



Configurare i componenti hardware di MetroCluster

ONTAP MetroCluster

NetApp
April 25, 2024

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

Sommario

- Configurare i componenti hardware di MetroCluster 1
 - Parti di una configurazione IP MetroCluster..... 1
 - Componenti IP MetroCluster richiesti e convenzioni di denominazione 5
 - Scaffalatura dei componenti hardware..... 9
 - Collegare via cavo gli switch IP MetroCluster 10
 - Cablaggio delle porte di peering, dati e gestione del controller 27
 - Configurare gli switch IP di MetroCluster 28

Configurare i componenti hardware di MetroCluster

Parti di una configurazione IP MetroCluster

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

Elementi hardware chiave

Una configurazione MetroCluster IP include i seguenti elementi hardware principali:

- Controller di storage

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

- Rete IP

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

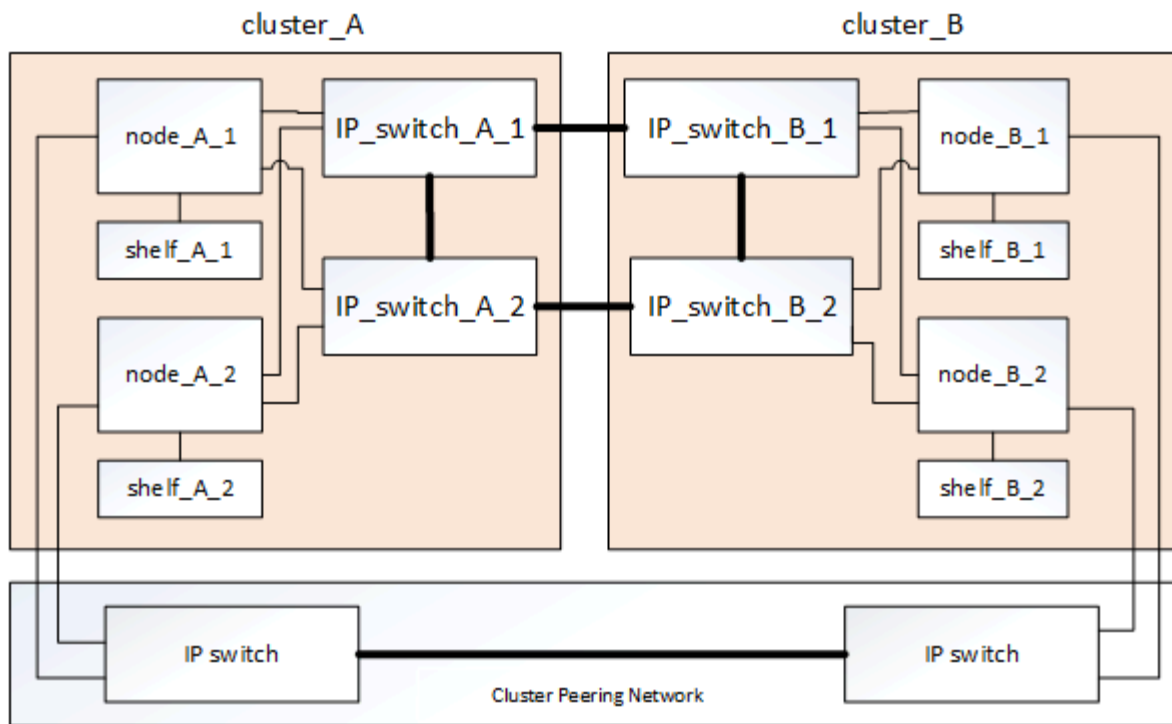
- Connettività cluster standard per comunicazioni intra-cluster.

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

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

- Rete di peering del cluster

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



Gruppi di disaster recovery (DR)

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

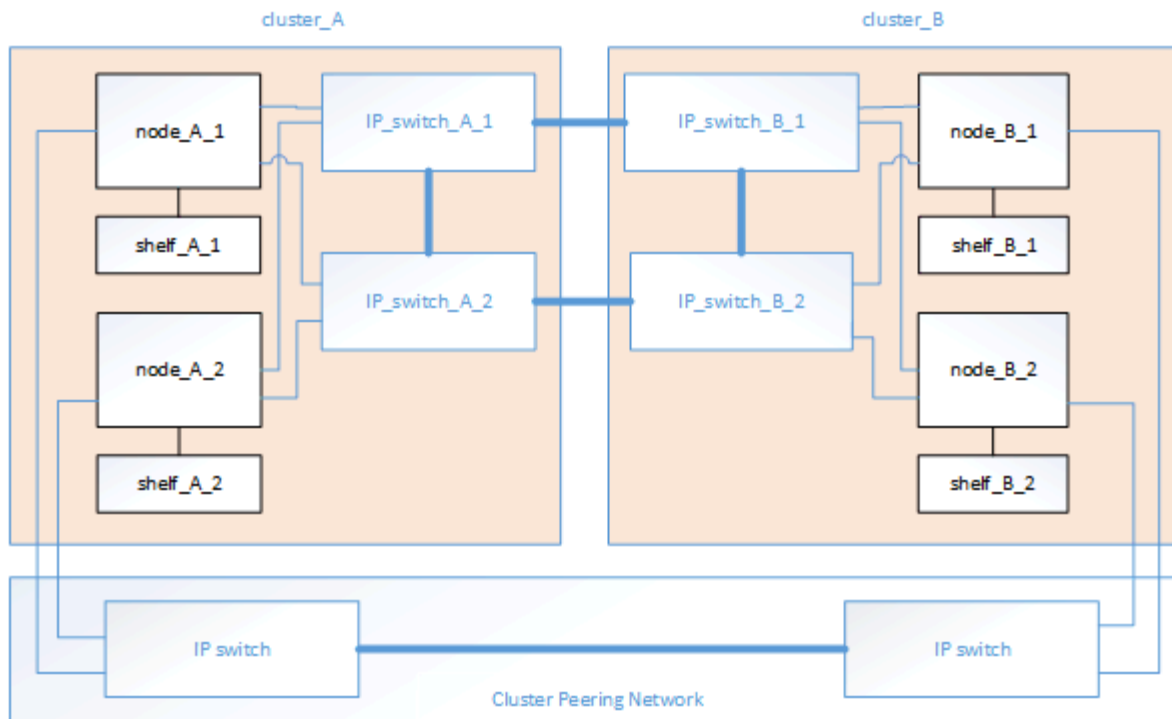
La figura seguente mostra l'organizzazione dei nodi in una configurazione MetroCluster a quattro nodi:



Immagine delle coppie ha locali in una configurazione MetroCluster

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

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

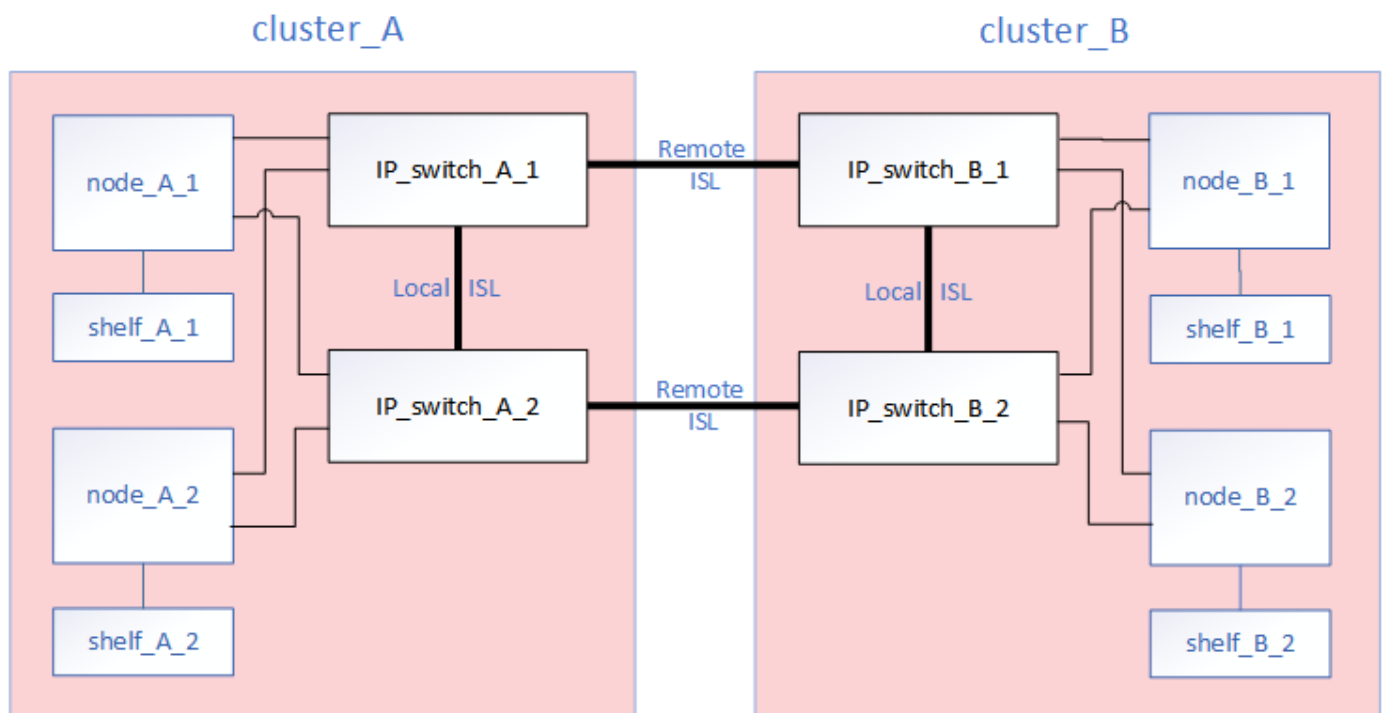


Informazioni correlate

"Concetti di ONTAP"

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

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

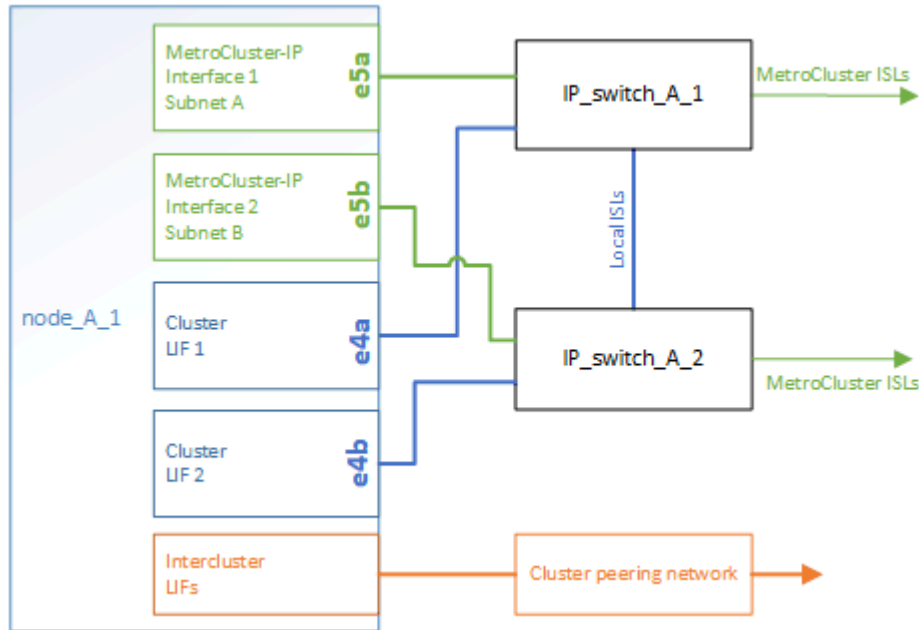


Ogni nodo nella configurazione IP MetroCluster dispone di interfacce dedicate per la connessione alla rete IP

back-end:

- Due interfacce IP MetroCluster
- Due interfacce cluster locali

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



Informazioni correlate

["Considerazioni per le configurazioni MetroCluster IP"](#)

Immagine della rete di peering del cluster

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

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



Informazioni correlate

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

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

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

["Peering dei cluster"](#)

Componenti IP MetroCluster richiesti e convenzioni di denominazione

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

Software e hardware supportati

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

["NetApp Hardware Universe"](#)

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

Requisiti di ridondanza dell'hardware in una configurazione MetroCluster IP

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

arbitrariamente i numeri 1 e 2.

Requisiti del cluster ONTAP in una configurazione IP MetroCluster

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

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

Nomi di esempio:

- Sito A: Cluster_A
- Sito B: Cluster_B

Requisiti dello switch IP in una configurazione IP MetroCluster

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

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

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

Nomi di esempio:

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

Requisiti del modulo controller in una configurazione IP MetroCluster

Le configurazioni MetroCluster IP richiedono quattro o otto moduli controller.

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

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

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

Nomi di esempio

Nella documentazione vengono utilizzati i seguenti nomi di esempio:

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

Requisiti dell'adattatore Gigabit Ethernet in una configurazione MetroCluster IP

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

Modello di piattaforma	Adattatore Gigabit Ethernet richiesto	Slot richiesto per l'adattatore	Porte
AFF A900, ASAA900 e FAS9500	X91146A	Slot 5, slot 7	e5b, e7b
AFF A700 e FAS9000	X91146A-C.	Slot 5	e5a, e5b
AFF A800, AFF C800, ASAA800 e ASA C800	X1146A/porte integrate	Slot 1	e0b, e1b
FAS8300, AFF A400, ASAA400, ASA C400 e AFF C400	X1146A	Slot 1	e1a, e1b
AFF A300 e FAS8200	X1116A	Slot 1	e1a, e1b
FAS2750, AFF A150, ASAA150 e AFF A220	Porte integrate	Slot 0	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250 e AFF C250	Porte integrate	Slot 0	e0c, e0d
AFF A320	Porte integrate	Slot 0	e0g, e0h

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

Requisiti di pool e disco (supporto minimo)

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

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

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

- Almeno sette dischi in ciascun pool.

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

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

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

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

Le configurazioni MetroCluster supportano RAID-DP e RAID4.

Considerazioni sulla posizione dei dischi per gli shelf parzialmente popolati

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

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

Considerazioni sulla posizione dei dischi interni di AFF A800

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

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

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

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

- Quattro dischi nel primo trimestre: 0, 1, 2, 3

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

Combinazione di moduli IOM12 e IOM 6 in uno stack

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

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

Scaffalatura dei componenti hardware

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

A proposito di questa attività

Questa attività deve essere eseguita su entrambi i siti MetroCluster.

Fasi

1. Pianificare il posizionamento dei componenti di MetroCluster.

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Installare gli switch IP nel rack o nell'armadietto.

5. Installare gli shelf di dischi, accenderli, quindi impostare gli ID degli shelf.

- È necessario spegnere e riaccendere ogni shelf di dischi.
- Per agevolare la risoluzione dei problemi, si consiglia di utilizzare ID shelf univoci per ogni shelf di dischi SAS all'interno di ciascun gruppo di DR MetroCluster.



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

Collegare via cavo gli switch IP MetroCluster

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

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

Prima di iniziare

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

Cablaggio di configurazioni MetroCluster a otto nodi

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

A proposito di questa attività

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

Ad esempio, la configurazione include quanto segue:

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

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

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

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

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

Utilizzare questa panoramica dei cavi per verificare il cablaggio.

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

Collegamento di due configurazioni MetroCluster agli switch

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

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

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

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

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

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

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

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

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

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



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

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

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

Esaminare queste considerazioni prima di utilizzare le tabelle:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Leggere queste informazioni prima di utilizzare le tabelle:

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

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

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

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

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

Note a cui si fa riferimento nelle tabelle:

- **Nota 1:** L'utilizzo di queste porte richiede una licenza aggiuntiva.
- **Nota 2:** È possibile collegare allo switch solo un singolo MetroCluster a quattro nodi che utilizza sistemi AFF A320.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Visualizza la configurazione del portachiavi:


```
show key chain name
```

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

Configurare un criterio MACsec

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Creare un criterio MACsec:

```
macsec policy name
```

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

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

```
cipher-suite name
```

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

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

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

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

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

```
security-policy security policy
```

Scegliere una policy di sicurezza tra le seguenti opzioni:

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

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

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



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

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

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

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

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

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

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

```
conf-offsetconfidentiality offset
```

Scegliere una delle seguenti opzioni:

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

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



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

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

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

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

10. Visualizzare la configurazione del criterio MACsec:

```
show macsec policy
```

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

Abilitare la crittografia Cisco MACsec sulle interfacce

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Selezionare l'interfaccia configurata con la crittografia MACsec.

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

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

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

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

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

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

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

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

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

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

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Disattivare la configurazione MACsec sul dispositivo:

```
macsec shutdown
```

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



Selezionando l'opzione "no" si ripristina la funzione MACsec.

3. Selezionare l'interfaccia già configurata con MACsec.

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

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

4. Rimuovere il portachiavi e il criterio configurati sull'interfaccia per rimuovere la configurazione MACsec:

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

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

5. Ripetere i passaggi 3 e 4 su tutte le interfacce in cui è configurato MACsec.

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

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

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

Verifica della configurazione MACsec

Fasi

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

È possibile verificare la configurazione MACsec utilizzando i seguenti comandi:

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

Configurare lo switch NVIDIA IP SN2100

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

Ripristina le impostazioni predefinite dello switch NVIDIA IP SN2100

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

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

ripristinare lo switch utilizzando l'opzione del file RCF

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

A proposito di questa attività

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

I seguenti dettagli di configurazione non vengono ripristinati:

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



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

Prima di iniziare

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

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

Fasi

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



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

```

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

```

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

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

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

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

reimpostare lo switch utilizzando l'opzione di installazione di Cumulus

A proposito di questa attività

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

Prima di iniziare

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



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

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

Fasi

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

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

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



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

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

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

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



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

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



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

```
Debian GNU/Linux 10 cumulus ttyS0

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

Welcome to NVIDIA Cumulus (R) Linux (R)

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

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configurare l'interfaccia di rete di gestione.



L'esempio seguente mostra come configurare il nome host (IP_switch_A_1), l'indirizzo IP (10.10.10.10), la netmask (255.255.255.0 (24)) e il gateway (10.10.10.1) utilizzando i comandi: `net add hostname <hostname>`, `net add interface eth0 ip address <IPAddress/mask>`, e `net add interface eth0 ip gateway <Gateway>`.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending
```

```
.
.
.
```

```
cumulus@cumulus:mgmt:~$ net commit
```

```
.
.
.
```

net add/del commands since the last "net commit"

User Timestamp Command

```
cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1
```

```
cumulus@cumulus:mgmt:~$
```

6. Riavviare lo switch utilizzando `sudo reboot` comando.

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

Al riavvio dello switch, è possibile applicare una nuova configurazione seguendo la procedura descritta in [Scaricare e installare il file NVIDIA RCF](#).

Scarica e installa i file NVIDIA RCF

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

Prima di iniziare

- È necessario disporre della password root per `sudo` accesso ai comandi.
- Il software dello switch è installato e la rete di gestione è configurata.

- È stata eseguita la procedura per installare inizialmente lo switch utilizzando il metodo 1 o il metodo 2.
- Non è stata applicata alcuna configurazione aggiuntiva dopo l'installazione iniziale.



Se si esegue un'ulteriore configurazione dopo aver reimpostato lo switch e prima di applicare il file RCF, non è possibile utilizzare questa procedura.

A proposito di questa attività

Ripetere questa procedura su ciascuno switch IP nella configurazione MetroCluster IP (nuova installazione) o sullo switch sostitutivo (sostituzione dello switch).

Fasi

1. Generare i file NVIDIA RCF per MetroCluster IP.
 - a. Scaricare il ["RcfFileGenerator per MetroCluster IP"](#).
 - b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.
 - c. Accedere alla home directory. Se si è registrati come 'cumulo', il percorso del file è /home/cumulus.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

- d. Scaricare il file RCF in questa directory. L'esempio seguente mostra che si utilizza SCP per scaricare il file MSN2100_v1.0_IP_switch_A_1.txt dal server '50.50.50.50' alla home directory e salvarlo con nome MSN2100_v1.0_IP_switch_A_1.py:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/MSN2100_v1.0_IP_switch_A_1.txt
./MSN2100_v1.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*****
**
Banner of the SCP server
*****
**
username@50.50.50.50's password:
MSN2100_v1.0-X2_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Eseguire il file RCF. Il file RCF richiede un'opzione per applicare uno o più passaggi. Se non richiesto dal supporto tecnico, eseguire il file RCF senza l'opzione della riga di comando. Per verificare lo stato di completamento delle varie fasi del file RCF, utilizzare l'opzione '-1' o 'all' per applicare tutte le fasi (in sospenso).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes

... the steps will apply - this is generating a lot of output ...

Running Step 24: Final reboot of the switch

... The switch will reboot if all steps applied successfully ...
```

Disattivare le porte e i canali delle porte ISL non utilizzati

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

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



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

```
net show interface
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati utilizzando il file RCF.

```

cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version   : 5.4.0
    Running RCF file version  : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
    sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$

```

Il seguente comando di esempio disattiva la porta "swp14":

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Ripetere questo passaggio per ogni porta o canale di porta non utilizzato identificato.

Configurare gli switch IP MetroCluster per il monitoraggio dello stato

Nelle configurazioni IP di MetroCluster, è possibile configurare SNMPv3 per monitorare lo stato degli switch IP.

Passaggio 1: Configurare l'utente SNMPv3 sugli switch IP MetroCluster

Per configurare l'utente SNMPv3 sugli switch IP MetroCluster, procedere come segue.



Nei comandi è necessario utilizzare sia i protocolli di autenticazione che quelli di privacy. L'utilizzo dell'autenticazione senza privacy non è supportato.

Per gli switch IP Broadcom

Fasi

1. Se il gruppo utenti 'network-admin' non esiste già, crearlo:

```
(IP_switch_1) (Config)# snmp-server group network-admin v3 auth read  
"Default"
```

2. Confermare che il gruppo "network-admin" è stato creato:

```
(IP_switch_1) (Config)# show snmp group
```

3. Configurare l'utente SNMPv3 sugli switch IP Broadcom:

```
(IP_switch_1)# config  
(IP_switch_1) (Config)# snmp-server user <user_name> network-admin  
[auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]  
"<priv_password>"
```

È necessario utilizzare le virgolette intorno alle password di autenticazione e privacy, come illustrato nell'esempio seguente:

```
snmp-server user admin1 network-admin auth-md5 "password" priv-des  
"password"
```

Per gli switch IP Cisco

Fasi

1. Eseguire i seguenti comandi per configurare l'utente SNMPv3 su uno switch IP Cisco:

```
IP_switch_A_1 # configure terminal  
IP_switch_A_1 (config) # snmp-server user <user_name> auth  
[md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
```

2. Verificare che l'utente SNMPv3 sia configurato sullo switch:

```
IP_switch_A_1 (config) # show snmp user <user_name>
```

L'output di esempio riportato di seguito mostra che l'utente admin È configurato per SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User          Auth          Priv(enforce) Groups
acl_filter
_____
_____
admin          md5          aes-128(no)  network-admin
```

Passaggio 2: Configurare l'utente SNMPv3 in ONTAP

Per configurare l'utente SNMPv3 in ONTAP, procedere come segue.

1. Configurare l'utente SNMPv3 in ONTAP:

```
security login create -user-or-group-name <user_name> -application snmp
-authentication-method usm -remote-switch-ipaddress <ip_address>
```

2. Configurare il monitoraggio dello stato dello switch per monitorare lo switch utilizzando il nuovo utente SNMPv3:

```
system switch ethernet modify -device <device_id> -snmp-version SNMPv3
-community-or-username <user_name>
```

3. Verificare che il numero di serie della periferica che verrà monitorato con l'utente SNMPv3 appena creato sia corretto:

a. Visualizzare il periodo di tempo di polling del monitoraggio dello stato dello switch:

```
system switch ethernet polling-interval show
```

b. Eseguire il comando seguente dopo aver esaurito il tempo di polling:

```
system switch ethernet show-all -instance -device <device_serial_number>
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.