia verificata un'interruzione.

A proposito di questa attività

Questa attività deve essere eseguita su ciascun sito MetroCluster.

Fasi

1. Per impedire la generazione automatica del caso di supporto, inviare un messaggio AutoSupport per indicare che l'aggiornamento è in corso.

   a. Immettere il seguente comando:

   ```
   system node autosupport invoke -node * -type all -message "MAINT=10h
   Upgrading old-model to new-model"
   ```

   Questo esempio specifica una finestra di manutenzione di 10 ore. A seconda del piano, potrebbe essere necessario dedicare più tempo.

   Se la manutenzione viene completata prima che sia trascorso il tempo, è possibile richiamare un messaggio AutoSupport che indica la fine del periodo di manutenzione:

```
system node autosupport invoke -node * -type all -message MAINT=end
```

   a. Ripetere il comando sul cluster partner.

Verifica dello stato della configurazione MetroCluster

Prima di eseguire la transizione, è necessario verificare lo stato e la connettività della configurazione di MetroCluster

Fasi

1. Verificare il funzionamento della configurazione MetroCluster in ONTAP:

   a. Verificare che il sistema sia multipercorso:

   ```
   node run -node node-name sysconfig -a
   ```

   b. Verificare la presenza di eventuali avvisi sullo stato di salute su entrambi i cluster:

   ```
   system health alert show
   ```

   c. Verificare la configurazione MetroCluster e che la modalità operativa sia normale:

   ```
   metrocluster show
   ```

   d. Eseguire un controllo MetroCluster:

   ```
   metrocluster check run
   ```

e. Visualizzare i risultati del controllo MetroCluster:

```
metrocluster check show
```

f. Eseguire Config Advisor.

"Download NetApp: Config Advisor"

g. Dopo aver eseguito Config Advisor, esaminare l'output dello strumento e seguire le raccomandazioni nell'output per risolvere eventuali problemi rilevati.

2. Verificare che il cluster funzioni correttamente:

```
cluster show
```

```
cluster_A::> cluster show
Node            Health  Eligibility
--------------- ------  -----------
node_A_1        true    true
node_A_2        true    true

cluster_A::>
```

3. Verificare che tutte le porte del cluster siano installate:

```
network port show -ipspace Cluster
```

```
cluster_A::> network port show -ipspace Cluster

Node: node_A_1-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                   Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verificare che tutte le LIF del cluster siano operative:

   `network interface show -vserver Cluster`

   Ogni LIF del cluster dovrebbe visualizzare true per is Home e avere uno stato Admin/Oper di up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verificare che l'autorevert sia attivato su tutte le LIF del cluster:

```
network interface show -vserver Cluster -fields auto-revert
```

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Rimozione della configurazione dalle applicazioni di monitoraggio

Se la configurazione esistente viene monitorata con il software MetroCluster Tiebreaker, il mediatore ONTAP o altre applicazioni di terze parti (ad esempio, ClusterLion) che possono avviare uno switchover, è necessario rimuovere la configurazione MetroCluster dal software di monitoraggio prima di eseguire l'aggiornamento.

Fasi

1. Rimuovere la configurazione MetroCluster esistente da Tiebreaker, Mediator o altro software in grado di avviare lo switchover.

Se si utilizza…	Utilizzare questa procedura…
Spareggio	"Rimozione delle configurazioni MetroCluster".
Mediatore	Immettere il seguente comando dal prompt di ONTAP: `metrocluster configuration-settings mediator remove`
Applicazioni di terze parti	Consultare la documentazione del prodotto.

2. Rimuovere la configurazione MetroCluster esistente da qualsiasi applicazione di terze parti in grado di avviare lo switchover.

   Consultare la documentazione dell'applicazione.

Preparazione dei nuovi moduli controller

È necessario preparare i quattro nuovi nodi MetroCluster e installare la versione corretta di ONTAP.

A proposito di questa attività

Questa attività deve essere eseguita su ciascuno dei nuovi nodi:

- Node_A_3-new
- Node_A_4-new
- Node_B_3-new
- Node_B_4-new

In questa procedura, si cancella la configurazione sui nodi e si cancella l'area della mailbox sui nuovi dischi.

Fasi

1. Inserire in rack i nuovi controller.
2. Collegare i nuovi nodi IP MetroCluster agli switch IP come illustrato nella sezione *installazione e configurazione di MetroCluster.*

   "Cablaggio degli switch IP"

3. Configurare i nodi IP MetroCluster utilizzando le seguenti sezioni della sezione *installazione e configurazione di MetroCluster.*
   a. "Raccolta delle informazioni richieste"
   b. "Ripristino delle impostazioni predefinite di sistema su un modulo controller"
   c. "Verifica dello stato ha-config dei componenti"
   d. "Assegnazione manuale dei dischi per il pool 0 (ONTAP 9.4 e versioni successive)"
4. Dalla modalità Maintenance, eseguire il comando halt per uscire dalla modalità Maintenance, quindi eseguire il comando boot_ontap per avviare il sistema e accedere alla configurazione del cluster.

   Non completare la procedura guidata del cluster o del nodo.

Aggiornare i file RCF

Se si sta installando un nuovo firmware dello switch, è necessario installare il firmware dello switch prima di aggiornare il file RCF.

A proposito di questa attività

Questa procedura interrompe il traffico sullo switch in cui viene aggiornato il file RCF. Il traffico riprenderà una volta applicato il nuovo file RCF.

Fasi

1. Verificare lo stato della configurazione.
   a. Verificare che i componenti di MetroCluster siano integri:

      ```
      metrocluster check run
      ```

```
cluster_A::*> metrocluster check run
```

L'operazione viene eseguita in background.

b. Dopo il `metrocluster check run` operazione completata, eseguire `metrocluster check show` per visualizzare i risultati.

Dopo circa cinque minuti, vengono visualizzati i seguenti risultati:

```
-----------
::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Controllare lo stato dell'operazione di controllo MetroCluster in esecuzione:

```
metrocluster operation history show -job-id 38
```

b. Verificare che non siano presenti avvisi sullo stato di salute:

```
system health alert show
```

2. Preparare gli switch IP per l'applicazione dei nuovi file RCF.

Seguire la procedura per il fornitore dello switch:

- "Ripristino delle impostazioni predefinite dello switch IP Broadcom"
- "Ripristino delle impostazioni predefinite dello switch IP Cisco"

3. Scaricare e installare il file RCF IP, a seconda del fornitore dello switch.

> Aggiornare gli switch nel seguente ordine: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2

- "Download e installazione dei file Broadcom IP RCF"
- "Download e installazione dei file Cisco IP RCF"

Se si dispone di una configurazione di rete L2 condivisa o L3, potrebbe essere necessario regolare le porte ISL sugli switch intermedi/clienti. La modalità switchport potrebbe passare dalla modalità 'access' alla modalità 'trunk'. Procedere all'aggiornamento della seconda coppia di switch (A_2, B_2) solo se la connettività di rete tra gli switch A_1 e B_1 è completamente operativa e la rete funziona correttamente.

Unire i nuovi nodi ai cluster

È necessario aggiungere i quattro nuovi nodi IP MetroCluster alla configurazione MetroCluster esistente.

A proposito di questa attività

È necessario eseguire questa attività su entrambi i cluster.

Fasi

1. Aggiungere i nuovi nodi IP MetroCluster alla configurazione MetroCluster esistente.
   a. Collegare il primo nuovo nodo IP MetroCluster (Node_A_1-new) alla configurazione IP MetroCluster esistente.

```
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]: 172.17.8.93
```

```
172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:


Do you want to create a new cluster or join an existing cluster?
{create, join}:
join


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Collegare il secondo nuovo nodo IP MetroCluster (Node_A_2-new) alla configurazione IP MetroCluster esistente.

2. Ripetere questi passaggi per unire node_B_1-new e node_B_2-new a cluster_B.

Configurazione delle LIF tra cluster, creazione delle interfacce MetroCluster e mirroring degli aggregati root

È necessario creare le LIF di peering del cluster e le interfacce MetroCluster sui nuovi nodi IP MetroCluster.

A proposito di questa attività

La porta home utilizzata negli esempi è specifica per la piattaforma. Utilizzare la porta home appropriata specifica per la piattaforma del nodo IP MetroCluster.

Fasi

1. Sui nuovi nodi IP di MetroCluster, configurare le LIF di intercluster seguendo le seguenti procedure:

   "Configurazione di LIF intercluster su porte dedicate"

   "Configurazione delle LIF tra cluster su porte dati condivise"

2. In ogni sito, verificare che il peering del cluster sia configurato:

   ```
   cluster peer show
   ```

   L'esempio seguente mostra la configurazione del peering del cluster su cluster_A:

   ```
   cluster_A:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_B                 1-80-000011           Available      ok
   ```

   L'esempio seguente mostra la configurazione del peering del cluster su cluster_B:

   ```
   cluster_B:> cluster peer show
   Peer Cluster Name         Cluster Serial Number Availability
   Authentication
   ------------------------- --------------------- --------------
   --------------
   cluster_A                 1-80-000011           Available      ok
   cluster_B::>
   ```

3. Creare il gruppo DR per i nodi IP MetroCluster:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

   Per ulteriori informazioni sulle impostazioni di configurazione e sulle connessioni di MetroCluster, consultare quanto segue:

   "Considerazioni per le configurazioni MetroCluster IP"

   "Creazione del gruppo DR"

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verificare che il gruppo DR sia stato creato.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                     Node                DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                        node_A_1-old         node_B_1-old
                                        node_A_2-old         node_B_2-old
            cluster_B
                                        node_B_1-old         node_A_1-old
                                        node_B_2-old         node_A_2-old
2           cluster_A
                                        node_A_1-new         node_B_1-new
                                        node_A_2-new         node_B_2-new
            cluster_B
                                        node_B_1-new         node_A_1-new
                                        node_B_2-new         node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Configurare le interfacce IP MetroCluster per i nodi IP MetroCluster appena entrati:

   `metrocluster configuration-settings interface create -cluster-name`

   - Alcune piattaforme utilizzano una VLAN per l'interfaccia IP di MetroCluster. Per impostazione predefinita, ciascuna delle due porte utilizza una VLAN diversa: 10 e 20. È inoltre possibile specificare una VLAN diversa (non predefinita) superiore a 100 (tra 101 e 4095) utilizzando `-vlan-id parameter` in `metrocluster configuration-settings interface create` comando.
   - A partire da ONTAP 9.9.1, se si utilizza una configurazione Layer 3, è necessario specificare anche `-gateway` Parametro durante la creazione di interfacce IP MetroCluster. Fare riferimento a. "Considerazioni per le reti wide-area di livello 3".

I seguenti modelli di piattaforma possono essere aggiunti alla configurazione MetroCluster esistente se le VLAN utilizzate sono 10/20 o superiori a 100. Se si utilizzano altre VLAN, queste piattaforme non possono essere aggiunte alla configurazione esistente, in quanto l'interfaccia MetroCluster non può essere configurata. Se si utilizza un'altra piattaforma, la configurazione della VLAN non è rilevante in quanto non è richiesta in ONTAP.

Piattaforme AFF	Piattaforme FAS
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

È possibile configurare le interfacce IP di MetroCluster da entrambi i cluster.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verificare che le interfacce IP MetroCluster siano state create:

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show
```

```
DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
```

```
                 Home Port: e1a
                      172.17.28.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                 Home Port: e1a
                      172.17.28.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                 Home Port: e1a
                      172.17.28.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Collegare le interfacce IP di MetroCluster:

   `metrocluster configuration-settings connection connect`

   > Il completamento di questo comando potrebbe richiedere alcuni minuti.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verificare che le connessioni siano state stabilite correttamente: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
```

```
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
```

```
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_1-new**
```

```
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
```

```
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.11    DR Partner
completed
                Home Port: e1a
                     172.17.26.13    172.17.26.10    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.11    DR Partner
completed
                Home Port: e1b
                     172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_1-new
                Home Port: e1a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.10    DR Partner
completed
                Home Port: e1a
                     172.17.26.12    172.17.26.11    DR Auxiliary
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.10    DR Partner
completed
                Home Port: e1b
                     172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Verificare l’assegnazione automatica e il partizionamento del disco:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0               546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3               546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5               546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6               546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7               546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10              546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Mirroring degli aggregati root:

```
storage aggregate mirror -aggregate aggr0_node_A_1-new
```

> È necessario completare questo passaggio su ciascun nodo IP MetroCluster.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                                Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verificare che gli aggregati root siano mirrorati:

    `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Finalizzare l’aggiunta dei nuovi nodi

È necessario incorporare il nuovo gruppo DR nella configurazione MetroCluster e creare aggregati di dati mirrorati sui nuovi nodi.

Fasi

1. Aggiornare la configurazione MetroCluster:

   a. Accedere alla modalità avanzata dei privilegi:

      ```
      set -privilege advanced
      ```

   b. Aggiornare la configurazione MetroCluster su uno dei nuovi nodi:

```
metrocluster configure
```

L'esempio seguente mostra la configurazione MetroCluster aggiornata su entrambi i gruppi di DR:

```
cluster_A::*> metrocluster configure -refresh true

[Job 726] Job succeeded: Configure is successful.
```

a. Riavviare ciascuno dei nuovi nodi:

```
node reboot -node <node_name> -inhibit-takeover true
```

b. Tornare alla modalità privilegi di amministratore:

```
set -privilege admin
```

2. Creare aggregati di dati mirrorati su ciascuno dei nuovi nodi MetroCluster:

```
storage aggregate create -aggregate aggregate-name -node node-name -diskcount
no-of-disks -mirror true
```

> È necessario creare almeno un aggregato di dati mirrorati per sito. Si consiglia di disporre di due aggregati di dati mirrorati per sito su nodi IP MetroCluster per ospitare i volumi MDV, tuttavia è supportato un singolo aggregato per sito (ma non consigliato). È possibile che un sito di MetroCluster disponga di un singolo aggregato di dati mirrorati e l'altro sito disponga di più aggregato di dati mirrorati.

Nell'esempio seguente viene illustrata la creazione di un aggregato su Node_A_1-New.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
```

```
          data       5.10.17                  SAS         546.9GB
547.1GB
          data       5.10.18                  SAS         546.9GB
558.9GB
          data       5.10.19                  SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                  SAS               -
-
          parity     4.20.14                  SAS               -
-
          data       4.20.18                  SAS         546.9GB
547.1GB
          data       4.20.19                  SAS         546.9GB
547.1GB
          data       4.20.16                  SAS         546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

3. Verificare che i nodi siano aggiunti al gruppo di DR.

```
cluster_A::*> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Spostare i volumi MDV_CRS dai vecchi nodi ai nuovi nodi con privilegi avanzati.

   a. Visualizzare i volumi per identificare i volumi MDV:

   > Se si dispone di un singolo aggregato di dati mirrorati per sito, spostare entrambi i volumi MDV in questo singolo aggregato. Se si dispone di due o più aggregati di dati mirrorati, spostare ciascun volume MDV in un aggregato diverso.

   L'esempio seguente mostra i volumi MDV in `volume show` uscita:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Impostare il livello di privilegio avanzato:

   `set -privilege advanced`

c. Spostare i volumi MDV uno alla volta:

   `volume move start -volume` *`mdv-volume`* `-destination-aggregate` *`aggr-on-new-node`* `-vserver` *`vserver-name`*

   L'esempio seguente mostra il comando e l'output per spostare "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" per aggregare "data_a3" su "Node_A_3".

```
cluster_A::*> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Utilizzare il comando di visualizzazione del volume per verificare che il volume MDV sia stato spostato correttamente:

   `volume show` *`mdv-name`*

   Il seguente output indica che il volume MDV è stato spostato correttamente.

```
cluster_A::*> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                      aggr_a2      online     RW         10GB
9.50GB    0%
```

5. Spostare epsilon da un nodo vecchio a un nuovo nodo:

   a. Identificare il nodo attualmente dotato di epsilon:

      `cluster show -fields epsilon`

```
cluster_B::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Impostare epsilon su false sul vecchio nodo (node_A_1-old):

   `cluster modify -node old-node -epsilon false*`

c. Impostare epsilon su true sul nuovo nodo (node_A_3-new):

   `cluster modify -node new-node -epsilon true`

d. Verificare che epsilon sia stato spostato nel nodo corretto:

   `cluster show -fields epsilon`

```
cluster_A::*> cluster show -fields epsilon
node              epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

Rimozione di un gruppo di disaster recovery

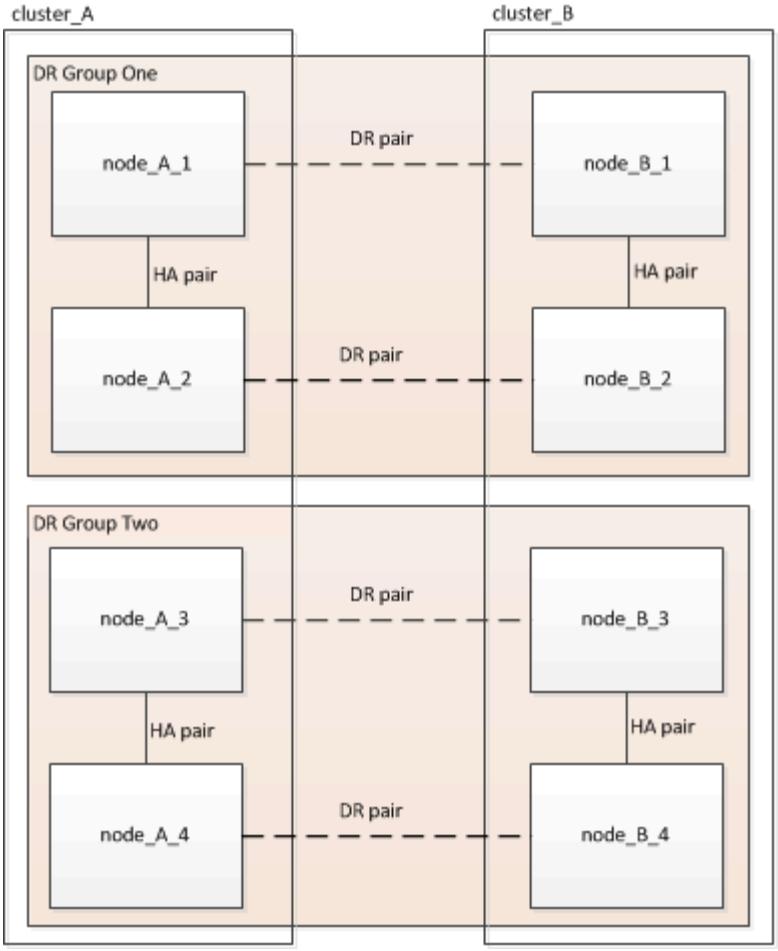
A partire da ONTAP 9.8, è possibile rimuovere un gruppo di DR da una configurazione MetroCluster a otto nodi per creare una configurazione MetroCluster a quattro nodi.

Questa procedura è supportata in ONTAP 9.8 e versioni successive. Per i sistemi che eseguono ONTAP 9.7 o versioni precedenti, consultare l'articolo della Knowledge base

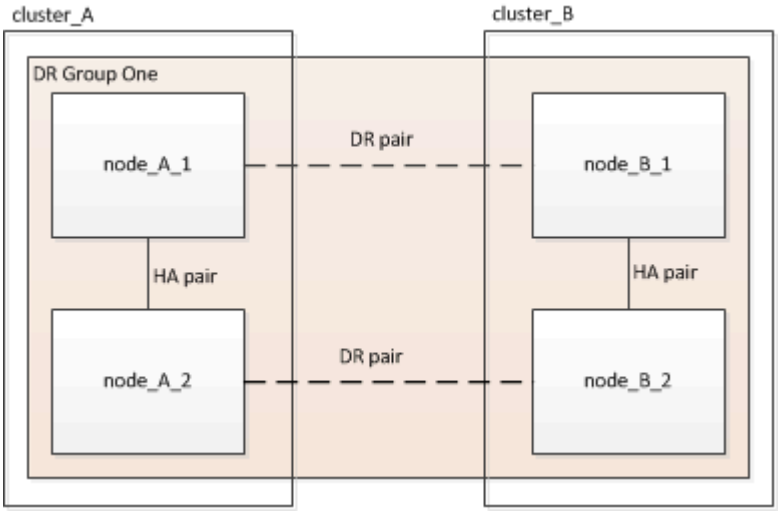
"Come rimuovere un gruppo DR da una configurazione MetroCluster"

"Supporto NetApp"

Una configurazione a otto nodi include otto nodi organizzati in due gruppi DR a quattro nodi.



Rimuovendo un gruppo di DR, nella configurazione rimangono quattro nodi.



Rimozione dei nodi del gruppo di DR da ciascun cluster

Prima di iniziare

- È necessario eseguire questa operazione su entrambi i cluster.
- Il `metrocluster remove-dr-group` Il comando è supportato solo su ONTAP 9.8 e versioni successive.

Fasi

1. Se non lo hai già fatto, preparati per la rimozione del gruppo di DR.

   a. Spostare tutti i volumi di dati in un altro gruppo di DR.

   b. Se il gruppo DR da rimuovere contiene volumi mirror per la condivisione del carico, non è possibile spostarli. Ricreare tutti i volumi mirror di condivisione del carico in un altro gruppo DR, quindi eliminare i volumi mirror di condivisione del carico nel gruppo DR da rimuovere.

   c. Spostare tutti i volumi di metadati MDV_CRS in un altro gruppo DR seguendo la "Spostamento di un volume di metadati nelle configurazioni MetroCluster" procedura.

   d. Eliminare tutti i volumi di metadati MDV_aud che potrebbero esistere nel gruppo di DR da rimuovere.

   e. Eliminare tutti gli aggregati di dati nel gruppo DR da rimuovere, come illustrato nell'esempio seguente:

```
ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
-fields aggregate ,node
ClusterA::> aggr delete -aggregate aggregate_name
ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
-fields aggregate ,node
ClusterB::> aggr delete -aggregate aggregate_name
```

   Gli aggregati root non vengono cancellati.

   f. Spostare i dati LIF offline. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin down`

   g. Eseguire la migrazione di tutte le LIF dei dati nei nodi domestici di un altro gruppo di DR.
   `network interface show -home-node` *`old_node`*

   `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-node` *`new_node`* `-home-port` *`port-id`*

   h. Riportare online i dati LIF. `network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-status-admin up`

   i. Eseguire la migrazione della LIF di gestione del cluster a un nodo principale in un altro gruppo di DR.

   `network interface show -role cluster-mgmt`

   `network interface modify -vserver` *`svm-name`* `-lif` *`cluster_mgmt`* `-home-node` *`new_node`* `-home-port` *`port-id`*

La gestione dei nodi e le LIF tra cluster non vengono migrate.

   a. Trasferire epsilon a un nodo di un altro gruppo DR, se necessario.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identificare e rimuovere il gruppo DR.

   a. Identificare il gruppo DR corretto per la rimozione:

      ```
      metrocluster node show
      ```

   b. Rimuovere i nodi del gruppo di DR:
      ```
      metrocluster remove-dr-group -dr-group-id 1
      ```

      Nell’esempio seguente viene illustrata la rimozione della configurazione del gruppo di DR sul cluster_A.

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B"to remove the remote nodes in the DR
group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not completed
on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Ripetere il passaggio precedente sul cluster partner.
4. In una configurazione MetroCluster IP, rimuovere le connessioni MetroCluster sui nodi del vecchio gruppo di DR.

   Questi comandi possono essere emessi da entrambi i cluster e applicati all'intero gruppo di DR che copre entrambi i cluster.

   a. Scollegare i collegamenti:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Eliminare le interfacce MetroCluster sui nodi del vecchio gruppo di DR:

```
metrocluster configuration-settings interface delete
```

c. Eliminare la configurazione del vecchio gruppo di DR.
```
metrocluster configuration-settings dr-group delete
```

5. Disunire i nodi nel vecchio gruppo di DR.

È necessario eseguire questa operazione su ciascun cluster.

a. Impostare il livello di privilegio avanzato:

```
set -privilege advanced
```

b. Disattivare il failover dello storage:

```
storage failover modify -node node-name -enable false
```

c. Disunire il nodo:
```
cluster unjoin -node node-name
```

Ripetere questo passaggio per l'altro nodo locale del vecchio gruppo DR.

d. Impostare il livello di privilegio admin:
```
set -privilege admin
```

6. Riattivare il cluster ha nel nuovo gruppo di DR:

```
cluster ha modify -configured true
```

È necessario eseguire questa operazione su ciascun cluster.

7. Arrestare, spegnere e rimuovere i vecchi moduli controller e gli shelf di storage.

Dove trovare ulteriori informazioni

Scopri di più sulla configurazione e sul funzionamento di MetroCluster.

MetroCluster e informazioni varie

Informazioni	Soggetto
"Documentazione MetroCluster"	• Tutte le informazioni MetroCluster

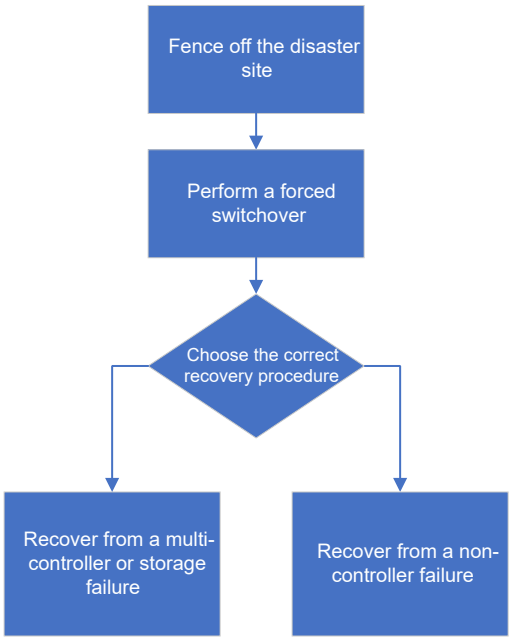
"Installazione e configurazione di Fabric-Attached MetroCluster"	• Architettura Fabric-Attached MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione degli switch FC • Configurazione di MetroCluster in ONTAP
"Estensione dell'installazione e della configurazione di MetroCluster"	• Estendi l'architettura MetroCluster • Cablaggio della configurazione • Configurazione dei bridge FC-SAS • Configurazione di MetroCluster in ONTAP
"Gestione MetroCluster e disaster recovery"	• Informazioni sulla configurazione di MetroCluster • Switchover, healing e switchback • Disaster recovery
"Gestire i componenti di MetroCluster"	• Linee guida per la manutenzione in una configurazione MetroCluster FC • Procedure di sostituzione o aggiornamento dell'hardware e aggiornamento del firmware per bridge FC-SAS e switch FC • Aggiunta a caldo di uno shelf di dischi in una configurazione MetroCluster FC fabric-attached o stretch • Rimozione a caldo di uno shelf di dischi in una configurazione MetroCluster FC con connessione fabric o stretch • Sostituzione dell'hardware in un sito di emergenza in una configurazione FC MetroCluster Fabric-Attached o Stretch • Espansione di una configurazione MetroCluster FC a due nodi collegata a fabric o estesa a una configurazione MetroCluster a quattro nodi. • Espansione di una configurazione FC MetroCluster con collegamento fabric a quattro nodi o estensione in una configurazione FC MetroCluster a otto nodi.
"Upgrade, transizione ed espansione di MetroCluster"	• Aggiornamento o aggiornamento di una configurazione MetroCluster • Passaggio da una configurazione MetroCluster FC a una configurazione MetroCluster IP • Espansione di una configurazione MetroCluster mediante l'aggiunta di nodi aggiuntivi

"Installazione e configurazione del software MetroCluster Tiebreaker"	• Monitoraggio della configurazione MetroCluster con il software MetroCluster Tiebreaker
"Documentazione dei sistemi hardware ONTAP" Le procedure di manutenzione standard dello shelf storage possono essere utilizzate con le configurazioni IP di MetroCluster.	• Aggiunta a caldo di uno shelf di dischi • Rimozione a caldo di uno shelf di dischi
"Transizione basata sulla copia"	• Transizione dei dati dai sistemi storage 7-Mode ai sistemi storage in cluster
"Concetti di ONTAP"	• Come funzionano gli aggregati mirrorati

Ripristino in caso di disastro

Workflow per il disaster recovery

Utilizza il workflow per eseguire il disaster recovery.



Eseguire uno switchover forzato dopo un disastro

In caso di disastro, è necessario eseguire le operazioni sul cluster di emergenza e sul cluster sopravvissuto dopo lo switchover per garantire un servizio dati sicuro e continuo.

Per determinare se si è verificato un disastro, procedere come segue:

- Un amministratore
- Il software MetroCluster Tiebreaker, se configurato
- Il software del mediatore ONTAP, se configurato

Recinzione fuori dal sito di disastro

Dopo il disastro, se i nodi del sito di emergenza devono essere sostituiti, è necessario arrestarli per evitare che il sito riprenda il servizio. In caso contrario, si rischia di danneggiare i dati se i client iniziano ad accedere ai nodi prima del completamento della procedura di sostituzione.

Fase

1. Arrestare i nodi nel sito di disastro e mantenerli spenti o al prompt DEL CARICATORE fino a quando non viene richiesto di avviare ONTAP:

   ```
   system node halt -node disaster-site-node-name
   ```

Se i nodi del sito di emergenza sono stati distrutti o non possono essere arrestati, spegnere i nodi e non avviare i nodi sostitutivi fino a quando non viene indicato nella procedura di ripristino.

Esecuzione di uno switchover forzato

Il processo di switchover, oltre a fornire operazioni senza interruzioni durante i test e la manutenzione, consente di eseguire il ripristino da un guasto del sito con un singolo comando.

Prima di iniziare

- Almeno uno dei nodi del sito sopravvissuti deve essere attivo e in esecuzione prima di eseguire lo switchover.
- Prima di eseguire un'operazione di switchback, è necessario completare tutte le modifiche di configurazione precedenti.

  In questo modo si evita la concorrenza con lo switchover negoziato o con l'operazione di switchback.

> Le configurazioni SnapMirror e SnapVault vengono eliminate automaticamente.

A proposito di questa attività

Il `metrocluster switchover` Command consente di passare dai nodi di tutti i gruppi di DR nella configurazione MetroCluster. Ad esempio, in una configurazione MetroCluster a otto nodi, viene eseguita la commutazione dei nodi in entrambi i gruppi di DR.

Fasi

1. Eseguire lo switchover eseguendo il seguente comando nel sito sopravvissuto:

   ```
   metrocluster switchover -forced-on-disaster true
   ```

   > Il completamento dell'operazione può richiedere alcuni minuti. È possibile verificare l'avanzamento utilizzando `metrocluster operation show` comando.

2. Risposta `y` quando viene richiesto di continuare con lo switchover.
3. Verificare che lo switchover sia stato completato correttamente eseguendo il `metrocluster operation show` comando.

```
mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

Se lo switchover è vetoed, è possibile emettere nuovamente il `metrocluster switchover-forced-on-disaster true` con il `--override-vetoes` opzione. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi soft veto che impediva lo switchover.

Al termine

Le relazioni di SnapMirror devono essere ristabilita dopo lo switchover.

L'output per il comando di visualizzazione plesso dell'aggregato di storage 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 (non riuscito). Durante questo periodo, la root commutata non viene aggiornata. Lo stato effettivo di questo plex può essere determinato solo dopo la fase di riparazione MetroCluster.

Accesso ai volumi in stato NVFAIL dopo uno switchover

Dopo uno switchover, è necessario cancellare lo stato NVFAIL ripristinando `-in-nvfailed-state` del parametro `volume modify` comando per rimuovere la restrizione di accesso dei client ai dati.

Prima di iniziare

Il database o il file system non deve essere in esecuzione o non deve tentare di accedere al volume interessato.

A proposito di questa attività

Impostazione di `-in-nvfailed-state` il parametro richiede privilegi di livello avanzato.

Fase

1. Ripristinare il volume utilizzando `volume modify` con il `-in-nvfailed-state` parametro impostato su false.

Al termine

Per istruzioni sull'esame della validità del file di database, consultare la documentazione relativa al software di database specifico.

Se il database utilizza LUN, rivedere la procedura per rendere le LUN accessibili all'host dopo un errore della NVRAM.

Informazioni correlate

"Monitoraggio e protezione della validità del database mediante NVFAIL"

Scelta della procedura di ripristino corretta

Dopo un errore in una configurazione MetroCluster, selezionare la procedura di ripristino corretta. Utilizzare la tabella e gli esempi seguenti per selezionare la procedura di ripristino appropriata.

Le informazioni contenute in questa tabella presuppongono che l'installazione o la transizione siano completate, il che significa che `metrocluster configure` comando eseguito correttamente.

Scopo dei guasti in un sito di disastro	Procedura
• Nessun guasto hardware	"Ripristino da un guasto non del controller"
• Nessun guasto al modulo controller • Si è verificato un guasto nell'altro hardware	"Ripristino da un guasto non del controller"
• Guasto al modulo controller singolo o guasto dei componenti FRU all'interno del modulo controller • I dischi non si sono guastati	Se un guasto è limitato a un singolo modulo controller, è necessario utilizzare la procedura di sostituzione FRU del modulo controller per il modello di piattaforma. In una configurazione MetroCluster a quattro o otto nodi, tale errore viene isolato alla coppia ha locale. **Nota:** la procedura di sostituzione FRU del modulo controller può essere utilizzata in una configurazione MetroCluster a due nodi se non si verificano guasti al disco o ad altri hardware. "Documentazione dei sistemi hardware ONTAP"
• Guasto al modulo controller singolo o guasto dei componenti FRU all'interno del modulo controller • I dischi si sono guastati	"Ripristino in seguito a un errore di storage o multi-controller"
• Guasto al modulo controller singolo o guasto dei componenti FRU all'interno del modulo controller • I dischi non si sono guastati • Si è verificato un guasto all'hardware aggiuntivo esterno del modulo controller	"Ripristino in seguito a un errore di storage o multi-controller" Saltare tutti i passaggi per l'assegnazione del disco.
• Guasto di più moduli controller (con o senza guasti aggiuntivi) all'interno di un gruppo di DR	"Ripristino in seguito a un errore di storage o multi-controller"

Scenari di guasto del modulo controller durante l'installazione di MetroCluster

La risposta a un errore del modulo controller durante la procedura di configurazione MetroCluster dipende dal fatto che il `metrocluster configure` comando completato correttamente.

- Se il `metrocluster configure` Il comando non è stato ancora eseguito o non è stato eseguito; è necessario riavviare la procedura di configurazione del software MetroCluster dall'inizio con un modulo controller sostitutivo.

  > Eseguire le operazioni descritte in "Ripristino delle impostazioni predefinite di sistema su un modulo controller" su ciascun controller (incluso il controller sostitutivo) per verificare che la configurazione precedente sia stata rimossa.

- Se il `metrocluster configure` il comando è stato completato correttamente e il modulo controller ha avuto esito negativo. utilizzare la tabella precedente per determinare la procedura di ripristino corretta.

Scenari di guasto del modulo controller durante la transizione MetroCluster FC-IP

La procedura di ripristino può essere utilizzata se si verifica un guasto del sito durante la transizione. Tuttavia, può essere utilizzato solo se la configurazione è una configurazione mista stabile, con il gruppo FC DR e il gruppo IP DR completamente configurati. L'output di `metrocluster node show` Il comando dovrebbe mostrare entrambi i gruppi DR con tutti e otto i nodi.

> Se il guasto si è verificato durante la transizione quando i nodi sono in fase di aggiunta o rimozione, è necessario contattare il supporto tecnico.

Scenari di guasto del modulo controller nelle configurazioni MetroCluster a otto nodi

Scenari di guasto:

- Guasti a un singolo modulo controller in un singolo gruppo di DR
- Due guasti del modulo controller in un singolo gruppo di DR
- Guasti a un singolo modulo controller in gruppi di DR separati
- Tre guasti del modulo controller distribuiti tra i gruppi di DR

Guasti a un singolo modulo controller in un singolo gruppo di DR

In questo caso il guasto è limitato a una coppia ha.

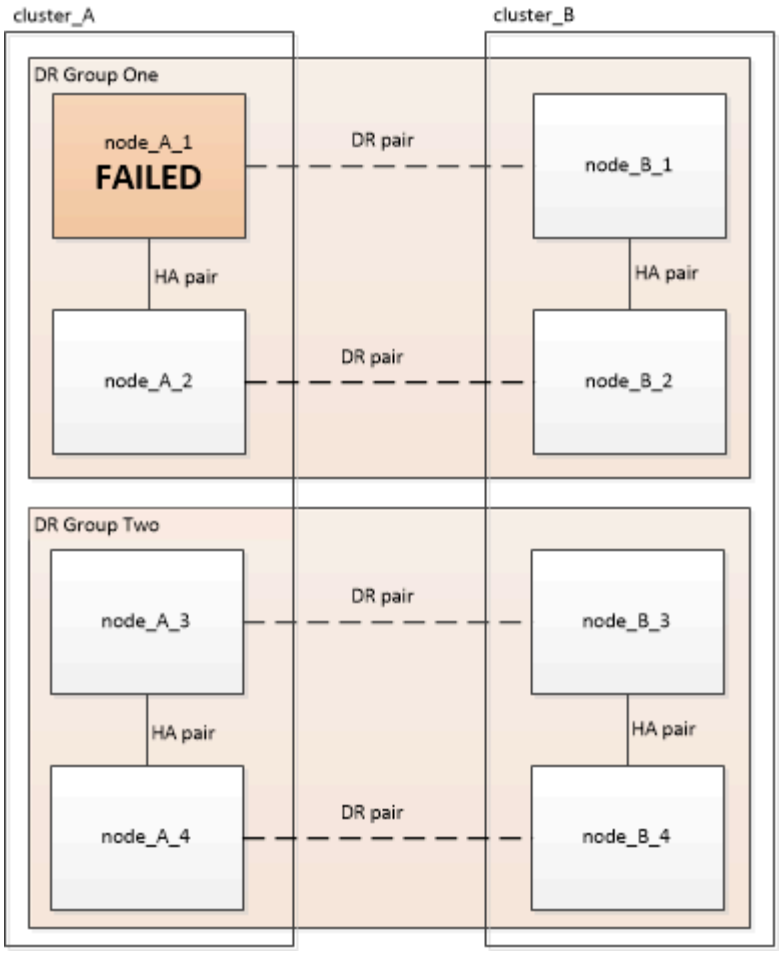
- Se non è necessario sostituire lo storage, è possibile utilizzare la procedura di sostituzione FRU del modulo controller per il modello di piattaforma.

  "Documentazione dei sistemi hardware ONTAP"

- Se lo storage deve essere sostituito, è possibile utilizzare la procedura di ripristino del modulo multi-controller.

  "Ripristino in seguito a un errore di storage o multi-controller"

  Questo scenario si applica anche alle configurazioni MetroCluster a quattro nodi.

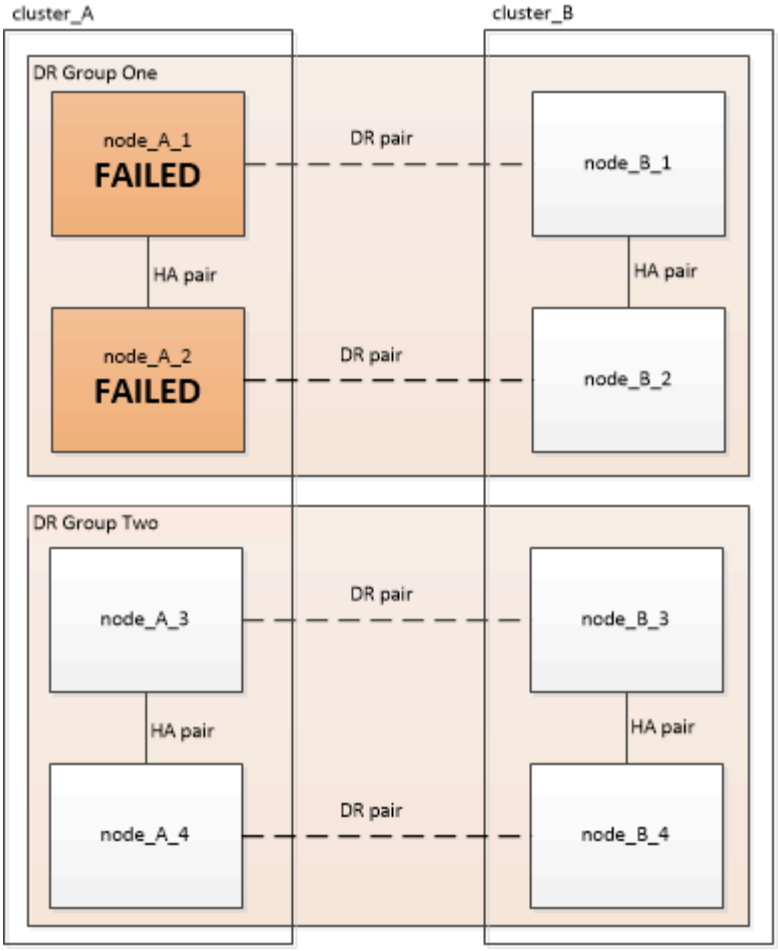


Due guasti del modulo controller in un singolo gruppo di DR

In questo caso il guasto richiede uno switchover. È possibile utilizzare la procedura di failure recovery del modulo multi-controller.

"Ripristino in seguito a un errore di storage o multi-controller"

Questo scenario si applica anche alle configurazioni MetroCluster a quattro nodi.



Guasti a un singolo modulo controller in gruppi di DR separati

In questo caso il guasto è limitato a coppie ha separate.

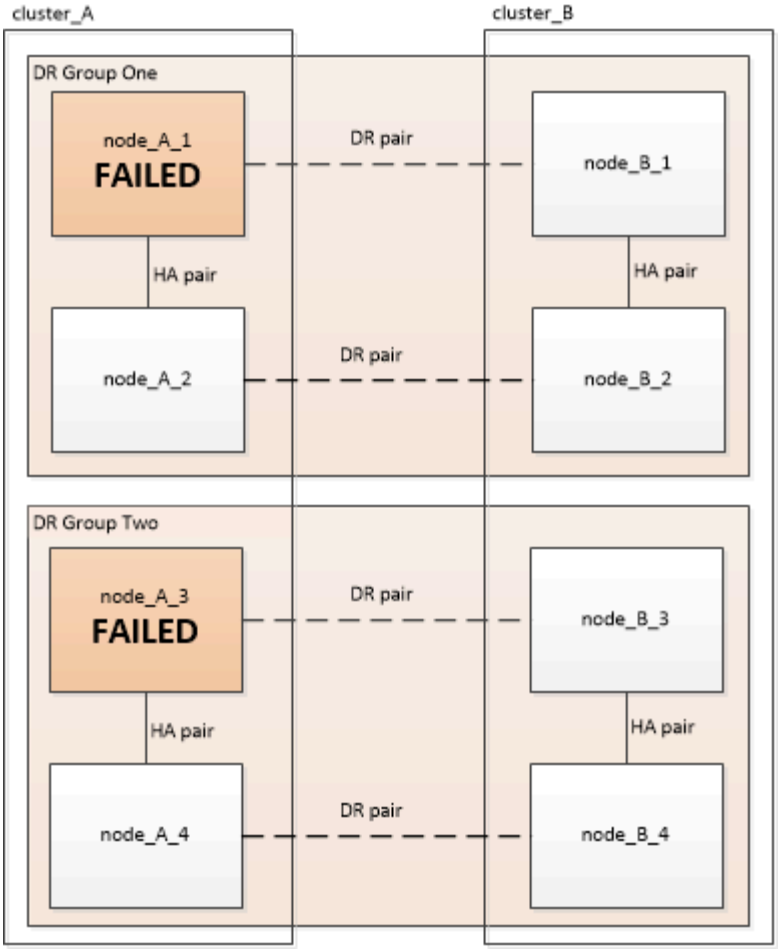
- Se non è necessario sostituire lo storage, è possibile utilizzare la procedura di sostituzione FRU del modulo controller per il modello di piattaforma.

  La procedura di sostituzione della FRU viene eseguita due volte, una per ogni modulo controller guasto.

  "Documentazione dei sistemi hardware ONTAP"

- Se lo storage deve essere sostituito, è possibile utilizzare la procedura di ripristino del modulo multi-controller.

  "Ripristino in seguito a un errore di storage o multi-controller"



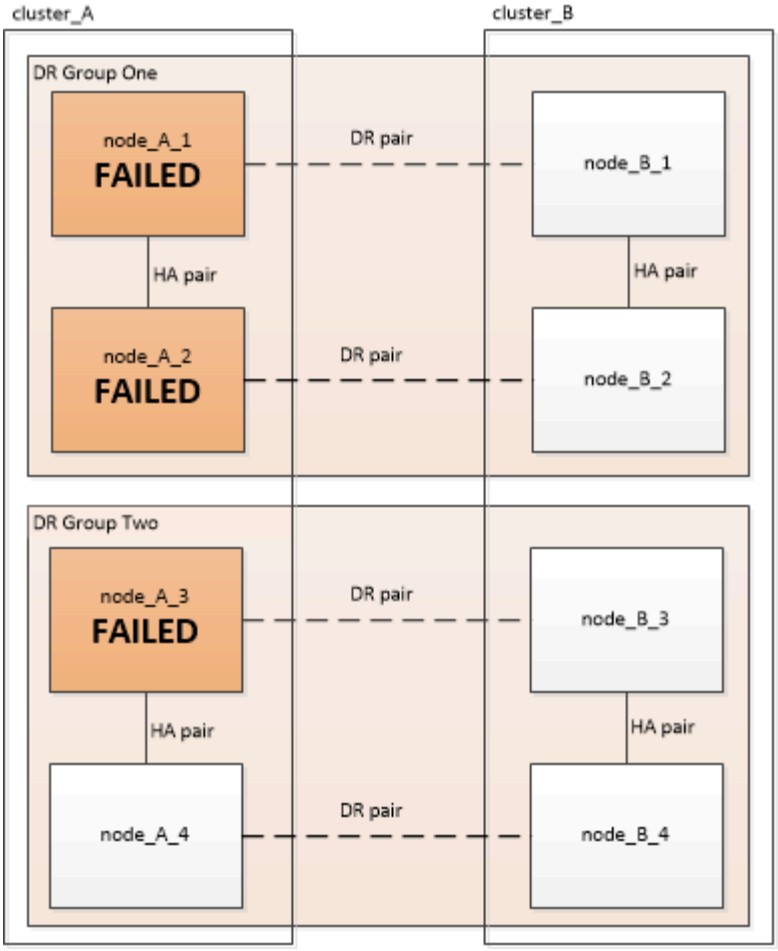
Tre guasti del modulo controller distribuiti tra i gruppi di DR

In questo caso il guasto richiede uno switchover. È possibile utilizzare la procedura di failure recovery del modulo multi-controller per il gruppo DR uno.

"Ripristino in seguito a un errore di storage o multi-controller"

È possibile utilizzare la procedura di sostituzione FRU del modulo controller specifico della piattaforma per DR Gruppo due.

"Documentazione dei sistemi hardware ONTAP"



Scenari di guasto del modulo controller nelle configurazioni MetroCluster a due nodi

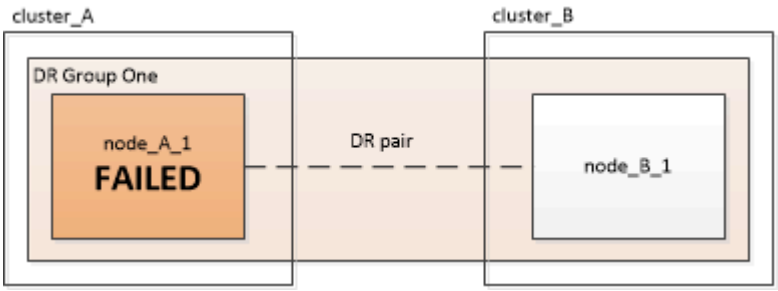
La procedura utilizzata dipende dall'entità del guasto.

- Se non è necessario sostituire lo storage, è possibile utilizzare la procedura di sostituzione FRU del modulo controller per il modello di piattaforma.

  "Documentazione dei sistemi hardware ONTAP"

- Se lo storage deve essere sostituito, è possibile utilizzare la procedura di ripristino del modulo multi-controller.

  "Ripristino in seguito a un errore di storage o multi-controller"



Ripristino in caso di guasto di un multi-controller o di uno storage

Ripristino in seguito a un errore di storage o multi-controller

Se il guasto del controller si estende a tutti i moduli controller su un lato di un gruppo DR in una configurazione MetroCluster (incluso un singolo controller in una configurazione MetroCluster a due nodi) o se lo storage è stato sostituito, è necessario sostituire l'apparecchiatura e riassegnare la proprietà dei dischi per il ripristino dal disastro.

- Prima di decidere di utilizzare questa procedura, esaminare le procedure di ripristino disponibili.

  "Scelta della procedura di ripristino corretta"

- Il sito di disastro deve essere recintato.

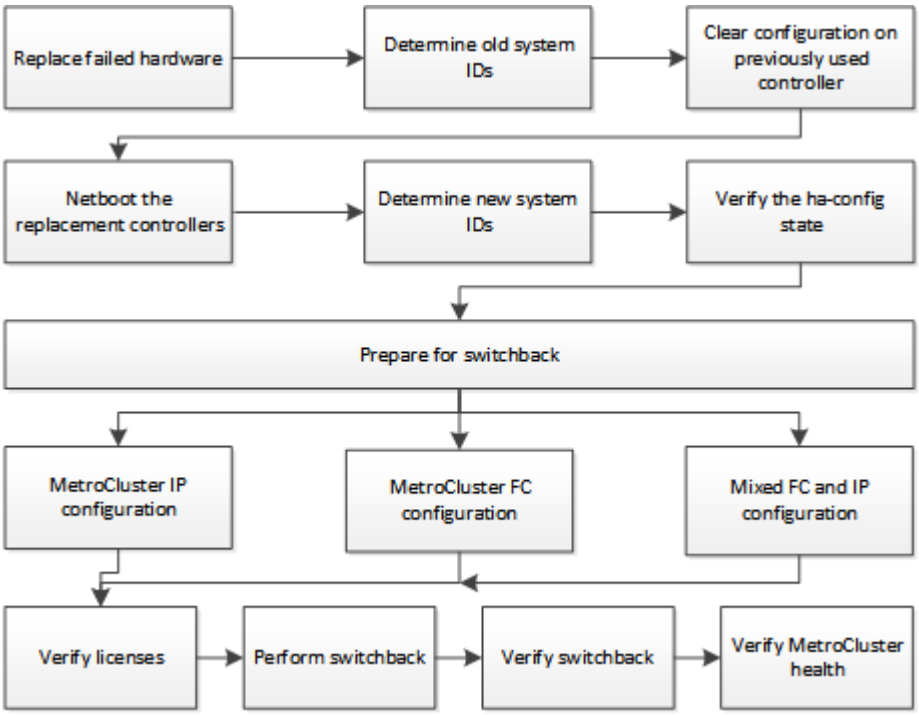
  "Recinzione fuori dal sito di disastro".

- Lo switchover deve essere stato eseguito.

  "Esecuzione di uno switchover forzato".

- Le unità sostitutive e i moduli controller devono essere nuovi e non devono essere stati assegnati in precedenza.
- Gli esempi di questa procedura mostrano configurazioni a due o quattro nodi. Se si dispone di una configurazione a otto nodi (due gruppi di DR), è necessario prendere in considerazione eventuali errori ed eseguire l'attività di ripristino richiesta sui moduli controller aggiuntivi.

Questa procedura utilizza il seguente flusso di lavoro:



Questa procedura può essere utilizzata quando si esegue il ripristino su un sistema che si trovava a metà della

transizione quando si è verificato il guasto. In tal caso, è necessario eseguire le fasi appropriate durante la preparazione per lo switchback, come indicato nella procedura.

Sostituzione dell'hardware e avvio di nuovi controller

Se i componenti hardware devono essere sostituiti, sostituirli utilizzando le rispettive guide di installazione e sostituzione dell'hardware.

Sostituzione dell'hardware nel sito di disastro

Prima di iniziare

I controller di storage devono essere spenti o devono rimanere spenti (mostrando il prompt DEL CARICATORE).

Fasi

1. Sostituire i componenti secondo necessità.

> In questa fase, è possibile sostituire e cablare i componenti esattamente come erano cablati prima del disastro. Non accendere i componenti.

In caso di sostituzione…	Eseguire questa procedura…	Utilizzo di queste guide…
Switch FC in una configurazione MetroCluster FC	a. Installare i nuovi switch. b. Collegare i collegamenti ISL. Non accendere gli switch FC in questo momento.	"Gestire i componenti di MetroCluster"
Switch IP in una configurazione MetroCluster IP	a. Installare i nuovi switch. b. Collegare i collegamenti ISL. Non accendere gli switch IP in questo momento.	"Installazione e configurazione di MetroCluster IP: Differenze tra le configurazioni di ONTAP MetroCluster"
Shelf di dischi	a. Installare i dischi e gli shelf di dischi. ◦ Gli stack di shelf di dischi devono avere la stessa configurazione del sito sopravvissuto. ◦ I dischi possono avere le stesse dimensioni o dimensioni maggiori, ma devono essere dello stesso tipo (SAS o SATA). b. Collegare gli shelf di dischi agli shelf adiacenti all'interno dello stack e al bridge FC-SAS. Non accendere gli shelf di dischi in questo momento.	"Documentazione dei sistemi hardware ONTAP"

Cavi SAS	a. Installare i nuovi cavi. Non accendere gli shelf di dischi in questo momento.	"Documentazione dei sistemi hardware ONTAP"
Bridge FC-SAS in una configurazione MetroCluster FC	a. Installare i bridge FC-SAS. b. Collegare i bridge FC-SAS. Cablarli agli switch FC o ai moduli controller, a seconda del tipo di configurazione MetroCluster in uso. Non accendere i bridge FC-SAS in questo momento.	"Installazione e configurazione di Fabric-Attached MetroCluster" "Estensione dell'installazione e della configurazione di MetroCluster"

Moduli controller	a. Installare i nuovi moduli controller: ◦ I moduli controller devono essere dello stesso modello di quelli da sostituire. Ad esempio, 8080 moduli controller devono essere sostituiti con 8080 moduli controller. ◦ I moduli controller non devono essere stati precedentemente parte di alcun cluster all'interno della configurazione MetroCluster o di qualsiasi configurazione cluster esistente in precedenza. In tal caso, è necessario impostare i valori predefiniti ed eseguire un processo "wpeconfig". ◦ Assicurarsi che tutte le schede di interfaccia di rete (ad esempio Ethernet o FC) si trovino negli stessi slot utilizzati sui vecchi moduli controller. b. Collegare i nuovi moduli controller esattamente come quelli precedenti. Le porte che collegano il modulo controller allo storage (tramite connessioni a switch IP o FC, bridge FC-SAS o direttamente) devono essere le stesse utilizzate prima del disastro. Non accendere i moduli controller in questo momento.	"Documentazione dei sistemi hardware ONTAP"

2. Verificare che tutti i componenti siano cablati correttamente per la configurazione.
   - "Configurazione IP MetroCluster"
   - "Configurazione MetroCluster Fabric-attached"

Determinazione degli ID di sistema e degli ID VLAN dei vecchi moduli controller

Dopo aver sostituito tutto l'hardware nel sito di emergenza, è necessario determinare gli ID di sistema dei moduli controller sostituiti. Quando si riassegnano i dischi ai nuovi moduli controller, sono necessari i vecchi ID di sistema. Se i sistemi sono AFF A220, AFF A250, AFF A400, AFF A800, FAS2750, I modelli FAS500f, FAS8300 o FAS8700 devono anche determinare gli ID VLAN utilizzati dalle interfacce IP di MetroCluster.

Prima di iniziare

Tutte le apparecchiature del sito di emergenza devono essere spente.

A proposito di questa attività

Questa discussione fornisce esempi per configurazioni a due e quattro nodi. Per le configurazioni a otto nodi, è necessario tenere conto degli eventuali errori nei nodi aggiuntivi del secondo gruppo di DR.

Per una configurazione MetroCluster a due nodi, è possibile ignorare i riferimenti al secondo modulo controller in ogni sito.

Gli esempi di questa procedura si basano sui seguenti presupposti:

- Il sito A è il sito di disastro.
- Node_A_1 non riuscito e sostituito completamente.
- Node_A_2 ha avuto un guasto e viene sostituito completamente.

  Il nodo _A_2 è presente solo in una configurazione MetroCluster a quattro nodi.

- Il sito B è il sito sopravvissuto.
- Node_B_1 è integro.
- Node_B_2 è integro.

  Node_B_2 è presente solo in una configurazione MetroCluster a quattro nodi.

I moduli controller hanno i seguenti ID di sistema originali:

Numero di nodi nella configurazione MetroCluster	Nodo	ID di sistema originale
Quattro	Node_A_1	4068741258
Node_A_2	4068741260	Node_B_1
4068741254	Node_B_2	4068741256
Due	Node_A_1	4068741258

Fasi

1. Dal sito sopravvissuto, visualizzare gli ID di sistema dei nodi nella configurazione MetroCluster.

Numero di nodi nella configurazione MetroCluster	Utilizzare questo comando

Quattro o otto	`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`
Due	`metrocluster node show -fields node-systemid,dr-partner-systemid`

In questo esempio per una configurazione MetroCluster a quattro nodi, vengono recuperati i seguenti vecchi ID di sistema:

- Node_A_1: 4068741258
- Node_A_2: 4068741260

  I dischi di proprietà dei vecchi moduli controller sono ancora di proprietà di questi ID di sistema.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  4068741258    4068741260
4068741254          4068741256
1           Cluster_A  Node_A_2  4068741260    4068741258
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

  In questo esempio per una configurazione MetroCluster a due nodi, viene recuperato il seguente vecchio ID di sistema:

- Node_A_1: 4068741258

  I dischi di proprietà del vecchio modulo controller sono ancora di proprietà di questo ID di sistema.

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1  4068741258    4068741254
1           Cluster_B  Node_B_1  -             -
2 entries were displayed.
```

2. Per le configurazioni IP di MetroCluster che utilizzano il servizio di supporto ONTAP, ottenere l'indirizzo IP del servizio di supporto ONTAP:

   ```
   storage iscsi-initiator show -node * -label mediator
   ```

3. Se i sistemi sono modelli AFF A220, AFF A400, FAS2750, FAS8300 o FAS8700, Determinare gli ID VLAN:

   ```
   metrocluster interconnect show
   ```

   Gli ID VLAN sono inclusi nel nome della scheda di rete mostrato nella colonna Adapter dell'output.

   In questo esempio, gli ID VLAN sono 120 e 130:

```
metrocluster interconnect show
                          Mirror   Mirror
                  Partner Admin    Oper
Node Partner Name Type    Status   Status  Adapter Type   Status
---- ------------ ------- -------- ------- ------- ------ ------
Node_A_1 Node_A_2 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
Node_A_2 Node_A_1 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
12 entries were displayed.
```

Isolamento delle unità sostitutive dal sito sopravvissuto (configurazioni MetroCluster IP)

È necessario isolare eventuali dischi sostitutivi eliminando le connessioni MetroCluster iSCSI Initiator dai nodi sopravvissuti.

A proposito di questa attività

Questa procedura è necessaria solo per le configurazioni MetroCluster IP.

Fasi

1. Dal prompt di uno dei nodi sopravvissuti, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

   Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

2. Scollegare gli iniziatori iSCSI su entrambi i nodi sopravvissuti nel gruppo DR:

   ```
   storage iscsi-initiator disconnect -node surviving-node -label *
   ```

   Questo comando deve essere emesso due volte, una volta per ciascuno dei nodi sopravvissuti.

   L'esempio seguente mostra i comandi per scollegare gli iniziatori sul sito B:

   ```
   site_B::*> storage iscsi-initiator disconnect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator disconnect -node node_B_2 -label *
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Cancellazione della configurazione su un modulo controller

Prima di utilizzare un nuovo modulo controller nella configurazione MetroCluster, è necessario cancellare la configurazione esistente.

Fasi

1. Se necessario, arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

2. Al prompt DEL CARICATORE, impostare le variabili ambientali sui valori predefiniti:

   ```
   set-defaults
   ```

3. Salvare l'ambiente:

   ```
   saveenv
   ```

4. Al prompt DEL CARICATORE, avviare il menu di avvio:

```
boot_ontap menu
```

5. Al prompt del menu di avvio, cancellare la configurazione:

   ```
   wipeconfig
   ```

   Rispondere `yes` al prompt di conferma.

   Il nodo si riavvia e viene visualizzato di nuovo il menu di avvio.

6. Nel menu di avvio, selezionare l'opzione **5** per avviare il sistema in modalità di manutenzione.

   Rispondere `yes` al prompt di conferma.

Avvio in rete dei nuovi moduli controller

Se i nuovi moduli controller hanno una versione di ONTAP diversa da quella dei moduli controller sopravvissuti, è necessario eseguire il netboot dei nuovi moduli controller.

Prima di iniziare

- È necessario disporre dell'accesso a un server HTTP.
- Per scaricare i file di sistema necessari per la piattaforma e la versione del software ONTAP in esecuzione, è necessario accedere al sito del supporto NetApp.

  "Supporto NetApp"

Fasi

1. Accedere a. "Sito di supporto NetApp" per scaricare i file utilizzati per eseguire il netboot del sistema.
2. Scaricare il software ONTAP appropriato dalla sezione di download del software del sito di supporto NetApp e memorizzare il file ontap-version_image.tgz in una directory accessibile dal Web.
3. Accedere alla directory accessibile dal Web e verificare che i file necessari siano disponibili.

Se il modello di piattaforma è…	Quindi…
Sistemi della serie FAS/AFF8000	Estrarre il contenuto del file ontap-version_image.tgznella directory di destinazione: Tar -zxvf ontap-version_image.tgz NOTA: Se si sta estraendo il contenuto su Windows, utilizzare 7-zip o WinRAR per estrarre l'immagine netboot. L'elenco delle directory deve contenere una cartella netboot con un file kernel:netboot/kernel
Tutti gli altri sistemi	L'elenco delle directory deve contenere una cartella netboot con un file del kernel: ontap-version_image.tgz non è necessario estrarre il file ontap-version_image.tgz.

4. Al prompt DEL CARICATORE, configurare la connessione netboot per una LIF di gestione:
   - Se l'indirizzo IP è DHCP, configurare la connessione automatica:

     ```
     ifconfig e0M -auto
     ```

- Se l'indirizzo IP è statico, configurare la connessione manuale:

  ```
  ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway
  ```

5. Eseguire il netboot.
   - Se la piattaforma è un sistema della serie 80xx, utilizzare questo comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel
     ```

   - Se la piattaforma è un altro sistema, utilizzare il seguente comando:

     ```
     netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
     version_image.tgz
     ```

6. Dal menu di avvio, selezionare l'opzione **(7) installare prima il nuovo software** per scaricare e installare la nuova immagine software sul dispositivo di avvio.

   ```
    Disregard the following message: "This procedure is not supported for
   Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
   upgrades of software, not to upgrades of controllers.
   . Se viene richiesto di continuare la procedura, immettere `y`E quando
   viene richiesto il pacchetto, inserire l'URL del file immagine:
   `\http://web_server_ip/path_to_web-accessible_directory/ontap-
   version_image.tgz`
   ```

   ```
   Enter username/password if applicable, or press Enter to continue.
   ```

7. Assicurarsi di entrare `n` per ignorare il ripristino del backup quando viene visualizzato un prompt simile a quanto segue:

   ```
   Do you want to restore the backup configuration now? {y|n}
   ```

8. Riavviare immettendo `y` quando viene visualizzato un prompt simile a quanto segue:

   ```
   The node must be rebooted to start using the newly installed software.
   Do you want to reboot now? {y|n}
   ```

9. Dal menu di avvio, selezionare **opzione 5** per accedere alla modalità di manutenzione.
10. Se si dispone di una configurazione MetroCluster a quattro nodi, ripetere questa procedura sull'altro nuovo modulo controller.

Determinazione degli ID di sistema dei moduli controller sostitutivi

Dopo aver sostituito tutto l'hardware nel sito di emergenza, è necessario determinare l'ID di sistema del modulo o dei moduli controller di storage appena installati.

A proposito di questa attività

Questa procedura deve essere eseguita con i moduli controller sostitutivi in modalità manutenzione.

Questa sezione fornisce esempi di configurazioni a due e quattro nodi. Per le configurazioni a due nodi, è possibile ignorare i riferimenti al secondo nodo in ogni sito. Per le configurazioni a otto nodi, è necessario tenere conto dei nodi aggiuntivi nel secondo gruppo di DR. Gli esempi fanno le seguenti ipotesi:

- Il sito A è il sito di disastro.
- Il nodo_A_1 è stato sostituito.
- Il nodo_A_2 è stato sostituito.

  Presente solo nelle configurazioni MetroCluster a quattro nodi.

- Il sito B è il sito sopravvissuto.
- Node_B_1 è integro.
- Node_B_2 è integro.

  Presente solo nelle configurazioni MetroCluster a quattro nodi.

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Numero di nodi nella configurazione MetroCluster	Nodo	ID di sistema originale	Nuovo ID di sistema	Verrà associato a questo nodo come partner DR
Quattro	Node_A_1	4068741258	1574774970	Node_B_1
Node_A_2	4068741260	1574774991	Node_B_2	Node_B_1
4068741254	invariato	Node_A_1	Node_B_2	4068741256
invariato	Node_A_2	Due	Node_A_1	4068741258
1574774970	Node_B_1	Node_B_1	4068741254	invariato

In una configurazione MetroCluster a quattro nodi, il sistema determina le partnership di DR associando il nodo con l'ID di sistema più basso nel sito_A e il nodo con l'ID di sistema più basso nel sito_B. Poiché gli ID di sistema cambiano, le coppie di DR potrebbero essere diverse dopo il completamento della sostituzione del controller rispetto a prima del disastro.

Nell'esempio precedente:

- Node_A_1 (1574774970) verrà abbinato a Node_B_1 (4068741254)
- Node_A_2 (1574774991) verrà abbinato a Node_B_2 (4068741256)

Fasi

1. Con il nodo in modalità Maintenance (manutenzione), visualizzare l'ID di sistema locale del nodo da ciascun nodo: `disk show`

Nell'esempio seguente, il nuovo ID di sistema locale è 1574774970:

```
*> disk show
 Local System ID: 1574774970
 ...
```

2. Sul secondo nodo, ripetere il passaggio precedente.

   Questo passaggio non è richiesto in una configurazione MetroCluster a due nodi.

   Nell'esempio seguente, il nuovo ID di sistema locale è 1574774991:

```
*> disk show
 Local System ID: 1574774991
 ...
```

Verifica dello stato ha-config dei componenti

In una configurazione MetroCluster, lo stato ha-config del modulo controller e dei componenti del telaio deve essere impostato su "mcc" o "mcc-2n" in modo che si avviino correttamente.

Prima di iniziare

Il sistema deve essere in modalità di manutenzione.

A proposito di questa attività

Questa attività deve essere eseguita su ogni nuovo modulo controller.

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 modify chassis mcc-2n`
Configurazione IP MetroCluster	`ha-config modify chassis mccip`

4. Ripetere questi passaggi sull'altro nodo sostitutivo.

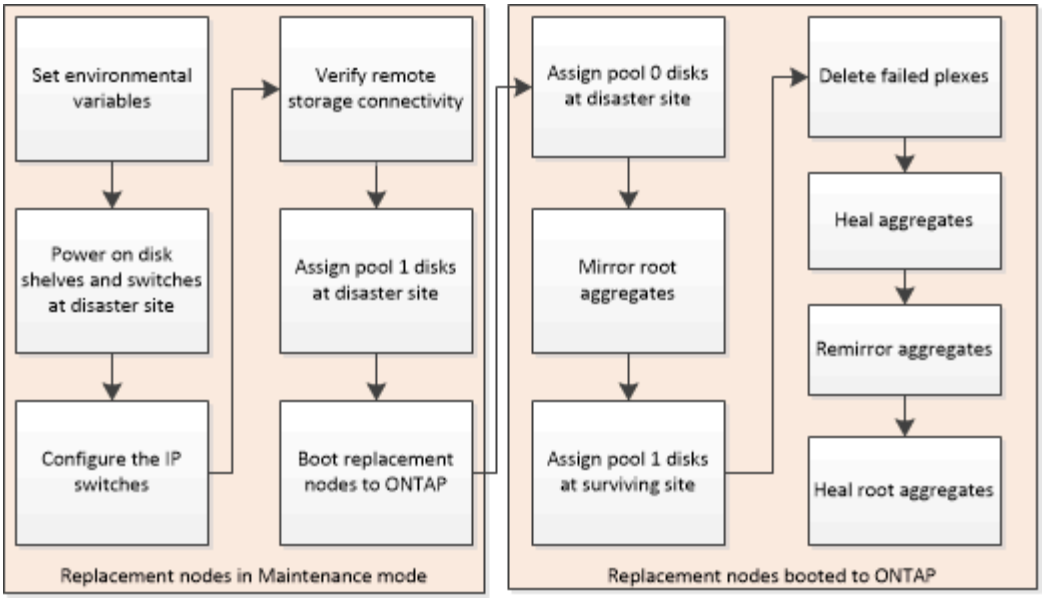
Prepararsi per lo switchback in una configurazione IP MetroCluster

Prepararsi per lo switchback in una configurazione IP MetroCluster

È necessario eseguire alcune attività per preparare la configurazione IP di MetroCluster per l'operazione di switchback.

A proposito di questa attività

nbsp;



Impostazione delle variabili ambientali richieste nelle configurazioni MetroCluster IP

Nelle configurazioni MetroCluster IP, è necessario recuperare l'indirizzo IP delle interfacce MetroCluster sulle porte Ethernet e utilizzarli per configurare le interfacce sui moduli controller sostitutivi.

A proposito di questa attività

Questa attività è necessaria solo nelle configurazioni IP di MetroCluster.

I comandi di questa attività vengono eseguiti dal prompt del cluster del sito sopravvissuto e dal prompt DEL CARICATORE dei nodi nel sito di emergenza.

I nodi in questi esempi hanno i seguenti indirizzi IP per le connessioni IP MetroCluster:

> Questi esempi si riferiscono a un sistema AFF A700 o FAS9000. Le interfacce variano in base al modello di piattaforma.

Nodo	Porta	Indirizzo IP
Node_A_1	e5a	172.17.26.10
e5b	172.17.27.10	Node_A_2
e5a	172.17.26.11	e5b
172.17.27.11	Node_B_1	e5a
172.17.26.13	e5b	172.17.27.13
Node_B_2	e5a	172.17.26.12

Nella tabella seguente sono riepilogate le relazioni tra i nodi e gli indirizzi IP MetroCluster di ciascun nodo.

Nodo	Partner HA	Partner DR	Partner ausiliario DR
Node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	Node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	Node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	Node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12
Node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	Node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	Node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	Node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13
Node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	Node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	Node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	Node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11
Node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	Node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	Node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	Node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10

La seguente tabella elenca i modelli di piattaforma che utilizzano gli ID VLAN sulle interfacce IP MetroCluster. Questi modelli potrebbero richiedere ulteriori passaggi se non si utilizzano gli ID VLAN predefiniti.

Modelli di piattaforme che utilizzano ID VLAN con le interfacce IP MetroCluster	
• AFF A220 • AFF A250 • AFF A400	• FAS500f • FAS2750 • FAS8300 • FAS8700

Fasi

1. Dal sito sopravvissuto, raccogliere gli indirizzi IP delle interfacce MetroCluster sul sito di emergenza:

   ```
   metrocluster configuration-settings connection show
   ```

   Gli indirizzi richiesti sono gli indirizzi partner DR indicati nella colonna **Indirizzo di rete di destinazione**.

   Il seguente output mostra gli indirizzi IP per una configurazione con i sistemi AFF A700 e FAS9000 con le interfacce IP MetroCluster sulle porte e5a e e5b. Le interfacce variano a seconda del tipo di piattaforma.

   ```
   cluster_B::*> metrocluster configuration-settings connection show
   DR                    Source          Destination
   DR                    Source          Destination
   Group Cluster Node    Network Address Network Address Partner Type
   Config State
   ```

```
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.10    DR Partner
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.11    DR Auxiliary
completed
              node_B_2
                 Home Port: e5a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.11    DR Partner
completed
                 Home Port: e5a
                      172.17.26.12    172.17.26.10    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.11    DR Partner
completed
                 Home Port: e5b
                      172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

2. Se è necessario determinare l’ID VLAN o l’indirizzo del gateway per l’interfaccia, determinare gli ID VLAN dal sito sopravvissuto:

```
metrocluster configuration-settings interface show
```

- È necessario l'ID VLAN se i modelli di piattaforma utilizzano gli ID VLAN (vedere l'elenco sopra) e se non si utilizzano gli ID VLAN predefiniti.
- Se si utilizza, è necessario l'indirizzo del gateway "Reti wide-area Layer 3".

  Gli ID VLAN sono inclusi nella colonna **Indirizzo di rete** dell'output. La colonna **Gateway** mostra l'indirizzo IP del gateway.

  In questo esempio le interfacce sono e0a con VLAN ID 120 e e0b con VLAN ID 130:

```
Cluster-A::*> metrocluster configuration-settings interface show
DR
Config
Group Cluster Node     Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1
      cluster_A
              node_A_1
                  Home Port: e0a-120
                          172.17.26.10  255.255.255.0  -
completed
                  Home Port: e0b-130
                          172.17.27.10  255.255.255.0  -
completed
```

3. Se i nodi del sito di emergenza utilizzano gli ID VLAN (vedere l'elenco sopra), al prompt DEL CARICATORE per ciascuno dei nodi del sito di emergenza, impostare i seguenti bootargs:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-address,DR-
aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-address,DR-
aux-partnerIP-address,vlan-id
```

- Se le interfacce utilizzano le VLAN predefinite o il modello di piattaforma non richiede una VLAN (vedere l'elenco precedente), non è necessario il *vlan-id*.
- Se la configurazione non utilizza "Layer3 Wide-Area Network", Il valore per *gateway-IP-address* è **0** (zero).

- Se le interfacce utilizzano le VLAN predefinite o il modello di piattaforma non richiede una VLAN (vedere l'elenco precedente), non è necessario il *vlan-id*.

- Se la configurazione non utilizza "connessioni back-end di livello 3", Il valore per *gateway-IP-address* è **0** (zero).

  I seguenti comandi impostano i valori per Node_A_1 utilizzando la VLAN 120 per la prima rete e la VLAN 130 per la seconda rete:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

L'esempio seguente mostra i comandi per Node_A_1 senza ID VLAN:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

4. Se i nodi del sito di emergenza non sono sistemi che utilizzano ID VLAN, al prompt DEL CARICATORE per ciascuno dei nodi di emergenza, impostare i seguenti bootargs con local_IP/mask,gateway:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address


setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address
```

- Se le interfacce utilizzano le VLAN predefinite o il modello di piattaforma non richiede una VLAN (vedere l'elenco precedente), non è necessario il *vlan-id*.
- Se la configurazione non utilizza "Reti wide-area Layer 3", Il valore per *gateway-IP-address* è **0** (zero).

I seguenti comandi impostano i valori per Node_A_1. In questo esempio, i valori *gateway-IP-address* e *vlan-id* non vengono utilizzati.

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

5. Dal sito sopravvissuto, raccogliere gli UUID per il sito di emergenza:

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid

  (metrocluster node show)
dr-group-id cluster     node     node-uuid
node-cluster-uuid
----------- ----------- -------- ------------------------------------
------------------------------
1           cluster_A   node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_A   node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_B   node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098

c9e55d
1           cluster_B   node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098

c9e55d
4 entries were displayed.
cluster_A::*>
```

Nodo	UUID
Cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
Node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
Node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
Cluster_A.	ee7db9d5-9a82-11e7-b68b-00a098908039
Node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
Node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

6. Al prompt DEL CARICATORE dei nodi sostitutivi, impostare gli UUID:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID`
```

a. Impostare gli UUID su Node_A_1.

   L'esempio seguente mostra i comandi per impostare gli UUID su Node_A_1:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f

setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
00a098908039
```

b. Impostare gli UUID su Node_A_2:

   L'esempio seguente mostra i comandi per impostare gli UUID su Node_A_2:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f

setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-00a098c9e55d

setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-00a098908c35
```

7. Se i sistemi originali sono stati configurati per ADP, al prompt DEL CARICATORE di ciascun nodo

sostitutivo, abilitare ADP:

```
setenv bootarg.mcc.adp_enabled true
```

8. Se si esegue ONTAP 9.5, 9.6 o 9.7, al prompt DEL CARICATORE di ciascun nodo sostitutivo, attivare la seguente variabile:

```
setenv bootarg.mcc.lun_part true
```

   a. Impostare le variabili su Node_A_1.

      Nell'esempio seguente vengono illustrati i comandi per l'impostazione dei valori su Node_A_1 quando si esegue ONTAP 9.6:

      ```
      setenv bootarg.mcc.lun_part true
      ```

   b. Impostare le variabili su Node_A_2.

      L'esempio seguente mostra i comandi per l'impostazione dei valori su Node_A_2 quando si esegue ONTAP 9.6:

```
setenv bootarg.mcc.lun_part true
```

9. Se i sistemi originali sono stati configurati per ADP, al prompt DEL CARICATORE di ciascun nodo sostitutivo, impostare l'ID di sistema originale (**non** l'ID di sistema del modulo controller sostitutivo) e l'ID di sistema del partner DR del nodo:

```
setenv bootarg.mcc.local_config_id original-sysID

setenv bootarg.mcc.dr_partner dr_partner-sysID
```

"Determinazione degli ID di sistema e degli ID VLAN dei vecchi moduli controller"

   a. Impostare le variabili su Node_A_1.

      L'esempio seguente mostra i comandi per impostare gli ID di sistema su Node_A_1:

      - Il vecchio ID di sistema di Node_A_1 è 4068741258.
      - L'ID di sistema di Node_B_1 è 4068741254.

      ```
      setenv bootarg.mcc.local_config_id 4068741258
      setenv bootarg.mcc.dr_partner 4068741254
      ```

   b. Impostare le variabili su Node_A_2.

      L'esempio seguente mostra i comandi per impostare gli ID di sistema su Node_A_2:

      - Il vecchio ID di sistema di Node_A_1 è 4068741260.

- L'ID di sistema di Node_B_1 è 4068741256.

```
setenv bootarg.mcc.local_config_id 4068741260
setenv bootarg.mcc.dr_partner 4068741256
```

Accensione dell'apparecchiatura nel sito di emergenza (configurazioni MetroCluster IP)

È necessario accendere gli shelf di dischi e i componenti degli switch IP MetroCluster nel sito di emergenza. I moduli controller nel sito di emergenza rimangono al prompt DEL CARICATORE.

A proposito di questa attività

Gli esempi di questa procedura presuppongono quanto segue:

- Il sito A è il sito di disastro.
- Il sito B è il sito sopravvissuto.

Fasi

1. Accendere gli shelf di dischi nel sito di disastro e assicurarsi che tutti i dischi siano in esecuzione.
2. Accendere gli switch IP MetroCluster se non sono già accesi.

Configurazione degli switch IP (configurazioni IP MetroCluster)

È necessario configurare gli switch IP sostituiti.

A proposito di questa attività

Questa attività si applica solo alle configurazioni IP di MetroCluster.

Questa operazione deve essere eseguita su entrambi gli switch. Dopo aver configurato il primo switch, verificare che l'accesso allo storage nel sito esistente non sia influenzato.

> Non è necessario procedere con il secondo switch se l'accesso allo storage sul sito sopravvissuto è compromesso.

Fasi

1. Fare riferimento a. "Installazione e configurazione di MetroCluster IP: : Differenze tra le configurazioni di ONTAP MetroCluster" per le procedure di cablaggio e configurazione di uno switch sostitutivo.

   È possibile utilizzare le procedure descritte nelle seguenti sezioni:

   - Cablaggio degli switch IP
   - Configurazione degli switch IP
2. Se gli ISL sono stati disattivati nel sito sopravvissuto, attivare gli ISL e verificare che siano online.

   a. Abilitare le interfacce ISL sul primo switch:

   ```
   no shutdown
   ```

I seguenti esempi mostrano i comandi per uno switch IP Broadcom o Cisco.

Vendor di switch	Comandi

Broadcom	`(IP_Switch_A_1)> enable`
	`(IP_switch_A_1)# configure`
	`(IP_switch_A_1)(Config)# interface 0/13-0/16`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# no shutdown`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# exit`
	`(IP_switch_A_1)(Config)# exit`

Cisco	`IP_switch_A_1# conf t`
	`IP_switch_A_1(config)# int eth1/15-eth1/20`
	`IP_switch_A_1(config)# no shutdown`
	`IP_switch_A_1(config)# copy running startup`
	`IP_switch_A_1(config)# show interface brief`

b. Abilitare le interfacce ISL sullo switch partner:

```
no shutdown
```

I seguenti esempi mostrano i comandi per uno switch IP Broadcom o Cisco.

Vendor di switch	Comandi

Broadcom	`(IP_Switch_A_2)> enable`
	`(IP_switch_A_2)# configure`
	`(IP_switch_A_2)(Config)# interface 0/13-0/16`
	`(IP_switch_A_2)(Interface 0/13-0/16 )# no shutdown`
	`(IP_switch_A_2)(Interface 0/13-0/16 )# exit`
	`(IP_switch_A_2)(Config)# exit`

Cisco	`IP_switch_A_2# conf t`
	`IP_switch_A_2(config)# int eth1/15-eth1/20`
	`IP_switch_A_2(config)# no shutdown`
	`IP_switch_A_2(config)# copy running startup`
	`IP_switch_A_2(config)# show interface brief`

c. Verificare che le interfacce siano attivate:

```
show interface brief
```

L'esempio seguente mostra l'output di uno switch Cisco.

```
IP_switch_A_2(config)# show interface brief

--------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------
mt0 -- up 10.10.99.10 100 1500
--------------------------------------------------------
Ethernet    VLAN Type Mode    Status Reason Speed   Port
Interface                                           Ch
#
--------------------------------------------------------
.
.
.
Eth1/15    10   eth   access  up     none   40G(D)  --
Eth1/16    10   eth   access  up     none   40G(D)  --
Eth1/17    10   eth   access  down   none   auto(D) --
Eth1/18    10   eth   access  down   none   auto(D) --
Eth1/19    10   eth   access  down   none   auto(D) --
Eth1/20    10   eth   access  down   none   auto(D) --
.
.
.
IP_switch_A_2#
```

Verificare la connettività dello storage al sito remoto (configurazioni MetroCluster IP)

È necessario confermare che i nodi sostituiti dispongono di connettività agli shelf di dischi nel sito sopravvissuto.

A proposito di questa attività

Questa attività viene eseguita sui nodi sostitutivi del sito di emergenza.

Questa attività viene eseguita in modalità manutenzione.

Fasi

1. Visualizzare i dischi di proprietà dell'ID di sistema originale.

   ```
   disk show -s old-system-ID
   ```

   I dischi remoti possono essere riconosciuti dal dispositivo 0m. 0m indica che il disco è collegato tramite la connessione iSCSI MetroCluster. Questi dischi devono essere riassegnati in un secondo momento della procedura di ripristino.

   ```
   *> disk show -s 4068741256
   Local System ID: 1574774970

     DISK     OWNER                 POOL  SERIAL NUMBER   HOME
   DR HOME
   ---------- --------------------- ----- -------------
   --------------------- ----------------------
   0m.i0.0L11 node_A_2 (4068741256) Pool1 S396NA0HA02128  node_A_2
   (4068741256) node_A_2  (4068741256)
   0m.i0.1L38 node_A_2 (4068741256) Pool1 S396NA0J148778  node_A_2
   (4068741256) node_A_2  (4068741256)
   0m.i0.0L52 node_A_2 (4068741256) Pool1 S396NA0J148777  node_A_2
   (4068741256) node_A_2  (4068741256)
   ...
   ...
   NOTE: Currently 49 disks are unowned. Use 'disk show -n' for additional
   information.
   *>
   ```

2. Ripetere questo passaggio sugli altri nodi sostitutivi

Riassegnazione della proprietà dei dischi per il pool 1 nel sito di emergenza (configurazioni MetroCluster IP)

Se uno o entrambi i moduli controller o le schede NVRAM sono stati sostituiti nel sito di emergenza, l'ID del sistema è stato modificato ed è necessario riassegnare i dischi appartenenti agli aggregati root ai moduli controller sostitutivi.

A proposito di questa attività

Poiché i nodi sono in modalità switchover, solo i dischi contenenti gli aggregati root del pool1 del sito di disastro verranno riassegnati in questa attività. Si tratta degli unici dischi ancora di proprietà del vecchio ID di sistema a questo punto.

Questa attività viene eseguita sui nodi sostitutivi del sito di emergenza.

Questa attività viene eseguita in modalità manutenzione.

Gli esempi fanno le seguenti ipotesi:

- Il sito A è il sito di disastro.
- Il nodo_A_1 è stato sostituito.
- Il nodo_A_2 è stato sostituito.
- Il sito B è il sito sopravvissuto.
- Node_B_1 è integro.
- Node_B_2 è integro.

Gli ID di sistema vecchi e nuovi sono stati identificati in "Determinazione dei nuovi ID di sistema dei moduli controller sostitutivi".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Nodo	ID di sistema originale	Nuovo ID di sistema
Node_A_1	4068741258	1574774970
Node_A_2	4068741260	1574774991
Node_B_1	4068741254	invariato
Node_B_2	4068741256	invariato

Fasi

1. Con il nodo sostitutivo in modalità manutenzione, riassegnare i dischi aggregati root, utilizzando il comando corretto, a seconda che il sistema sia configurato con ADP e la versione di ONTAP.

   È possibile procedere con la riassegnazione quando richiesto.

Se il sistema utilizza ADP…	Utilizzare questo comando per la riassegnazione del disco…
Sì (ONTAP 9.8)	`disk reassign -s old-system-ID -d new-system-ID -r dr-partner-system-ID`
Sì (ONTAP 9.7.x e versioni precedenti)	`disk reassign -s old-system-ID -d new-system-ID -p old-partner-system-ID`

No	`disk reassign -s old-system-ID -d new-system-ID`

L'esempio seguente mostra la riassegnazione dei dischi su un sistema non ADP:

```
*> disk reassign -s 4068741256 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537037643.
Do you want to continue (y/n)? y
disk reassign parameters: new_home_owner_id 537070473 ,
new_home_owner_name
Disk 0m.i0.3L14 will be reassigned.
Disk 0m.i0.1L6 will be reassigned.
Disk 0m.i0.1L8 will be reassigned.
Number of disks to be reassigned: 3
```

2. Distruggere il contenuto dei dischi della mailbox:

   `mailbox destroy local`

   Quando richiesto, è possibile procedere con l'operazione Destroy.

   L'esempio seguente mostra l'output per il comando local di Destroy della mailbox:

```
*> mailbox destroy local
Destroying mailboxes forces a node to create new empty mailboxes,
which clears any takeover state, removes all knowledge
of out-of-date plexes of mirrored volumes, and will prevent
management services from going online in 2-node cluster
HA configurations.
Are you sure you want to destroy the local mailboxes? y
...............Mailboxes destroyed.
*>
```

3. Se i dischi sono stati sostituiti, ci saranno dei plessi locali guasti che devono essere cancellati.

   a. Visualizzare lo stato dell'aggregato:

   ```
   aggr status
   ```

   Nell'esempio seguente, il nodo plex_A_1_aggr0/plex0 non è riuscito.

   ```
   *> aggr status
   Aug 18 15:00:07 [node_B_1:raid.vol.mirror.degraded:ALERT]: Aggregate
   node_A_1_aggr0 is
      mirrored and one plex has failed. It is no longer protected by
   mirroring.
   Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
   node_A_1_aggr0 has plex0
      clean(-1), online(0)
   Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
   node_A_1_aggr0 has plex2
      clean(0), online(1)
   Aug 18 15:00:07 [node_B_1:raid.mirror.vote.noRecord1Plex:error]:
   WARNING: Only one plex
      in aggregate node_A_1_aggr0 is available. Aggregate might contain
   stale data.
   Aug 18 15:00:07 [node_B_1:raid.debug:info]:
   volobj_mark_sb_recovery_aggrs: tree:
      node_A_1_aggr0 vol_state:1 mcc_dr_opstate: unknown
   Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
   /node_A_1_aggr0 (VOL):
      raid state change UNINITD -> NORMAL
   Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
   /node_A_1_aggr0 (MIRROR):
      raid state change UNINITD -> DEGRADED
   Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
   /node_A_1_aggr0/plex0
      (PLEX): raid state change UNINITD -> FAILED
   Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
   /node_A_1_aggr0/plex2
      (PLEX): raid state change UNINITD -> NORMAL
   Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
   /node_A_1_aggr0/plex2/rg0
      (GROUP): raid state change UNINITD -> NORMAL
   Aug 18 15:00:07 [node_B_1:raid.debug:info]: Topology updated for
   aggregate node_A_1_aggr0
      to plex plex2
   *>
   ```

b. Eliminare il plesso guasto:

```
aggr destroy plex-id
```

```
*> aggr destroy node_A_1_aggr0/plex0
```

4. Arrestare il nodo per visualizzare il prompt DEL CARICATORE:

```
halt
```

5. Ripetere questi passaggi sull'altro nodo del sito di emergenza.

Avvio di ONTAP su moduli controller sostitutivi in configurazioni MetroCluster IP

È necessario avviare i nodi sostitutivi nel sito di emergenza sul sistema operativo ONTAP.

A proposito di questa attività

Questa attività inizia con i nodi nel sito di emergenza in modalità manutenzione.

Fasi

1. Su uno dei nodi sostitutivi, uscire al prompt DEL CARICATORE: `halt`
2. Visualizzare il menu di avvio: `boot_ontap menu`
3. Dal menu di avvio, selezionare l'opzione 6, **Update flash from backup config** (Aggiorna flash da configurazione backup).

   Il sistema si avvia due volte. Dovresti rispondere `yes` quando viene richiesto di continuare. Dopo il secondo avvio, dovresti rispondere `y` Quando viene richiesto di indicare la mancata corrispondenza dell'ID di sistema.

   > Se il contenuto della NVRAM di un modulo controller sostitutivo usato non è stato ancora deseleziona, potrebbe essere visualizzato il seguente messaggio di emergenza: `PANIC: NVRAM contents are invalid…`. In tal caso, avviare nuovamente il sistema al prompt ONTAP (`boot_ontap menu`). Quindi, è necessario Ripristinare boot_recovery e i bootargs rdb_corrotto

   - Richiesta di conferma per continuare:

     ```
     Selection (1-9)? 6

     This will replace all flash-based configuration with the last backup
     to
     disks. Are you sure you want to continue?: yes
     ```

   - Richiesta di mancata corrispondenza ID sistema:

```
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
```

4. Dal sito sopravvissuto, verificare che ai nodi siano stati applicati gli ID di sistema del partner corretti:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   In questo esempio, i seguenti nuovi ID di sistema dovrebbero apparire nell'output:

   - Node_A_1: 1574774970
   - Node_A_2: 1574774991

   La colonna "ha-partner-systemid" dovrebbe mostrare i nuovi ID di sistema.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  1574774970    1574774991
4068741254          4068741256
1           Cluster_A  Node_A_2  1574774991    1574774970
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

5. Se gli ID del sistema partner non sono stati impostati correttamente, è necessario impostare manualmente il valore corretto:
   a. Arrestare e visualizzare il prompt DEL CARICATORE sul nodo.
   b. Verificare il valore corrente del bootarg partner-sysID:

      `printenv`

   c. Impostare il valore sull'ID di sistema del partner corretto:

      `setenv partner-sysid partner-sysID`

   d. Avviare il nodo:

```
boot_ontap
```

e. Se necessario, ripetere questi passaggi secondari sull'altro nodo.

6. Verificare che i nodi sostitutivi nel sito di disastro siano pronti per lo switchback:

```
metrocluster node show
```

I nodi sostitutivi devono essere in attesa della modalità di recovery switchback. Se invece si trovano in modalità normale, è possibile riavviare i nodi sostitutivi. Dopo l'avvio, i nodi devono essere in attesa della modalità di ripristino switchback.

L'esempio seguente mostra che i nodi sostitutivi sono pronti per lo switchback:

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1          configured     enabled   switchover
completed
              node_B_2          configured     enabled   switchover
completed
      cluster_A
              node_A_1          configured     enabled   waiting for
switchback recovery
              node_A_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

7. Verificare le impostazioni di configurazione della connessione MetroCluster:

```
metrocluster configuration-settings connection show
```

Lo stato di configurazione deve indicare Completed (completato).

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2
                 Home Port: e5a
```

```
                     172.17.26.13    172.17.26.12    HA Partner
completed
                Home Port: e5a
                     172.17.26.13    172.17.26.10    DR Partner
completed
                Home Port: e5a
                     172.17.26.13    172.17.26.11    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.12    HA Partner
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.10    DR Partner
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.11    DR Auxiliary
completed
             node_B_1
                Home Port: e5a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.11    DR Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.10    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.11    DR Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.10    DR Auxiliary
completed
      cluster_A
             node_A_2
                Home Port: e5a
                     172.17.26.11    172.17.26.10    HA Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.12    DR Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.13    DR Auxiliary
```

```
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.12    DR Partner
completed
                 Home Port: e5b
                      172.17.27.11    172.17.27.13    DR Auxiliary
completed
              node_A_1
                 Home Port: e5a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.13    DR Partner
completed
                 Home Port: e5a
                      172.17.26.10    172.17.26.12    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.13    DR Partner
completed
                 Home Port: e5b
                      172.17.27.10    172.17.27.12    DR Auxiliary
completed
24 entries were displayed.

cluster_B::*>
```

8. Ripetere i passaggi precedenti sull'altro nodo del sito di emergenza.

Ripristina boot_recovery e bootargs rdb_corrotto

Se necessario, è possibile ripristinare boot_recovery e rdb_corrotto_bootargs

Fasi

1. Arrestare nuovamente il nodo al prompt DEL CARICATORE:

```
node_A_1::*> halt -node _node-name_
```

2. Controllare se sono stati impostati i seguenti bootargs:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se uno dei due bootarg è stato impostato su un valore, disimpostarlo e avviare ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Ripristino della connettività dai nodi sopravvissuti al sito di emergenza (configurazioni MetroCluster IP)

È necessario ripristinare le connessioni MetroCluster iSCSI Initiator dai nodi sopravvissuti.

A proposito di questa attività

Questa procedura è necessaria solo per le configurazioni MetroCluster IP.

Fasi

1. Dal prompt di uno dei nodi sopravvissuti, passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

   Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

2. Collegare gli iniziatori iSCSI su entrambi i nodi sopravvissuti nel gruppo DR:

   ```
   storage iscsi-initiator connect -node surviving-node -label *
   ```

   L'esempio seguente mostra i comandi per la connessione degli iniziatori sul sito B:

   ```
   site_B::*> storage iscsi-initiator connect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator connect -node node_B_2 -label *
   ```

3. Tornare al livello di privilegio admin:

   ```
   set -privilege admin
   ```

Verifica dell'assegnazione automatica o assegnazione manuale dei dischi del pool 0

Nei sistemi configurati per ADP, è necessario verificare che il pool di dischi 0 sia stato assegnato automaticamente. Nei sistemi non configurati per ADP, è necessario assegnare manualmente il pool 0 dischi.

Verifica dell'assegnazione dei dischi del pool 0 su sistemi ADP nel sito di emergenza (sistemi IP MetroCluster)

Se i dischi sono stati sostituiti nel sito di emergenza e il sistema è configurato per ADP, è necessario verificare che i dischi remoti siano visibili ai nodi e siano stati assegnati correttamente.

Fase

1. Verificare che i dischi del pool 0 siano assegnati automaticamente:

   ```
   disk show
   ```

   Nell'esempio seguente per un sistema AFF A800 senza shelf esterni, un quarto (8 dischi) è stato assegnato automaticamente al nodo_A_1 e un quarto è stato assegnato automaticamente al nodo_A_2. I dischi rimanenti saranno unità remote (pool 1) per Node_B_1 e Node_B_2.

   ```
   cluster_A::*> disk show
                   Usable     Disk      Container           Container
   Disk            Size       Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   ```

```
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Assegnazione di pool 0 dischi su sistemi non ADP nel sito di disastro (configurazioni IP MetroCluster)

Se i dischi sono stati sostituiti nel sito di emergenza e il sistema non è configurato per ADP, è necessario assegnare manualmente i nuovi dischi al pool 0.

A proposito di questa attività

Per i sistemi ADP, i dischi vengono assegnati automaticamente.

Fasi

1. Su uno dei nodi di sostituzione nel sito di disastro, riassegnare il pool di nodi 0 dischi:

   ```
   storage disk assign -n number-of-replacement disks -p 0
   ```

   Questo comando assegna i dischi appena aggiunti (e non posseduti) nel sito di emergenza. È necessario assegnare lo stesso numero e dimensione (o superiore) dei dischi che il nodo aveva prima del disastro. Il `storage disk assign` la pagina man contiene ulteriori informazioni su come eseguire un'assegnazione più granulare dei dischi.

2. Ripetere il passaggio sull'altro nodo sostitutivo nel sito di emergenza.

Assegnazione di unità pool 1 sul sito sopravvissuto (configurazioni IP MetroCluster)

Se i dischi sono stati sostituiti nel sito di disastro e il sistema non è configurato per ADP, nel sito di sopravvivenza è necessario assegnare manualmente i dischi remoti situati nel sito di disastro al pool di nodi sopravvissuti 1. È necessario identificare il numero di dischi da assegnare.

A proposito di questa attività

Per i sistemi ADP, i dischi vengono assegnati automaticamente.

Fase

1. Sul sito sopravvissuto, assegnare al primo nodo il pool di 1 unità (remote): `storage disk assign -n number-of-replacement disks -p 1 0m*`

   Questo comando assegna i dischi appena aggiunti e non posseduti sul sito di emergenza.

   Il seguente comando assegna 22 dischi:

   ```
   cluster_B::> storage disk assign -n 22 -p 1 0m*
   ```

Eliminazione dei plex guasti di proprietà del sito sopravvissuto (configurazioni IP MetroCluster)

Dopo la sostituzione dell'hardware e l'assegnazione dei dischi, è necessario eliminare i plessi remoti guasti di proprietà dei nodi del sito sopravvissuti ma che si trovano nel sito di emergenza.

A proposito di questa attività

Questi passaggi vengono eseguiti sul cluster esistente.

Fasi

1. Identificare gli aggregati locali: `storage aggregate show -is-home true`

   ```
   cluster_B::> storage aggregate show -is-home true

   cluster_B Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_B_1_aggr0 1.49TB  74.12GB 95% online       1 node_B_1
   raid4,

   mirror

   degraded
   node_B_2_aggr0 1.49TB  74.12GB 95% online       1 node_B_2
   raid4,

   mirror

   degraded
   node_B_1_aggr1 2.99TB  2.88TB   3% online      15 node_B_1
   raid_dp,
   ```

```
mirror

degraded
node_B_1_aggr2 2.99TB  2.91TB   3% online      14 node_B_1
raid_tec,

mirror

degraded
node_B_2_aggr1 2.95TB  2.80TB   5% online      37 node_B_2
raid_dp,

mirror

degraded
node_B_2_aggr2 2.99TB  2.87TB   4% online      35 node_B_2
raid_tec,

mirror

degraded
6 entries were displayed.

cluster_B::>
```

2. Identificare i plessi remoti guasti:

   ```
   storage aggregate plex show
   ```

   Nell’esempio riportato di seguito vengono indicati i plex remoti (non plex0) con stato "failed" (non riuscito):

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_1_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr2 plex0 normal,active true     0
node_B_1_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr2 plex0 normal,active true     0
node_B_2_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
20 entries were displayed.

cluster_B::>
```

3. Portare offline ciascuno dei plessi guasti, quindi eliminarli:

   a. Take offline the failed plex:

      `storage aggregate plex offline -aggregate aggregate-name -plex plex-id`

      L'esempio seguente mostra l'aggregato "Node_B_2_aggr1/plex1" che viene portato offline:

      ```
      cluster_B::> storage aggregate plex offline -aggregate node_B_1_aggr0
      -plex plex4

      Plex offline successful on plex: node_B_1_aggr0/plex4
      ```

   b. Eliminare il plesso guasto:

      `storage aggregate plex delete -aggregate aggregate-name -plex plex-id`

      Quando richiesto, è possibile distruggere il plex.

Nell’esempio seguente viene mostrato il nodo plex_B_2_aggr1/plex1 cancellato.

```
cluster_B::> storage aggregate plex delete -aggregate  node_B_1_aggr0
-plex plex4

Warning: Aggregate "node_B_1_aggr0" is being used for the local
management root
         volume or HA partner management root volume, or has been
marked as
         the aggregate to be used for the management root volume
after a
         reboot operation. Deleting plex "plex4" for this aggregate
could lead
         to unavailability of the root volume after a disaster
recovery
         procedure. Use the "storage aggregate show -fields
         has-mroot,has-partner-mroot,root" command to view such
aggregates.

Warning: Deleting plex "plex4" of mirrored aggregate "node_B_1_aggr0"
on node
         "node_B_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you
want to
         destroy this plex? {y|n}: y
[Job 633] Job succeeded: DONE

cluster_B::>
```

È necessario ripetere questi passaggi per ciascuno dei plessi guasti.

4. Verificare che i plessi siano stati rimossi:

   ```
   storage aggregate plex show -fields aggregate,status,is-online,plex,pool
   ```

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

5. Identificare gli aggregati di switchover:

   `storage aggregate show -is-home false`

   È inoltre possibile utilizzare `storage aggregate plex show -fields aggregate,status,is-online,plex,pool` comando per identificare aggregati di switchover plex 0. Avranno lo stato "failed, inactive" (non riuscito, inattivo).

   I seguenti comandi mostrano quattro aggregati di switchover:

   - Node_A_1_aggr1
   - Node_A_1_aggr2
   - Node_A_2_aggr1
   - Node_A_2_aggr2

```
cluster_B::> storage aggregate show -is-home false

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.12TB  1.88TB   11% online      91 node_B_1
raid_dp,

mirror

degraded
node_A_1_aggr2 2.89TB  2.64TB    9% online      90 node_B_1
raid_tec,

mirror

degraded
node_A_2_aggr1 2.12TB  1.86TB   12% online      91 node_B_2
raid_dp,

mirror

degraded
node_A_2_aggr2 2.89TB  2.64TB    9% online      90 node_B_2
raid_tec,

mirror

degraded
4 entries were displayed.

cluster_B::>
```

6. Identificare i plessi di switchover:

   `storage aggregate plex show -fields aggregate,status,is-online,Plex,pool`

   Si desidera identificare i plessi con lo stato "failed, inactive" (non riuscito, inattivo).

   I seguenti comandi mostrano quattro aggregati di switchover:

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

7. Eliminare il plesso guasto:

   `storage aggregate plex delete -aggregate node_A_1_aggr1 -plex plex0`

   Quando richiesto, è possibile distruggere il plex.

   Il seguente esempio mostra che il nodo plex_A_1_aggr1/plex0 è stato cancellato:

```
cluster_B::> storage aggregate plex delete -aggregate node_A_1_aggr1
-plex plex0

Warning: Aggregate "node_A_1_aggr1" hosts MetroCluster metadata volume
         "MDV_CRS_e8457659b8a711e78b3b00a0988fe74b_A". Deleting plex
"plex0"
         for this aggregate can lead to the failure of configuration
         replication across the two DR sites. Use the "volume show
-vserver
         <admin-vserver> -volume MDV_CRS*" command to verify the
location of
         such volumes.

Warning: Deleting plex "plex0" of mirrored aggregate "node_A_1_aggr1" on
node
         "node_A_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you want
to
         destroy this plex? {y|n}: y
[Job 639] Job succeeded: DONE

cluster_B::>
```

È necessario ripetere questi passaggi per ciascuno degli aggregati guasti.

8. Verificare che non vi siano altri plex guasti sul sito sopravvissuto.

   Il seguente output mostra che tutti i plessi sono normali, attivi e online.

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex1 normal,active true     1
10 entries were displayed.

cluster_B::>
```

Esecuzione della riparazione degli aggregati e ripristino dei mirror (configurazioni MetroCluster IP)

Dopo la sostituzione dell'hardware e l'assegnazione dei dischi, nei sistemi che eseguono ONTAP 9.5 o versioni precedenti è possibile eseguire le operazioni di riparazione di MetroCluster. In tutte le versioni di ONTAP, è necessario confermare che gli aggregati sono sottoposti a mirroring e, se necessario, riavviare il mirroring.

A proposito di questa attività

A partire da ONTAP 9.6, le operazioni di riparazione vengono eseguite automaticamente all'avvio dei nodi del sito di emergenza. I comandi di riparazione non sono richiesti.

Questi passaggi vengono eseguiti sul cluster esistente.

Fasi

1. Se si utilizza ONTAP 9.6 o versione successiva, è necessario verificare che la riparazione automatica sia stata completata correttamente:

   a. Verificare che le operazioni heal-aggr-auto e heal-root-aggr-auto siano state completate:

      ```
      metrocluster operation history show
      ```

      Il seguente output mostra che le operazioni sono state completate correttamente su cluster_A.

```
cluster_B::*> metrocluster operation history show
Operation                     State          Start Time       End
Time
----------------------------- -------------- ----------------
----------------
heal-root-aggr-auto           successful      2/25/2019 06:45:58

2/25/2019 06:46:02
heal-aggr-auto                successful     2/25/2019 06:45:48

2/25/2019 06:45:52
.
.
.
```

b. Verificare che il sito di emergenza sia pronto per lo switchback:

```
metrocluster node show
```

Il seguente output mostra che le operazioni sono state completate correttamente su cluster_A.

```
cluster_B::*> metrocluster node show
DR                          Configuration  DR
Group Cluster Node          State          Mirroring Mode
----- ------- ------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1      configured     enabled   heal roots
completed
              node_A_2      configured     enabled   heal roots
completed
      cluster_B
              node_B_1      configured     enabled   waiting for
switchback recovery
              node_B_2      configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Se si utilizza ONTAP 9.5 o versioni precedenti, è necessario eseguire la riparazione aggregata:

a. Verificare lo stato dei nodi:

```
metrocluster node show
```

Il seguente output mostra che lo switchover è stato completato, quindi è possibile eseguire la riparazione.

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1          configured     enabled   switchover
completed
              node_B_2          configured     enabled   switchover
completed
      cluster_A
              node_A_1          configured     enabled   waiting for
switchback recovery
              node_A_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

b. Eseguire la fase di riparazione degli aggregati:

```
metrocluster heal -phase aggregates
```

Il seguente output mostra una tipica operazione di riparazione degli aggregati.

```
cluster_B::*> metrocluster heal -phase aggregates
[Job 647] Job succeeded: Heal Aggregates is successful.

cluster_B::*> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 10/26/2017 12:01:15
   End Time: 10/26/2017 12:01:17
     Errors: -

cluster_B::*>
```

c. Verificare che la riparazione degli aggregati sia stata completata e che il sito di emergenza sia pronto per lo switchback:

```
metrocluster node show
```

Il seguente output mostra che la fase "Heal aggregates" è stata completata su cluster_A.

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1          configured     enabled   heal
aggregates completed
              node_A_2          configured     enabled   heal
aggregates completed
      cluster_B
              node_B_1          configured     enabled   waiting for
switchback recovery
              node_B_2          configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

3. Se i dischi sono stati sostituiti, è necessario eseguire il mirroring degli aggregati locali e di switchover:

   a. Visualizzare gli aggregati:

      `storage aggregate show`

```
cluster_B::> storage aggregate show
cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

normal
node_B_1_aggr1 3.14TB  3.04TB    3% online     15 node_B_1
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.06TB    3% online     14 node_B_1
raid_tec,
```

```
normal
node_B_1_aggr1 3.14TB  2.99TB    5% online     37 node_B_2
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.02TB    4% online     35 node_B_2
raid_tec,

normal

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.36TB  2.12TB   10% online     91 node_B_1
raid_dp,

normal
node_A_1_aggr2 3.14TB  2.90TB    8% online     90 node_B_1
raid_tec,

normal
node_A_2_aggr1 2.36TB  2.10TB   11% online     91 node_B_2
raid_dp,

normal
node_A_2_aggr2 3.14TB  2.89TB    8% online     90 node_B_2
raid_tec,

normal
12 entries were displayed.

cluster_B::>
```

b. Mirroring dell'aggregato:

```
storage aggregate mirror -aggregate aggregate-name
```

Il seguente output mostra una tipica operazione di mirroring.

```
cluster_B::> storage aggregate mirror -aggregate node_B_1_aggr1

Info: Disks would be added to aggregate "node_B_1_aggr1" on node
"node_B_1" in
      the following manner:

      Second Plex

        RAID Group rg0, 6 disks (block checksum, raid_dp)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          dparity    5.20.6                    SSD
-
          parity     5.20.14                   SSD
-
          data       5.21.1                    SSD
894.0GB
          data       5.21.3                    SSD
894.0GB
          data       5.22.3                    SSD
894.0GB
          data       5.21.13                   SSD
894.0GB

      Aggregate capacity available for volume use would be 2.99TB.

Do you want to continue? {y|n}: y
```

c. Ripetere il passaggio precedente per ciascuno degli aggregati del sito sopravvissuto.

d. Attendere la risincronizzazione degli aggregati; è possibile controllare lo stato con `storage aggregate show` comando.

   Il seguente output mostra che alcuni aggregati sono in risincronizzazione.

```
cluster_B::> storage aggregate show

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,
```

```
mirrored,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

mirrored,

normal
node_B_1_aggr1 2.86TB  2.76TB    4% online     15 node_B_1
raid_dp,

resyncing
node_B_1_aggr2 2.89TB  2.81TB    3% online     14 node_B_1
raid_tec,

resyncing
node_B_2_aggr1 2.73TB  2.58TB    6% online     37 node_B_2
raid_dp,

resyncing
node_B-2_aggr2 2.83TB  2.71TB    4% online     35 node_B_2
raid_tec,

resyncing

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 1.86TB  1.62TB   13% online     91 node_B_1
raid_dp,

resyncing
node_A_1_aggr2 2.58TB  2.33TB   10% online     90 node_B_1
raid_tec,

resyncing
node_A_2_aggr1 1.79TB  1.53TB   14% online     91 node_B_2
raid_dp,

resyncing
node_A_2_aggr2 2.64TB  2.39TB    9% online     90 node_B_2
raid_tec,
```

```
resyncing
12 entries were displayed.
```

e. Verificare che tutti gli aggregati siano online e risincronizzati:

```
storage aggregate plex show
```

Il seguente output mostra che tutti gli aggregati sono risincronizzati.

```
cluster_A::> storage aggregate plex show
  ()
                    Is      Is         Resyncing
Aggregate Plex      Online  Resyncing    Percent Status
--------- --------- ------- ---------- --------- ---------------
node_B_1_aggr0 plex0 true    false              - normal,active
node_B_1_aggr0 plex8 true    false              - normal,active
node_B_2_aggr0 plex0 true    false              - normal,active
node_B_2_aggr0 plex8 true    false              - normal,active
node_B_1_aggr1 plex0 true    false              - normal,active
node_B_1_aggr1 plex9 true    false              - normal,active
node_B_1_aggr2 plex0 true    false              - normal,active
node_B_1_aggr2 plex5 true    false              - normal,active
node_B_2_aggr1 plex0 true    false              - normal,active
node_B_2_aggr1 plex9 true    false              - normal,active
node_B_2_aggr2 plex0 true    false              - normal,active
node_B_2_aggr2 plex5 true    false              - normal,active
node_A_1_aggr1 plex4 true    false              - normal,active
node_A_1_aggr1 plex8 true    false              - normal,active
node_A_1_aggr2 plex1 true    false              - normal,active
node_A_1_aggr2 plex5 true    false              - normal,active
node_A_2_aggr1 plex4 true    false              - normal,active
node_A_2_aggr1 plex8 true    false              - normal,active
node_A_2_aggr2 plex1 true    false              - normal,active
node_A_2_aggr2 plex5 true    false              - normal,active
20 entries were displayed.
```

4. Nei sistemi che eseguono ONTAP 9.5 e versioni precedenti, eseguire la fase di healing degli aggregati root:

```
metrocluster heal -phase root-aggregates
```

```
cluster_B::> metrocluster heal -phase root-aggregates
[Job 651] Job is queued: MetroCluster Heal Root Aggregates Job.Oct 26
13:05:00
[Job 651] Job succeeded: Heal Root Aggregates is successful.
```

5. Verificare che la fase "Heal Roots" sia stata completata e che il sito di disastro sia pronto per lo switchback:

   Il seguente output mostra che la fase "Heal Roots" è stata completata su cluster_A.

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal roots
completed
              node_A_2           configured     enabled   heal roots
completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

Verificare le licenze sui nodi sostituiti.

"Verifica delle licenze sui nodi sostituiti"

Prepararsi per lo switchback in una configurazione MetroCluster FC

Verifica della configurazione delle porte (solo configurazioni MetroCluster FC)

È necessario impostare le variabili ambientali sul nodo e quindi spegnerlo per prepararlo alla configurazione MetroCluster.

A proposito di questa attività

Questa procedura viene eseguita con i moduli controller sostitutivi in modalità di manutenzione.

La procedura per controllare la configurazione delle porte è necessaria solo nei sistemi in cui le porte FC o CNA vengono utilizzate in modalità initiator.

Fasi

1. In modalità Maintenance (manutenzione), ripristinare la configurazione della porta FC:

   ```
   ucadmin modify -m fc -t initiatoradapter_name
   ```

   Se si desidera utilizzare solo una coppia di porte nella configurazione dell'iniziatore, immettere un nome adattatore preciso.

2. Eseguire una delle seguenti operazioni, a seconda della configurazione:

Se la configurazione della porta FC è…	Quindi…
Lo stesso vale per entrambe le porte	Rispondere "y" quando richiesto dal sistema, perché la modifica di una porta in una coppia di porte modifica anche l'altra porta.
Diverso	a. Rispondere "n" quando richiesto dal sistema. b. Ripristinare la configurazione della porta FC: `ucadmin modify -m fc -t initiator

3. Uscire dalla modalità di manutenzione:

   ```
   halt
   ```

   Dopo aver inviato il comando, attendere che il sistema 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 i valori delle variabili:

   ```
   ucadmin show
   ```

6. Uscire dalla modalità di manutenzione e visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

Configurazione dei bridge FC-SAS (solo configurazioni MetroCluster FC)

Se sono stati sostituiti i bridge FC-SAS, è necessario configurarli al momento del ripristino della configurazione MetroCluster. La procedura è identica alla configurazione iniziale di un bridge FC-SAS.

Fasi

1. Accendere i bridge FC-SAS.
2. Impostare l'indirizzo IP sulle porte Ethernet utilizzando `set IPAddress port ipaddress` comando.
   - `port` Può essere "MP1" o "MP2".
   - `ipaddress` Può essere un indirizzo IP nel formato xxx.xxx.xxx.xxx.

Nell'esempio seguente, l'indirizzo IP è 10.10.10.55 sulla porta Ethernet 1:

```
Ready.
set IPAddress MP1 10.10.10.55

Ready. *
```

3. Impostare la subnet mask IP sulle porte Ethernet utilizzando `set IPSubnetMask port mask` comando.
   - `port` Può essere "MP1" o "MP2".
   - `mask` può essere una subnet mask nel formato xxx.xxx.xxx.xxx.

   Nell'esempio seguente, la subnet mask IP è 255.255.255.0 sulla porta Ethernet 1:

```
Ready.
set IPSubnetMask MP1 255.255.255.0

Ready. *
```

4. Impostare la velocità sulle porte Ethernet utilizzando `set EthernetSpeed port speed` comando.
   - `port` Può essere "MP1" o "MP2".
   - `speed` può essere "100" o "1000".

   Nell'esempio seguente, la velocità Ethernet è impostata su 1000 sulla porta Ethernet 1.

```
Ready.
set EthernetSpeed MP1 1000

Ready. *
```

5. Salvare la configurazione utilizzando `saveConfiguration` e riavviare il bridge quando richiesto.

   Il salvataggio della configurazione dopo la configurazione delle porte Ethernet consente di procedere con la configurazione del bridge utilizzando Telnet e consente di accedere al bridge utilizzando FTP per eseguire gli aggiornamenti del firmware.

   Nell'esempio riportato di seguito viene illustrato il `saveConfiguration` e il prompt per riavviare il bridge.

```
Ready.
SaveConfiguration
  Restart is necessary....
  Do you wish to restart (y/n) ?
Confirm with 'y'. The bridge will save and restart with the new
settings.
```

6. Dopo il riavvio del bridge FC-SAS, accedere nuovamente.
7. Impostare la velocità sulle porte FC utilizzando `set fcdatarate port speed` comando.
   - `port` può essere "1" o "2".
   - `speed` Può essere "2 GB", "4 GB", "8 GB" o "16 GB", a seconda del modello di bridge in uso.

     Nell'esempio seguente, la velocità della porta FC1 è impostata su "8 GB".

```
Ready.
set fcdatarate 1 8Gb

Ready. *
```

8. Impostare la topologia sulle porte FC utilizzando `set FCConnMode port mode` comando.
   - `port` può essere "1" o "2".
   - `mode` può essere "ptp", "loop", "loop ptp" o "auto".

     Nell'esempio seguente, la topologia della porta FC1 è impostata su "ptp".

```
Ready.
set FCConnMode 1 ptp

Ready. *
```

9. Salvare la configurazione utilizzando `saveConfiguration` e riavviare il bridge quando richiesto.

Nell'esempio riportato di seguito viene illustrato il `saveConfiguration` e il prompt per riavviare il bridge.

```
 Ready.
 SaveConfiguration
    Restart is necessary....
    Do you wish to restart (y/n) ?
 Confirm with 'y'. The bridge will save and restart with the new
settings.
```

10. Dopo il riavvio del bridge FC-SAS, accedere nuovamente.
11. Se sul bridge FC-SAS è in esecuzione il firmware 1.60 o successivo, attivare SNMP.

```
Ready.
set snmp enabled

Ready. *
saveconfiguration

Restart is necessary....
Do you wish to restart (y/n) ?

Verify with 'y' to restart the FibreBridge.
```

12. Spegnere i bridge FC-SAS.

Configurazione degli switch FC (solo configurazioni MetroCluster FC)

Se sono stati sostituiti gli switch FC nel sito di emergenza, è necessario configurarli utilizzando le procedure specifiche del vendor. È necessario configurare uno switch, verificare che l'accesso allo storage nel sito sopravvissuto non sia influenzato, quindi configurare il secondo switch.

Attività correlate

"Assegnazioni delle porte per switch FC quando si utilizza 9.0"

"Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Configurazione di uno switch Brocade FC dopo un disastro del sito

Per configurare lo switch sostitutivo e abilitare le porte ISL, è necessario utilizzare questa procedura specifica di Brocade.

A proposito di questa attività

Gli esempi di questa procedura si basano sui seguenti presupposti:

- Il sito A è il sito di disastro.
- FC_switch_A_1 sostituito.
- FC_switch_A_2 è stato sostituito.
- Il sito B è il sito sopravvissuto.
- FC_switch_B_1 è in buone condizioni.
- FC_switch_B_2 è in buone condizioni.

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"
- "Assegnazioni delle porte per gli switch FC quando si utilizza ONTAP 9.1 e versioni successive"

Gli esempi mostrano due bridge FC-SAS. Se si dispone di più bridge, è necessario disattivare e successivamente attivare le porte aggiuntive.

Fasi

1. Avviare e preconfigurare il nuovo switch:

   a. Accendere il nuovo switch e lasciarlo avviare.

   b. Controllare la versione del firmware sullo switch per verificare che corrisponda alla versione degli altri switch FC:

      ```
      firmwareShow
      ```

   c. Configurare il nuovo switch come descritto nei seguenti argomenti, ignorando i passaggi per la configurazione dello zoning sullo switch.

      "Installazione e configurazione di Fabric-Attached MetroCluster"

      "Estensione dell'installazione e della configurazione di MetroCluster"

   d. Disattivare lo switch in modo persistente:

      ```
      switchcfgpersistentdisable
      ```

      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:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

2. Configurazione completa del nuovo switch:

   a. Abilitare gli ISL sul sito sopravvissuto:

      ```
      portcfgpersistentenable port-number
      ```

      ```
      FC_switch_B_1:admin> portcfgpersistentenable 10
      FC_switch_B_1:admin> portcfgpersistentenable 11
      ```

   b. Abilitare gli ISL sugli switch sostitutivi:

      ```
      portcfgpersistentenable port-number
      ```

```
FC_switch_A_1:admin> portcfgpersistentenable 10
FC_switch_A_1:admin> portcfgpersistentenable 11
```

c. Sullo switch sostitutivo (FC_switch_A_1 in questo esempio) verificare che gli ISL siano in linea:

```
switchshow
```

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port 10:00:00:05:33:86:89:cb
"FC_switch_A_1" (downstream)
...
```

3. Abilitare costantemente lo switch:

```
switchcfgpersistentenable
```

4. Verificare che le porte siano in linea:

```
switchshow
```

Configurazione di uno switch FC Cisco dopo un disastro del sito

È necessario utilizzare la procedura specifica di Cisco per configurare lo switch sostitutivo e abilitare le porte ISL.

A proposito di questa attività

Gli esempi di questa procedura si basano sui seguenti presupposti:

- Il sito A è il sito di disastro.
- FC_switch_A_1 sostituito.

- FC_switch_A_2 è stato sostituito.
- Il sito B è il sito sopravvissuto.
- FC_switch_B_1 è in buone condizioni.
- FC_switch_B_2 è in buone condizioni.

Fasi

1. Configurare lo switch:
   a. Fare riferimento a. "Installazione e configurazione di Fabric-Attached MetroCluster"
   b. Seguire la procedura per la configurazione dello switch in "Configurazione degli switch FC Cisco" Sezione, *tranne* per la sezione "Configurazione dello zoning su uno switch FC Cisco":

      Lo zoning viene configurato più avanti in questa procedura.

2. Sullo switch integro (in questo esempio, FC_switch_B_1), attivare le porte ISL.

   L'esempio seguente mostra i comandi per abilitare le porte:

   ```
   FC_switch_B_1# conf t
   FC_switch_B_1(config)# int fc1/14-15
   FC_switch_B_1(config)# no shut
   FC_switch_B_1(config)# end
   FC_switch_B_1# copy running-config startup-config
   FC_switch_B_1#
   ```

3. Verificare che le porte ISL siano in funzione utilizzando il comando show interface brief.
4. Recuperare le informazioni di zoning dal fabric.

   L'esempio seguente mostra i comandi per distribuire la configurazione dello zoning:

   ```
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 10
   FC_switch_B_1(config-zone)# zoneset distribute full vsan 20
   FC_switch_B_1(config-zone)# end
   ```

   FC_switch_B_1 viene distribuito a tutti gli altri switch del fabric per "vsan 10" e "vsan 20" e le informazioni di zoning vengono recuperate da FC_switch_A_1.

5. Sullo switch integro, verificare che le informazioni di zoning siano recuperate correttamente dallo switch del partner:

   ```
   show zone
   ```

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

6. Determinare i nomi internazionali (WWN) degli switch nel fabric dello switch.

   In questo esempio, i due WWN dello switch sono i seguenti:

   - FC_switch_A_1: 20:00:54:7f:ee:b8:24:c0
   - FC_switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

7. Accedere alla modalità di configurazione della zona e rimuovere i membri della zona che non appartengono ai WWN dei due switch:

   ```
   no member interface interface-ide swwn wwn
   ```

   In questo esempio, i seguenti membri non sono associati al WWN di uno degli switch del fabric e devono essere rimossi:

   - Nome della zona FC-VI_zone_1_10 vsan 10
     - Interfaccia fc1/1 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/2 swwn 20:00:54:7f:ee:e3:86:50

     > I sistemi AFF A700 e FAS9000 supportano quattro porte FC-VI. È necessario rimuovere tutte e quattro le porte dalla zona FC-VI.

   - Nome zona STOR_zone_1_20_25A vsan 20
     - Interfaccia fc1/5 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/11 swwn 20:00:54:7f:ee:e3:86:50
   - Nome zona STOR_zone_1_20_25B vsan 20
     - Interfaccia fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - Interfaccia fc1/11 swwn 20:00:54:7f:ee:e3:86:50

   Nell’esempio seguente viene illustrata la rimozione di queste interfacce:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

8. aggiungere le porte del nuovo switch alle zone.

   Nell’esempio seguente si presuppone che il cablaggio dello switch sostitutivo sia identico a quello dello switch precedente:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

9. Verificare che lo zoning sia configurato correttamente: `show zone`

   Il seguente esempio di output mostra le tre zone:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

Verifica della configurazione dello storage

È necessario confermare che tutto lo storage sia visibile dai nodi sopravvissuti.

Fasi

1. Verificare che tutti i componenti di storage del sito di emergenza siano uguali in quantità e tipo nel sito di sopravvivenza.

   Il sito sopravvissuto e il sito di emergenza devono avere lo stesso numero di stack di shelf di dischi, shelf di dischi e dischi. In una configurazione MetroCluster con collegamento a ponte o con collegamento a fabric, i siti devono avere lo stesso numero di bridge FC-SAS.

2. Verificare che tutti i dischi che sono stati sostituiti nel sito di disastro non siano di proprietà:

   ```
   run local disk show-n
   ```

   I dischi dovrebbero apparire come non di proprietà.

3. Se non sono stati sostituiti dischi, verificare che siano presenti tutti i dischi:

   ```
   disk show
   ```

Accensione dell'apparecchiatura nel sito di emergenza

Quando si è pronti per lo switchback, è necessario accendere i componenti MetroCluster nel sito di emergenza. Inoltre, è necessario recuperare le connessioni di storage SAS anche in configurazioni MetroCluster direct-attached e abilitare le porte non Inter-Switch link nelle configurazioni Fabric-attached MetroCluster.

Prima di iniziare

È necessario aver già sostituito e cablato i componenti MetroCluster esattamente come quelli precedenti.

"Installazione e configurazione di Fabric-Attached MetroCluster"

"Estensione dell'installazione e della configurazione di MetroCluster"

A proposito di questa attività

Gli esempi di questa procedura presuppongono quanto segue:

- Il sito A è il sito di disastro.
  - FC_switch_A_1 sostituito.
  - FC_switch_A_2 è stato sostituito.
- Il sito B è il sito sopravvissuto.
  - FC_switch_B_1 è in buone condizioni.
  - FC_switch_B_2 è in buone condizioni.

Gli switch FC sono presenti solo nelle configurazioni Fabric-Attached MetroCluster.

Fasi

1. In una configurazione stretch MetroCluster con cablaggio SAS (senza fabric switch FC o bridge FC-SAS), collegare tutto lo storage, incluso lo storage remoto, in entrambi i siti.

   Il controller del sito di emergenza deve rimanere spento o al prompt DEL CARICATORE.

2. Nel sito sopravvissuto, disattivare l'assegnazione automatica del disco:

   ```
   storage disk option modify -autoassign off *
   ```

   ```
   cluster_B::> storage disk option modify -autoassign off *
   2 entries were modified.
   ```

3. Sul sito sopravvissuto, verificare che l'assegnazione automatica del disco sia disattivata:

   ```
   storage disk option show
   ```

```
cluster_B::> storage disk option show
Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          off             default
node_B_2       on            on          off             default
2 entries were displayed.

 cluster_B::>
```

4. Accendere gli shelf di dischi nel sito di disastro e assicurarsi che tutti i dischi siano in esecuzione.
5. In una configurazione MetroCluster con collegamento a ponte o con collegamento a fabric, attivare tutti i bridge FC-SAS nel sito di emergenza.
6. Se sono stati sostituiti dischi, lasciare i controller spenti o quando richiesto DAL CARICATORE.
7. In una configurazione Fabric-Attached MetroCluster, abilitare le porte non ISL sugli switch FC.

Se il vendor dello switch è…	Quindi, procedere come segue per attivare le porte…

Brocade	a. Abilitare in modo persistente le porte collegate ai bridge FC-SAS: `portpersistentenable port-number`
	
	Nell'esempio seguente, le porte 6 e 7 sono attivate:
	
	`FC_switch_A_1:admin> portpersistentenable 6`
	`FC_switch_A_1:admin> portpersistentenable 7`
	
	`FC_switch_A_1:admin>`
	
	b. Abilitare in modo persistente le porte collegate agli HBA e agli adattatori FC-VI: `portpersistentenable port-number`
	
	Nell'esempio seguente, le porte 6 e 7 sono attivate:
	
	`FC_switch_A_1:admin> portpersistentenable 1`
	`FC_switch_A_1:admin> portpersistentenable 2`
	`FC_switch_A_1:admin> portpersistentenable 4`
	`FC_switch_A_1:admin> portpersistentenable 5`
	`FC_switch_A_1:admin>`
	
	Per i sistemi AFF A700 e FAS9000, è necessario abilitare costantemente tutte e quattro le porte FC-VI utilizzando il comando switchcfgpersistentenable.
	
	c. Ripetere i passaggi secondari a e b per il secondo switch FC nel sito sopravvissuto.

Cisco	a. Accedere alla modalità di configurazione per l'interfaccia, quindi attivare le porte con il comando no shut.
	
	Nell'esempio seguente, la porta fc1/36 è disattivata:
	
	`FC_switch_A_1# conf t`
	`FC_switch_A_1(config)# interface fc1/36`
	`FC_switch_A_1(config)# no shut`
	`FC_switch_A_1(config-if)# end`
	`FC_switch_A_1# copy running-config startup-config`
	
	b. Verificare che la porta dello switch sia abilitata: `show interface brief`
	
	c. Ripetere i passaggi secondari a e b sulle altre porte collegate ai bridge FC-SAS, agli HBA e agli adattatori FC-VI.
	
	d. Ripetere i passaggi secondari a, b e c per il secondo switch FC nel sito sopravvissuto.

Assegnazione della proprietà per i dischi sostituiti

Se sono stati sostituiti i dischi durante il ripristino dell'hardware nel sito di disastro o si è dovuto azzerare i dischi o rimuovere la proprietà, è necessario assegnare la proprietà ai dischi interessati.

Prima di iniziare

Il sito di disaster recovery deve disporre di un numero di dischi almeno pari a quello disponibile prima del disastro.

La disposizione degli shelf di dischi e dei dischi deve soddisfare i requisiti di "Requisiti per il componente IP MetroCluster e le convenzioni di denominazione" della sezione "Installazione e configurazione di MetroCluster IP".

A proposito di questa attività

Questi passaggi vengono eseguiti sul cluster del sito di emergenza.

Questa procedura mostra la riassegnazione di tutti i dischi e la creazione di nuovi plessi nel sito di disastro. I nuovi plessi sono complessi remoti di siti sopravvissuti e plessi locali di siti di disastro.

Questa sezione fornisce esempi di configurazioni a due e quattro nodi. Per le configurazioni a due nodi, è possibile ignorare i riferimenti al secondo nodo in ogni sito. Per le configurazioni a otto nodi, è necessario tenere conto dei nodi aggiuntivi nel secondo gruppo di DR. Gli esempi fanno le seguenti ipotesi:

- Il sito A è il sito di disastro.

    - Il nodo_A_1 è stato sostituito.
    - Il nodo_A_2 è stato sostituito.

      Presente solo nelle configurazioni MetroCluster a quattro nodi.

- Il sito B è il sito sopravvissuto.
    - Node_B_1 è integro.
    - Node_B_2 è integro.

      Presente solo nelle configurazioni MetroCluster a quattro nodi.

I moduli controller hanno i seguenti ID di sistema originali:

Numero di nodi nella configurazione MetroCluster	Nodo	ID di sistema originale
Quattro	Node_A_1	4068741258
Node_A_2	4068741260	Node_B_1
4068741254	Node_B_2	4068741256
Due	Node_A_1	4068741258

Quando si assegnano i dischi, tenere presenti i seguenti punti:

- Il vecchio numero di dischi deve essere almeno lo stesso numero di dischi per ogni nodo presente prima del disastro.

  Se viene specificato o presente un numero inferiore di dischi, le operazioni di riparazione potrebbero non essere completate a causa dello spazio insufficiente.

- I nuovi plex da creare sono i plex remoti appartenenti al sito sopravvissuto (Node_B_x pool1) e i plex locali appartenenti al sito di disastro (Node_B_x pool0).
- Il numero totale di dischi richiesti non deve includere i dischi root aggr.

  Se n dischi sono assegnati al pool 1 del sito sopravvissuto, n-3 dischi devono essere assegnati al sito di emergenza con il presupposto che l'aggregato root utilizzi tre dischi.

- Nessuno dei dischi può essere assegnato a un pool diverso da quello a cui sono assegnati tutti gli altri dischi dello stesso stack.
- I dischi appartenenti al sito sopravvissuto vengono assegnati al pool 1 e i dischi appartenenti al sito di disastro vengono assegnati al pool 0.

Fasi

1. Assegnare i nuovi dischi non proprietari in base alla configurazione MetroCluster a quattro o due nodi:

    - Per le configurazioni MetroCluster a quattro nodi, assegnare i nuovi dischi non proprietari ai pool di dischi appropriati utilizzando la seguente serie di comandi sui nodi sostitutivi:

i. Assegnare sistematicamente i dischi sostituiti per ciascun nodo ai rispettivi pool di dischi:

```
disk assign -s sysid -n old-count-of-disks -p pool
```

Dal sito sopravvissuto, viene inviato un comando di assegnazione del disco per ciascun nodo:

```
cluster_B::> disk assign -s node_B_1-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_B_2-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_A_1-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
cluster_B::> disk assign -s node_A_2-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
```

L'esempio seguente mostra i comandi con gli ID di sistema:

```
cluster_B::> disk assign -s 4068741254 -n 21 -p 1
cluster_B::> disk assign -s 4068741256 -n 21 -p 1
cluster_B::> disk assign -s 4068741258 -n 21 -p 0
cluster_B::> disk assign -s 4068741260 -n 21 -p 0
```

i. Confermare la proprietà dei dischi:

```
storage disk show -fields owner, pool
```

```
storage disk show -fields owner, pool
cluster_A::> storage disk show -fields owner, pool
disk     owner          pool
-------- ------------- -----
0c.00.1  node_A_1      Pool0
0c.00.2  node_A_1      Pool0
.
.
.
0c.00.8  node_A_1      Pool1
0c.00.9  node_A_1      Pool1
.
.
.
0c.00.15 node_A_2      Pool0
0c.00.16 node_A_2      Pool0
.
.
.
0c.00.22 node_A_2      Pool1
0c.00.23 node_A_2      Pool1
.
.
.
```

- Per le configurazioni MetroCluster a due nodi, assegnare i nuovi dischi non proprietari ai pool di dischi appropriati utilizzando la seguente serie di comandi sul nodo sostitutivo:
  i. Visualizzare gli ID dello shelf locale:

     ```
     run local storage show shelf
     ```

  ii. Assegnare i dischi sostituiti per il nodo integro al pool 1:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 1 -s
     node_B_1-sysid -f
     ```

  iii. Assegnare i dischi sostituiti per il nodo sostitutivo al pool 0:

     ```
     run local disk assign -shelf shelf-id -n old-count-of-disks -p 0 -s
     node_A_1-sysid -f
     ```

2. Sul sito sopravvissuto, attivare nuovamente l’assegnazione automatica del disco:

   ```
   storage disk option modify -autoassign on *
   ```

```
cluster_B::> storage disk option modify -autoassign on *
2 entries were modified.
```

3. Sul sito sopravvissuto, verificare che l'assegnazione automatica del disco sia attivata:

   `storage disk option show`

```
 cluster_B::> storage disk option show
 Node      BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          on             default
node_B_2       on            on          on             default
2 entries were displayed.

 cluster_B::>
```

Informazioni correlate

"Gestione di dischi e aggregati"

"In che modo le configurazioni MetroCluster utilizzano SyncMirror per fornire ridondanza dei dati"

Esecuzione della riparazione degli aggregati e ripristino dei mirror (configurazioni MetroCluster FC)

Dopo la sostituzione dell'hardware e l'assegnazione dei dischi, è possibile eseguire le operazioni di riparazione del MetroCluster. È quindi necessario confermare che gli aggregati sono sottoposti a mirroring e, se necessario, riavviare il mirroring.

Fasi

1. Eseguire le due fasi di riparazione (riparazione aggregata e riparazione root) sul sito di emergenza:

```
cluster_B::> metrocluster heal -phase aggregates

cluster_B::> metrocluster heal -phase root-aggregates
```

2. Monitorare la riparazione e verificare che gli aggregati siano in stato di risyncing o mirrorato:

   `storage aggregate show -node local`

Se l'aggregato mostra questo stato…	Quindi…
risyncing	Non è richiesta alcuna azione. Consentire all'aggregato di completare la risyncing.

mirror degradato	Passare a. Se uno o più plessi rimangono offline, sono necessari ulteriori passaggi per ricostruire il mirror.
mirrorato, normale	Non è richiesta alcuna azione.
sconosciuto, offline	L'aggregato root mostra questo stato se sono stati sostituiti tutti i dischi dei siti di disastro.

```
cluster_B::> storage aggregate show -node local

 Aggregate     Size Available Used% State   #Vols  Nodes      RAID
Status
 --------- -------- --------- ----- ------- ------ ----------
------------
 node_B_1_aggr1
           227.1GB   11.00GB   95% online       1 node_B_1   raid_dp,
                                                              resyncing
 NodeA_1_aggr2
           430.3GB   28.02GB   93% online       2 node_B_1   raid_dp,
                                                              mirror
                                                              degraded
 node_B_1_aggr3
           812.8GB   85.37GB   89% online       5 node_B_1   raid_dp,
                                                              mirrored,
                                                              normal
 3 entries were displayed.

cluster_B::>
```

Nei seguenti esempi, i tre aggregati si trovano ciascuno in uno stato diverso:

Nodo	Stato
Node_B_1_aggr1	risyncing
Node_B_1_aggr2	mirror degradato
Node_B_1_aggr3	mirrorato, normale

3. se uno o più plessi rimangono offline, sono necessari ulteriori passaggi per ricostruire il mirror.

   Nella tabella precedente, il mirror per node_B_1_aggr2 deve essere ricostruito.

   a. Visualizza i dettagli dell'aggregato per identificare eventuali plessi guasti:

```
storage aggregate show -r -aggregate node_B_1_aggr2
```

Nell'esempio seguente, plex /node_B_1_aggr2/plex0 è in uno stato di errore:

```
cluster_B::> storage aggregate show -r -aggregate node_B_1_aggr2

 Owner Node: node_B_1
  Aggregate: node_B_1_aggr2 (online, raid_dp, mirror degraded) (block
checksums)
   Plex: /node_B_1_aggr2/plex0 (offline, failed, inactive, pool0)
    RAID Group /node_B_1_aggr2/plex0/rg0 (partial)
                                                                    Usable
Physical
      Position Disk                      Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------

   Plex: /node_B_1_aggr2/plex1 (online, normal, active, pool1)
    RAID Group /node_B_1_aggr2/plex1/rg0 (normal, block checksums)
                                                                    Usable
Physical
      Position Disk                      Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------
      dparity  1.44.8                     1   SAS    15000  265.6GB
273.5GB (normal)
      parity   1.41.11                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.42.8                     1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.11                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.44.9                     1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.18                    1   SAS    15000  265.6GB
273.5GB (normal)
 6 entries were displayed.

 cluster_B::>
```

a. Eliminare il plesso guasto:

```
storage aggregate plex delete -aggregate aggregate-name -plex plex
```

b. Ristabilire il mirror:

```
storage aggregate mirror -aggregate aggregate-name
```

c. Monitorare la risincronizzazione e lo stato di mirroring del plex fino a quando tutti i mirror non vengono ristabilita e tutti gli aggregati mostrano lo stato normale e mirrorato:

```
storage aggregate show
```

Riassegnazione della proprietà dei dischi per gli aggregati root ai moduli controller sostitutivi (configurazioni MetroCluster FC)

Se uno o entrambi i moduli controller o le schede NVRAM sono stati sostituiti nel sito di emergenza, l'ID del sistema è stato modificato ed è necessario riassegnare i dischi appartenenti agli aggregati root ai moduli controller sostitutivi.

A proposito di questa attività

Poiché i nodi sono in modalità switchover ed è stata eseguita la riparazione, in questa sezione verranno riassegnati solo i dischi contenenti gli aggregati root del pool 1 del sito di disastro. Si tratta degli unici dischi ancora di proprietà del vecchio ID di sistema a questo punto.

Questa sezione fornisce esempi di configurazioni a due e quattro nodi. Per le configurazioni a due nodi, è possibile ignorare i riferimenti al secondo nodo in ogni sito. Per le configurazioni a otto nodi, è necessario tenere conto dei nodi aggiuntivi nel secondo gruppo di DR. Gli esempi fanno le seguenti ipotesi:

- Il sito A è il sito di disastro.
  - Il nodo_A_1 è stato sostituito.
  - Il nodo_A_2 è stato sostituito.

    Presente solo nelle configurazioni MetroCluster a quattro nodi.
- Il sito B è il sito sopravvissuto.
  - Node_B_1 è integro.
  - Node_B_2 è integro.

    Presente solo nelle configurazioni MetroCluster a quattro nodi.

Gli ID di sistema vecchi e nuovi sono stati identificati in "Determinazione degli ID di sistema dei moduli controller sostitutivi".

Gli esempi di questa procedura utilizzano controller con i seguenti ID di sistema:

Numero di nodi	Nodo	ID di sistema originale	Nuovo ID di sistema

Quattro	Node_A_1	4068741258	1574774970
	Node_A_2	4068741260	1574774991
	Node_B_1	4068741254	invariato
	Node_B_2	4068741256	invariato
Due	Node_A_1	4068741258	1574774970

Fasi

1. Con il nodo sostitutivo in modalità Maintenance, riassegnare i dischi aggregati root:

   ```
   disk reassign -s old-system-ID -d new-system-ID
   ```

   ```
   *> disk reassign -s 4068741258 -d 1574774970
   ```

2. Visualizzare i dischi per confermare la modifica della proprietà dei dischi aggiuntivi root del pool 1 del sito di disastro al nodo sostitutivo:

   ```
   disk show
   ```

   L'output potrebbe visualizzare un numero maggiore o minore di dischi, a seconda del numero di dischi presenti nell'aggregato root e se uno di questi dischi è guasto e se è stato sostituito. Se i dischi sono stati sostituiti, i dischi Pool0 non vengono visualizzati nell'output.

   I dischi aggregati root del pool 1 del sito di emergenza devono ora essere assegnati al nodo sostitutivo.

```
*> disk show
Local System ID: 1574774970

  DISK             OWNER                POOL   SERIAL NUMBER   HOME
DR HOME
------------       -------------        -----  -------------
-------------       -------------
sw_A_1:6.126L19    node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L3     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_A_1:6.126L7     node_A_1(1574774970) Pool0  serial-number
node_A_1(1574774970)
sw_B_1:6.126L8     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L24    node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)
sw_B_1:6.126L2     node_A_1(1574774970) Pool1  serial-number
node_A_1(1574774970)

*> aggr status
         Aggr State           Status
 node_A_1_root online          raid_dp, aggr
                               mirror degraded
                               64-bit
*>
```

3. Visualizzare lo stato aggregato:

   ```
   aggr status
   ```

   L'output potrebbe visualizzare un numero maggiore o minore di dischi, a seconda del numero di dischi presenti nell'aggregato root e se uno di questi dischi è guasto e se è stato sostituito. Se i dischi sono stati sostituiti, i dischi Pool0 non vengono visualizzati nell'output.

   ```
   *> aggr status
            Aggr State           Status
     node_A_1_root online          raid_dp, aggr
                                   mirror degraded
                                   64-bit
   *>
   ```

4. Eliminare il contenuto dei dischi della mailbox:

   ```
   mailbox destroy local
   ```

5. Se l'aggregato non è online, portalo online:

   ```
   aggr online aggr_name
   ```

6. Arrestare il nodo per visualizzare il prompt DEL CARICATORE:

   ```
   halt
   ```

Avvio dei nuovi moduli controller (configurazioni MetroCluster FC)

Una volta completata la riparazione degli aggregati sia per i dati che per gli aggregati root, è necessario avviare il nodo o i nodi nel sito di emergenza.

A proposito di questa attività

Questa attività inizia con i nodi che mostrano il prompt DEL CARICATORE.

Fasi

1. Visualizzare il menu di avvio:

   ```
   boot_ontap menu
   ```

2. [[fase 2,fase 2]]dal menu di avvio, selezionare l'opzione 6, **Aggiorna flash dalla configurazione del backup**.
3. Rispondere `y` al seguente prompt:

   ```
   This will replace all flash-based configuration with the last backup to disks.
   Are you sure you want to continue?: y
   ```

   Il sistema si avvia due volte, la seconda volta per caricare la nuova configurazione.

   > Se il contenuto della NVRAM di un controller sostitutivo usato non è stato ancora desuso, potrebbe essere visualizzato un messaggio di emergenza con il seguente messaggio: `PANIC: NVRAM contents are invalid…`In tal caso, ripetere Dal menu di avvio, selezionare l'opzione 6, **Update flash from backup config** (Aggiorna flash da configurazione backup). Per avviare il sistema al prompt di ONTAP. Quindi, è necessario Ripristinare il boot recovery e i bootargs rdb_corrotto

4. Mirroring dell'aggregato root su plex 0:
   a. Assegnare tre dischi pool 0 al nuovo modulo controller.
   b. Mirroring del pool aggregato root 1 plex:

      ```
      aggr mirror root-aggr-name
      ```

   c. Assegnare dischi non posseduti al pool 0 sul nodo locale
5. Se si dispone di una configurazione a quattro nodi, ripetere i passaggi precedenti sull'altro nodo del sito di emergenza.
6. Aggiornare la configurazione MetroCluster:
   a. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

b. Aggiornare la configurazione:

```
metrocluster configure -refresh true
```

c. Tornare alla modalità privilegi di amministratore:

```
set -privilege admin
```

7. Verificare che i nodi sostitutivi nel sito di disastro siano pronti per lo switchback:

```
metrocluster node show
```

I nodi sostitutivi devono essere in modalità “Waiting for switchback recovery” (in attesa di ripristino switchback). Se invece si trovano in modalità “normal”, è possibile riavviare i nodi sostitutivi. Dopo l’avvio, i nodi dovrebbero essere in modalità “Waiting for switchback recovery” (in attesa di ripristino switchback).

L’esempio seguente mostra che i nodi sostitutivi sono pronti per lo switchback:

```
cluster_B::> metrocluster node show
DR                    Configuration  DR
Grp Cluster Node      State          Mirroring Mode
--- ------- --------- -------------- --------- --------------------
1   cluster_B
            node_B_1  configured     enabled   switchover completed
            node_B_2  configured     enabled   switchover completed
    cluster_A
            node_A_1  configured     enabled   waiting for switchback
recovery
            node_A_2  configured     enabled   waiting for switchback
recovery
4 entries were displayed.

cluster_B::>
```

Cosa fare in seguito

Passare a. "Completare il processo di disaster recovery".

Ripristina boot_recovery e bootargs rdb_corrotto

Se necessario, è possibile ripristinare boot_recovery e rdb_corrotto_bootargs

Fasi

1. Arrestare nuovamente il nodo al prompt DEL CARICATORE:

```
node_A_1::*> halt -node _node-name_
```

2. Controllare se sono stati impostati i seguenti bootargs:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se uno dei due bootarg è stato impostato su un valore, disimpostarlo e avviare ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Preparazione per lo switchback in una configurazione mista (recovery durante la transizione)

È necessario eseguire alcune attività per preparare la configurazione mista MetroCluster IP e FC per l'operazione di switchback. Questa procedura si applica solo alle configurazioni che hanno riscontrato un errore durante il processo di transizione da MetroCluster FC a IP.

A proposito di questa attività

Questa procedura deve essere utilizzata solo quando si esegue il ripristino su un sistema che si trovava a metà della transizione quando si è verificato l'errore.

In questo scenario, MetroCluster è una configurazione mista:

- Un gruppo DR è costituito da nodi FC MetroCluster collegati al fabric.

  È necessario eseguire le procedure di ripristino MetroCluster FC su questi nodi.

- Un gruppo di DR è costituito da nodi IP MetroCluster.

  È necessario eseguire le operazioni di ripristino dell'IP MetroCluster su questi nodi.

Fasi

Eseguire le operazioni nell'ordine indicato di seguito.

1. Preparare i nodi FC per lo switchback eseguendo le seguenti operazioni nell'ordine indicato:
   a. "Verifica della configurazione delle porte (solo configurazioni MetroCluster FC)"
   b. "Configurazione dei bridge FC-SAS (solo configurazioni MetroCluster FC)"
   c. "Configurazione degli switch FC (solo configurazioni MetroCluster FC)"
   d. "Verifica della configurazione dello storage" (Eseguire questa procedura solo sui dischi sostituiti sui nodi FC MetroCluster)
   e. "Accensione dell'apparecchiatura nel sito di emergenza" (Eseguire questa procedura solo sui dischi sostituiti sui nodi FC MetroCluster)

f. "Assegnazione della proprietà per i dischi sostituiti" (Eseguire questa procedura solo sui dischi sostituiti sui nodi FC MetroCluster)

g. Eseguire le operazioni descritte in "Riassegnazione della proprietà dei dischi per gli aggregati root ai moduli controller sostitutivi (configurazioni MetroCluster FC)", fino al passaggio per l'emissione del comando di distruzione della mailbox.

h. Distruggere il plex locale (plex 0) dell'aggregato root:

```
aggr destroy plex-id
```

i. Se l'aggr root non è online, portalo online.

2. Avviare i nodi FC MetroCluster.

È necessario eseguire questi passaggi su entrambi i nodi FC MetroCluster.

a. Visualizzare il menu di avvio:

```
boot_ontap menu
```

b. Dal menu di avvio, selezionare l'opzione 6, **Update flash from backup config** (Aggiorna flash da configurazione backup).

c. Rispondere `y` al seguente prompt:

```
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?: y
```

Il sistema si avvia due volte, la seconda volta per caricare la nuova configurazione.

> Se il contenuto della NVRAM di un controller sostitutivo usato non è stato ancora desuso, potrebbe essere visualizzato un messaggio di emergenza con il seguente messaggio: `PANIC: NVRAM contents are invalid…` In tal caso, ripetere questi passaggi secondari per avviare il sistema al prompt di ONTAP. Quindi, è necessario Ripristinare il boot recovery e i bootargs rdb_corrotto

3. Mirroring dell'aggregato root su plex 0:

È necessario eseguire questi passaggi su entrambi i nodi FC MetroCluster.

a. Assegnare tre dischi pool 0 al nuovo modulo controller.

b. Mirroring del pool aggregato root 1 plex:

```
aggr mirror root-aggr-name
```

c. Assegnare dischi non posseduti al pool 0 sul nodo locale

4. Tornare alla modalità di manutenzione.

È necessario eseguire questi passaggi su entrambi i nodi FC MetroCluster.

a. Arrestare il nodo:

```
halt
```

b. Avviare il nodo in Maintenance (manutenzione):

```
mode:boot_ontap maint
```

5. Eliminare il contenuto dei dischi della mailbox:

```
mailbox destroy local
```

È necessario eseguire questi passaggi su entrambi i nodi FC MetroCluster.

6. Arrestare i nodi:
```
halt
```

7. Dopo l'avvio dei nodi, verificare lo stato del nodo:

```
metrocluster node show
```

```
siteA::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     siteA
              wmc66-a1           configured     enabled   waiting for
switchback recovery
              wmc66-a2           configured     enabled   waiting for
switchback recovery
      siteB
              wmc66-b1           configured     enabled   switchover
completed
              wmc66-b2           configured     enabled   switchover
completed
2     siteA
              wmc55-a1           -              -         -
              wmc55-a2           unreachable    -         -
      siteB
              wmc55-b1           configured     enabled   switchover
completed
              wmc55-b2           configured
```

8. Preparare i nodi IP MetroCluster per lo switchback eseguendo le attività descritte in "Preparazione per lo switchback in una configurazione IP MetroCluster" fino a e incluso "Eliminazione dei plex guasti di proprietà del sito sopravvissuto (configurazioni IP MetroCluster)".
9. Sui nodi MetroCluster FC, eseguire le operazioni descritte in "Esecuzione della riparazione degli aggregati e ripristino dei mirror (configurazioni MetroCluster FC)".
10. Sui nodi IP MetroCluster, eseguire le operazioni descritte in "Esecuzione della riparazione degli aggregati e ripristino dei mirror (configurazioni MetroCluster IP)".

11. Procedere con le attività rimanenti del processo di ripristino che iniziano con "Ripristino degli archivi di oggetti per le configurazioni FabricPool".

Ripristina boot_recovery e bootargs rdb_corrotto

Se necessario, è possibile ripristinare boot_recovery e rdb_corrotto_bootargs

Fasi

1. Arrestare nuovamente il nodo al prompt DEL CARICATORE:

```
node_A_1::*> halt -node _node-name_
```

2. Controllare se sono stati impostati i seguenti bootargs:

```
LOADER> printenv bootarg.init.boot_recovery
LOADER> printenv bootarg.rdb_corrupt
```

3. Se uno dei due bootarg è stato impostato su un valore, disimpostarlo e avviare ONTAP:

```
LOADER> unsetenv bootarg.init.boot_recovery
LOADER> unsetenv bootarg.rdb_corrupt
LOADER> saveenv
LOADER> bye
```

Completamento del ripristino

Eseguire le attività richieste per completare il ripristino da un errore di controller multiplo o di storage.

Ripristino degli archivi di oggetti per le configurazioni FabricPool

Se uno degli archivi di oggetti in un mirror FabricPool è stato co-localizzato con il sito di emergenza MetroCluster ed è stato distrutto, è necessario ristabilire l'archivio di oggetti e il mirror FabricPool.

A proposito di questa attività

- Se gli archivi di oggetti sono remoti e un sito MetroCluster viene distrutto, non è necessario ricostruire l'archivio di oggetti e conservare le configurazioni dell'archivio di oggetti originale e il contenuto dei dati cold.
- Per ulteriori informazioni sulle configurazioni FabricPool, consultare "Gestione di dischi e aggregati".

Fase

1. Seguire la procedura "Sostituzione di un mirror FabricPool in una configurazione MetroCluster" in "Gestione di dischi e aggregati".

Verifica delle licenze sui nodi sostituiti

È necessario installare nuove licenze per i nodi sostitutivi se i nodi con problemi utilizzavano funzionalità ONTAP che richiedono una licenza standard (bloccata da nodo). Per le funzionalità con licenze standard, ogni nodo del cluster deve disporre di una propria chiave per la funzionalità.

A proposito di questa attività

Fino all'installazione delle chiavi di licenza, le funzionalità che richiedono licenze standard continuano a essere disponibili per il nodo sostitutivo. Tuttavia, se il nodo compromesso era l'unico nodo nel cluster con una licenza per la funzione, non sono consentite modifiche di configurazione alla funzione. Inoltre, l'utilizzo di funzionalità senza licenza sul nodo potrebbe non essere conforme al contratto di licenza, pertanto è necessario installare la chiave o le chiavi di licenza sostitutive sul nodo sostitutivo il prima possibile.

Le chiavi di licenza devono essere in formato a 28 caratteri.

Si dispone di un periodo di prova di 90 giorni per l'installazione delle chiavi di licenza. Dopo il periodo di tolleranza, tutte le vecchie licenze vengono invalidate. Dopo aver installato una chiave di licenza valida, si hanno a disposizione 24 ore per installare tutte le chiavi prima della fine del periodo di tolleranza.

> Se tutti i nodi di un sito sono stati sostituiti (un singolo nodo nel caso di una configurazione MetroCluster a due nodi), le chiavi di licenza devono essere installate sul nodo o sui nodi sostitutivi prima dello switchback.

Fasi

1. Identificare le licenze sul nodo:

   ```
   license show
   ```

   Nell'esempio seguente vengono visualizzate le informazioni sulle licenze nel sistema:

   ```
   cluster_B::>  license show
            (system license show)

   Serial Number: 1-80-00050
   Owner: site1-01
   Package           Type       Description             Expiration
   -------          -------     -------------           -----------
   Base             license     Cluster Base License        -
   NFS              site        NFS License                 -
   CIFS             site        CIFS License                -
   iSCSI            site        iSCSI License               -
   FCP              site        FCP License                 -
   FlexClone        site        FlexClone License           -

   6 entries were displayed.
   ```

2. Verificare che le licenze siano valide per il nodo dopo lo switchback:

   ```
   metrocluster check license show
   ```

Nell'esempio seguente vengono visualizzate le licenze valide per il nodo:

```
cluster_B::> metrocluster check license show

Cluster           Check                              Result
-------           -------                            -------------
Cluster_B         negotiated-switchover-ready        not-applicable
NFS               switchback-ready                   not-applicable
CIFS              job-schedules                      ok
iSCSI             licenses                           ok
FCP               periodic-check-enabled             ok
```

3. Se sono necessarie nuove chiavi di licenza, procurarsi le chiavi di licenza sostitutive sul sito di supporto NetApp nella sezione My Support (Assistenza) sotto Software licenss (licenze software).

> Le nuove chiavi di licenza richieste vengono generate automaticamente e inviate all'indirizzo e-mail in archivio. Se non si riceve l'e-mail contenente le chiavi di licenza entro 30 giorni, consultare la sezione *"Chi contattare in caso di problemi con le licenze?"* dell'articolo della Knowledge base "Processo di sostituzione della scheda madre per aggiornare le licenze su un sistema AFF/FAS."

4. Installare ogni chiave di licenza:

   `system license add -license-code license-key, license-key…+`

5. Rimuovere le vecchie licenze, se necessario:
   a. Verificare la presenza di licenze inutilizzate:

      `license clean-up -unused -simulate`

   b. Se l'elenco appare corretto, rimuovere le licenze inutilizzate:

      `license clean-up -unused`

Ripristino della gestione delle chiavi

Se i volumi di dati sono crittografati, è necessario ripristinare la gestione delle chiavi. Se il volume root è crittografato, è necessario ripristinare la gestione delle chiavi.

Fasi

1. Se i volumi di dati sono crittografati, ripristinare le chiavi utilizzando il comando corretto per la configurazione di gestione delle chiavi.

Se si utilizza…	Utilizzare questo comando…
Gestione delle chiavi integrata	`security key-manager onboard sync` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia integrate per la gestione delle chiavi".

Gestione esterna delle chiavi	`security key-manager key query -node node-name` Per ulteriori informazioni, vedere "Ripristino delle chiavi di crittografia esterne per la gestione delle chiavi".

2. Se il volume root è crittografato, seguire la procedura descritta in "Ripristino della gestione delle chiavi se il volume root è crittografato".

Esecuzione di uno switchback

Dopo aver corretto la configurazione MetroCluster, è possibile eseguire l'operazione di switchback MetroCluster. L'operazione di switchback MetroCluster riporta la configurazione al suo normale stato operativo, con le macchine virtuali dello storage di origine di sincronizzazione (SVM) sul sito di emergenza attive e i dati provenienti dai pool di dischi locali.

Prima di iniziare

- Il cluster di emergenza deve essere passato correttamente al cluster esistente.
- La riparazione deve essere stata eseguita sui dati e sugli aggregati root.
- I nodi del cluster sopravvissuti non devono trovarsi nello stato di failover ha (tutti i nodi devono essere attivi e in esecuzione per ogni coppia ha).
- I moduli controller del sito di emergenza devono essere completamente avviati e non in modalità ha Takeover.
- L'aggregato root deve essere mirrorato.
- I collegamenti Inter-Switch (ISL) devono essere online.
- Tutte le licenze richieste devono essere installate sul sistema.

Fasi

1. Verificare che tutti i nodi siano nello stato abilitato:

   ```
   metrocluster node show
   ```

   Nell'esempio riportato di seguito vengono visualizzati i nodi che si trovano nello stato abilitato:

```
cluster_B::>  metrocluster node show

DR                        Configuration  DR
Group Cluster Node        State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Verificare che la risincronizzazione sia completa su tutte le SVM:

   `metrocluster vserver show`

3. Verificare che tutte le migrazioni LIF automatiche eseguite dalle operazioni di riparazione siano state completate correttamente:

   `metrocluster check lif show`

4. Eseguire lo switchback eseguendo il `metrocluster switchback` comando da qualsiasi nodo del cluster esistente.
5. Controllare l'avanzamento dell'operazione di switchback:

   `metrocluster show`

   L'operazione di switchback è ancora in corso quando l'output visualizza "Waiting-for-switchback" (in attesa di switchback):

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   L'operazione di switchback è completa quando l'output visualizza "normale":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando il seguente comando a livello di privilegio avanzato:

```
metrocluster config-replication resync-status show
```

6. Ripristinare le configurazioni SnapMirror o SnapVault.

   In ONTAP 8.3, è necessario ristabilire manualmente una configurazione di SnapMirror persa dopo un'operazione di switchback MetroCluster. In ONTAP 9.0 e versioni successive, la relazione viene ristabilita automaticamente.

Verifica di uno switchback riuscito

Dopo aver eseguito lo switchback, si desidera confermare che tutti gli aggregati e le macchine virtuali di storage (SVM) siano ripristinati e in linea.

Fasi

1. Verificare che gli aggregati di dati di switchover siano ripristinati:

   ```
   storage aggregate show
   ```

   Nell'esempio seguente, aggr_b2 sul nodo B2 è tornato:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Se il sito di disastro includeva aggregati senza mirror e gli aggregati senza mirror non sono più presenti, l'aggregato potrebbe essere visualizzato con uno stato "Unknown" nell'output del comando show dell'aggregato di storage. Contattare il supporto tecnico per rimuovere le voci non aggiornate per gli aggregati senza mirror, fare riferimento all'articolo della Knowledge base "Come rimuovere le voci aggregate obsolete senza mirror in un MetroCluster in seguito a un disastro in cui lo storage è stato perso."

2. Verificare che tutte le SVM di destinazione della sincronizzazione sul cluster sopravvissuto siano inattive (mostrando uno stato Admin di "ssurfared") e che le SVM di origine della sincronizzazione sul cluster di emergenza siano attive e in esecuzione:

   ```
   vserver show -subtype sync-source
   ```

```
node_B_1::> vserver show -subtype sync-source
                               Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                               running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                               Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                          stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Gli aggregati Sync-destination nella configurazione MetroCluster hanno il suffisso "-mc" aggiunto automaticamente al loro nome per facilitarne l'identificazione.

3. Verificare che le operazioni di switchback siano riuscite utilizzando `metrocluster operation show` comando.

Se l'output del comando mostra…	Quindi…
Che lo stato operativo di switchback sia riuscito.	Il processo di switchback è completo ed è possibile procedere con il funzionamento del sistema.
Che l'operazione di switchback o l'operazione switchback-continuation-Agent abbia parzialmente esito positivo.	Eseguire la correzione suggerita nell'output del comando MetroCluster Operation show.

Al termine

Ripetere le sezioni precedenti per eseguire il switchback nella direzione opposta. Se Site_A ha eseguito uno switchover di Site_B, chiedere a Site_B di eseguire uno switchover di Site_A.

Mirroring degli aggregati root dei nodi sostitutivi

Se i dischi sono stati sostituiti, è necessario eseguire il mirroring degli aggregati root dei nuovi nodi nel sito di emergenza.

Fasi

1. Nel sito di disaster recovery, identificare gli aggregati che non sono mirrorati:

   ```
   storage aggregate show
   ```

   ```
   cluster_A::> storage aggregate show

   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1_aggr0
              1.49TB   74.12GB   95% online       1 node_A_1
   raid4,

   normal
   node_A_2_aggr0
              1.49TB   74.12GB   95% online       1 node_A_2
   raid4,

   normal
   node_A_1_aggr1
              1.49TB   74.12GB   95% online       1 node_A_1         raid
   4, normal

   mirrored
   node_A_2_aggr1
              1.49TB   74.12GB   95% online       1 node_A_2         raid
   4, normal

   mirrored
   4 entries were displayed.

   cluster_A::>
   ```

2. Eseguire il mirroring di uno degli aggregati root:

   ```
   storage aggregate mirror -aggregate root-aggregate
   ```

   L'esempio seguente mostra come il comando seleziona i dischi e richiede la conferma durante il mirroring dell'aggregato.

```
cluster_A::> storage aggregate mirror -aggregate node_A_2_aggr0

Info: Disks would be added to aggregate "node_A_2_aggr0" on node
"node_A_2" in
      the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid4)
          Position   Disk                      Type
Size
          ---------- ------------------------- ----------
---------------
          parity     2.10.0                    SSD
-
          data       1.11.19                   SSD
894.0GB
          data       2.10.2                    SSD
894.0GB

      Aggregate capacity available for volume use would be 1.49TB.

Do you want to continue? {y|n}: y

cluster_A::>
```

3. Verificare che il mirroring dell'aggregato root sia completo:

   `storage aggregate show`

   L'esempio seguente mostra che gli aggregati root sono mirrorati.

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr0
            2.24TB   838.5GB   63% online       1 node_A_2    raid4,
                                                               mirrored,
                                                               normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2    raid4
                                                               mirrored,
                                                               normal
4 entries were displayed.

cluster_A::>
```

4. Ripetere questi passaggi per gli altri aggregati root.

   Qualsiasi aggregato root che non ha lo stato di mirrored deve essere mirrorato.

Riconfigurazione del servizio ONTAP Mediator (configurazioni MetroCluster IP)

Se si dispone di una configurazione IP MetroCluster configurata con il servizio ONTAP Mediator, è necessario rimuovere e riconfigurare l'associazione con il mediatore.

Prima di iniziare

- È necessario disporre dell'indirizzo IP, del nome utente e della password per il servizio di supporto ONTAP.
- Il servizio ONTAP deve essere configurato e funzionante sull'host Linux.

Fasi

1. Rimuovere la configurazione esistente del mediatore ONTAP:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Riconfigurare la configurazione del mediatore ONTAP:

   ```
   metrocluster configuration-settings mediator add -mediator-address mediator-
   ```

```
IP-address
```

Verifica dello stato della configurazione MetroCluster

Verificare lo stato della configurazione MetroCluster per verificarne il corretto funzionamento.

Fasi

1. Verificare che MetroCluster sia configurato e in modalità normale su ciascun cluster:

   ```
   metrocluster show
   ```

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Verificare che il mirroring sia attivato su ciascun nodo:

   ```
   metrocluster node show
   ```

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Verificare che i componenti di MetroCluster siano in buone condizioni:

   ```
   metrocluster check run
   ```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the `metrocluster check show -instance` command
or sub-commands in `metrocluster check` directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run `metrocluster switchover -simulate` or `metrocluster
switchback -simulate`, respectively.
```

4. Verificare che non siano presenti avvisi sullo stato di salute:

   `system health alert show`

5. Simulare un'operazione di switchover:

   a. Dal prompt di qualsiasi nodo, passare al livello di privilegio avanzato:

      `set -privilege advanced`

   Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

   a. Eseguire l'operazione di switchover con `-simulate` parametro:

      `metrocluster switchover -simulate`

   b. Tornare al livello di privilegio admin:

      `set -privilege admin`

6. Per le configurazioni MetroCluster IP che utilizzano il servizio ONTAP Mediator, verificare che il servizio sia attivo e operativo.

   a. Verificare che i dischi Mediator siano visibili al sistema:

      `storage failover mailbox-disk show`

      L'esempio seguente mostra che i dischi della mailbox sono stati riconosciuti.

```
node_A_1::*> storage failover mailbox-disk show
                 Mailbox
Node             Owner     Disk    Name        Disk UUID
-------------     ------   -----   -----        ----------------
sti113-vsim-ucs626g
.
.
     local     0m.i2.3L26
7BBA77C9:AD702D14:831B3E7E:0B0730EE:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i2.3L27
928F79AE:631EA9F9:4DCB5DE6:3402AC48:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i1.0L60
B7BCDB3C:297A4459:318C2748:181565A3:00000000:00000000:00000000:000000
00:00000000:00000000
.
.
.
     partner   0m.i1.0L14
EA71F260:D4DD5F22:E3422387:61D475B2:00000000:00000000:00000000:000000
00:00000000:00000000
     partner   0m.i2.3L64
4460F436:AAE5AB9E:D1ED414E:ABF811F7:00000000:00000000:00000000:000000
00:00000000:00000000
28 entries were displayed.
```

b. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

c. Verificare che i LUN della mailbox siano visibili al sistema:

```
storage iscsi-initiator show
```

L'output mostra la presenza dei LUN della mailbox:

```
Node    Type       Label      Target Portal     Target Name
Admin/Op
----    ----       --------   ---------    ---------
--------------------------------       --------
.
.
.
.node_A_1
               mailbox
                     mediator 172.16.254.1    iqn.2012-
05.local:mailbox.target.db5f02d6-e3d3    up/up
.
.
.
17 entries were displayed.
```

a. Tornare al livello di privilegi amministrativi:

```
set -privilege admin
```

Ripristino da un guasto non del controller

Dopo che l'apparecchiatura nel sito di emergenza ha subito qualsiasi manutenzione o sostituzione richiesta, ma non è stato sostituito alcun controller, è possibile iniziare il processo di ripristino della configurazione MetroCluster in uno stato completamente ridondante. Ciò include la riparazione della configurazione (prima gli aggregati di dati e poi gli aggregati root) e l'esecuzione dell'operazione di switchback.

Prima di iniziare

- Tutto l'hardware MetroCluster nel cluster di emergenza deve essere funzionale.
- La configurazione generale di MetroCluster deve essere in switchover.
- In una configurazione Fabric-Attached MetroCluster, l'ISL deve essere attivo e funzionante tra i siti MetroCluster.

Correzione della configurazione in una configurazione MetroCluster

Nelle configurazioni FC di MetroCluster è possibile eseguire le operazioni di riparazione in un ordine specifico per ripristinare la funzionalità MetroCluster in seguito a uno switchover.

Nelle configurazioni IP di MetroCluster, le operazioni di riparazione dovrebbero avviarsi automaticamente in seguito a uno switchover. In caso contrario, è possibile eseguire le operazioni di riparazione manualmente.

Prima di iniziare

- Lo switchover deve essere stato eseguito e il sito sopravvissuto deve fornire i dati.
- I nodi nel sito di disastro devono essere arrestati o spenti.

Non devono essere completamente avviati durante il processo di riparazione.

- Lo storage nel sito di disastro deve essere accessibile (gli shelf sono accesi, funzionali e accessibili).
- Nelle configurazioni Fabric-Attached MetroCluster, i collegamenti inter-switch (ISL) devono essere operativi.
- Nelle configurazioni MetroCluster a quattro nodi, i nodi nel sito sopravvissuto non devono essere in stato di failover ha (tutti i nodi devono essere attivi e in esecuzione per ogni coppia ha).

A proposito di questa attività

L'operazione di riparazione deve essere eseguita prima sugli aggregati di dati, quindi sugli aggregati root.

Riparazione degli aggregati di dati

È necessario riparare gli aggregati di dati dopo aver riparato e sostituito qualsiasi hardware nel sito di disastro. Questo processo risincronizza gli aggregati di dati e prepara il sito di emergenza (ora riparato) per il normale funzionamento. È necessario riparare gli aggregati di dati prima di riparare gli aggregati root.

A proposito di questa attività

Nell'esempio seguente viene illustrato uno switchover forzato, in cui è possibile portare online l'aggregato switchover. Tutti gli aggiornamenti della configurazione nel cluster remoto vengono replicati correttamente nel cluster locale. L'alimentazione dello storage nel sito di disastro viene eseguita nell'ambito di questa procedura, ma non è necessario accendere i moduli controller nel sito di disastro.

Fasi

1. Verificare che lo switchover sia stato completato:

   `metrocluster operation show`

   ```
   controller_A_1::> metrocluster operation show
     Operation: switchover
         State: successful
    Start Time: 7/25/2014 20:01:48
      End Time: 7/25/2014 20:02:14
        Errors: -
   ```

2. Risincronizzare gli aggregati di dati eseguendo il seguente comando dal cluster esistente:

   `metrocluster heal -phase aggregates`

   ```
   controller_A_1::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.
   ```

   Se la riparazione è vetoed, si ha la possibilità di riemettere il `metrocluster heal` con il `--override -vetoes` parametro. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

3. Verificare che l'operazione sia stata completata:

`metrocluster operation show`

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Controllare lo stato degli aggregati:

   `storage aggregate show` comando.

```
controller_A_1::> storage aggregate show
Aggregate Size     Available Used% State   #Vols  Nodes        RAID
Status
--------- -------- --------- ----- ------- ------ ------------
------------
...
aggr_b2   227.1GB  227.1GB   0%    online  0      mcc1-a2      raid_dp,
mirrored, normal...
```

5. Se lo storage è stato sostituito nel sito di disastro, potrebbe essere necessario eseguire il remirrore degli aggregati.

Riparazione degli aggregati root dopo un disastro

Una volta guariti gli aggregati di dati, è necessario riparare gli aggregati root in preparazione dell'operazione di switchback.

Prima di iniziare

La fase di aggregazione dei dati del processo di riparazione MetroCluster deve essere stata completata correttamente.

Fasi

1. Ripristinare gli aggregati mirrorati:

   `metrocluster heal -phase root-aggregates`

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

   Se la riparazione è vetoed, si ha la possibilità di riemettere il `metrocluster heal` con il `--override -vetoes` parametro. Se si utilizza questo parametro opzionale, il sistema sovrascrive qualsiasi veto soft che impedisca l'operazione di riparazione.

2. Assicurarsi che l'operazione di riparazione sia completa eseguendo il seguente comando sul cluster di destinazione:

   `metrocluster operation show`

   ```
   mcc1A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

Verificare che il sistema sia pronto per lo switchback

Se il sistema si trova già nello stato di switchover, è possibile utilizzare `-simulate` opzione per visualizzare in anteprima i risultati di un'operazione di switchback.

Fasi

1. Accendere ciascun modulo controller nel sito di emergenza.

   Se i nodi sono spenti:

   Accendere i nodi.

   Se i nodi sono al prompt del CARICATORE:

   Eseguire il comando: `boot_ontap`

2. Una volta completato il boot del nodo, verificare che gli aggregati root siano mirrorati.

   Se sono presenti entrambi i plessi, la risincronizzazione viene avviata automaticamente. Se un plex non riesce, distruggerlo e ristabilire la relazione di mirroring utilizzando il seguente comando per ricreare il mirror:

   `storage aggregate mirror -aggregate <aggregate-name>`

3. Simulare l'operazione di switchback:

   a. Dal prompt di uno dei nodi sopravvissuti, passare al livello di privilegio avanzato:

      `set -privilege advanced`

   Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

   a. Eseguire l'operazione di switchback con `-simulate` parametro:

      `metrocluster switchback -simulate`

   b. Tornare al livello di privilegio admin:

```
    set -privilege admin
```

4. Esaminare l'output restituito.

   L'output mostra se l'operazione di switchback si sarebbe arresa in errori.

Esempio di risultati della verifica

L'esempio seguente mostra la verifica riuscita di un'operazione di switchback:

```
cluster4::*> metrocluster switchback -simulate
  (metrocluster switchback)
[Job 130] Setting up the nodes and cluster components for the switchback
operation...DBG:backup_api.c:327:backup_nso_sb_vetocheck : MetroCluster
Switch Back
[Job 130] Job succeeded: Switchback simulation is successful.

cluster4::*> metrocluster op show
  (metrocluster operation show)
  Operation: switchback-simulate
      State: successful
 Start Time: 5/15/2014 16:14:34
   End Time: 5/15/2014 16:15:04
     Errors: -

cluster4::*> job show -name Me*
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
130    MetroCluster Switchback
                            cluster4
                                       cluster4-01
                                                      Success
       Description: MetroCluster Switchback Job - Simulation
```

Esecuzione di uno switchback

Dopo aver corretto la configurazione MetroCluster, è possibile eseguire l'operazione di switchback MetroCluster. L'operazione di switchback MetroCluster riporta la configurazione al suo normale stato operativo, con le macchine virtuali dello storage di origine di sincronizzazione (SVM) sul sito di emergenza attive e i dati provenienti dai pool di dischi locali.

Prima di iniziare

- Il cluster di emergenza deve essere passato correttamente al cluster esistente.
- La riparazione deve essere stata eseguita sui dati e sugli aggregati root.
- I nodi del cluster sopravvissuti non devono trovarsi nello stato di failover ha (tutti i nodi devono essere attivi e in esecuzione per ogni coppia ha).

- I moduli controller del sito di emergenza devono essere completamente avviati e non in modalità ha Takeover.
- L'aggregato root deve essere mirrorato.
- I collegamenti Inter-Switch (ISL) devono essere online.
- Tutte le licenze richieste devono essere installate sul sistema.

Fasi

1. Verificare che tutti i nodi siano nello stato abilitato:

   ```
   metrocluster node show
   ```

   Nell'esempio seguente vengono visualizzati i nodi che si trovano nello stato "Enabled" (attivato):

   ```
   cluster_B::>  metrocluster node show

   DR                        Configuration  DR
   Group Cluster Node        State          Mirroring Mode
   ----- ------- ----------- -------------- --------- --------------------
   1     cluster_A
                 node_A_1    configured     enabled   heal roots completed
                 node_A_2    configured     enabled   heal roots completed
         cluster_B
                 node_B_1    configured     enabled   waiting for
   switchback recovery
                 node_B_2    configured     enabled   waiting for
   switchback recovery
   4 entries were displayed.
   ```

2. Verificare che la risincronizzazione sia completa su tutte le SVM:

   ```
   metrocluster vserver show
   ```

3. Verificare che tutte le migrazioni LIF automatiche eseguite dalle operazioni di riparazione siano state completate correttamente:

   ```
   metrocluster check lif show
   ```

4. Eseguire lo switchback eseguendo il seguente comando da qualsiasi nodo del cluster esistente.

   ```
   metrocluster switchback
   ```

5. Controllare l'avanzamento dell'operazione di switchback:

   ```
   metrocluster show
   ```

   L'operazione di switchback è ancora in corso quando l'output visualizza "Waiting-for-switchback" (in attesa di switchback):

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

L'operazione di switchback è completa quando l'output visualizza "normale":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

Se il completamento di uno switchback richiede molto tempo, è possibile verificare lo stato delle linee di base in corso utilizzando il comando seguente a livello di privilegi avanzati.

```
metrocluster config-replication resync-status show
```

6. Ripristinare le configurazioni SnapMirror o SnapVault.

   In ONTAP 8.3, è necessario ristabilire manualmente una configurazione di SnapMirror persa dopo un'operazione di switchback MetroCluster. In ONTAP 9.0 e versioni successive, la relazione viene ristabilita automaticamente.

Verifica di uno switchback riuscito

Dopo aver eseguito lo switchback, si desidera confermare che tutti gli aggregati e le macchine virtuali di storage (SVM) siano ripristinati e in linea.

Fasi

1. Verificare che gli aggregati di dati di switchover siano ripristinati:

   ```
   storage aggregate show
   ```

   Nell'esempio seguente, aggr_b2 sul nodo B2 è tornato:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

Se il sito di disastro includeva aggregati senza mirror e gli aggregati senza mirror non sono più presenti, l'aggregato potrebbe essere visualizzato con uno stato "sconosciuto" nell'output di `storage aggregate show` comando. Contattare il supporto tecnico per rimuovere le voci non aggiornate per gli aggregati senza mirror e consultare l'articolo della Knowledge base "Come rimuovere le voci aggregate obsolete senza mirror in un MetroCluster in seguito a un disastro in cui lo storage è stato perso."

2. Verificare che tutte le SVM di destinazione della sincronizzazione sul cluster sopravvissuto siano inattive (mostrando uno stato di amministrazione "arrestato") e che le SVM di origine della sincronizzazione sul cluster di emergenza siano attive e in esecuzione:

   ```
   vserver show -subtype sync-source
   ```

```
node_B_1::> vserver show -subtype sync-source
                               Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                               running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                               Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                          stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Gli aggregati Sync-destination nella configurazione MetroCluster hanno il suffisso "-mc" aggiunto automaticamente al loro nome per facilitarne l'identificazione.

3. Verificare che le operazioni di switchback siano riuscite:

   `metrocluster operation show`

Se l'output del comando mostra…	Quindi…
Che lo stato operativo di switchback sia riuscito.	Il processo di switchback è completo ed è possibile procedere con il funzionamento del sistema.
Che l'operazione di switchback o. `switchback-continuation-agent` operazione parzialmente riuscita.	Eseguire la correzione suggerita nell'output di `metrocluster operation show` comando.

Al termine

Ripetere le sezioni precedenti per eseguire il switchback nella direzione opposta. Se Site_A ha eseguito uno

switchover di Site_B, chiedere a Site_B di eseguire uno switchover di Site_A.

Eliminazione di elenchi aggregati obsoleti dopo lo switchback

In alcuni casi, dopo lo switchback, si potrebbe notare la presenza di aggregati *obsoleti*. Gli aggregati obsoleti sono aggregati che sono stati rimossi da ONTAP, ma le cui informazioni rimangono registrate su disco. Gli aggregati obsoleti vengono visualizzati con `nodeshell aggr status -r` ma non con `storage aggregate show` comando. È possibile eliminare questi record in modo che non vengano più visualizzati.

A proposito di questa attività

Gli aggregati obsoleti possono verificarsi se si riallocano gli aggregati mentre la configurazione MetroCluster era in switchover. Ad esempio:

1. Il sito A passa al sito B.
2. Si elimina il mirroring per un aggregato e si ricolloca l'aggregato da Node_B_1 a Node_B_2 per il bilanciamento del carico.
3. Si esegue la riparazione aggregata.

A questo punto viene visualizzato un aggregato obsoleto su Node_B_1, anche se l'aggregato effettivo è stato cancellato da quel nodo. Questo aggregato viene visualizzato nell'output di `nodeshell aggr status -r` comando. Non viene visualizzato nell'output di `storage aggregate show` comando.

1. Confrontare l'output dei seguenti comandi:

   ```
   storage aggregate show
   ```

   ```
   run local aggr status -r
   ```

   Gli aggregati obsoleti vengono visualizzati in `run local aggr status -r` output ma non in `storage aggregate show` output. Ad esempio, il seguente aggregato potrebbe essere visualizzato in `run local aggr status -r` uscita:

```
Aggregate aggr05 (failed, raid_dp, partial) (block checksums)
Plex /aggr05/plex0 (offline, failed, inactive)
  RAID group /myaggr/plex0/rg0 (partial, block checksums)

 RAID Disk Device  HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)
Phys (MB/blks)
 --------- ------  ------------- ---- ---- ----  ----- --------------
--------------
 dparity   FAILED          N/A                        82/ -
 parity    0b.5    0b    -   -   SA:A   0 VMDISK  N/A 82/169472
88/182040
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 Raid group is missing 7 disks.
```

2. Rimuovere l’aggregato obsoleta:

   a. Dal prompt di entrambi i nodi, passare al livello di privilegio avanzato:

      ```
      set -privilege advanced
      ```

   Devi rispondere con `y` quando viene richiesto di passare alla modalità avanzata e di visualizzare il prompt della modalità avanzata (*).

   a. Rimuovere l’aggregato obsoleta:

      ```
      aggregate remove-stale-record -aggregate aggregate_name
      ```

   b. Tornare al livello di privilegio admin:

      ```
      set -privilege admin
      ```

3. Confermare che il record aggregato obsoleta è stato rimosso:

   ```
   run local aggr status -r
   ```

Note legali

Le note legali forniscono l’accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all’indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Informazioni sulla sicurezza e avvisi normativi

https://library.netapp.com/ecm/ecm_download_file/ECMP12475945