Riferimento alla configurazione SAN

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/san-config/index.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Riferimento alla configurazione SAN . . . 1
- Informazioni sulla configurazione SAN di ONTAP . . . 1
- Configurazioni iSCSI . . . 1
  - Configurare le reti iSCSI con i sistemi ONTAP . . . 1
  - Vantaggi dell'utilizzo di VLAN con sistemi ONTAP nelle configurazioni iSCSI . . . 3
- Configurazioni FC . . . 4
  - Configurare i fabric FC o FC-NVME con i sistemi ONTAP . . . 4
  - Best practice per la configurazione degli switch FC con i sistemi ONTAP . . . 6
  - Configurazione consigliata delle porte di destinazione FC e velocità per sistemi ONTAP . . . 6
  - Configurare le porte dell'adattatore FC ONTAP . . . 7
  - Comandi ONTAP per la gestione degli adattatori FC . . . 10
  - Evitare la perdita di connettività a un sistema ONTAP utilizzando un adattatore X1133A-R6 . . . 12
- Configurazioni FCoE . . . 12
  - Configurare i fabric FCoE con i sistemi ONTAP . . . 12
  - ONTAP supporta le combinazioni di porte di destinazione e iniziatore FCoE . . . 15
- Zoning FC e FCoE . . . 16
  - Scoprite lo zoning FC e FCoE con i sistemi ONTAP . . . 16
  - Configurazioni consigliate per lo zoning FC e FCoE per i sistemi ONTAP . . . 16
- Requisiti per host SAN connessi a sistemi ONTAP e non NetApp . . . 19
- Configurazioni SAN in un ambiente MetroCluster . . . 20
  - Configurazioni SAN supportate in un ambiente ONTAP MetroCluster . . . 20
  - Evitare la sovrapposizione delle porte durante lo switchover e lo switchback della ONTAP MetroCluster . . . 20
- Supporto ONTAP per multipathing di host SAN . . . 23
  - Numero consigliato di percorsi da host a nodi nel cluster . . . 23
- Limiti di configurazione . . . 24
  - Determina il numero massimo di nodi e host SAN supportati per il cluster ONTAP . . . 24
  - Limiti di configurazione e supporto degli array SAN all-flash . . . 25
  - Limiti di configurazione per gli switch FC utilizzati con i sistemi ONTAP . . . 27
  - Numero massimo di nodi FC e FCoE supportati in ONTAP . . . 28
  - Calcolare la profondità della coda per gli host FC ONTAP . . . 28
  - Consente di modificare le profondità delle code per gli host SAN ONTAP . . . 30

Riferimento alla configurazione SAN

Informazioni sulla configurazione SAN di ONTAP

Una rete SAN è costituita da una soluzione storage connessa agli host tramite un protocollo di trasporto SAN come iSCSI o FC. È possibile configurare la RETE SAN in modo che la soluzione di storage si colleghi agli host tramite uno o più switch. Se si utilizza iSCSI, è anche possibile configurare la SAN in modo che la soluzione di storage si colleghi direttamente all'host senza utilizzare uno switch.

In una SAN, più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere alla soluzione di storage contemporaneamente. È possibile utilizzare "Mappatura selettiva delle LUN" e. "portset" per limitare l'accesso ai dati tra gli host e lo storage.

Per iSCSI, la topologia di rete tra la soluzione di storage e gli host viene definita rete. Per FC, FC/NVMe e FCoE la topologia della rete tra la soluzione di storage e gli host è indicata come fabric. Per creare la ridondanza, che protegge dai rischi di perdita dell'accesso ai dati, è necessario impostare la SAN con coppie ha in una configurazione multi-network o multi-fabric. Le configurazioni che utilizzano nodi singoli o reti/fabric singoli non sono completamente ridondanti, quindi non sono consigliate.

Una volta configurato il SAN, è possibile "Provisioning dello storage per iSCSI o FC"oppure è possibile "Eseguire il provisioning dello storage per FC/NVMe". Quindi, è possibile connettersi agli host per iniziare la manutenzione dei dati.

Il supporto del protocollo SAN varia in base alla versione di ONTAP in uso, alla piattaforma e alla configurazione in uso. Per ulteriori informazioni sulla configurazione specifica, consultare la "Tool di matrice di interoperabilità NetApp".

Informazioni correlate

- "Panoramica dell'amministrazione SAN"
- "Configurazione, supporto e limitazioni NVMe"

Configurazioni iSCSI

Configurare le reti iSCSI con i sistemi ONTAP

È necessario configurare la configurazione iSCSI con coppie ha (High Availability) che si collegano direttamente agli host SAN iSCSI o che si connettono agli host tramite uno o più switch IP.

"Coppie HA" Sono definiti come nodi di reporting per i percorsi Active/Optimized e Active/UnOptimized che verranno utilizzati dagli host per accedere alle LUN. Più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere allo storage contemporaneamente. Gli host richiedono che sia installata e configurata una soluzione multipathing supportata che supporti ALUA. I sistemi operativi supportati e le soluzioni multipathing possono essere verificati sul "Tool di matrice di interoperabilità NetApp".

In una configurazione multi-network, esistono due o più switch che collegano gli host al sistema di storage. Le configurazioni multi-rete sono consigliate perché sono completamente ridondanti. In una configurazione a singola rete, è presente uno switch che connette gli host al sistema di storage. Le configurazioni di rete singola non sono completamente ridondanti.

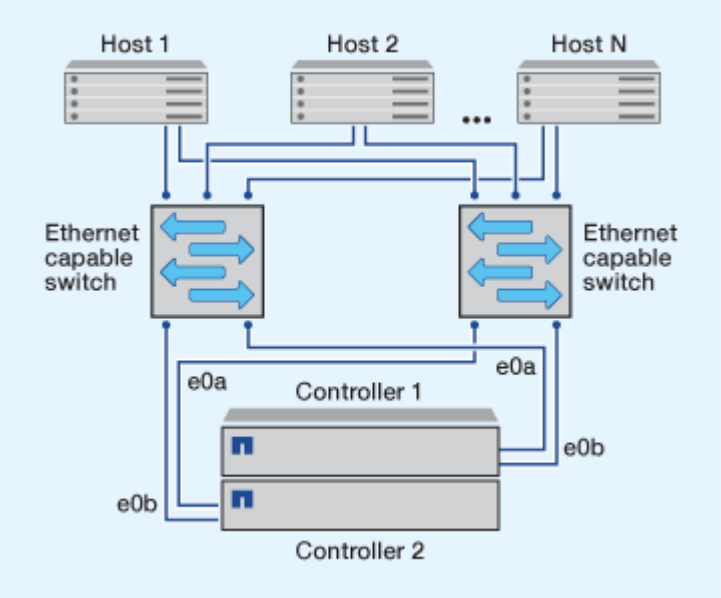
"Configurazioni a nodo singolo" sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

Informazioni correlate

- Scopri come "Mappatura selettiva delle LUN (SLM)" limitare i percorsi utilizzati per accedere alle LUN di proprietà di una coppia ha.
- Scopri di più "LIF SAN".
- Ulteriori informazioni su "Vantaggi delle VLAN in iSCSI".

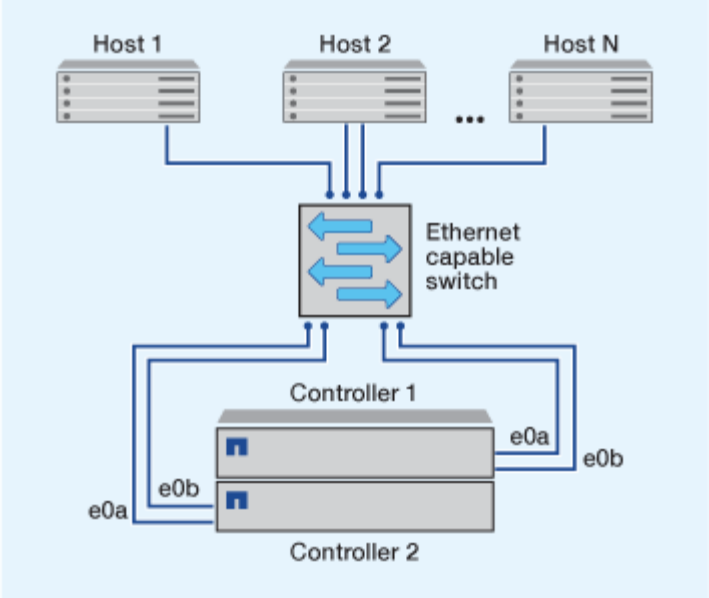
Configurazioni iSCSI multi-rete

Nelle configurazioni di coppia ha multi-rete, due o più switch connettono la coppia ha a uno o più host. Poiché esistono più switch, questa configurazione è completamente ridondante.



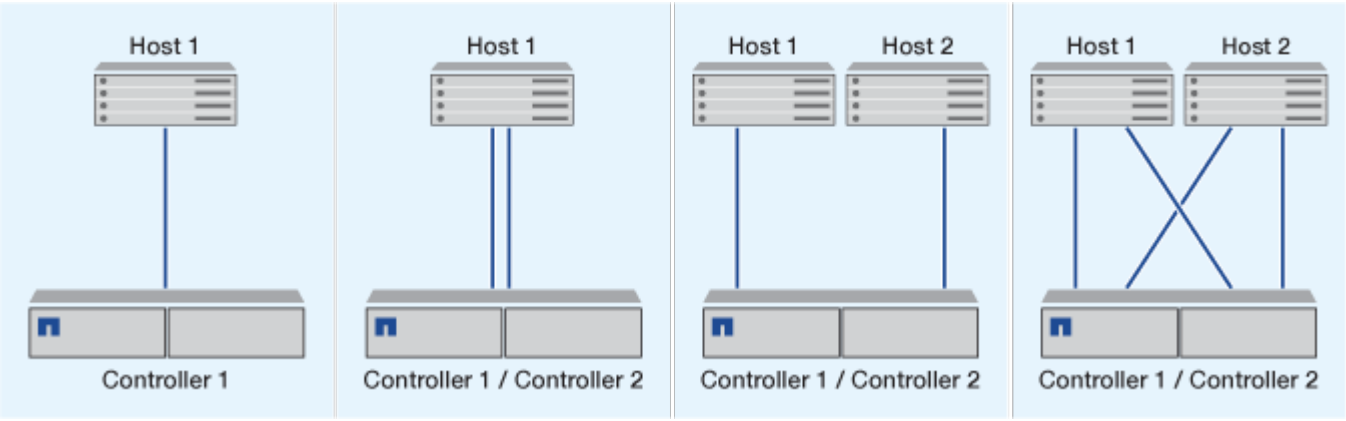
Configurazioni iSCSI a rete singola

Nelle configurazioni a coppia ha a rete singola, uno switch connette la coppia ha a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.



Configurazione iSCSI a collegamento diretto

In una configurazione direct-attached, uno o più host sono collegati direttamente ai controller.



Vantaggi dell'utilizzo di VLAN con sistemi ONTAP nelle configurazioni iSCSI

Una VLAN è costituita da un gruppo di porte dello switch raggruppate in un dominio di broadcast. Una VLAN può essere su un singolo switch o può abbracciare più chassis switch. Le VLAN statiche e dinamiche consentono di aumentare la sicurezza, isolare i problemi e limitare i percorsi disponibili all'interno dell'infrastruttura di rete IP.

Quando si implementano VLAN in infrastrutture di rete IP di grandi dimensioni, si ottengono i seguenti vantaggi:

- Maggiore sicurezza.

  Le VLAN consentono di sfruttare l'infrastruttura esistente pur garantendo una maggiore sicurezza in quanto limitano l'accesso tra diversi nodi di una rete Ethernet o di una SAN IP.

- Maggiore affidabilità della rete Ethernet e della SAN IP grazie all'isolamento dei problemi.
- Riduzione dei tempi di risoluzione dei problemi limitando lo spazio dei problemi.

- Riduzione del numero di percorsi disponibili per una determinata porta di destinazione iSCSI.
- Riduzione del numero massimo di percorsi utilizzati da un host.

  La presenza di troppi percorsi rallenta i tempi di riconnessione. Se un host non dispone di una soluzione multipathing, è possibile utilizzare le VLAN per consentire un solo percorso.

VLAN dinamiche

Le VLAN dinamiche sono basate sull'indirizzo MAC. È possibile definire una VLAN specificando l'indirizzo MAC dei membri che si desidera includere.

Le VLAN dinamiche offrono flessibilità e non richiedono il mapping alle porte fisiche in cui il dispositivo è fisicamente collegato allo switch. È possibile spostare un cavo da una porta all'altra senza riconfigurare la VLAN.

VLAN statiche

Le VLAN statiche sono basate su porta. Lo switch e la porta dello switch vengono utilizzati per definire la VLAN e i relativi membri.

Le VLAN statiche offrono una maggiore sicurezza perché non è possibile violare le VLAN utilizzando lo spoofing MAC (Media Access Control). Tuttavia, se qualcuno ha accesso fisico allo switch, la sostituzione di un cavo e la riconfigurazione dell'indirizzo di rete possono consentire l'accesso.

In alcuni ambienti, è più semplice creare e gestire VLAN statiche rispetto alle VLAN dinamiche. Questo perché le VLAN statiche richiedono solo la specifica dello switch e dell'identificatore della porta, invece dell'indirizzo MAC a 48 bit. Inoltre, è possibile etichettare gli intervalli di porte dello switch con l'identificatore VLAN.

Configurazioni FC

Configurare i fabric FC o FC-NVME con i sistemi ONTAP

Si consiglia di configurare gli host SAN FC e FC-NVMe utilizzando coppie ha e un minimo di due switch. Questo garantisce ridondanza a livello di fabric e di sistema storage per supportare la tolleranza agli errori e le operazioni senza interruzioni. Non è possibile collegare direttamente host FC o FC-NVMe SAN a coppie ha senza utilizzare uno switch.

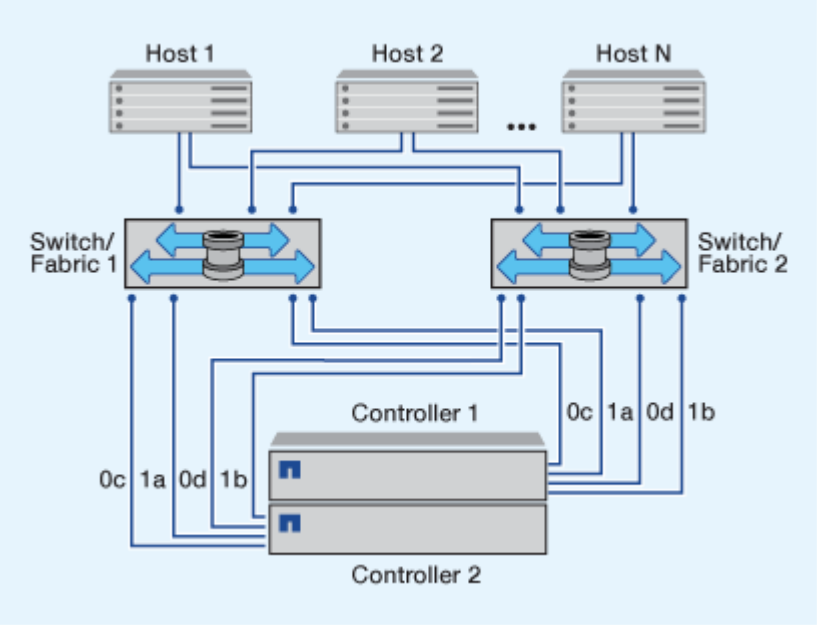
Cascade, Partial Mesh, full mesh, core-edge e director fabric sono tutti metodi standard di settore per collegare switch FC a un fabric e sono tutti supportati. L'utilizzo di fabric switch FC eterogenei non è supportato, tranne nel caso di switch blade integrati. Le eccezioni specifiche sono elencate nella "Tool di matrice di interoperabilità". Un fabric può essere costituito da uno o più switch e i controller di storage possono essere collegati a più switch.

Più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere contemporaneamente ai controller di storage. Gli host richiedono l'installazione e la configurazione di una soluzione multipathing supportata. È possibile verificare i sistemi operativi e le soluzioni multipathing supportate tramite Interoperability Matrix Tool.

Configurazioni FC e FC-NVMe multi-fabric

Nelle configurazioni ha Pair multi-fabric, sono presenti due o più switch che collegano coppie ha a uno o più host. Per semplicità, la seguente figura di coppia ha multi-fabric mostra solo due fabric, ma puoi avere due o più fabric in qualsiasi configurazione multi-fabric.

I numeri delle porte di destinazione FC (0C, 0d, 1a, 1b) nelle illustrazioni sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.

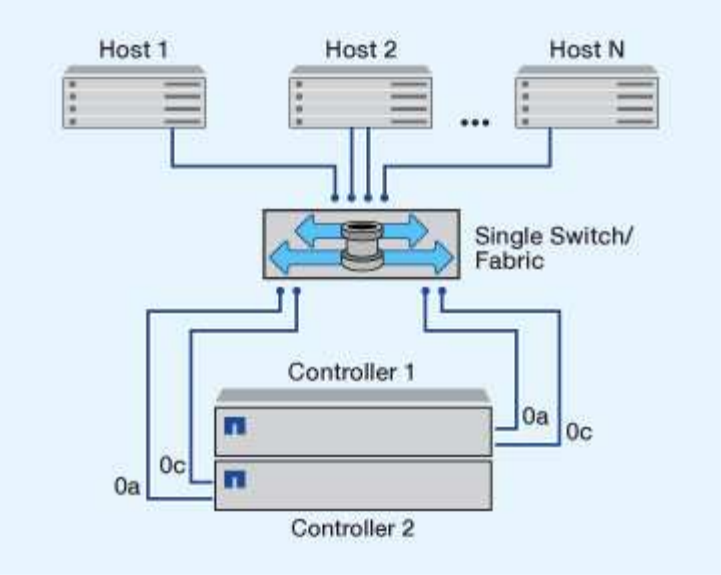


Configurazioni FC e FC-NVMe single-fabric

Nelle configurazioni a coppia ha a fabric singolo, esiste un fabric che collega entrambi i controller della coppia ha a uno o più host. Poiché gli host e i controller sono connessi tramite un singolo switch, le configurazioni ha Pair single-fabric non sono completamente ridondanti.

I numeri delle porte di destinazione FC (0A, 0C) nelle illustrazioni sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.

Tutte le piattaforme che supportano le configurazioni FC supportano le configurazioni ha Pair single-fabric.



"Configurazioni a nodo singolo" sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

Informazioni correlate

- Scopri come "Mappatura selettiva delle LUN (SLM)" limitare i percorsi utilizzati per accedere alle LUN di proprietà di una coppia ha.
- Scopri di più "LIF SAN".

Best practice per la configurazione degli switch FC con i sistemi ONTAP

Per ottenere prestazioni ottimali, è necessario prendere in considerazione alcune Best practice durante la configurazione dello switch FC.

Un'impostazione della velocità di collegamento fissa è la procedura migliore per le configurazioni degli switch FC, in particolare per i fabric di grandi dimensioni, in quanto offre le migliori prestazioni per le ricostruzioni del fabric e può risparmiare significativamente tempo. Sebbene la negoziazione automatica offra la massima flessibilità, la configurazione dello switch FC non sempre funziona come previsto e aggiunge tempo alla sequenza generale di fabric-build.

Tutti gli switch collegati al fabric devono supportare la virtualizzazione NPIV (N_Port ID Virtualization) e attivare NPIV. ONTAP utilizza NPIV per presentare i target FC a un fabric.

Per ulteriori informazioni sugli ambienti supportati, vedere "Tool di matrice di interoperabilità NetApp".

Per le Best practice FC e iSCSI, vedere "Report tecnico NetApp 4080: Best practice per le SAN moderne".

Configurazione consigliata delle porte di destinazione FC e velocità per sistemi ONTAP

È possibile configurare e utilizzare le porte di destinazione FC per il protocollo FC-NVMe nello stesso modo in cui sono configurate e utilizzate per il protocollo FC. Il supporto per il protocollo FC-NVMe varia in base alla tua piattaforma e alla versione di ONTAP. Utilizzare NetApp Hardware Universe per verificare l'assistenza.

Per ottenere le migliori prestazioni e la massima disponibilità, è necessario utilizzare la configurazione della porta di destinazione consigliata indicata in "NetApp Hardware Universe" per la piattaforma specifica.

Configurazione delle porte di destinazione FC con ASIC condivisi

Le seguenti piattaforme dispongono di coppie di porte con circuiti integrati specifici per le applicazioni (ASIC) condivisi. Se si utilizza un adattatore di espansione con queste piattaforme, è necessario configurare le porte FC in modo che non utilizzino lo stesso ASIC per la connettività.

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte consigliate
• FAS8200 • AFF A300	0g+0h	1: 0g 2: 0g, 0h
• FAS2720 • FAS2750 • AFF A220	0c+0d 0e+0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Velocità supportate dalla porta di destinazione FC

Le porte di destinazione FC possono essere configurate per funzionare a velocità diverse. Tutte le porte di destinazione utilizzate da un determinato host devono essere impostate alla stessa velocità. Impostare la velocità della porta di destinazione in modo che corrisponda alla velocità del dispositivo a cui si connette. Non utilizzare la negoziazione automatica per la velocità della porta. Una porta impostata per la negoziazione automatica può richiedere più tempo per riconnettersi dopo un takeover/giveback o un'altra interruzione.

È possibile configurare le porte integrate e gli adattatori di espansione in modo che funzionino alle seguenti velocità. Ogni porta del controller e dell'adattatore di espansione può essere configurata singolarmente per diverse velocità in base alle esigenze.

Porte da 4 GB	Porte da 8 GB	Porte da 16 GB	Porte da 32 GB
• 4 GB • 2 GB • 1 GB	• 8 GB • 4 GB • 2 GB	• 16 GB • 8 GB • 4 GB	• 32 GB • 16 GB • 8 GB

Per un elenco completo delle schede di rete supportate e delle relative velocità supportate, vedere "NetApp Hardware Universe" .

Configurare le porte dell'adattatore FC ONTAP

Gli adattatori FC integrati e alcune schede adattatore FC possono essere configurati singolarmente come iniziatori o porte di destinazione. Gli altri adattatori di espansione FC sono configurati come iniziatori o target in fabbrica e non possono essere modificati. Sono disponibili anche porte FC aggiuntive tramite le schede UTA2 supportate configurate con adattatori FC SFP+.

È possibile utilizzare le porte Initiator per il collegamento diretto agli shelf di dischi back-end e agli array di

storage di altri produttori. Le porte di destinazione possono essere utilizzate per collegare solo switch FC.

Il numero di porte integrate e le porte CNA/UTA2 configurate per FC varia a seconda del modello del controller. Anche gli adattatori di espansione target supportati variano a seconda del modello di controller. Consulta "NetApp Hardware Universe" per un elenco completo delle porte FC integrate e degli adattatori di espansione di destinazione supportati per il tuo modello di controller.

Configurare gli adattatori FC per la modalità Initiator

La modalità iniziatore viene utilizzata per connettere le porte a unità nastro, librerie nastro o sistemi di archiviazione di terze parti con importazione di LUN esterne (FLI).

Prima di iniziare

- Le LIF della scheda di rete devono essere rimosse da tutti i set di porte di cui sono membri.
- Tutti i LIF di ogni macchina virtuale di storage (SVM) che utilizza la porta fisica da modificare devono essere migrati o distrutti prima di cambiare la personalità della porta fisica da destinazione a iniziatore.

NVMe/FC supporta la modalità Initiator.

Fasi

1. Rimuovere tutti i file LIF dalla scheda:

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. Porta l'adattatore offline:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

3. Cambiare la scheda di rete da destinazione a iniziatore:

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. Riavviare il nodo che ospita l'adattatore modificato.
5. Verificare che le porte FC siano configurate nello stato corretto per la configurazione:

```
system hardware unified-connect show
```

6. Riportare l'adattatore online:

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

Configurare gli adattatori FC per la modalità di destinazione

La modalità di destinazione viene utilizzata per collegare le porte agli iniziatori FC.

Vengono eseguite le stesse operazioni per configurare gli adattatori FC per il protocollo FC e il protocollo FC-NVMe. Tuttavia, solo alcuni adattatori FC supportano FC-NVMe. Consulta la "NetApp Hardware Universe" per un elenco di adattatori che supportano il protocollo FC-NVMe.

Fasi

1. Portare l'adattatore offline:

   ```
   node run -node _node_name_ storage disable adapter _adapter_name_
   ```

   Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

2. Cambiare la scheda di rete da iniziatore a destinazione:

   ```
   system node hardware unified-connect modify -t target -node _node_name_
   adapter _adapter_name_
   ```

3. Riavviare il nodo che ospita l'adattatore modificato.
4. Verificare che la porta di destinazione abbia la configurazione corretta:

   ```
   network fcp adapter show -node _node_name_
   ```

5. Porta online il tuo adattatore:

   ```
   network fcp adapter modify -node _node_name_ -adapter _adapter_port_
   -state up
   ```

Configurare la velocità della scheda FC

È necessario configurare la velocità della porta di destinazione della scheda di rete in modo che corrisponda alla velocità del dispositivo a cui si connette, anziché utilizzare la negoziazione automatica. Una porta impostata per la negoziazione automatica può richiedere più tempo per riconnettersi dopo un takeover/giveback o un'altra interruzione.

A proposito di questa attività

Poiché questa attività comprende tutte le macchine virtuali di storage (SVM) e tutte le LIF in un cluster, è necessario utilizzare `-home-port` e. `-home-lif` parametri per limitare l'ambito di questa operazione. Se non si utilizzano questi parametri, l'operazione si applica a tutte le LIF del cluster, cosa che potrebbe non essere auspicabile.

Prima di iniziare

Tutte le LIF che utilizzano questo adattatore come porta home devono essere offline.

Fasi

1. Porta tutti i LIF su questo adattatore offline:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. Portare l'adattatore offline:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

   Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

3. Determinare la velocità massima per l'adattatore porta:

```
fcp adapter show -instance
```

   Non è possibile modificare la velocità della scheda oltre la velocità massima.

4. Modificare la velocità dell'adattatore:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Portare l'adattatore online:

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Portare online tutti i file LIF della scheda di rete:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

Comandi ONTAP per la gestione degli adattatori FC

È possibile utilizzare i comandi FC per gestire gli adattatori di destinazione FC, gli adattatori FC Initiator e gli adattatori FC integrati per lo storage controller. Gli stessi comandi vengono utilizzati per gestire gli adattatori FC per il protocollo FC e il protocollo FC-NVMe.

I comandi FC Initiator Adapter funzionano solo a livello di nodo. È necessario utilizzare `run -node` *`node_name`* Prima di poter utilizzare i comandi FC Initiator Adapter.

Comandi per la gestione degli adattatori di destinazione FC

Se si desidera…	Utilizzare questo comando…
Visualizza le informazioni sulla scheda FC su un nodo	`network fcp adapter show`
Modificare i parametri dell'adattatore di destinazione FC	`network fcp adapter modify`
Visualizza le informazioni sul traffico del protocollo FC	`run -node node_name sysstat -f`
Visualizza per quanto tempo il protocollo FC è in esecuzione	`run -node node_name uptime`
Visualizzare la configurazione e lo stato dell'adattatore	`run -node node_name sysconfig -v adapter`
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	`run -node node_name sysconfig -ac`
Visualizzare una pagina man per un comando	`man command_name`

Comandi per la gestione degli adattatori FC Initiator

Se si desidera…	Utilizzare questo comando…
Visualizza le informazioni per tutti gli iniziatori e i relativi adattatori in un nodo	`run -node node_name storage show adapter`
Visualizzare la configurazione e lo stato dell'adattatore	`run -node node_name sysconfig -v adapter`
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	`run -node node_name sysconfig -ac`

Comandi per la gestione degli adattatori FC integrati

Se si desidera…	Utilizzare questo comando…
Visualizza lo stato delle porte FC integrate	`system node hardware unified-connect show`

Informazioni correlate

- "adattatore fcp di rete"

Evitare la perdita di connettività a un sistema ONTAP utilizzando un adattatore X1133A-R6

È possibile evitare la perdita di connettività durante un errore di porta configurando il sistema con percorsi ridondanti per separare gli HBA X1133A-R6.

X1133A-R6 HBA è un adattatore FC da 16 GB a 4 porte composto da due coppie di 2 porte. L'adattatore X1133A-R6 può essere configurato come modalità di destinazione o Initiator. Ogni coppia di 2 porte è supportata da un singolo ASIC (ad esempio, porta 1 e porta 2 su ASIC 1 e porta 3 e porta 4 su ASIC 2). Entrambe le porte di un singolo ASIC devono essere configurate per funzionare nella stessa modalità, sia in modalità di destinazione che in modalità iniziatore. Se si verifica un errore con ASIC che supporta una coppia, entrambe le porte della coppia passano offline.

Per evitare questa perdita di connettività, configurare il sistema con percorsi ridondanti per separare gli HBA X1133A-R6 o con percorsi ridondanti alle porte supportate da diversi ASIC sull'HBA.

Configurazioni FCoE

Configurare i fabric FCoE con i sistemi ONTAP

FCoE può essere configurato in vari modi utilizzando gli switch FCoE. Le configurazioni direct-attached non sono supportate in FCoE.

Tutte le configurazioni FCoE sono dual-fabric, completamente ridondanti e richiedono software di multipathing lato host. In tutte le configurazioni FCoE, è possibile disporre di più switch FCoE e FC nel percorso tra l'iniziatore e la destinazione, fino al limite massimo del numero di hop. Per collegare gli switch tra loro, è necessario che gli switch eseguano una versione del firmware che supporti gli ISL Ethernet. Ogni host in qualsiasi configurazione FCoE può essere configurato con un sistema operativo diverso.

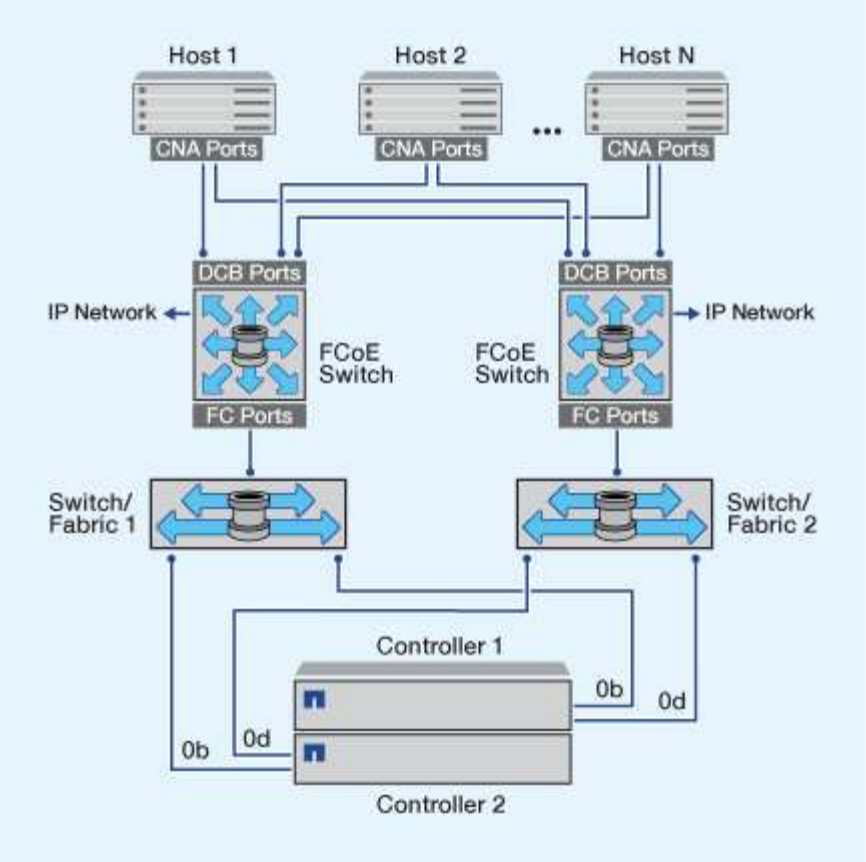
Le configurazioni FCoE richiedono switch Ethernet che supportano esplicitamente le funzionalità FCoE. Le configurazioni FCoE vengono validate attraverso lo stesso processo di interoperabilità e di garanzia della qualità degli switch FC. Le configurazioni supportate sono elencate nella matrice di interoperabilità. Alcuni dei parametri inclusi in queste configurazioni supportate sono il modello di switch, il numero di switch implementabili in un singolo fabric e la versione del firmware dello switch supportata.

I numeri delle porte dell'adattatore di espansione FC target nelle illustrazioni sono esempi. I numeri effettivi delle porte possono variare a seconda degli slot di espansione in cui sono installati gli adattatori di espansione di destinazione FCoE.

Iniziatore FCoE su destinazione FC

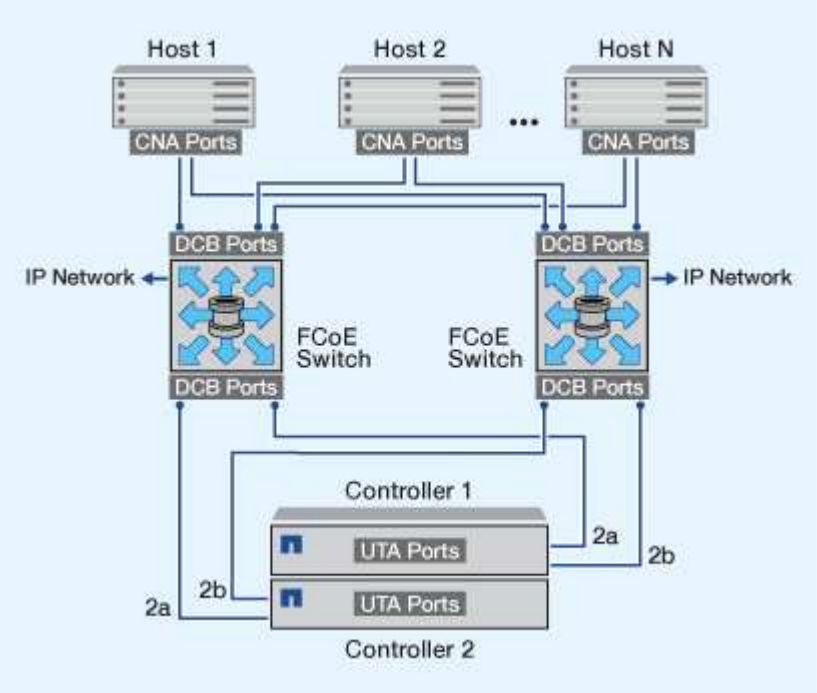
Utilizzando gli iniziatori FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha attraverso gli switch FCoE alle porte di destinazione FC. Lo switch FCoE deve anche disporre di porte FC. L'iniziatore FCoE host si connette sempre allo switch FCoE. Lo switch FCoE può connettersi direttamente alla destinazione FC o alla destinazione FC tramite switch FC.

La figura seguente mostra i CNA host che si collegano a uno switch FCoE e quindi a uno switch FC prima di connettersi alla coppia ha:



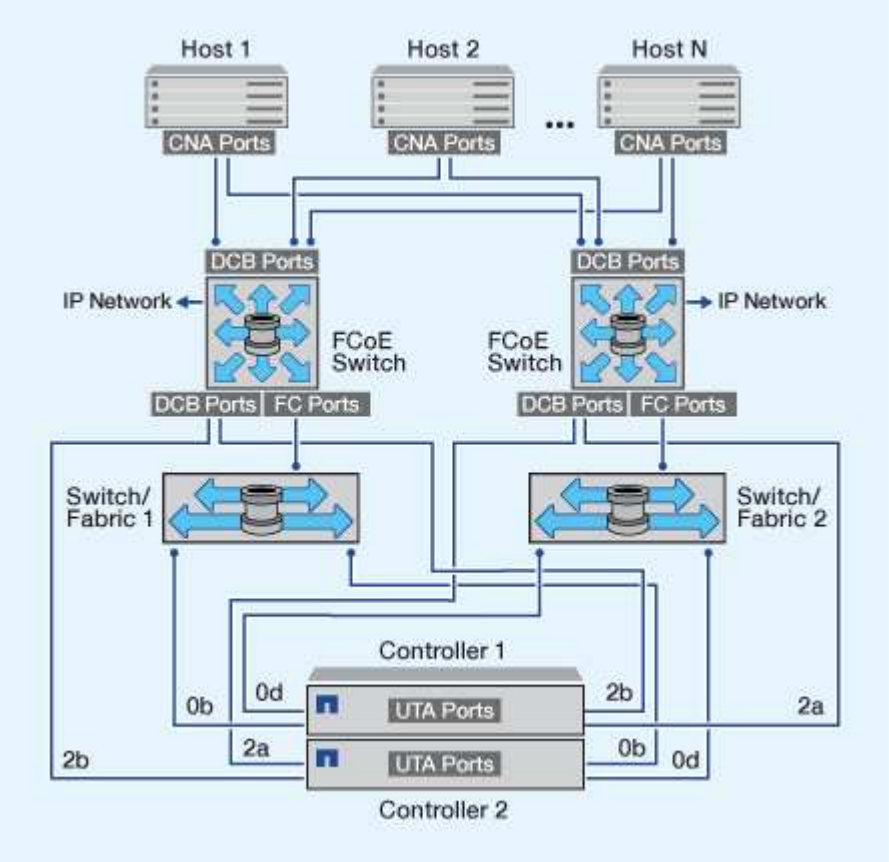
Iniziatore FCoE alla destinazione FCoE

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE.



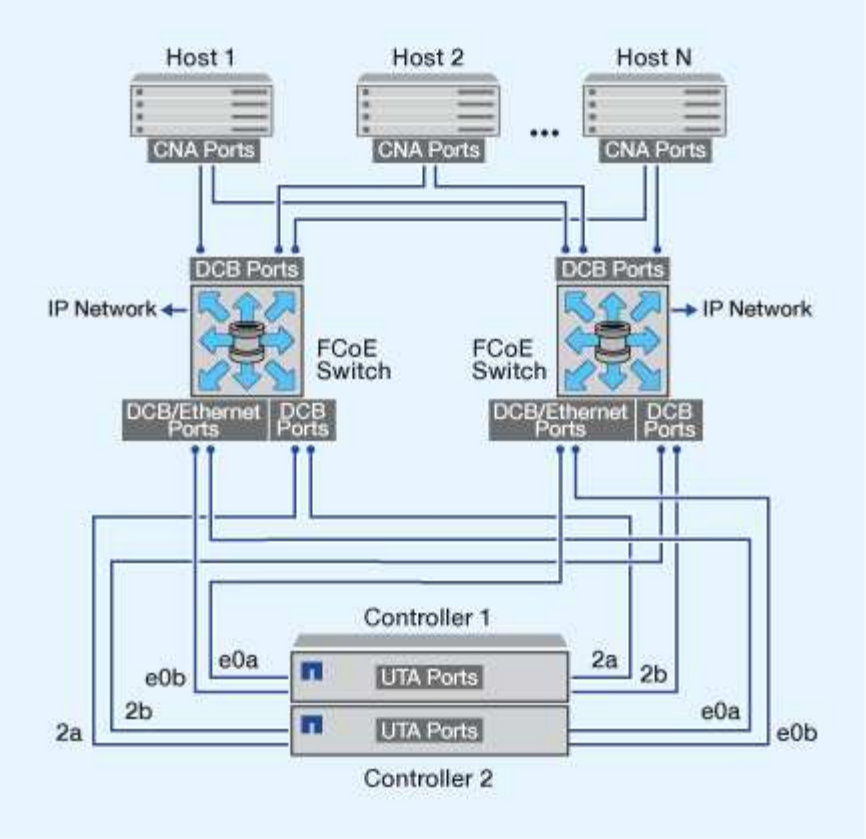
Iniziatore FCoE per destinazioni FCoE e FC

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE e FC (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE.



FCoE combinato con i protocolli di storage IP

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE. Le porte FCoE non possono utilizzare l'aggregazione di collegamenti tradizionale per un singolo switch. Gli switch Cisco supportano un tipo speciale di aggregazione di collegamenti (Virtual Port Channel) che supporta FCoE. Un Virtual Port Channel aggrega i singoli collegamenti a due switch. È inoltre possibile utilizzare Virtual Port Channels per altri tipi di traffico Ethernet. Le porte utilizzate per il traffico diverso da FCoE, tra cui NFS, SMB, iSCSI e altro traffico Ethernet, possono utilizzare le normali porte Ethernet degli switch FCoE.



ONTAP supporta le combinazioni di porte di destinazione e iniziatore FCoE

Sono supportate alcune combinazioni di FCoE e iniziatori e target FC tradizionali.

Iniziatori FCoE

È possibile utilizzare gli iniziatori FCoE nei computer host con destinazioni FCoE e FC tradizionali nei controller di storage. L'iniziatore FCoE host deve connettersi a uno switch FCoE DCB (data center bridging); la connessione diretta a una destinazione non è supportata.

La tabella seguente elenca le combinazioni supportate:

Iniziatore	Destinazione	Supportato?
FC	FC	Sì
FC	FCoE	Sì
FCoE	FC	Sì
FCoE	FCoE	Sì

Obiettivi FCoE

È possibile combinare porte di destinazione FCoE con porte FC da 4 GB, 8 GB o 16 GB sul controller di storage, indipendentemente dal fatto che le porte FC siano adattatori di destinazione aggiuntivi o porte

integrate. È possibile avere sia FCoE che FC Target Adapter nello stesso controller di storage.

Le regole per la combinazione delle porte FC integrate e di espansione sono ancora valide.

Zoning FC e FCoE

Scoprite lo zoning FC e FCoE con i sistemi ONTAP

Una zona FC, FC-NVMe o FCoE è un raggruppamento logico di una o più porte all'interno di un fabric. Affinché i dispositivi siano in grado di vedersi, connettersi, creare sessioni l'uno con l'altro e comunicare, entrambe le porte devono essere membri della stessa zona.

Lo zoning aumenta la sicurezza limitando l'accesso e la connettività agli end-point che condividono una zona comune. Le porte che non si trovano nella stessa zona non possono comunicare tra loro. Questo riduce o elimina *crosstalk* tra gli HBA iniziatori. In caso di problemi di connettività, lo zoning consente di isolare i problemi a un set specifico di porte, riducendo così i tempi di risoluzione.

Lo zoning riduce il numero di percorsi disponibili per una determinata porta e il numero di percorsi tra un host e il sistema storage. Ad esempio, alcune soluzioni di multipathing del sistema operativo host hanno un limite al numero di percorsi che possono gestire. Lo zoning può ridurre il numero di percorsi visibili all'host in modo che i percorsi verso l'host non superino il numero massimo consentito dal sistema operativo host.

Zoning basato sul nome

La suddivisione in zone in base al nome globale (WWN) specifica il numero WWN dei membri da includere nella zona. Sebbene la suddivisione in zone WWNN (World Wide Node Name) sia possibile con alcuni fornitori di switch, quando si esegue la zoning in ONTAP, è necessario utilizzare la suddivisione in zone WWPN (World Wide Port Name).

La suddivisione in zone WWPN è necessaria per definire correttamente una porta specifica e per utilizzare NPIV in modo efficace. Gli switch FC devono essere zonati utilizzando i WWPN delle interfacce logiche (LIF) di destinazione, non i WWPN delle porte fisiche sul nodo. Le WWPN delle porte fisiche iniziano con "50" e le WWPN delle LIF iniziano con "20".

Lo zoning WWPN offre flessibilità perché l'accesso non è determinato dalla posizione in cui il dispositivo è fisicamente collegato al fabric. È possibile spostare un cavo da una porta all'altra senza riconfigurare le zone.

Configurazioni consigliate per lo zoning FC e FCoE per i sistemi ONTAP

È necessario creare una configurazione di zoning se l'host non dispone di una soluzione multipathing installata, se quattro o più host sono connessi alla SAN o se la mappatura selettiva LUN non è implementata sui nodi nel cluster.

Nella configurazione consigliata dello zoning FC e FCoE, ogni zona include una porta initiator e una o più LIF di destinazione. Questa configurazione consente a ciascun iniziatore dell'host di accedere a qualsiasi nodo, impedendo agli host che accedono allo stesso nodo di vedere le porte degli altri

Aggiungere tutte le LIF dalla Storage Virtual Machine (SVM) alla zona con l'iniziatore dell'host. Ciò consente di spostare volumi o LUN senza modificare le zone esistenti o creare nuove zone.

Configurazioni di zoning a doppio fabric

Sono consigliate configurazioni di zoning dual-fabric perché forniscono protezione contro la perdita di dati a causa di un guasto a un singolo componente. In una configurazione dual-fabric, ogni iniziatore dell'host è connesso a ogni nodo del cluster mediante switch diversi. Se uno switch non è disponibile, l'accesso ai dati viene mantenuto attraverso lo switch rimanente. Per gestire percorsi multipli, è necessario un software multipathing sull'host.

Nella figura seguente, l'host dispone di due iniziatori e sta eseguendo un software multipathing. Esistono due zone. "Mappatura selettiva delle LUN (SLM)" è configurato in modo che tutti i nodi siano considerati come nodi di reporting.

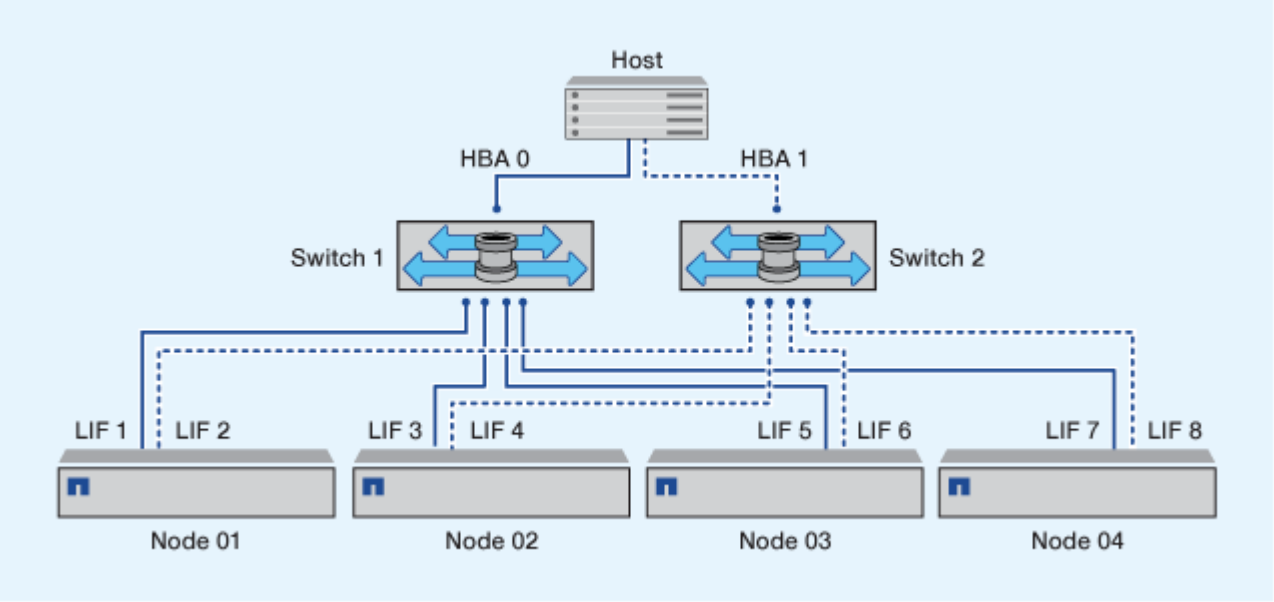
> La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- Zona 1: HBA 0, LIF_1, LIF_3, LIF_5 e LIF_7
- Zona 2: HBA 1, LIF_2, LIF_4, LIF_6 e LIF_8

Ogni iniziatore host viene associato a zone attraverso uno switch differente. L'accesso alla zona 1 avviene tramite l'interruttore 1. L'accesso alla zona 2 avviene tramite l'interruttore 2.

Ogni host può accedere a una LIF su ogni nodo. In questo modo, l'host può continuare ad accedere ai propri LUN in caso di guasto di un nodo. Le SVM hanno accesso a tutte le LIF iSCSI e FC su ogni nodo del cluster in base alla configurazione dei nodi di reporting SLM. È possibile utilizzare lo zoning di SLM, portset o switch FC per ridurre il numero di percorsi da una SVM all'host e il numero di percorsi da una SVM a una LUN.

Se la configurazione include più nodi, le LIF per i nodi aggiuntivi sono incluse in queste zone.



> Il sistema operativo host e il software di multipathing devono supportare il numero di percorsi utilizzati per accedere alle LUN sui nodi.

Zoning a fabric singolo

In una configurazione a fabric singolo, ogni iniziatore dell'host viene connesso a ciascun nodo storage tramite un singolo switch. Le configurazioni di zoning a fabric singolo non sono consigliate in quanto non forniscono

protezione contro la perdita di dati a causa del guasto di un singolo componente. Se si sceglie di configurare la zoning a fabric singolo, ogni host deve avere due initiator per il multipathing per garantire la resilienza nella soluzione. Per gestire percorsi multipli, è necessario un software multipathing sull'host.

Ciascun iniziatore dell'host deve disporre di almeno un LIF per ciascun nodo a cui può accedere l'iniziatore. Lo zoning deve consentire almeno un percorso dall'iniziatore host alla coppia di nodi ha nel cluster per fornire un percorso per la connettività LUN. Ciò significa che ogni iniziatore sull'host potrebbe avere un solo LIF di destinazione per nodo nella configurazione di zona. Se è necessario eseguire il multipath sullo stesso nodo o su più nodi del cluster, ciascun nodo avrà più LIF per nodo nella configurazione della zona. In questo modo, l'host può comunque accedere ai propri LUN in caso di guasto di un nodo o di spostamento di un volume contenente il LUN in un nodo diverso. Ciò richiede inoltre che i nodi di reporting siano impostati in modo appropriato.

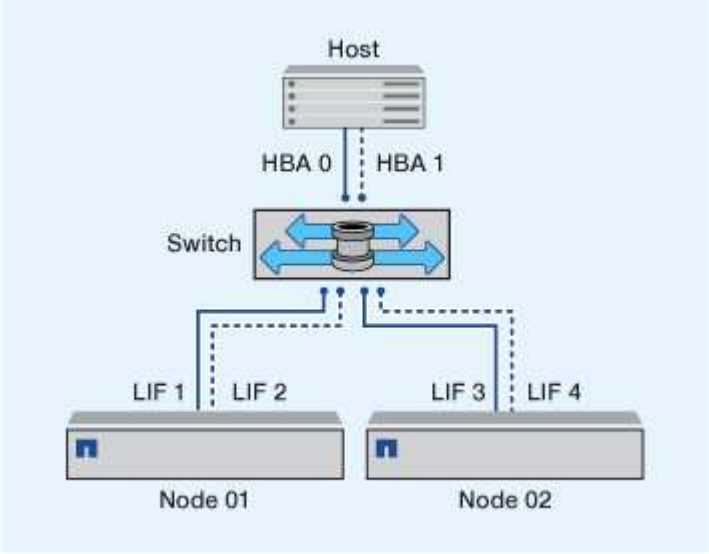
Quando si utilizzano switch Cisco FC e FCoE, una singola zona fabric non deve contenere più LIF di destinazione per la stessa porta fisica. Se più LIF sulla stessa porta si trovano nella stessa zona, le porte LIF potrebbero non riuscire a ripristinarsi a causa di una perdita di connessione.

Nella figura seguente, l'host dispone di due iniziatori e sta eseguendo un software multipathing. Esistono due zone:

> La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- Zona 1: HBA 0, LIF_1 e LIF_3
- Zona 2: HBA 1, LIF_2 e LIF_4

Se la configurazione include più nodi, le LIF per i nodi aggiuntivi sono incluse in queste zone.s.



In questo esempio, è possibile avere tutte e quattro le LIF in ciascuna zona. In tal caso, le zone saranno le seguenti:

- Zona 1: HBA 0, LIF_1, LIF_2, LIF_3 e LIF_4
- Zona 2: HBA 1, LIF_1, LIF_2, LIF_3 e LIF_4

Il sistema operativo host e il software di multipathing devono supportare il numero di percorsi supportati utilizzati per accedere alle LUN sui nodi. Per determinare il numero di percorsi utilizzati per accedere alle LUN sui nodi, vedere la sezione limiti della configurazione SAN.

Restrizioni di zoning per switch Cisco FC e FCoE

Quando si utilizzano gli switch Cisco FC e FCoE, si applicano determinate restrizioni all'utilizzo di porte fisiche e interfacce logiche (LIF) in zone.

Porte fisiche

- FC-NVMe e FC possono condividere la stessa porta fisica da 32 GB
- FC-NVMe e FCoE non possono condividere la stessa porta fisica
- FC e FCoE possono condividere la stessa porta fisica, ma le LIF dei protocolli devono essere in zone separate.

Interfacce logiche (LIF)

- Una zona può contenere una LIF di ogni porta di destinazione del cluster.

  Verificare la configurazione SLM in modo da non superare il numero massimo di percorsi consentito all'host.

- Ogni LIF di una data porta deve trovarsi in una zona separata dalle altre LIF di quella porta
- Le LIF su diverse porte fisiche possono trovarsi nella stessa zona.

Requisiti per host SAN connessi a sistemi ONTAP e non NetApp

Le configurazioni SAN condivise sono definite come host collegati sia ai sistemi storage ONTAP che ai sistemi storage di altri vendor. L'accesso ai sistemi storage ONTAP e ai sistemi storage di altri vendor da un singolo host è supportato purché vengano soddisfatti diversi requisiti.

Per tutti i sistemi operativi host, è consigliabile utilizzare adattatori separati per connettersi ai sistemi storage di ciascun vendor. L'utilizzo di adattatori separati riduce la possibilità di conflitti tra driver e impostazioni. Per le connessioni a un sistema storage ONTAP, il modello di adattatore, il BIOS, il firmware e il driver devono essere elencati come supportati nel tool matrice di interoperabilità NetApp.

È necessario impostare i valori di timeout richiesti o consigliati e altri parametri di storage per l'host. È sempre necessario installare il software NetApp o applicare le impostazioni NetApp per ultime.

- Per AIX, è necessario applicare i valori della versione delle utility host AIX elencata nello strumento matrice di interoperabilità per la configurazione.
- Per ESX, è necessario applicare le impostazioni host utilizzando Virtual Storage Console per VMware vSphere.
- Per HP-UX, utilizzare le impostazioni di storage predefinite di HP-UX.
- Per Linux, è necessario applicare i valori della versione di Linux host Utilities elencata nello strumento Interoperability Matrix per la configurazione.
- Per Solaris, è necessario applicare i valori della versione di Solaris host Utilities elencata nel tool

Interoperability Matrix per la propria configurazione.

- Per Windows, è necessario installare la versione di Windows host Utilities elencata nello strumento Interoperability Matrix per la configurazione in uso.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Configurazioni SAN in un ambiente MetroCluster

Configurazioni SAN supportate in un ambiente ONTAP MetroCluster

Quando si utilizzano le configurazioni SAN in un ambiente MetroCluster, è necessario tenere presente alcune considerazioni.

- Le configurazioni MetroCluster non supportano le configurazioni vSAN del fabric FC front-end “Routed”.
- A partire da ONTAP 9.15.1, le configurazioni MetroCluster IP a quattro nodi sono supportate su NVMe/TCP.
- A partire da ONTAP 9.12.1, le configurazioni IP MetroCluster a quattro nodi sono supportate su NVMe/FC. Le configurazioni MetroCluster non sono supportate per le reti NVMe front-end prima di ONTAP 9.12.1.
- Altri protocolli SAN come iSCSI, FC e FCoE sono supportati nelle configurazioni MetroCluster.
- Quando si utilizzano configurazioni client SAN, è necessario verificare se eventuali considerazioni speciali per le configurazioni MetroCluster sono incluse nelle note fornite in "Tool di matrice di interoperabilità NetApp" (IMT).
- I sistemi operativi e le applicazioni devono fornire una resilienza i/o di 120 secondi per supportare lo switchover automatico non pianificato di MetroCluster e lo switchover con interruttore a leva o avviato da un mediatore.
- Le configurazioni MetroCluster utilizzano gli stessi WWN e WWPN su entrambi i lati del fabric FC front-end.

Informazioni correlate

- "Comprensione della protezione dei dati e del disaster recovery di MetroCluster"
- "Knowledge Base NetApp : quali sono le considerazioni sul supporto dell’host AIX in una configurazione MetroCluster ?"
- "Knowledge Base NetApp : considerazioni sul supporto host Solaris in una configurazione MetroCluster"

Evitare la sovrapposizione delle porte durante lo switchover e lo switchback della ONTAP MetroCluster

In un ambiente SAN, è possibile configurare gli switch front-end in modo da evitare sovrapposizioni quando la vecchia porta passa offline e la nuova porta entra in linea.

Durante lo switchover, la porta FC del sito sopravvissuto potrebbe accedere al fabric prima che il fabric abbia rilevato che la porta FC del sito di emergenza non è in linea e abbia rimosso questa porta dai servizi di nome e directory.

Se la porta FC del disastro non viene ancora rimossa, il tentativo di accesso fabric della porta FC nel sito sopravvissuto potrebbe essere rifiutato a causa di un WWPN duplicato. Questo comportamento degli switch FC può essere modificato per rispettare l’accesso del dispositivo precedente e non quello esistente. Verificare

gli effetti di questo comportamento su altri dispositivi fabric. Per ulteriori informazioni, contattare il fornitore dello switch.

Scegliere la procedura corretta in base al tipo di switch.

Esempio 1. Fasi

Switch Cisco

1. Connettersi allo switch ed effettuare l'accesso.
2. Accedere alla modalità di configurazione:

```
switch# config t
switch(config)#
```

3. Sovrascrivere la prima voce di dispositivo nel database del server dei nomi con la nuova periferica:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Negli switch che eseguono NX-OS 8.x, verificare che il timeout di quiesce flogi sia impostato su zero:

   a. Visualizzare il timer di quiesce:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Se l'output del passo precedente non indica che il timerval è zero, impostarlo su zero:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Switch Brocade

1. Connettersi allo switch ed effettuare l'accesso.
2. Inserire il `switchDisable` comando.
3. Inserire il `configure` e premere `y` quando richiesto.

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. Scegliere l'impostazione 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Rispondere alle richieste rimanenti oppure premere **Ctrl + D**.

6. Inserire il `switchEnable` comando.

Informazioni correlate

"Esecuzione di uno switchover per test o manutenzione"

Supporto ONTAP per multipathing di host SAN

ONTAP utilizza il software ALUA (Asymmetric Logical Unit Access) per il multipathing con gli host FC e iSCSI.

A partire da ONTAP 9,5, il failover/giveback della coppia ha (Multipath High Availability) è supportato per gli host NVMe utilizzando l'accesso asincrono al namespace (ANA). In ONTAP 9,4, NVMe supporta solo un percorso dall'host alla destinazione, pertanto l'host dell'applicazione deve gestire il failover del percorso al partner ha.

Il software multipathing è necessario sull'host SAN se può accedere a un namespace LUN o NVMe tramite più percorsi. Presenta un singolo disco al sistema operativo per tutti i percorsi a un LUN o namespace NVMe. Senza di esso, il sistema operativo potrebbe trattare ciascun percorso come un disco separato, causando la corruzione dei dati.

La soluzione è considerata avere più percorsi se si dispone di uno dei seguenti elementi:

- Una singola porta iniziatore nell'host che si collega a più LIF SAN nella SVM
- Più porte initiator collegate a una singola LIF SAN nella SVM
- Più porte initiator collegate a più LIF SAN nella SVM

Il software multipathing, noto anche come software MPIO (multipath i/o), è consigliato nelle configurazioni ha. In aggiunta alla mappatura selettiva delle LUN, si consiglia di utilizzare lo zoning a switch FC o i set di porte per limitare i percorsi utilizzati per accedere ai LUN.

Per informazioni su quali configurazioni host specifiche supportano ALUA o ANA, consultare "Tool di matrice di interoperabilità NetApp" e. "Configurazione host SAN ONTAP" per il sistema operativo host.

Numero consigliato di percorsi da host a nodi nel cluster

Non superare più di otto percorsi dall'host a ciascun nodo del cluster. Non superare il numero totale di percorsi supportati per il sistema operativo host e il multipathing utilizzato sull'host.

È necessario disporre di almeno due percorsi per LUN che si collegano a ciascun nodo di reporting mediante l'"Mappa LUN selettiva (SLM)"utilizzo della Storage Virtual Machine (SVM) del cluster. In questo modo si eliminano i singoli punti di errore e si consente al sistema di sopravvivere ai guasti dei componenti.

Se nel cluster sono presenti quattro o più nodi o più di quattro porte di destinazione utilizzate dalle SVM in uno dei nodi, È possibile utilizzare i seguenti metodi per limitare il numero di percorsi che è possibile utilizzare per accedere alle LUN sui nodi in modo da non superare il numero massimo consigliato di otto percorsi.

- SLM

  SLM riduce il numero di percorsi dall'host al LUN solo nei percorsi sul nodo proprietario del LUN e del partner ha del nodo proprietario. SLM è attivato per impostazione predefinita.

- "Portset per iSCSI"
- Mappature FC igroup dall'host
- Zoning dello switch FC

Limiti di configurazione

Determina il numero massimo di nodi e host SAN supportati per il cluster ONTAP

Il numero di nodi supportati per cluster varia in base alla versione di ONTAP in uso, ai modelli di controller e al protocollo dei nodi del cluster. Il numero massimo di host SAN che è possibile connettere a un cluster varia anche in base alla configurazione specifica.

Determina il numero massimo di nodi supportati per cluster

Se un nodo del cluster è configurato per FC, FC-NVMe, FCoE o iSCSI, tale cluster è limitato ai limiti dei nodi SAN. I limiti dei nodi in base ai controller del cluster sono elencati nel *Hardware Universe*.

Fasi

1. Passare a. "NetApp Hardware Universe".
2. In alto a sinistra, accanto a **Home**, selezionare **piattaforme**, quindi selezionare il tipo di piattaforma.
3. Selezionare la versione di ONTAP in uso.

   Viene visualizzata una nuova colonna per la scelta delle piattaforme.

4. Selezionare le piattaforme utilizzate nella soluzione.
5. In **Scegli le tue specifiche**, deseleziona **Seleziona tutto**.
6. Selezionare **numero massimo di nodi per cluster (NAS/SAN)**.
7. Fare clic su **Mostra risultati**.

Risultati

Viene visualizzato il numero massimo di nodi per cluster per le piattaforme selezionate.

Determina se il tuo cluster può supportare più host FC

Per le configurazioni FC e FC-NVMe, è necessario utilizzare il numero di ITN (Initiator-Target Nexuses) nel sistema per determinare se è possibile aggiungere altri host al cluster.

Un ITN rappresenta un percorso dall'iniziatore dell'host alla destinazione del sistema di storage. Il numero massimo di ITN per nodo nelle configurazioni FC e FC-NVMe è 2,048. Se si è al di sotto del numero massimo di ITN, è possibile continuare ad aggiungere host al cluster.

Per determinare il numero di ITN utilizzati nel cluster, attenersi alla seguente procedura per ciascun nodo del cluster.

Fasi

1. Identificare tutte le LIF su un nodo specifico.
2. Eseguire il seguente comando per ogni LIF sul nodo:

```
fcp initiator show -fields wwpn, lif
```

Il numero di voci visualizzate nella parte inferiore dell'output del comando rappresenta il numero di ITN per la LIF.

3. Registrare il numero di ITN visualizzati per ciascun LIF.
4. Aggiungere il numero di ITN per ogni LIF su ogni nodo del cluster.

   Questo totale rappresenta il numero di ITN nel cluster.

Determinare se il cluster è in grado di supportare più host iSCSI

Il numero di host che è possibile collegare direttamente a un nodo o tramite uno o più switch dipende dal numero di porte Ethernet disponibili. Il numero di porte Ethernet disponibili dipende dal modello del controller e dal numero e dal tipo di adattatori installati nel controller. Il numero di porte Ethernet supportate per controller e adattatori è disponibile in *Hardware Universe*.

Per tutte le configurazioni di cluster a più nodi, è necessario determinare il numero di sessioni iSCSI per nodo per sapere se è possibile aggiungere altri host al cluster. Se il cluster è al di sotto del numero massimo di sessioni iSCSI per nodo, è possibile continuare ad aggiungere host al cluster. Il numero massimo di sessioni iSCSI per nodo varia in base ai tipi di controller nel cluster.

Fasi

1. Identificare tutti i gruppi di portali di destinazione sul nodo.
2. Controllare il numero di sessioni iSCSI per ogni gruppo di portali di destinazione sul nodo:

```
iscsi session show -tpgroup _tpgroup_
```

   Il numero di voci visualizzate nella parte inferiore dell'output del comando rappresenta il numero di sessioni iSCSI per il gruppo di portali di destinazione.

3. Registrare il numero di sessioni iSCSI visualizzate per ciascun gruppo di portali di destinazione.
4. Aggiungere il numero di sessioni iSCSI per ciascun gruppo di portali di destinazione sul nodo.

   Il totale rappresenta il numero di sessioni iSCSI sul nodo.

Limiti di configurazione e supporto degli array SAN all-flash

I limiti di configurazione e il supporto degli array SAN all-flash (ASA) variano in base alla versione di ONTAP.

I dettagli più aggiornati sui limiti di configurazione supportati sono disponibili in "NetApp Hardware Universe".

> Queste limitazioni si applicano ai sistemi ASA. Se si dispone di un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), vedere "Limiti di archiviazione del sistema ASA R2" .

Protocolli SAN e numero di nodi supportati per cluster

I protocolli SAN supportati e il numero massimo di nodi per cluster dipendono dalla configurazione non MetroCluster o MetroCluster:

Configurazioni non MetroCluster

La tabella seguente mostra il supporto ASA per i protocolli SAN e il numero supportato di nodi per cluster nelle configurazioni non MetroCluster:

Inizio con ONTAP…	Supporto del protocollo	Numero massimo di nodi per cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • ISCSI	12
9.7	• FC • ISCSI	2

Configurazioni IP MetroCluster

La tabella seguente mostra il supporto di ASA per i protocolli SAN e il numero supportato di nodi per cluster nelle configurazioni IP di MetroCluster:

Inizio con ONTAP…	Supporto del protocollo	Numero massimo di nodi per cluster
9.15.1	• NVMe/TCP	2 nodi per cluster in configurazioni MetroCluster IP a quattro nodi
9.12.1	• NVMe/FC	2 nodi per cluster in configurazioni MetroCluster IP a quattro nodi
9.9.1	• FC • ISCSI	4 nodi per cluster in configurazioni MetroCluster IP a 8 nodi
9.7	• FC • ISCSI	2 nodi per cluster in configurazioni MetroCluster IP a quattro nodi

Supporto per porte persistenti

A partire da ONTAP 9,8, le porte persistenti sono abilitate per impostazione predefinita sugli array All-Flash SAN (ASA) configurati per utilizzare il protocollo FC. Le porte persistenti sono disponibili solo per FC e richiedono l'appartenenza alla zona identificata dal World Wide Port Name (WWPN).

Le porte persistenti riducono l'impatto dei takeover creando una LIF ombra sulla porta fisica corrispondente del partner ad alta disponibilità (ha). Quando un nodo viene sostituito, la LIF shadow sul nodo partner assume l'identità della LIF originale, inclusa la WWPNe. Prima che lo stato del percorso verso il nodo preso in consegna venga modificato in difettoso, la LIF shadow viene visualizzata come percorso attivo/ottimizzato verso lo stack MPIO host e l'i/o viene spostato. In questo modo si riducono le interruzioni di i/o perché l'host rileva sempre lo stesso numero di percorsi verso la destinazione, anche durante le operazioni di failover dello storage.

Per le porte persistenti, le seguenti caratteristiche della porta FCP devono essere identiche all'interno della coppia ha:

- Numero di porte FCP
- Nomi delle porte FCP
- Velocità delle porte FCP
- Zoning basato su WWPN FCP LIF

Se una di queste caratteristiche non è identica all'interno della coppia ha, viene generato il seguente messaggio EMS:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Per ulteriori informazioni sulle porte permanenti, vedere "Report tecnico NetApp 4080: Best practice per le SAN moderne".

Limiti di configurazione per gli switch FC utilizzati con i sistemi ONTAP

Gli switch Fibre Channel hanno limiti di configurazione massimi, incluso il numero di accessi supportati per porta, gruppo di porte, blade e switch. I vendor di switch documentano i propri limiti supportati.

Ogni interfaccia logica FC (LIF) accede a una porta dello switch FC. Il numero totale di accessi da una singola destinazione sul nodo equivale al numero di LIF più un accesso per la porta fisica sottostante. Non superare i limiti di configurazione del vendor dello switch per gli accessi o altri valori di configurazione. Ciò vale anche per gli iniziatori utilizzati sul lato host in ambienti virtualizzati con NPIV attivato. Non superare i limiti di configurazione del vendor dello switch per gli accessi per la destinazione o per gli iniziatori utilizzati nella soluzione.

Limiti dello switch Brocade

I limiti di configurazione per gli switch Brocade sono indicati nelle *linee guida sulla scalabilità Brocade*.

Limiti degli switch Cisco Systems

I limiti di configurazione per gli switch Cisco sono disponibili in "Limiti di configurazione Cisco" Guida alla versione del software dello switch Cisco in uso.

Numero massimo di nodi FC e FCoE supportati in ONTAP

Il numero di hop viene definito come il numero di switch nel percorso tra l'iniziatore (host) e la destinazione (sistema di storage). Il numero massimo di nodi FC supportati tra un sistema host e storage varia in base al fornitore dello switch.

La documentazione di Cisco Systems fa anche riferimento a questo valore come *diametro del fabric SAN*.

Per FCoE, è possibile collegare gli switch FCoE agli switch FC. Per le connessioni FCoE end-to-end, gli switch FCoE devono eseguire una versione del firmware che supporti i collegamenti Ethernet tra switch (ISL).

Cambiare fornitore	Numero di hop supportato
Brocade	• 7 per FC • 5 per FCoE
Cisco	• 7 per FC • Fino a 3 switch possono essere switch FCoE.

Calcolare la profondità della coda per gli host FC ONTAP

Potrebbe essere necessario regolare la profondità della coda FC sull'host per ottenere i valori massimi per ITN per nodo e fan-in della porta FC. Il numero massimo di LUN e il numero di HBA che possono connettersi a una porta FC sono limitati dalla profondità di coda disponibile sulle porte di destinazione FC.

A proposito di questa attività

Queue Depth (profondità coda) è il numero di richieste i/o (comandi SCSI) che possono essere accodate contemporaneamente su un controller di storage. Ogni richiesta di i/o dall'HBA iniziatore dell'host all'adattatore di destinazione del controller di storage consuma una voce di coda. In genere, una maggiore profondità della coda equivale a prestazioni migliori. Tuttavia, se viene raggiunta la profondità massima della coda del controller di storage, il controller di storage rifiuta i comandi in entrata restituendo una risposta QFULL. Se un gran numero di host accede a un controller di storage, è necessario pianificare attentamente per evitare le condizioni QFULL, che degradano significativamente le prestazioni del sistema e possono causare errori su alcuni sistemi.

In una configurazione con più iniziatori (host), tutti gli host devono avere profondità di coda simili. A causa della diseguaglianza nella profondità della coda tra gli host connessi allo storage controller attraverso la stessa porta di destinazione, gli host con profondità di coda inferiori vengono privati dell'accesso alle risorse da parte degli host con profondità di coda maggiori.

È possibile fornire i seguenti consigli generali sulle profondità della coda "tuning":

- Per i sistemi di piccole e medie dimensioni, utilizzare una profondità di coda HBA di 32.
- Per i sistemi di grandi dimensioni, utilizzare una profondità della coda HBA pari a 128.
- In caso di eccezioni o di test delle prestazioni, utilizzare una profondità della coda di 256 per evitare possibili problemi di accodamento.
- Tutti gli host devono avere le profondità della coda impostate su valori simili per garantire un accesso uguale a tutti gli host.

- Per evitare errori o penalizzazioni delle performance, non superare la profondità della coda della porta FC di destinazione del controller di storage.

Fasi

1. Contare il numero totale di iniziatori FC in tutti gli host che si connettono a una porta di destinazione FC.
2. Moltiplicare per 128.
   - Se il risultato è inferiore a 2,048, impostare la profondità della coda per tutti gli iniziatori su 128. Si dispone di 15 host con un iniziatore connesso a ciascuna delle due porte di destinazione sul controller di storage. 15 × 128 = 1,920. Poiché 1,920 è inferiore al limite di profondità totale della coda di 2,048, è possibile impostare la profondità della coda per tutti gli iniziatori su 128.
   - Se il risultato è superiore a 2,048, passare alla fase 3. Si dispone di 30 host con un iniziatore connesso a ciascuna delle due porte di destinazione sul controller di storage. 30 × 128 = 3,840. Poiché 3,840 è maggiore del limite di profondità totale della coda di 2,048, è necessario scegliere una delle opzioni indicate al punto 3 per la risoluzione dei problemi.
3. Scegliere una delle seguenti opzioni per aggiungere altri host al controller dello storage.
   - Opzione 1:
     i. Aggiungere altre porte di destinazione FC.
     ii. Ridistribuire gli iniziatori FC.
     iii. Ripetere i passaggi 1 e 2. + la profondità di coda desiderata di 3,840 supera la profondità di coda disponibile per porta. Per risolvere questo problema, è possibile aggiungere un adattatore di destinazione FC a due porte a ciascun controller, quindi eseguire la zona degli switch FC in modo che 15 host su 30 si connettano a un set di porte e gli altri 15 host si connettano a un secondo set di porte. La profondità della coda per porta viene quindi ridotta a 15 × 128 = 1,920.
   - Opzione 2:
     i. Indicare ciascun host come “Large” o “sMall” in base alle esigenze di i/o previste.
     ii. Moltiplicare il numero di iniziatori grandi per 128.
     iii. Moltiplicare il numero di piccoli iniziatori per 32.
     iv. Unire i due risultati.
     v. Se il risultato è inferiore a 2,048, impostare la profondità della coda per gli host di grandi dimensioni su 128 e la profondità della coda per gli host di piccole dimensioni su 32.
     vi. Se il risultato è ancora maggiore di 2,048 per porta, ridurre la profondità della coda per iniziatore fino a quando la profondità totale della coda non è inferiore o uguale a 2,048.

> Per stimare la profondità della coda necessaria per ottenere un determinato throughput i/o al secondo, utilizzare questa formula:
>
> Profondità della coda richiesta = (numero di i/o al secondo) × (tempo di risposta)
>
> Ad esempio, se si necessita di 40,000 i/o al secondo con un tempo di risposta di 3 millisecondi, la profondità della coda richiesta = 40,000 × (.003) = 120.

Il numero massimo di host che è possibile collegare a una porta di destinazione è 64, se si decide di limitare la profondità della coda alla raccomandazione di base di 32. Tuttavia, se si decide di avere una profondità di coda di 128, è possibile collegare un massimo di 16 host a una porta di destinazione. Maggiore è la profondità della coda, minore è il numero di host supportati da una singola porta di destinazione. Se il tuo requisito è tale da non poter scendere a compromessi sulla profondità della coda, dovresti ottenere più porte di destinazione.

La profondità della coda desiderata di 3,840 supera la profondità della coda disponibile per porta. Sono disponibili 10 host “Large” con esigenze di i/o dello storage elevate e 20 host “sMall” con esigenze di i/o ridotte. Impostare la profondità della coda dell’iniziatore sugli host di grandi dimensioni su 128 e la profondità della coda dell’iniziatore sugli host di piccole dimensioni su 32.

La profondità totale della coda risultante è (10 × 128) + (20 × 32) = 1,920.

È possibile distribuire la profondità della coda disponibile in modo uniforme in ciascun iniziatore.

La profondità della coda risultante per iniziatore è di 2,048 ÷ 30 = 68.

Consente di modificare le profondità delle code per gli host SAN ONTAP

Potrebbe essere necessario modificare la profondità della coda sull’host per ottenere i valori massimi per ITN per nodo e fan-in della porta FC. È possibile farlo per l’ambiente in uso."calcolare la profondità ottimale della coda"

Host AIX

È possibile modificare la profondità della coda sugli host AIX utilizzando `chdev` comando. Modifiche apportate utilizzando `chdev` il comando persiste durante i riavvii.

Esempi:

- Per modificare la profondità della coda per il dispositivo hdisk7, utilizzare il seguente comando:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Per modificare la profondità della coda per l’HBA fcs0, utilizzare il seguente comando:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  Il valore predefinito per `num_cmd_elems` è 200. Il valore massimo è 2,048.

> Potrebbe essere necessario portare l’HBA offline per modificarlo `num_cmd_elems` e poi riportarlo online utilizzando `rmdev -l fcs0 -R` e. `makdev -l fcs0 -P` comandi.

Host HP-UX

È possibile modificare la profondità della coda LUN o periferica sugli host HP-UX utilizzando il parametro kernel `scsi_max_qdepth`. È possibile modificare la profondità della coda HBA utilizzando il parametro kernel `max_fcp_reqs`.

- Il valore predefinito per `scsi_max_qdepth` è 8. Il valore massimo è 255.

  `scsi_max_qdepth` può essere modificato dinamicamente su un sistema in esecuzione utilizzando `-u` sul `kmtune` comando. La modifica sarà effettiva per tutti i dispositivi del sistema. Ad esempio, utilizzare il seguente comando per aumentare la profondità della coda LUN a 64:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  È possibile modificare la profondità della coda per i singoli file del dispositivo utilizzando `scsictl`

comando. Modifiche tramite `scsictl` i comandi non sono persistenti durante i riavvii del sistema. Per visualizzare e modificare la profondità della coda per un determinato file di dispositivo, eseguire il seguente comando:

```
scsictl -a /dev/rdsk/c2t2d0

scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
```

- Il valore predefinito per `max_fcp_reqs` è 512. Il valore massimo è 1024.

  Il kernel deve essere ricostruito e il sistema deve essere riavviato per apportare modifiche a. `max_fcp_reqs` per avere effetto. Per impostare la profondità della coda HBA su 256, ad esempio, utilizzare il seguente comando:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Host Solaris

È possibile impostare la profondità della coda LUN e HBA per gli host Solaris.

- Per la profondità della coda LUN: Il numero di LUN in uso su un host moltiplicato per l'accelerazione per LUN (lun-queue-depth) deve essere inferiore o uguale al valore tgt-queue-depth sull'host.
- Per la profondità della coda in uno stack Sun: I driver nativi non consentono per LUN o per destinazione `max_throttle` Impostazioni a livello di HBA. Metodo consigliato per l'impostazione di `max_throttle` Il valore per i driver nativi si trova a livello di tipo per dispositivo (VID_PID) in `/kernel/drv/sd.conf` e. `/kernel/drv/ssd.conf` file. L'utility host imposta questo valore su 64 per le configurazioni MPIxIO e 8 per le configurazioni Veritas DMP.

Fasi

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. Cercare `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   Il valore predefinito viene impostato su 32 al momento dell'installazione.

4. Impostare il valore desiderato in base alla configurazione dell'ambiente.
5. Salvare il file.
6. Riavviare l'host utilizzando `sync; sync; sync; reboot -- -r` comando.

VMware ospita un HBA QLogic

Utilizzare `esxcfg-module` Per modificare le impostazioni di timeout dell'HBA. Aggiornamento manuale di `esx.conf` file sconsigliato.

Fasi

1. Accedere alla console di servizio come utente root.
2. Utilizzare `#vmkload_mod -l` Comando per verificare quale modulo Qlogic HBA è attualmente caricato.

3. Per una singola istanza di un HBA Qlogic, eseguire il seguente comando:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

> In questo esempio viene utilizzato il modulo qla2300_707. Utilizzare il modulo appropriato in base all'output di `vmkload_mod -l`.

4. Salvare le modifiche utilizzando il seguente comando:

```
#/usr/sbin/esxcfg-boot -b
```

5. Riavviare il server utilizzando il seguente comando:

```
#reboot
```

6. Confermare le modifiche utilizzando i seguenti comandi:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware ospita un HBA Emulex

Utilizzare `esxcfg-module` Per modificare le impostazioni di timeout dell'HBA. Aggiornamento manuale di `esx.conf` file sconsigliato.

Fasi

1. Accedere alla console di servizio come utente root.
2. Utilizzare `#vmkload_mod -l grep lpfc` Comando per verificare quale HBA Emulex è attualmente caricato.
3. Per una singola istanza di un HBA Emulex, immettere il seguente comando:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

> A seconda del modello dell'HBA, il modulo può essere lpfcdd_7xx o lpfcdd_732. Il comando precedente utilizza il modulo lpfcdd_7xx. Utilizzare il modulo appropriato in base al risultato di `vmkload_mod -l`.

   L'esecuzione di questo comando imposta la profondità della coda LUN su 16 per l'HBA rappresentato da lpfc0.

4. Per istanze multiple di un HBA Emulex, eseguire il seguente comando:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

   La profondità della coda LUN per lpfc0 e la profondità della coda LUN per lpfc1 è impostata su 16.

5. Immettere il seguente comando:

```
#esxcfg-boot -b
```

6. Riavviare utilizzando `#reboot`.

Host Windows per un HBA Emulex

Sugli host Windows, è possibile utilizzare `LPUTILNT` Utility per aggiornare la profondità della coda per gli HBA Emulex.

Fasi

1. Eseguire `LPUTILNT` utility disponibile in `C:\WINNT\system32` directory.
2. Selezionare **Drive Parameters** (parametri unità) dal menu a destra.
3. Scorrere verso il basso e fare doppio clic su **QueueDepth**.

> Se si imposta **QueueDepth** maggiore di 150, è necessario aumentare in modo appropriato anche il seguente valore del Registro di sistema di Windows:
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Host Windows per un HBA Qlogic

Sugli host Windows, è possibile utilizzare il e il `SANsurfer` Utility di gestione HBA per aggiornare le profondità delle code per gli HBA Qlogic.

Fasi

1. Eseguire `SANsurfer` Utility HBA Manager.
2. Fare clic su **porta HBA** > **Impostazioni**.
3. Fare clic su **Advanced HBA port settings** (Impostazioni avanzate porta HBA) nella casella di riepilogo.
4. Aggiornare `Execution Throttle` parametro.

Host Linux per HBA Emulex

È possibile aggiornare le profondità della coda di un HBA Emulex su un host Linux. Per rendere gli aggiornamenti persistenti durante i riavvii, è necessario creare una nuova immagine del disco RAM e riavviare l'host.

Fasi

1. Identificare i parametri di profondità della coda da modificare:

   ```
   modinfo lpfc|grep queue_depth
   ```

   Viene visualizzato l'elenco dei parametri di profondità della coda con la relativa descrizione. A seconda della versione del sistema operativo in uso, è possibile modificare uno o più dei seguenti parametri di profondità della coda:

   - `lpfc_lun_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a un LUN specifico (uint)
   - `lpfc_hba_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a un HBA lpfc (uint)

- `lpfc_tgt_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a una specifica porta di destinazione (uint)

  Il `lpfc_tgt_queue_depth` Il parametro è valido solo per i sistemi Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11 SP4 e 12.x.

2. Aggiornare le profondità della coda aggiungendo i parametri di profondità della coda a `/etc/modprobe.conf` File per un sistema Red Hat Enterprise Linux 5.x e per `/etc/modprobe.d/scsi.conf` File per un sistema Red Hat Enterprise Linux 6.x o 7.x o un sistema SUSE Linux Enterprise Server 11.x o 12.x.

   A seconda della versione del sistema operativo in uso, è possibile aggiungere uno o più dei seguenti comandi:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Creare una nuova immagine del disco RAM, quindi riavviare l'host per rendere gli aggiornamenti persistenti durante i riavvii.

   Per ulteriori informazioni, consultare "Amministrazione del sistema" Per la versione del sistema operativo Linux in uso.

4. Verificare che i valori di profondità della coda siano aggiornati per ciascun parametro di profondità della coda modificato:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   Viene visualizzato il valore corrente della profondità della coda.

Host Linux per QLogic HBA

È possibile aggiornare la profondità della coda dei dispositivi di un driver QLogic su un host Linux. Per rendere gli aggiornamenti persistenti durante i riavvii, è necessario creare una nuova immagine del disco RAM e riavviare l'host. È possibile utilizzare la GUI di gestione dell'HBA QLogic o l'interfaccia della riga di comando (CLI) per modificare la profondità della coda dell'HBA QLogic.

Questa attività mostra come utilizzare la CLI QLogic HBA per modificare la profondità della coda QLogic HBA

Fasi

1. Identificare il parametro Device queue depth da modificare:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   È possibile modificare solo il `ql2xmaxqdepth` Queue depth, che indica la profondità massima della coda che può essere impostata per ogni LUN. Il valore predefinito è 64 per RHEL 7.5 e versioni successive. Il valore predefinito è 32 per RHEL 7.4 e versioni precedenti.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Aggiornare il valore di profondità della coda della periferica:
   - Se si desidera rendere persistenti le modifiche, attenersi alla seguente procedura:
     i. Aggiornare le profondità della coda aggiungendo il parametro queue depth al `/etc/modprobe.conf` File per un sistema Red Hat Enterprise Linux 5.x e per `/etc/modprobe.d/scsi.conf` File per un sistema Red Hat Enterprise Linux 6.x o 7.x o per un sistema SUSE Linux Enterprise Server 11.x o 12.x: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Creare una nuova immagine del disco RAM, quindi riavviare l'host per rendere gli aggiornamenti persistenti durante i riavvii.

     Per ulteriori informazioni, consultare "Amministrazione del sistema" Per la versione del sistema operativo Linux in uso.
   - Se si desidera modificare il parametro solo per la sessione corrente, eseguire il seguente comando:

     `echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

     Nell'esempio seguente, la profondità della coda è impostata su 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Verificare che i valori di profondità della coda siano aggiornati:

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   Viene visualizzato il valore corrente della profondità della coda.

4. Modificare la profondità della coda QLogic HBA aggiornando il parametro del firmware `Execution Throttle` Dal BIOS QLogic HBA.
   a. Accedere alla CLI di gestione dell'HBA QLogic:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. Dal menu principale, selezionare `Adapter Configuration` opzione.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

c. Dall'elenco dei parametri di configurazione dell'adattatore, selezionare `HBA Parameters` opzione.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Dall'elenco delle porte HBA, selezionare la porta HBA richiesta.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

Vengono visualizzati i dettagli della porta HBA.

e. Dal menu HBA Parameters (parametri HBA), selezionare `Display HBA Parameters` per visualizzare il valore corrente di `Execution Throttle` opzione.

Il valore predefinito di `Execution Throttle` l'opzione è 65535.

```
HBA Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
--------------------------------------------------------------------------
--------
Connection Options              : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                       : Auto
Frame Size                      : 2048
Hard Loop ID                    : 0
Loop Reset Delay (seconds)      : 5
Enable Host HBA BIOS            : Enabled
Enable Hard Loop ID             : Disabled
Enable FC Tape Support          : Enabled
Operation Mode                  : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)   : 0
**Execution Throttle              : 65535**
Login Retry Count               : 8
Port Down Retry Count           : 30
Enable LIP Full Login           : Enabled
Link Down Timeout (seconds)     : 30
Enable Target Reset             : Enabled
LUNs Per Target                 : 128
Out Of Order Frame Assembly     : Disabled
Enable LR Ext. Credits          : Disabled
Enable Fabric Assigned WWN      : N/A

Press <Enter> to continue:
```

a. Premere **Invio** per continuare.

b. Dal menu HBA Parameters (parametri HBA), selezionare `Configure HBA Parameters` Opzione per modificare i parametri HBA.

c. Dal menu Configure Parameters (Configura parametri), selezionare `Execute Throttle` e aggiornare il valore di questo parametro.

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Premere **Invio** per continuare.

e. Dal menu Configure Parameters (Configura parametri), selezionare `Commit Changes` opzione per salvare le modifiche.

f. Uscire dal menu.

Informazioni sul copyright

Copyright © 2026 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.