Riferimento alla configurazione SAN

ONTAP 9

NetApp
May 09, 2024

Sommario

Riferimento alla configurazione SAN

Panoramica della configurazione SAN

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

Metodi di configurazione degli host SAN iSCSI

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.

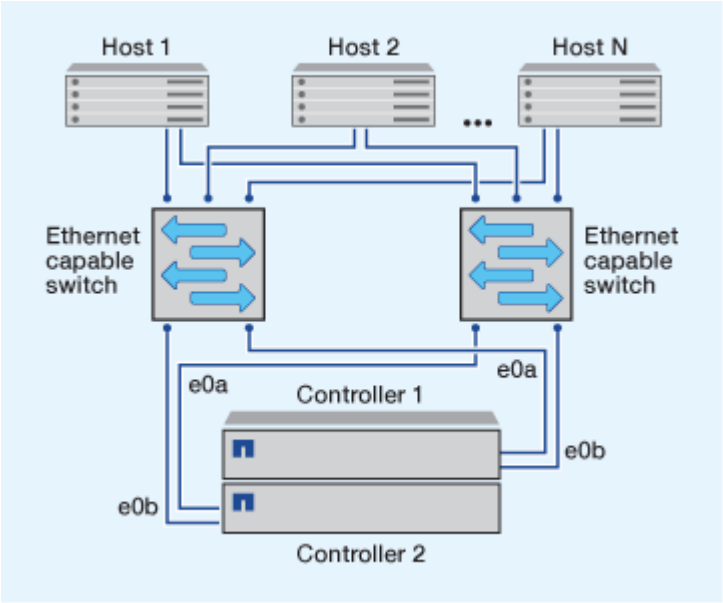
"Configurazioni a nodo singolo" sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

Informazioni correlate

- Scopri come "Mappatura selettiva delle LUN (SLM)" Limita 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".

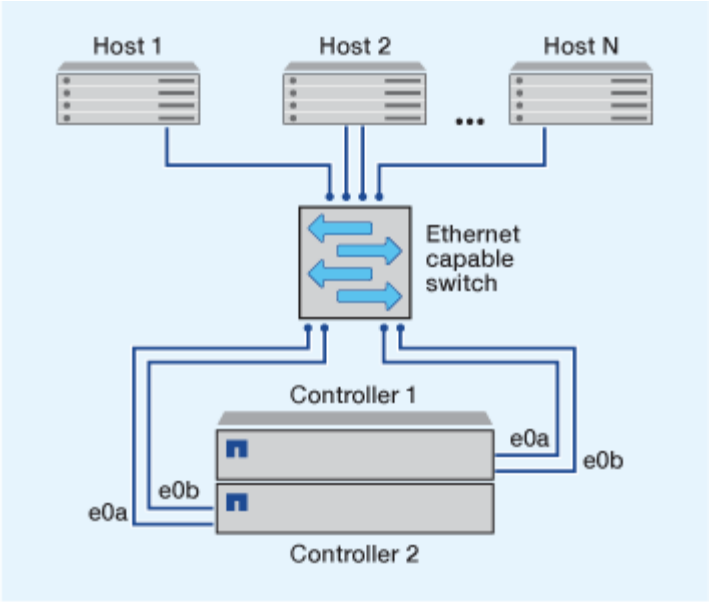
Configurazioni iSCSI multi-rete

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.



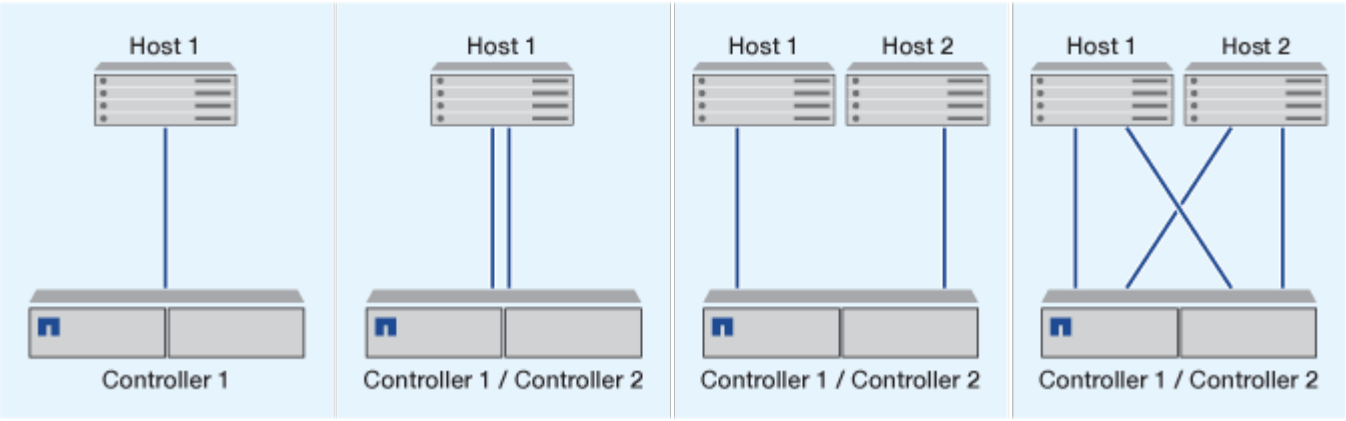
Configurazioni iSCSI a rete singola

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 delle VLAN 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

Modalità di configurazione degli host SAN FC & FC-NVMe

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.

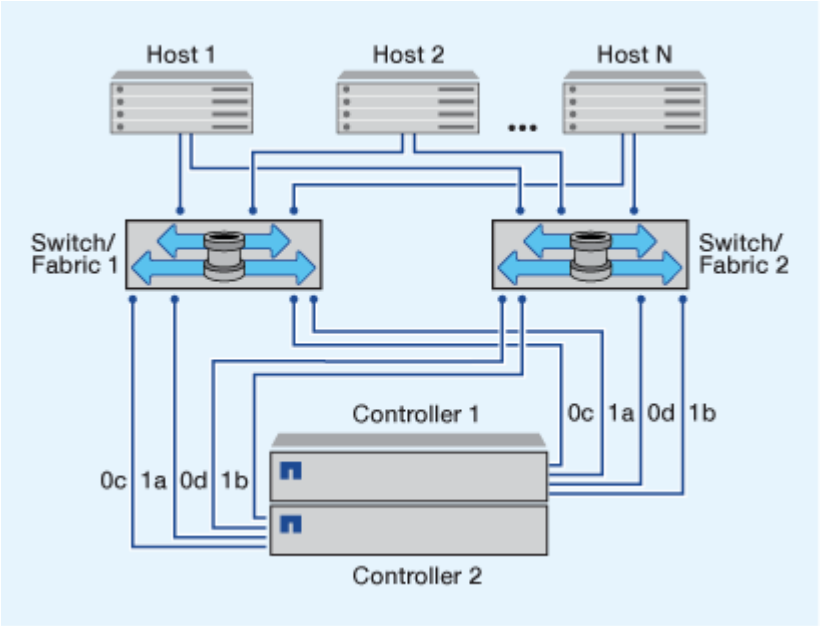
Cascade, Partial Mesh, full mesh, core-edge e director fabric sono tutti metodi standard di settore per collegare switch FC a un fabric e sono tutti supportati. L'utilizzo di fabric switch FC eterogenei non è supportato, tranne nel caso di switch blade integrati. Le eccezioni specifiche sono elencate 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.

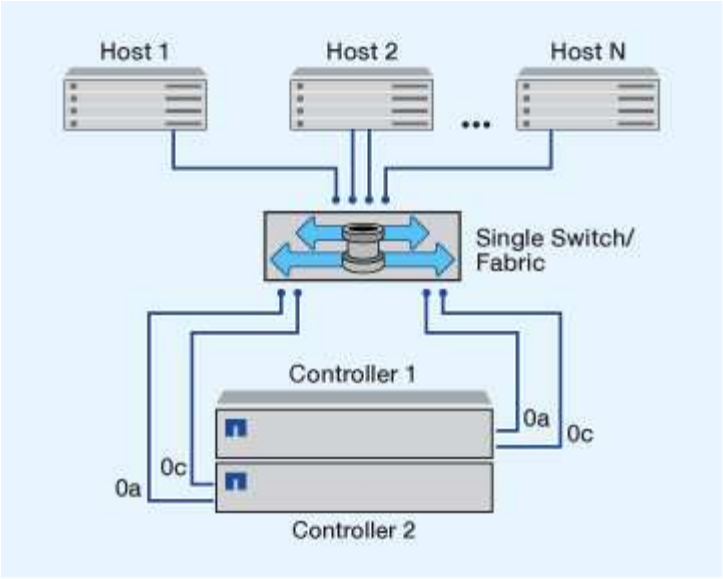


Configurazioni FC e FC-NVMe single-fabric

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)" Limita i percorsi utilizzati per accedere alle LUN di proprietà di una coppia ha.
- Scopri di più "LIF SAN".

Best practice per la configurazione dello switch FC

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

Numero supportato di conteggi FC hop

Il numero massimo di hop FC supportato tra un host e un sistema storage dipende dal fornitore dello switch e dal supporto del sistema storage per le configurazioni FC.

Il numero di hop viene definito come il numero di switch nel percorso tra l'iniziatore (host) e la destinazione (sistema di storage). Cisco fa anche riferimento a questo valore come *diametro del fabric SAN*.

Cambiare fornitore	Numero di hop supportato
Brocade	7 GB per FC, 5 GB per FCoE
Cisco	7 per FC, fino a 3 switch possono essere FCoE.

Informazioni correlate

"Download NetApp: Documenti matrice di scalabilità Brocade"

"Download NetApp: Documenti Cisco Scalability Matrix"

Velocità supportate dalla porta di destinazione FC

Le porte di destinazione FC possono essere configurate per funzionare a velocità diverse. Impostare la velocità della porta di destinazione in modo che corrisponda alla velocità del dispositivo a cui si connette. Tutte le porte di destinazione utilizzate da un determinato host devono essere impostate alla stessa velocità.

Le porte di destinazione FC possono essere utilizzate per le configurazioni FC-NVMe esattamente come per le configurazioni FC.

È necessario impostare la velocità della porta di destinazione in modo che corrisponda alla velocità del dispositivo a cui si connette invece di 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.

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

Le porte UTA2 possono utilizzare un adattatore SFP+ da 8 GB per supportare velocità da 8, 4 e 2 GB, se necessario.

Consigli per la configurazione della porta di destinazione FC

Per ottenere le migliori prestazioni e la massima disponibilità, è necessario utilizzare la configurazione della porta di destinazione FC consigliata.

La seguente tabella mostra l'ordine di utilizzo delle porte preferito per le porte di destinazione FC e FC-NVMe integrate. Per gli adattatori di espansione, le porte FC devono essere distribuite in modo che non utilizzino lo stesso ASIC per la connettività. L'ordine degli slot preferiti è riportato nella "NetApp Hardware Universe" Per la versione del software ONTAP utilizzata dal controller.

FC-NVMe è supportato sui seguenti modelli:

- AFF A300

> Le porte integrate AFF A300 non supportano FC-NVMe.

- AFF A700
- AFF A700
- AFF A800

> I sistemi FAS2520 non hanno porte FC integrate e non supportano adattatori aggiuntivi.

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte preferite
FAS9000, AFF A700, AFF A700 e AFF A800	Nessuno	Tutte le porte dati si trovano sugli adattatori di espansione. Vedere "NetApp Hardware Universe" per ulteriori informazioni.
8080, 8060 e 8040	0e+0f 0g+0h	1: 0e 2: 0e, 0g 3: 0e, 0g, 0h 4: 0e, 0g, 0f, 0h
FAS8200 e AFF A300	0g+0h	1: 0 g. 2: 0 g, 0 ore
8020	0c+0d	1: 0c 2: 0c, 0d
62xx	0a+0b 0c+0d	1: 0a 2: 0a, 0c 3: 0a, 0c, 0b 4: 0a, 0c, 0b, 0d
32xx	0c+0d	1: 0c 2: 0c, 0d

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte preferite
FAS2554, FAS2552, FAS2600, FAS2720, FAS2750, AFF A200 e AFF A220	0c+0d 0e+0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Gestire i sistemi con adattatori FC

Panoramica sulla gestione dei sistemi con adattatori FC

Sono disponibili comandi per gestire gli adattatori FC integrati e le schede adattatore FC. Questi comandi possono essere utilizzati per configurare la modalità dell'adattatore, visualizzare le informazioni sull'adattatore e modificare la velocità.

La maggior parte dei sistemi storage dispone di adattatori FC integrati che possono essere configurati come iniziatori o destinazioni. È inoltre possibile utilizzare schede adattatore FC configurate come iniziatori o destinazioni. Gli iniziatori si connettono agli shelf di dischi back-end e possibilmente a storage array esterni (FlexArray). Le destinazioni si connettono solo agli switch FC. Le porte HBA di destinazione FC e la velocità della porta dello switch devono essere impostate sullo stesso valore e non devono essere impostate su auto.

Comandi 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`

Se si desidera…	Utilizzare questo comando…
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`

Configurare gli adattatori FC per la modalità Initiator

È possibile configurare singole porte FC di adattatori integrati e alcune schede FC per la modalità Initiator. La modalità Initiator viene utilizzata per collegare le porte a unità a nastro, librerie a nastro o storage di terze parti con la virtualizzazione FlexArray o l'importazione di LUN esterne (FLI).

Di cosa hai bisogno

- 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.

A proposito di questa attività

Ogni porta FC integrata può essere configurata singolarmente come iniziatore o destinazione. Le porte di alcuni adattatori FC possono anche essere configurate singolarmente come una porta di destinazione o una porta initiator, proprio come le porte FC integrate. In è disponibile un elenco di adattatori che è possibile configurare per la modalità di destinazione "NetApp Hardware Universe".

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

È possibile configurare singole porte FC di adattatori integrati e alcune schede adattatore FC per la modalità di destinazione. La modalità di destinazione viene utilizzata per collegare le porte agli iniziatori FC.

A proposito di questa attività

Ogni porta FC integrata può essere configurata singolarmente come iniziatore o destinazione. Le porte di alcuni adattatori FC possono anche essere configurate singolarmente come una porta di destinazione o una porta initiator, proprio come le porte FC integrate. In è disponibile un elenco di adattatori che è possibile configurare per la modalità di destinazione "NetApp Hardware Universe".

La stessa procedura viene utilizzata per la configurazione degli adattatori FC per il protocollo FC e il protocollo FC-NVMe. Tuttavia, solo alcuni adattatori FC supportano FC-NVMe. Vedere "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
   ```

Visualizza informazioni su un adattatore di destinazione FC

È possibile utilizzare `network fcp adapter show` Per visualizzare le informazioni relative alla configurazione del sistema e all'adattatore FC del sistema.

Fase

1. Consente di visualizzare le informazioni sull'adattatore FC utilizzando `network fcp adapter show` comando.

   L'output visualizza le informazioni di configurazione del sistema e le informazioni sull'adattatore per ogni slot utilizzato.

   ```
   network fcp adapter show -instance -node node1 -adapter 0a
   ```

Modificare la velocità dell'adattatore FC

È necessario impostare la velocità della porta di destinazione dell'adattatore in modo che corrisponda alla velocità del dispositivo a cui si connette, invece di 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.

Di cosa hai bisogno

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

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.

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
   ```

Porte FC supportate

Il numero di porte FC integrate e di porte CNA/UTA2 configurate per FC varia in base al modello del controller. Le porte FC sono disponibili anche tramite adattatori di espansione FC target supportati o schede UTA2 aggiuntive configurate con adattatori FC SFP+.

Porte FC, UTA e UTA2 integrate

- Le porte onboard possono essere configurate singolarmente come porte FC di destinazione o iniziatore.
- Il numero di porte FC integrate varia a seconda del modello di controller.

  Il "NetApp Hardware Universe" Contiene un elenco completo delle porte FC integrate su ciascun modello di controller.

- I sistemi FAS2520 non supportano FC.

Porte FC dell'adattatore di espansione di destinazione

- Gli adattatori di espansione di destinazione disponibili variano a seconda del modello di controller.

  Il "NetApp Hardware Universe" contiene un elenco completo degli adattatori di espansione di destinazione per ciascun modello di controller.

- Le porte di alcuni adattatori di espansione FC sono configurate in fabbrica come iniziatori o destinazioni e non possono essere modificate.

  Altre porte possono essere configurate singolarmente come porte FC di destinazione o inizializzatore,

proprio come le porte FC integrate. Un elenco completo è disponibile in "NetApp Hardware Universe".

Evitare la perdita di connettività quando si utilizza l'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.

Gestire gli adattatori X1143A-R6

Panoramica delle configurazioni delle porte supportate per gli adattatori X1143A-R6

Per impostazione predefinita, l'adattatore X1143A-R6 è configurato in modalità di destinazione FC, ma è possibile configurarne le porte come porte Ethernet da 10 GB e FCoE (CNA) o come porte FC Initiator o di destinazione da 16 GB. Questo richiede diversi adattatori SFP+.

Se configurati per Ethernet e FCoE, gli adattatori X1143A-R6 supportano il traffico di destinazione simultaneo di NIC e FCoE sulla stessa porta 10-GBE. Se configurata per FC, ciascuna coppia di due porte che condivide lo stesso ASIC può essere configurata singolarmente per la destinazione FC o la modalità iniziatore FC. Ciò significa che un singolo adattatore X1143A-R6 può supportare la modalità di destinazione FC su una coppia a due porte e la modalità iniziatore FC su un'altra coppia a due porte. Le coppie di porte collegate allo stesso ASIC devono essere configurate nella stessa modalità.

In modalità FC, l'adattatore X1143A-R6 si comporta come qualsiasi dispositivo FC esistente con velocità fino a 16 Gbps. In modalità CNA, è possibile utilizzare l'adattatore X1143A-R6 per la condivisione simultanea del traffico NIC e FCoE sulla stessa porta 10 GbE. La modalità CNA supporta solo la modalità di destinazione FC per la funzione FCoE.

Configurare le porte

Per configurare l'adattatore di destinazione unificato (X1143A-R6), è necessario configurare le due porte adiacenti sullo stesso chip nella stessa modalità personality.

Fasi

1. Configurare le porte in base alle necessità per Fibre Channel (FC) o Converged Network Adapter (CNA) utilizzando `system node hardware unified-connect modify` comando.
2. Collegare i cavi appropriati per FC o Ethernet da 10 GB.
3. Verificare di avere installato il modulo SFP+ corretto:

   ```
   network fcp adapter show -instance -node -adapter
   ```

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, in base al fabric FC a cui è collegato.

Modificare la porta UTA2 dalla modalità CNA alla modalità FC

Modificare la porta UTA2 dalla modalità Converged Network Adapter (CNA) alla modalità Fibre Channel (FC) per supportare la modalità FC Initiator e FC target. È necessario modificare la personalità dalla modalità CNA alla modalità FC quando si desidera modificare il supporto fisico che collega la porta alla rete.

Fasi

1. Portare l'adattatore offline:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. Modificare la modalità della porta:

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. Riavviare il nodo, quindi portare l'adattatore in linea:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. Avvisare l'amministratore o il gestore VIF di eliminare o rimuovere la porta, a seconda dei casi:

   - Se la porta viene utilizzata come porta principale di una LIF, fa parte di un gruppo di interfacce (ifgrp) o ospita VLAN, un amministratore deve eseguire le seguenti operazioni:
     i. Spostare le LIF, rimuovere la porta da ifgrp o eliminare le VLAN, rispettivamente.
     ii. Eliminare manualmente la porta eseguendo `network port delete` comando.

     Se il `network port delete` il comando non riesce, l'amministratore dovrebbe risolvere gli errori ed eseguire di nuovo il comando.

   - Se la porta non viene utilizzata come porta home di un LIF, non è membro di un ifgrp e non ospita VLAN, il gestore VIF deve rimuovere la porta dai record al momento del riavvio.

     Se il gestore VIF non rimuove la porta, l'amministratore deve rimuoverla manualmente dopo il riavvio utilizzando `network port delete` comando.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                        Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
```

```
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                           Current  Current    Pending  Pending    Admin
    Node          Adapter  Mode     Type       Mode     Type
Status
    ------------  -------  -------  ---------  -------  ---------
-----------
    net-f8040-34-01
                  0e       cna      target     -        -
offline
    net-f8040-34-01
                  0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.
```

```
net-f8040-34::> reboot local
  (system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y
```

5. Verificare di avere installato il modulo SFP+ corretto:

   `network fcp adapter show -instance -node -adapter`

   Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, prima di modificare la configurazione sul nodo.

Sostituire i moduli ottici dell'adattatore target CNA/UTA2

È necessario modificare i moduli ottici sull'adattatore di destinazione unificato (CNA/UTA2) per supportare la modalità di personalità selezionata per l'adattatore.

Fasi

1. Verificare l'SFP+ corrente utilizzato nella scheda. Quindi, sostituire il modulo SFP+ corrente con il modulo SFP+ appropriato per il linguaggio preferito (FC o CNA).
2. Rimuovere i moduli ottici correnti dall'adattatore X1143A-R6.
3. Inserire i moduli corretti per l'ottica della modalità Personality (FC o CNA) preferita.
4. Verificare di avere installato il modulo SFP+ corretto:

   `network fcp adapter show -instance -node -adapter`

   I moduli SFP+ supportati e i cavi in rame (Twinax) con marchio Cisco sono elencati nella "NetApp Hardware Universe".

Visualizzare le impostazioni dell'adattatore

Per visualizzare le impostazioni dell'adattatore di destinazione unificato (X1143A-R6), è necessario eseguire `system hardware unified-connect show` comando per visualizzare tutti i moduli sul controller.

Fasi

1. Avviare il controller senza i cavi collegati.
2. Eseguire `system hardware unified-connect show` per visualizzare la configurazione delle porte e i moduli.
3. Visualizzare le informazioni sulla porta prima di configurare il CNA e le porte.

Configurazioni FCoE

Panoramica su come configurare FCoE

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.

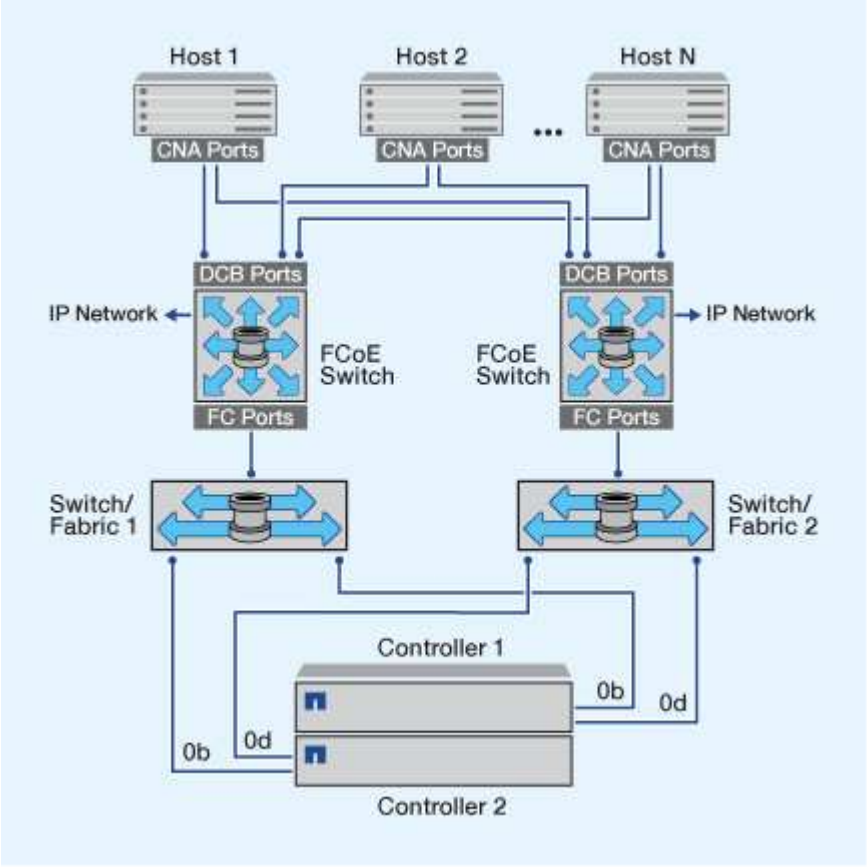
Le configurazioni FCoE richiedono switch Ethernet che supportano esplicitamente le funzionalità FCoE. Le configurazioni FCoE vengono validate attraverso lo stesso processo di interoperabilità e di garanzia della qualità degli switch FC. Le configurazioni supportate sono elencate nella matrice di interoperabilità. 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

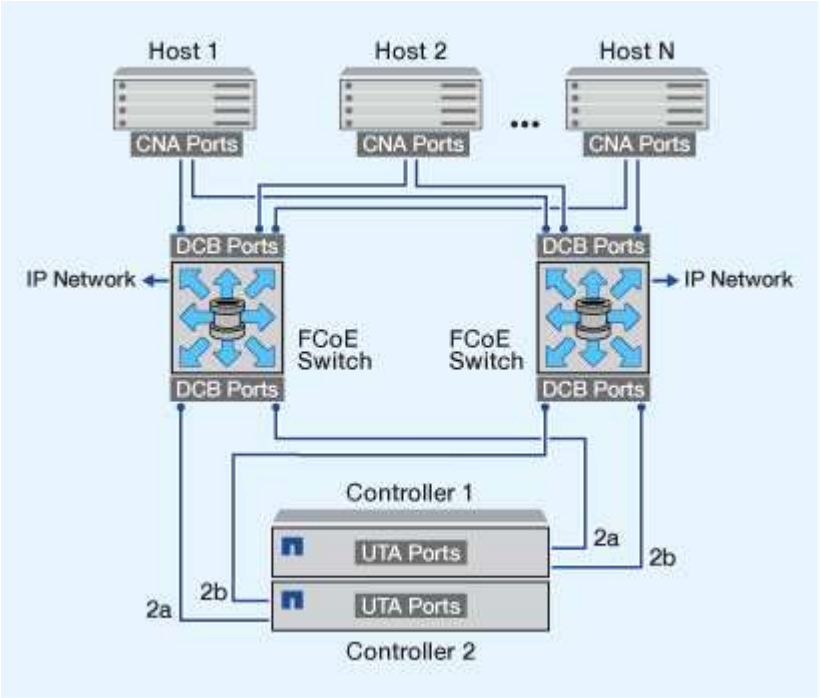
Utilizzando gli iniziatori FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha attraverso gli switch FCoE alle porte di destinazione FC. Lo switch FCoE deve anche disporre di porte FC. L'iniziatore FCoE host si connette sempre allo switch FCoE. Lo switch FCoE può connettersi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



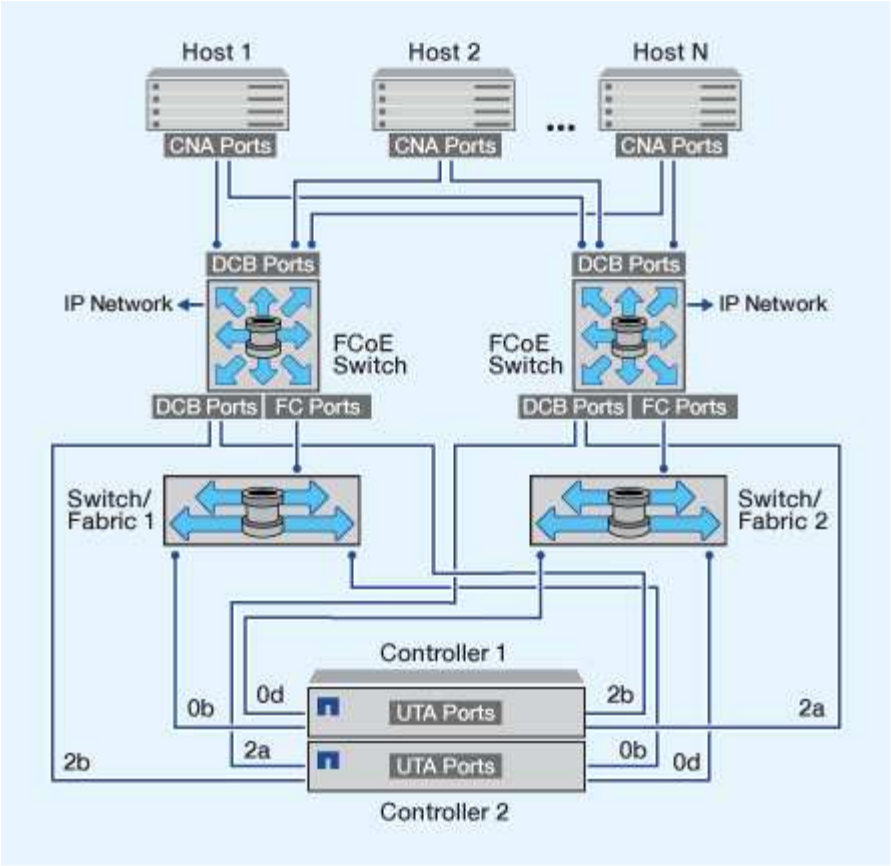
Iniziatore FCoE alla destinazione FCoE

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.



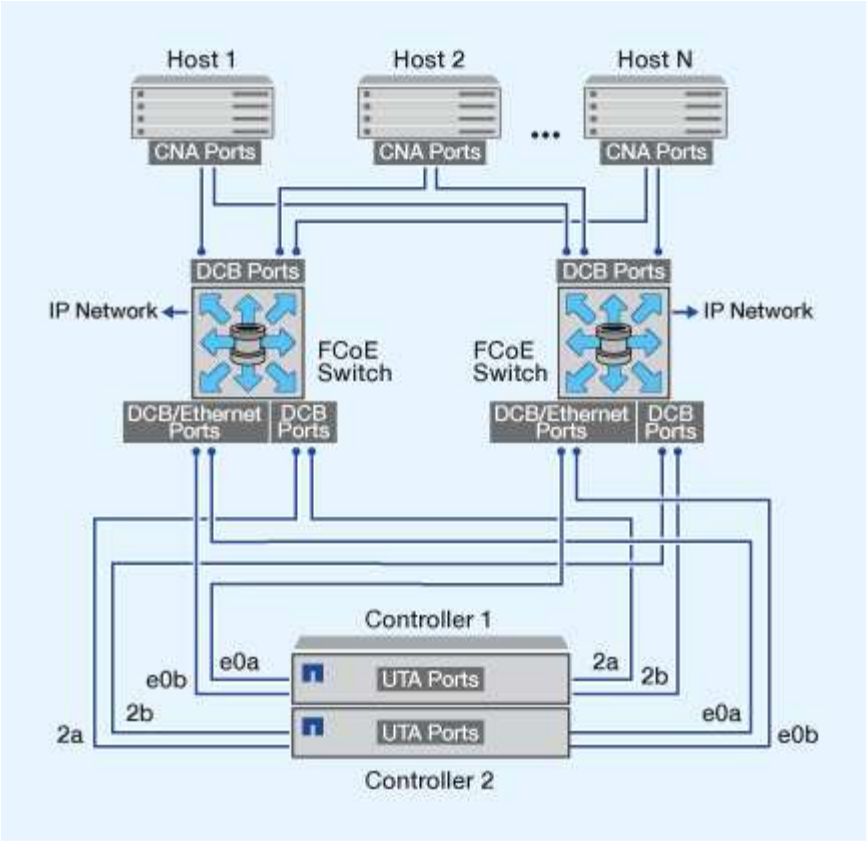
Iniziatore FCoE per destinazioni FCoE e FC

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.



FCoE Initiator e combinazioni di destinazione

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.

Numero di hop supportati da FCoE

Il numero massimo di hop Fibre Channel over Ethernet (FCoE) supportati tra un host e un sistema storage dipende dal fornitore dello switch e dal supporto del sistema storage per le configurazioni FCoE.

Il numero di hop viene definito come il numero di switch nel percorso tra l'iniziatore (host) e la destinazione (sistema di storage). 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).

La tabella seguente elenca i conteggi massimi di hop supportati:

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

Zoning FCoE e Fibre Channel

Panoramica dello zoning FCoE e Fibre Channel

Una zona FC, FC-NVMe o FCoE è un raggruppamento logico di una o più porte all'interno di un fabric. Affinché i dispositivi possano vederti, connettersi, creare sessioni e comunicare tra loro, entrambe le porte devono avere un'appartenenza di zona comune. Si consiglia di utilizzare lo zoning Single Initiator.

Motivi per lo zoning

- Lo zoning riduce o elimina *crosstalk* tra gli HBA iniziatori.

  Ciò si verifica anche in ambienti di piccole dimensioni ed è uno degli argomenti migliori per l'implementazione dello zoning. I sottoinsiemi di fabric logici creati con lo zoning eliminano i problemi di crosstalk.

- Lo zoning riduce il numero di percorsi disponibili per una determinata porta FC, FC-NVMe o FCoE e riduce il numero di percorsi tra un host e una particolare LUN visibili.

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 che un driver multipathing del sistema operativo vede. Se un host non dispone di una soluzione multipathing installata, è necessario verificare che sia visibile un solo percorso a un LUN utilizzando lo zoning nel fabric o una combinazione di mappatura LUN selettiva (SLM) e portset in SVM.

- Lo zoning aumenta la sicurezza limitando l'accesso e la connettività agli end-point che condividono una zona comune.

  Le porte che non hanno zone in comune non possono comunicare tra loro.

- Lo zoning migliora l'affidabilità DELLA SAN isolando i problemi che si verificano e aiuta a ridurre i tempi di risoluzione dei problemi limitando lo spazio dei problemi.

Consigli per lo zoning

- È necessario implementare lo zoning in qualsiasi momento, se quattro o più host sono connessi a una SAN o se SLM non è implementato sui nodi di una SAN.
- Sebbene sia possibile utilizzare lo zoning dei nomi dei nodi in tutto il mondo con alcuni fornitori di switch, è necessario utilizzare lo zoning dei nomi delle porte in tutto il mondo per definire correttamente una porta specifica e utilizzare NPIV in modo efficace.
- È necessario limitare le dimensioni della zona mantenendo la gestibilità.

  È possibile sovrapporre più zone per limitare le dimensioni. Idealmente, viene definita una zona per ciascun host o cluster di host.

- Utilizzare lo zoning a singolo iniziatore per eliminare il crosstalk tra gli HBA iniziatori.

Zoning basato sul nome

La suddivisione in zone in base al nome globale (WWN) specifica il numero WWN dei membri da includere nella zona. Quando si esegue lo zoning in ONTAP, è necessario utilizzare la zoning del nome della porta universale (WWPN).

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.

Per i percorsi Fibre Channel verso i controller di storage che eseguono ONTAP, assicurarsi che gli switch FC siano dotati di zone utilizzando le WWPN delle interfacce logiche di destinazione (LIF), non le WWPN delle porte fisiche sul nodo. Per ulteriori informazioni sulle schede LIF, consulta la *Guida alla gestione della rete ONTAP*.

"Gestione della rete"

Singole zone

Nella configurazione di zoning consigliata, esiste un iniziatore host per zona. La zona è costituita dalla porta dell'iniziatore host e da una o più LIF di destinazione sui nodi di storage che forniscono l'accesso alle LUN fino al numero desiderato di percorsi per destinazione. Ciò significa che gli host che accedono agli stessi nodi non possono vedere le porte dell'altro, ma ogni iniziatore può accedere a qualsiasi nodo.

È necessario aggiungere tutti i LIF dalla macchina virtuale di storage (SVM) nella zona con l'iniziatore host. Ciò consente di spostare volumi o LUN senza modificare le zone esistenti o creare nuove zone.

Per i percorsi Fibre Channel ai nodi che eseguono ONTAP, assicurarsi che gli switch FC siano dotati di zone utilizzando le WWPN delle interfacce logiche di destinazione (LIF), non le WWPN delle porte fisiche sul nodo. Le WWPN delle porte fisiche iniziano con "50" e le WWPN delle LIF iniziano con "20".

Zoning a fabric singolo

In una configurazione a fabric singolo, è comunque possibile connettere ciascun iniziatore host a ciascun nodo di storage. Per gestire percorsi multipli, è necessario un software multipathing sull'host. Ogni host deve disporre di due iniziatori per il multipathing per fornire resilienza nella soluzione.

Ciascun iniziatore deve disporre di almeno una LIF da ciascun nodo a cui l'iniziatore può accedere. 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.

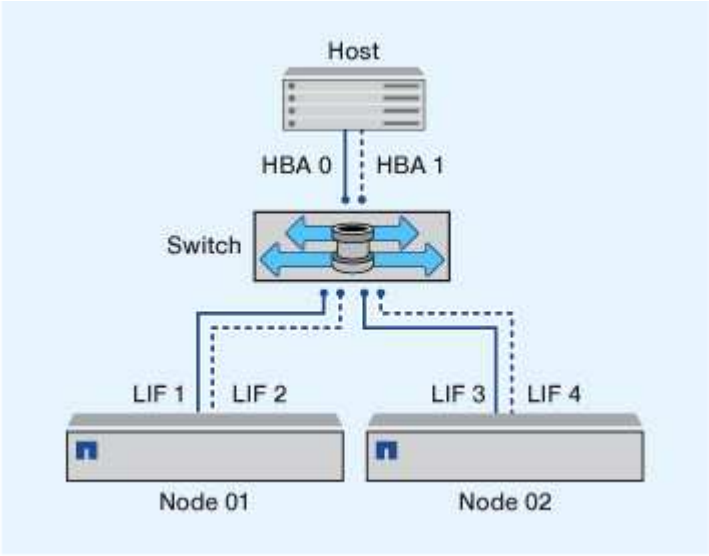
Le configurazioni a singolo fabric sono supportate, ma non sono considerate altamente disponibili. Il guasto di un singolo componente può causare la perdita di accesso ai dati.

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 includeva più nodi, le LIF per i nodi aggiuntivi sarebbero incluse in queste zone.



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.

Informazioni correlate

"NetApp Hardware Universe"

Zoning di coppia ha dual-fabric

Nelle configurazioni a doppio fabric, è possibile collegare ciascun iniziatore host a ciascun nodo del cluster. Ciascun iniziatore host utilizza uno switch diverso per accedere ai nodi del cluster. Per gestire percorsi multipli, è necessario un software multipathing sull'host.

Le configurazioni dual-fabric sono considerate ad alta disponibilità perché l'accesso ai dati viene mantenuto in caso di guasto di un singolo componente.

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

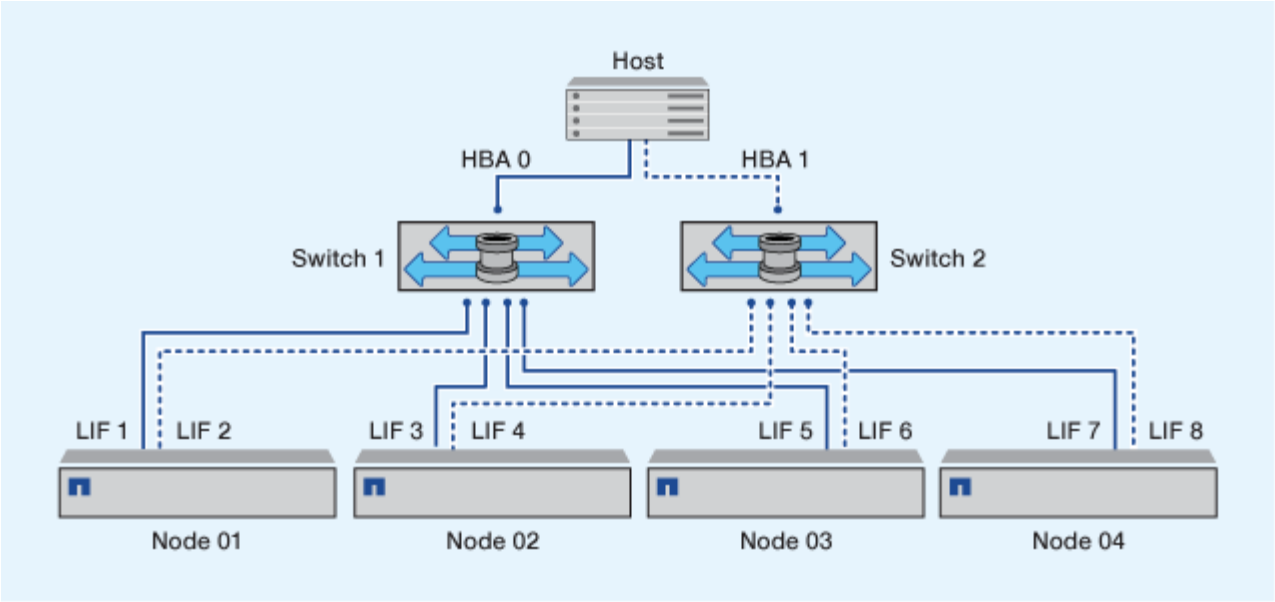
> La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- 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.

Ciascun iniziatore 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 di una soluzione in cluster in base all'impostazione della mappa LUN selettiva (SLM) e alla configurazione del nodo di reporting. 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 includeva più nodi, le LIF per i nodi aggiuntivi sarebbero 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.

Informazioni correlate

"NetApp Hardware Universe"

Restrizioni di zoning per switch Cisco FC e FCoE

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.

I normali switch FC vengono utilizzati per il protocollo FC-NVMe esattamente come per il protocollo FC.

- Più LIF per i protocolli FC e FCoE possono condividere porte fisiche su un nodo purché si trovino in zone diverse.
- FC-NVMe e FCoE non possono condividere la stessa porta fisica.
- FC e FC-NVMe possono condividere la stessa porta fisica da 32 GB.
- Gli switch Cisco FC e FCoE richiedono che ogni LIF su una determinata porta si trova in una zona separata dalle altre LIF su tale porta.
- Una singola zona può avere LIF FC e FCoE. Una zona può contenere una LIF da ogni porta di destinazione nel cluster, ma fare attenzione a non superare i limiti di percorso dell'host e verificare la configurazione SLM.
- Le LIF su diverse porte fisiche possono trovarsi nella stessa zona.
- Gli switch Cisco richiedono la separazione delle LIF.

  Sebbene non sia necessario, si consiglia di separare i LIF per tutti gli switch

Requisiti per le configurazioni SAN condivise

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 in un ambiente 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 9.12.1, le configurazioni IP MetroCluster a quattro nodi sono supportate su NVMe/FC. Le configurazioni MetroCluster non sono supportate su NVMe/TCP. Le configurazioni MetroCluster non sono supportate per NVMe precedenti a 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.

- MetroCluster utilizza le stesse WWPN su entrambi i lati DELLA SAN front-end.

Informazioni correlate

- "Comprensione della protezione dei dati e del disaster recovery di MetroCluster"
- "Articolo della Knowledge base: Quali sono le considerazioni sul supporto dell'host AIX in una configurazione MetroCluster?"
- "Articolo della Knowledge base: Considerazioni sul supporto degli host Solaris in una configurazione MetroCluster"

Impedire la sovrapposizione delle porte tra switchover e switchback

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 host per multipathing

Panoramica sul supporto host per multipathing

ONTAP utilizza sempre ALUA (Asymmetric Logical Unit Access) per i percorsi FC e iSCSI. Assicurarsi di utilizzare configurazioni host che supportino ALUA per i protocolli FC e iSCSI.

A partire da ONTAP 9.5 multipath ha Pair failover/giveback è supportato per le configurazioni NVMe che utilizzano l'accesso asincrono allo spazio dei nomi (ANA). In ONTAP 9.4, NVMe supporta un solo percorso da host a destinazione. L'host dell'applicazione deve gestire il failover del percorso verso il proprio partner ad alta disponibilità (ha).

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.

Quando è richiesto un software host multipathing

Se è presente più di un percorso tra le interfacce logiche (LIF) delle macchine virtuali di storage e il fabric, è necessario un software di multipathing. Il software multipathing è necessario sull'host ogni volta che l'host può accedere a un LUN attraverso più di un percorso.

Il software di multipathing presenta un singolo disco al sistema operativo per tutti i percorsi verso una LUN. Senza un software di multipathing, il sistema operativo potrebbe trattare ciascun percorso come un disco separato, con conseguente danneggiamento 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 è consigliato nelle configurazioni ha. Oltre alla mappatura LUN selettiva, si consiglia di utilizzare lo zoning o i portset dello switch FC per limitare i percorsi utilizzati per accedere alle LUN.

Il software multipathing è noto anche come software MPIO (multipath i/o).

Numero consigliato di percorsi da host a nodi nel cluster

Non superare più di otto percorsi dall'host a ciascun nodo del cluster, prestando attenzione al numero totale di percorsi che è possibile supportare per il sistema operativo host e al multipathing utilizzato sull'host.

È necessario disporre di almeno due percorsi per LUN che si connettono a ciascun nodo di reporting tramite la mappa LUN selettiva (SLM) utilizzata dalla macchina virtuale di storage (SVM) nel 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

Informazioni correlate

"Amministrazione SAN"

Limiti di configurazione

Determinare il numero di nodi supportati per le configurazioni SAN

Il numero di nodi per cluster supportati da ONTAP varia a seconda della versione di ONTAP, dei modelli di controller di storage nel cluster e del protocollo dei nodi del cluster.

A proposito di questa attività

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. Fare clic su **Platforms** in alto a sinistra (accanto al pulsante **Home**) e selezionare il tipo di piattaforma.
3. Selezionare la casella di controllo accanto alla versione di ONTAP in uso.

   Viene visualizzata una nuova colonna per la scelta delle piattaforme.

4. Selezionare le caselle di controllo accanto alle piattaforme utilizzate nella soluzione.
5. Deselezionare la casella di controllo **Seleziona tutto** nella colonna **Scegli specifiche**.
6. Selezionare la casella di controllo **Max Nodes per Cluster (NAS/SAN)**.
7. Fare clic su **Mostra risultati**.

Informazioni correlate

"NetApp Hardware Universe"

Determinare il numero di host supportati per cluster nelle configurazioni FC e FC-NVMe

Il numero massimo di host SAN che possono essere connessi a un cluster varia notevolmente in base alla combinazione specifica di più attributi del cluster, ad esempio il numero di host connessi a ciascun nodo del cluster, gli iniziatori per host, le sessioni per host e i nodi nel cluster.

A proposito di questa attività

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 il numero di host supportati nelle configurazioni iSCSI

Il numero massimo di host SAN che possono essere connessi nelle configurazioni iSCSI varia notevolmente in base alla combinazione specifica di più attributi del cluster, come il numero di host connessi a ciascun nodo del cluster, gli iniziatori per host, gli accessi per host e i nodi nel cluster.

A proposito di questa attività

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 dello switch FC

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.

Panoramica della profondità della coda di calcolo

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.

Impostare le profondità delle code sugli host SAN

Potrebbe essere necessario modificare le profondità della coda sull’host per ottenere i valori massimi per ITN per nodo e fan-in della porta FC.

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.