



# **Gestione dello storage SAN**

## **ONTAP 9**

NetApp  
February 12, 2026

# Sommario

Gestione dello storage SAN .....	1
Concetti SAN .....	1
Provisioning SAN con iSCSI .....	1
Gestione dei servizi iSCSI .....	2
Provisioning SAN con FC .....	9
Provisioning SAN con NVMe .....	10
Volumi SAN .....	11
Gestione dello spazio lato host SAN .....	16
A proposito di igroups .....	17
Specificare le WWPN dell'iniziatore e i nomi dei nodi iSCSI per un igroup .....	18
Vantaggi dell'utilizzo di un ambiente SAN virtualizzato .....	18
Migliorare le performance di VMware VAAI per gli host ESX .....	19
Scaricamento copia SAN .....	20
Amministrazione SAN .....	24
Provisioning SAN .....	24
Provisioning NVMe .....	34
Gestire le LUN .....	46
Gestire igroups e portset .....	59
Gestire il protocollo iSCSI .....	65
Gestire il protocollo FC .....	72
Gestire il protocollo NVMe .....	75
Gestire i sistemi con adattatori FC .....	85
Gestire le LIF per tutti i protocolli SAN .....	93
Attivare l'allocazione dello spazio ONTAP per i protocolli SAN .....	99
Combinazioni di configurazione di volume e file o LUN consigliate .....	101
Protezione dei dati SAN .....	107
Scopri i metodi di protezione dei dati ONTAP per gli ambienti SAN .....	107
Ripristinare una singola LUN da uno snapshot ONTAP .....	108
Ripristino di tutte le LUN di un volume da una snapshot ONTAP .....	109
Proteggere i tuoi dati con le LUN di ONTAP FlexClone .....	111
Configurare e utilizzare i backup SnapVault in un ambiente SAN .....	112
Configurazione consigliata per collegare un sistema di backup host a ONTAP .....	120
Utilizzare un sistema di backup host per proteggere un LUN sul sistema di storage ONTAP .....	120
Riferimento alla configurazione SAN .....	122
Informazioni sulla configurazione SAN di ONTAP .....	122
Configurazioni iSCSI .....	122
Configurazioni FC .....	125
Configurazioni FCoE .....	133
Zoning FC e FCoE .....	137
Requisiti per host SAN connessi a sistemi ONTAP e non NetApp .....	140
Configurazioni SAN in un ambiente MetroCluster .....	141
Supporto ONTAP per multipathing di host SAN .....	143
Limiti di configurazione .....	144

# Gestione dello storage SAN

## Concetti SAN

### Provisioning SAN con iSCSI

Negli ambienti SAN, i sistemi storage sono destinazioni che dispongono di dispositivi di destinazione dello storage. Per iSCSI e FC, i dispositivi di destinazione dello storage sono denominati LUN (unità logiche). Per NVMe (non-volatile Memory Express) su Fibre Channel, i dispositivi di destinazione dello storage vengono definiti namespace.

È possibile configurare lo storage creando LUN per iSCSI e FC o spazi dei nomi per NVMe. Gli host accedono quindi ai LUN o agli spazi dei nomi utilizzando le reti con protocollo iSCSI (Internet Small computer Systems Interface) o FC (Fibre Channel).

Per connettersi alle reti iSCSI, gli host possono utilizzare schede di rete Ethernet (NIC) standard, schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o HBA (host bus adapter) iSCSI dedicati.

Per connettersi alle reti FC, gli host richiedono HBA o CNA FC.

I protocolli FC supportati includono:

- FC
- FCoE
- NVMe

### Nomi e connessioni di rete del nodo di destinazione iSCSI

I nodi di destinazione iSCSI possono connettersi alla rete in diversi modi:

- Interfacce su Ethernet che utilizzano software integrato in ONTAP.
- Su più interfacce di sistema, con un'interfaccia utilizzata per iSCSI che può anche trasmettere il traffico per altri protocolli, come SMB e NFS.
- Utilizzando un adattatore di destinazione unificato (UTA) o un adattatore di rete convergente (CNA).

Ogni nodo iSCSI deve avere un nome di nodo.

I due formati, o designatori di tipo, per i nomi dei nodi iSCSI sono *iqn* e *eui*. La destinazione iSCSI SVM utilizza sempre il designatore di tipo *iqn*. L'iniziatore può utilizzare il designatore di tipo *iqn* o *eui*.

### Nome del nodo del sistema di storage

Ogni SVM che esegue iSCSI ha un nome di nodo predefinito basato su un nome di dominio inverso e un numero di codifica univoco.

Il nome del nodo viene visualizzato nel seguente formato:

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

L'esempio seguente mostra il nome del nodo predefinito per un sistema di storage con un numero di codifica

univoco:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

## Porta TCP per iSCSI

Il protocollo iSCSI è configurato in ONTAP per utilizzare la porta TCP numero 3260.

ONTAP non supporta la modifica del numero di porta per iSCSI. La porta numero 3260 è registrata come parte della specifica iSCSI e non può essere utilizzata da altre applicazioni o servizi.

### Informazioni correlate

["Documentazione NetApp: Configurazione host SAN ONTAP"](#)

## Gestione dei servizi iSCSI

### Gestione dei servizi iSCSI

È possibile gestire la disponibilità del servizio iSCSI sulle interfacce logiche iSCSI della macchina virtuale di storage (SVM) utilizzando `vserver iscsi interface enable` oppure `vserver iscsi interface disable` comandi.

Per impostazione predefinita, il servizio iSCSI è attivato su tutte le interfacce logiche iSCSI.

### Come viene implementato iSCSI sull'host

iSCSI può essere implementato sull'host utilizzando hardware o software.

È possibile implementare iSCSI in uno dei seguenti modi:

- Utilizzo di un software initiator che utilizza le interfacce Ethernet standard dell'host.
- Tramite un HBA (host bus adapter) iSCSI: Un HBA iSCSI viene visualizzato nel sistema operativo host come un adattatore disco SCSI con dischi locali.
- Utilizzando un adattatore TCP Offload Engine (TOE) che scarica l'elaborazione TCP/IP.

L'elaborazione del protocollo iSCSI viene ancora eseguita dal software host.

### Come funziona l'autenticazione iSCSI

Durante la fase iniziale di una sessione iSCSI, l'iniziatore invia una richiesta di accesso al sistema di storage per avviare una sessione iSCSI. Il sistema di storage quindi consente o nega la richiesta di accesso o determina che non è richiesto un accesso.

I metodi di autenticazione iSCSI sono:

- Challenge Handshake Authentication Protocol (CHAP): L'iniziatore effettua l'accesso utilizzando un nome utente e una password CHAP.

È possibile specificare una password CHAP o generare una password segreta esadecimale. Esistono due tipi di nomi utente e password CHAP:

- Inbound — il sistema storage autentica l'iniziatore.

Se si utilizza l'autenticazione CHAP, sono necessarie le impostazioni in entrata.

- Outbound (in uscita) - questa è un'impostazione opzionale che consente all'iniziatore di autenticare il sistema di storage.

È possibile utilizzare le impostazioni in uscita solo se si definiscono un nome utente e una password in entrata nel sistema di storage.

- Nega: All'iniziatore viene negato l'accesso al sistema di storage.
- Nessuno: Il sistema storage non richiede l'autenticazione per l'iniziatore.

È possibile definire l'elenco degli iniziatori e i relativi metodi di autenticazione. È inoltre possibile definire un metodo di autenticazione predefinito che si applica agli iniziatori non presenti nell'elenco.

### Informazioni correlate

["Opzioni di multipathing Windows con Data ONTAP: Fibre Channel e iSCSI"](#)

### Gestione della sicurezza di iSCSI Initiator

ONTAP offre una serie di funzionalità per la gestione della sicurezza per gli iniziatori iSCSI. È possibile definire un elenco di iniziatori iSCSI e il metodo di autenticazione per ciascuno di essi, visualizzare gli iniziatori e i relativi metodi di autenticazione nell'elenco di autenticazione, aggiungere e rimuovere gli iniziatori dall'elenco di autenticazione e definire il metodo di autenticazione iSCSI Initiator predefinito per gli iniziatori non presenti nell'elenco.

### Isolamento degli endpoint iSCSI

I comandi di protezione iSCSI esistenti possono accettare un intervallo di indirizzi IP o più indirizzi IP.

Tutti gli iniziatori iSCSI devono fornire indirizzi IP di origine quando si stabilisce una sessione o una connessione con una destinazione. Questa nuova funzionalità impedisce a un iniziatore di accedere al cluster se l'indirizzo IP di origine non è supportato o è sconosciuto, fornendo uno schema di identificazione univoco. Qualsiasi iniziatore che ha origine da un indirizzo IP non supportato o sconosciuto avrà il proprio login rifiutato nel layer di sessione iSCSI, impedendo all'iniziatore di accedere a qualsiasi LUN o volume all'interno del cluster.

Implementare questa nuova funzionalità con due nuovi comandi per gestire le voci preesistenti.

#### Aggiungere l'intervallo di indirizzi dell'iniziatore

Migliorare la gestione della sicurezza di iSCSI Initiator aggiungendo un intervallo di indirizzi IP o più indirizzi IP con `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

#### Rimuovere l'intervallo di indirizzi dell'iniziatore

Rimuovere un intervallo di indirizzi IP o più indirizzi IP con `vserver iscsi security remove-`

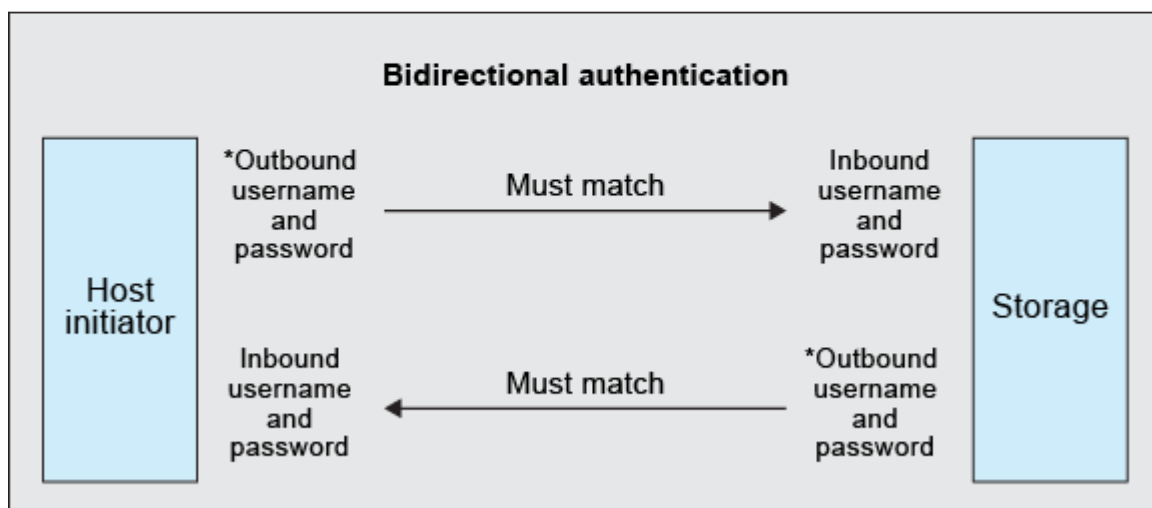
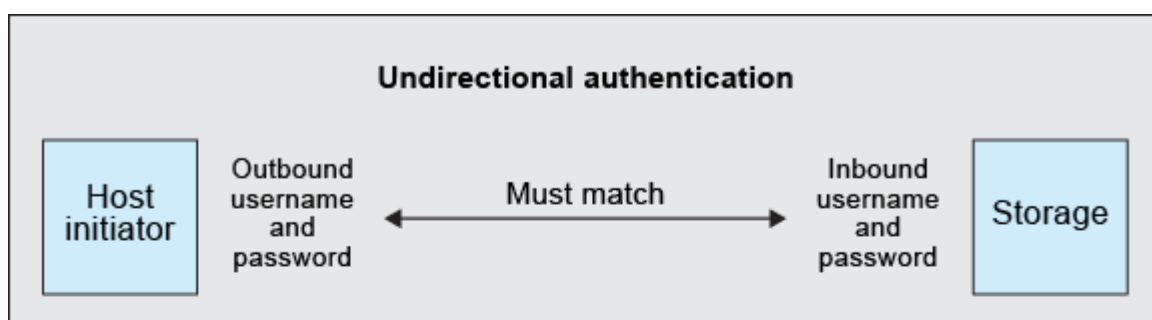
initiator-address-range comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

## Scopri di più sull'autenticazione CHAP per gli iniziatori iSCSI in ONTAP

Il protocollo CHAP (Challenge Handshake Authentication Protocol) consente la comunicazione autenticata tra gli iniziatori iSCSI e le destinazioni. Quando si utilizza l'autenticazione CHAP, si definiscono i nomi utente e le password CHAP sia sull'iniziatore che sul sistema di storage.

Durante la fase iniziale di una sessione iSCSI, l'iniziatore invia una richiesta di accesso al sistema di storage per iniziare la sessione. La richiesta di accesso include il nome utente CHAP dell'iniziatore e l'algoritmo CHAP. Il sistema storage risponde con una sfida CHAP. L'iniziatore fornisce una risposta CHAP. Il sistema storage verifica la risposta e autentica l'iniziatore. La password CHAP viene utilizzata per calcolare la risposta.



\*The outbound username and password for the host initiator must be different from the outbound username and password for the storage.

Autenticazione	In uscita	In entrata	Incontro?
Unidirezionale	Nome utente e password dell'iniziatore host	Nome utente e password di archiviazione	Deve corrispondere
Bidirezionale	Nome utente e password dell'iniziatore host	Nome utente e password di archiviazione	Deve corrispondere
Bidirezionale	Nome utente e password di archiviazione	Nome utente e password dell'iniziatore host	Deve corrispondere

Il nome utente e la password in uscita per l'iniziatore host devono essere diversi dal nome utente e dalla password in uscita per il sistema di archiviazione.

### Linee guida per l'utilizzo dell'autenticazione CHAP

Seguire queste linee guida quando si utilizza l'autenticazione CHAP.

- Se si definiscono un nome utente e una password in entrata nel sistema di storage, è necessario utilizzare lo stesso nome utente e password per le impostazioni CHAP in uscita sull'iniziatore. Se si definiscono anche un nome utente e una password in uscita sul sistema di storage per abilitare l'autenticazione bidirezionale, è necessario utilizzare lo stesso nome utente e la stessa password per le impostazioni CHAP in entrata sull'iniziatore.
- Non è possibile utilizzare lo stesso nome utente e password per le impostazioni in entrata e in uscita sul sistema di storage.
- I nomi utente CHAP possono essere da 1 a 128 byte.

Il sistema non consente nomi utente nulli.

- Le password CHAP (segreto) possono essere da 1 a 512 byte.

Le password possono essere valori esadecimali o stringhe. Per i valori esadecimali, è necessario immettere il valore con il prefisso "0x" o "0X".

Il sistema non consente password nulle.

ONTAP consente l'utilizzo di caratteri speciali, lettere non inglesi, numeri e spazi per le password CHAP (segreti). Tuttavia, questo è soggetto a restrizioni per l'host. Se uno di questi non è consentito dal tuo host specifico, non può essere utilizzato.



Ad esempio, l'iniziatore software iSCSI Microsoft richiede che le password CHAP di destinazione e di iniziatore siano almeno 12 byte se non viene utilizzata la crittografia IPsec. La lunghezza massima della password è di 16 byte, indipendentemente dall'utilizzo o meno di IPsec.

Per ulteriori restrizioni, consultare la documentazione dell'iniziatore.

### L'utilizzo degli elenchi di accesso alle interfacce iSCSI per limitare le interfacce initiator può aumentare le performance e la sicurezza

Gli elenchi DI accesso alle interfacce iSCSI possono essere utilizzati per limitare il numero di LIF in una SVM a cui un iniziatore può accedere, aumentando in tal modo le performance e la sicurezza.

Quando un iniziatore avvia una sessione di rilevamento utilizzando un iSCSI `SendTargets` Riceve gli indirizzi IP associati alla LIF (interfaccia di rete) presente nell'elenco degli accessi. Per impostazione predefinita, tutti gli iniziatori hanno accesso a tutte le LIF iSCSI nella SVM. È possibile utilizzare l'elenco di accesso per limitare il numero di LIF in una SVM a cui un iniziatore ha accesso.

## **iSNS (Internet Storage Name Service) in ONTAP**

Internet Storage Name Service (iSNS) è un protocollo che consente il rilevamento e la gestione automatici dei dispositivi iSCSI su una rete di storage TCP/IP. Un server iSNS conserva informazioni sui dispositivi iSCSI attivi sulla rete, inclusi i relativi indirizzi IP, i nomi dei nodi iSCSI IQN e i gruppi di portali.

È possibile ottenere un server iSNS da un fornitore di terze parti. Se si dispone di un server iSNS sulla rete configurato e abilitato per l'utilizzo da parte dell'iniziatore e della destinazione, è possibile utilizzare la LIF di gestione per una macchina virtuale di storage (SVM) per registrare tutte le LIF iSCSI per tale SVM sul server iSNS. Una volta completata la registrazione, iSCSI Initiator può eseguire una query sul server iSNS per rilevare tutte le LIF relative a una specifica SVM.

Se si decide di utilizzare un servizio iSNS, è necessario assicurarsi che le macchine virtuali dello storage (SVM) siano registrate correttamente con un server iSNS (Internet Storage Name Service).

Se non si dispone di un server iSNS sulla rete, è necessario configurare manualmente ciascuna destinazione in modo che sia visibile all'host.

### **Cosa fa un server iSNS**

Un server iSNS utilizza il protocollo iSNS (Internet Storage Name Service) per mantenere le informazioni sui dispositivi iSCSI attivi sulla rete, inclusi i relativi indirizzi IP, i nomi dei nodi iSCSI (IQN) e i gruppi di portali.

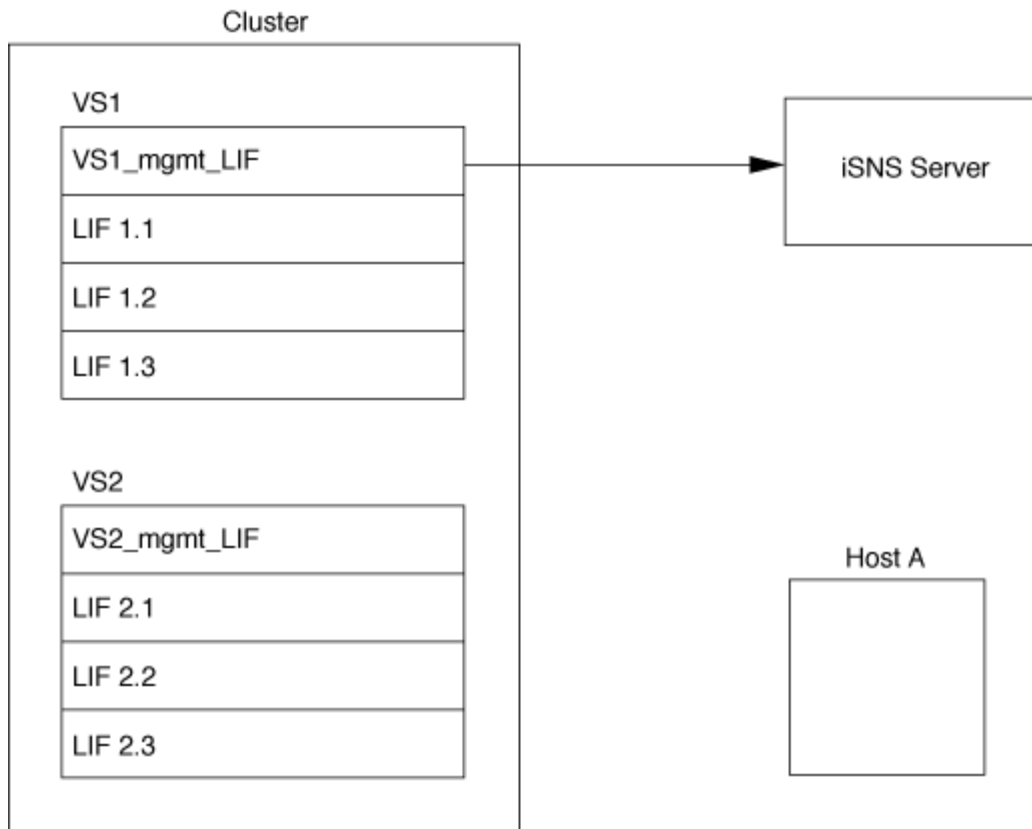
Il protocollo iSNS consente il rilevamento e la gestione automatizzati dei dispositivi iSCSI su una rete di storage IP. Un iniziatore iSCSI può eseguire query sul server iSNS per rilevare i dispositivi di destinazione iSCSI.

NetApp non fornisce o rivende server iSNS. È possibile ottenere questi server da un vendor supportato da NetApp.

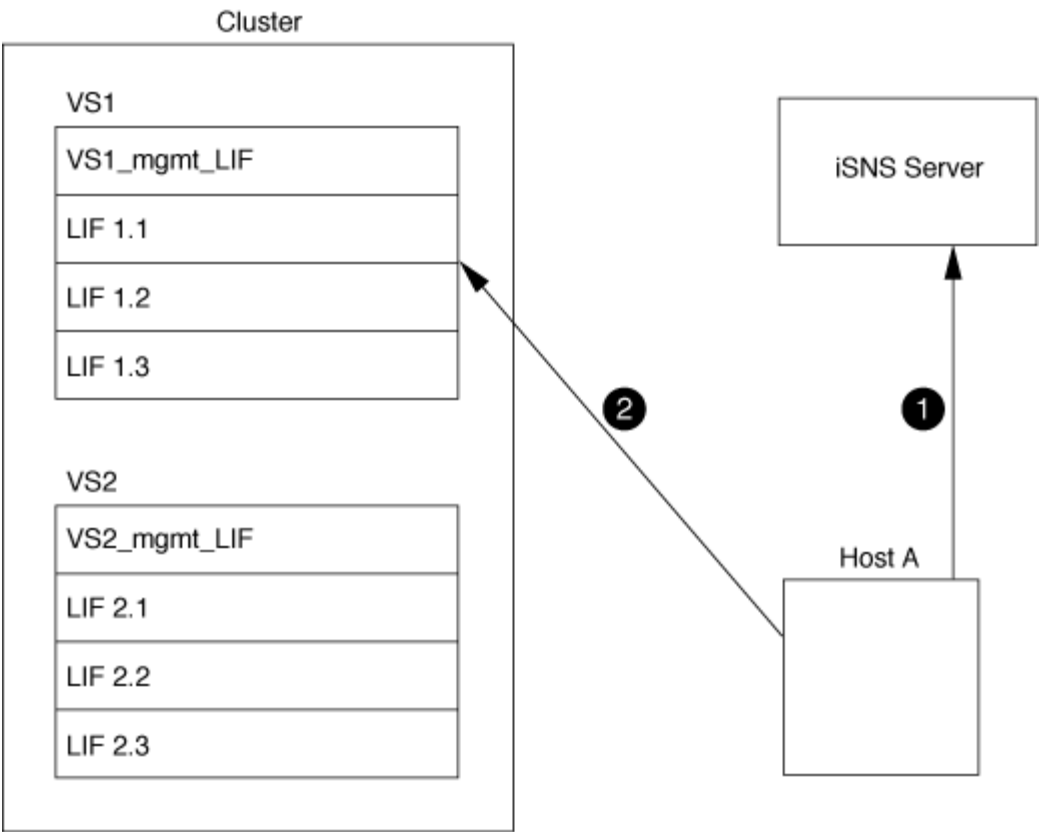
### **Come le SVM interagiscono con un server iSNS**

Il server iSNS comunica con ciascuna macchina virtuale di storage (SVM) attraverso la LIF di gestione SVM. La LIF di gestione registra tutte le informazioni relative a nome, alias e portale del nodo di destinazione iSCSI con il servizio iSNS per una SVM specifica.

Nell'esempio seguente, SVM "VS1" utilizza la LIF di gestione SVM "VS1\_mgmt\_lif" per la registrazione con il server iSNS. Durante la registrazione iSNS, una SVM invia tutte le LIF iSCSI attraverso la LIF di gestione SVM al server iSNS. Una volta completata la registrazione iSNS, il server iSNS dispone di un elenco di tutti i LIF che servono iSCSI in "VS1". Se un cluster contiene più SVM, ciascuna SVM deve registrarsi singolarmente con il server iSNS per utilizzare il servizio iSNS.



Nell'esempio successivo, dopo che il server iSNS ha completato la registrazione con la destinazione, l'host A è in grado di rilevare tutte le LIF per "VS1" attraverso il server iSNS, come indicato nella fase 1. Dopo che l'host A ha completato il rilevamento dei LIF per "VS1", l'host A può stabilire una connessione con una qualsiasi delle LIF in "VS1", come illustrato nella fase 2. L'host A non è a conoscenza di alcuna LIF in "VS2" fino a quando la LIF di gestione "VS2\_Mgmt\_LIF" per "VS2" non si registra con il server iSNS.



Tuttavia, se si definiscono gli elenchi di accesso all'interfaccia, l'host può utilizzare solo i LIF definiti nell'elenco di accesso all'interfaccia per accedere alla destinazione.

Una volta configurato iSNS, ONTAP aggiorna automaticamente il server iSNS quando cambiano le impostazioni di configurazione di SVM.

Potrebbe verificarsi un ritardo di alcuni minuti tra il momento in cui vengono apportate le modifiche alla configurazione e il momento in cui ONTAP invia l'aggiornamento al server iSNS. Forzare un aggiornamento immediato delle informazioni iSNS sul server iSNS: `vserver iscsi isns update`. Ulteriori informazioni su `vserver iscsi isns update` nella ["Riferimento al comando ONTAP"](#).

**Comandi per la gestione di iSNS**

ONTAP fornisce comandi per gestire il servizio iSNS.

Se si desidera...	Utilizzare questo comando...
Configurare un servizio iSNS	<code>vserver iscsi isns create</code>
Avviare un servizio iSNS	<code>vserver iscsi isns start</code>
Modificare un servizio iSNS	<code>vserver iscsi isns modify</code>
Visualizzare la configurazione del servizio iSNS	<code>vserver iscsi isns show</code>

Forzare un aggiornamento delle informazioni iSNS registrate	<code>vserver iscsi isns update</code>
Arrestare un servizio iSNS	<code>vserver iscsi isns stop</code>
Rimuovere un servizio iSNS	<code>vserver iscsi isns delete</code>
Visualizzare la pagina man per un comando	<code>man command name</code>

Ulteriori informazioni su `vserver iscsi isns` nella ["Riferimento al comando ONTAP"](#).

## Provisioning SAN con FC

È necessario conoscere i concetti importanti necessari per comprendere come ONTAP implementa una SAN FC.

### Modalità di connessione dei nodi di destinazione FC alla rete

I sistemi storage e gli host dispongono di adattatori che consentono di collegarli agli switch FC tramite cavi.

Quando un nodo è connesso alla SAN FC, ogni SVM registra il World Wide Port Name (WWPN) della propria LIF con lo switch Fabric Name Service. Il WWNN della SVM e il WWPN di ogni LIF vengono assegnati automaticamente da ONTAP.



La connessione diretta ai nodi dagli host con FC non è supportata, è necessario NPIV e questo richiede l'utilizzo di uno switch. con le sessioni iSCSI, la comunicazione funziona con connessioni che sono instradate in rete o a connessione diretta. Tuttavia, entrambi questi metodi sono supportati con ONTAP.

### Come vengono identificati i nodi FC

Ogni SVM configurato con FC è identificato da un nome di nodo mondiale (WWNN).

### Come vengono utilizzate le WWPN

Le WWPN identificano ogni LIF in una SVM configurata per supportare FC. Queste LIF utilizzano le porte FC fisiche di ciascun nodo del cluster, come schede di destinazione FC, UTA o UTA2, configurate come FC o FCoE nei nodi.

- Creazione di un gruppo iniziatore

Le WWPN degli HBA dell'host vengono utilizzate per creare un gruppo di iniziatori (igroup). Un igroup viene utilizzato per controllare l'accesso host a LUN specifiche. È possibile creare un igroup specificando una raccolta di WWPN di iniziatori in una rete FC. Quando si esegue il mapping di un LUN su un sistema storage a un igroup, è possibile concedere a tutti gli iniziatori di quel gruppo l'accesso a tale LUN. Se la WWPN di un host non si trova in un igroup mappato a una LUN, tale host non ha accesso alla LUN. Ciò significa che i LUN non vengono visualizzati come dischi su quell'host.

È inoltre possibile creare set di porte per rendere visibile un LUN solo su porte di destinazione specifiche. Un set di porte è costituito da un gruppo di porte di destinazione FC. È possibile associare un igroup a un

set di porte. Qualsiasi host del igroup può accedere ai LUN solo connettendosi alle porte di destinazione del set di porte.

- Identificazione univoca delle LIF FC

Le WWPN identificano in modo univoco ogni interfaccia logica FC. Il sistema operativo host utilizza la combinazione di WWNN e WWPN per identificare le SVM e le LIF FC. Alcuni sistemi operativi richiedono un binding persistente per garantire che il LUN appaia sullo stesso ID di destinazione sull'host.

## Come funzionano le assegnazioni dei nomi in tutto il mondo

I nomi in tutto il mondo vengono creati in sequenza in ONTAP. Tuttavia, a causa del modo in cui ONTAP li assegna, potrebbero sembrare assegnati in un ordine non sequenziale.

Ogni adattatore dispone di WWPN e WWNN preconfigurati, ma ONTAP non utilizza questi valori preconfigurati. Invece, ONTAP assegna le proprie WWPN o WWN, in base agli indirizzi MAC delle porte Ethernet integrate.

I nomi internazionali potrebbero sembrare non sequenziali se assegnati per i seguenti motivi:

- I nomi in tutto il mondo vengono assegnati a tutti i nodi e alle macchine virtuali di storage (SVM) del cluster.
- I nomi liberati in tutto il mondo vengono riciclati e aggiunti al pool di nomi disponibili.

## Identificazione degli switch FC

Gli switch Fibre Channel hanno un nome di nodo mondiale (WWNN) per il dispositivo stesso e un nome di porta mondiale (WWPN) per ciascuna delle porte.

Ad esempio, il seguente diagramma mostra come le WWPN vengono assegnate a ciascuna delle porte di uno switch Brocade a 16 porte. Per ulteriori informazioni sul numero delle porte per uno switch specifico, consultare la documentazione fornita dal vendor.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

## Provisioning SAN con NVMe

A partire da ONTAP 9.4, NVMe/FC è supportato in ambiente SAN. NVMe/FC consente agli amministratori dello storage di eseguire il provisioning degli spazi dei nomi e dei sottosistemi e di mappare gli spazi dei nomi ai sottosistemi, in modo simile al modo in cui i LUN vengono forniti e mappati a igroups per FC e iSCSI.

Uno spazio dei nomi NVMe è una quantità di memoria non volatile che può essere formattata in blocchi logici. Gli spazi dei nomi sono l'equivalente dei LUN per i protocolli FC e iSCSI e un sottosistema NVMe è analogo a un igroup. Un sottosistema NVMe può essere associato agli iniziatori in modo che gli iniziatori associati possano accedere agli spazi dei nomi all'interno del sottosistema.



Sebbene funzioni analoghe, gli spazi dei nomi NVMe non supportano tutte le funzionalità supportate dalle LUN.

A partire da ONTAP 9.5, è necessaria una licenza per supportare l'accesso ai dati rivolti all'host con NVMe. Se NVMe è attivato in ONTAP 9.4, viene concesso un periodo di valutazione di 90 giorni per l'acquisizione della licenza dopo l'aggiornamento a ONTAP 9.5. Se si dispone di "ONTAP uno", le licenze NVMe sono incluse. È possibile attivare la licenza utilizzando il seguente comando:

```
system license add -license-code NVMe_license_key
```

### Informazioni correlate

["Report tecnico di NetApp 4684: Implementazione e configurazione di SAN moderne con NVMe/FC"](#)

## Volumi SAN

### Panoramica sui volumi SAN

ONTAP offre tre opzioni di base per il provisioning dei volumi: Thick provisioning, thin provisioning e provisioning semi-thick. Ciascuna opzione utilizza diversi modi per gestire lo spazio del volume e i requisiti di spazio per le tecnologie di condivisione a blocchi di ONTAP. La comprensione del funzionamento delle opzioni consente di scegliere l'opzione migliore per il proprio ambiente.



Si sconsiglia di inserire LUN SAN e condivisioni NAS nello stesso volume FlexVol. È necessario eseguire il provisioning di volumi FlexVol separati specifici per LE LUN SAN e fornire volumi FlexVol separati in modo specifico alle condivisioni NAS. Ciò semplifica le implementazioni di gestione e replica e consente di utilizzare i volumi FlexVol supportati in Active IQ Unified Manager (in precedenza OnCommand Unified Manager).

### Thin provisioning per i volumi

Quando viene creato un volume con thin provisioning, ONTAP non riserva spazio extra quando viene creato il volume. Quando i dati vengono scritti nel volume, il volume richiede all'aggregato lo storage necessario per consentire l'operazione di scrittura. L'utilizzo di volumi con thin provisioning consente di eseguire l'overcommit dell'aggregato, il che introduce la possibilità che il volume non sia in grado di proteggere lo spazio necessario quando l'aggregato esaurisce lo spazio libero.

È possibile creare un volume FlexVol con thin provisioning impostandone l'impostazione `-space-guarantee` opzione a `none`.

### Thick provisioning per i volumi

Quando viene creato un volume con thick provisioning, ONTAP mette a disposizione una quantità di storage sufficiente dall'aggregato per garantire che qualsiasi blocco del volume possa essere scritto in qualsiasi momento. Quando si configura un volume per l'utilizzo del thick provisioning, è possibile utilizzare una qualsiasi delle funzionalità di efficienza dello storage ONTAP, come compressione e deduplica, per compensare i requisiti di storage anticipati più ampi.

È possibile creare un volume FlexVol con thick provisioning impostandone l'impostazione `-space-slo` (obiettivo del livello di servizio) opzione a. `thick`.

### Provisioning semi-spessi per i volumi

Quando viene creato un volume che utilizza il provisioning semi-thick, ONTAP mette da parte lo spazio di storage dell'aggregato per tenere conto delle dimensioni del volume. Se il volume sta esaurendo lo spazio libero perché i blocchi sono utilizzati dalle tecnologie di condivisione dei blocchi, ONTAP si occupa di eliminare gli oggetti di dati di protezione (snapshot, file FlexClone e LUN) per liberare lo spazio disponibile. Fino a quando ONTAP può eliminare gli oggetti dati di protezione abbastanza velocemente da tenere il passo con lo spazio richiesto per le sovrascritture, le operazioni di scrittura continuano a avere successo. Si tratta di una garanzia di scrittura "Best effort".

**Nota:** le seguenti funzionalità non sono supportate sui volumi che utilizzano il provisioning semi-spessi:

- Tecnologie per l'efficienza dello storage come deduplica, compressione e compaction
- ODX (Microsoft Offloaded Data Transfer)

È possibile creare un volume FlexVol con provisioning semi-thick impostandone il valore `-space-slo` (obiettivo del livello di servizio) opzione a. `semi-thick`.

### Da utilizzare con file e LUN con spazio riservato

Un file o LUN con spazio riservato è un file per il quale lo storage viene allocato al momento della creazione. Storicamente, NetApp ha utilizzato il termine "LUN con thin provisioning" per indicare un LUN per il quale la prenotazione dello spazio è disattivata (un LUN non riservato allo spazio).

**Nota:** i file non riservati allo spazio non sono generalmente denominati "thin-provisioning Files".

La seguente tabella riassume le principali differenze di utilizzo delle tre opzioni di provisioning dei volumi con file e LUN con spazio riservato:

Provisioning di volumi	Prenotazione di spazio LUN/file	Sovrascrive	Dati di protezione <sup>2</sup>	Efficienza dello storage <sup>3</sup>
Spesso	Supportato	Garantito <sup>1</sup>	Garantito	Supportato
Sottile	Nessun effetto	Nessuno	Garantito	Supportato
Semi-spessa	Supportato	Best effort <sup>1</sup>	Il massimo sforzo	Non supportato

### Note

1. La capacità di garantire le sovrascritture o fornire una garanzia di sovrascrittura con il massimo sforzo richiede che la riserva di spazio sia attivata sul LUN o sul file.
2. I dati di protezione includono snapshot, file FlexClone e LUN contrassegnati per la cancellazione automatica (cloni di backup).
3. L'efficienza dello storage include deduplica, compressione, qualsiasi file FlexClone e LUN non contrassegnati per l'eliminazione automatica (cloni attivi) e file secondari FlexClone (utilizzati per l'offload delle copie).

## Supporto per LUN con thin provisioning SCSI

ONTAP supporta LUN con thin provisioning SCSI T10 e LUN con thin provisioning NetApp. Il thin provisioning SCSI T10 consente alle applicazioni host di supportare funzionalità SCSI, tra cui funzionalità di recupero dello spazio del LUN e di monitoraggio dello spazio del LUN per gli ambienti a blocchi. Il thin provisioning SCSI T10 deve essere supportato dal software host SCSI.

Si utilizza ONTAP `space-allocation` Impostazione per abilitare/disabilitare il supporto per il thin provisioning T10 su un LUN. Si utilizza ONTAP `space-allocation enable` Impostazione per abilitare il thin provisioning SCSI T10 su un LUN.

IL `[-space-allocation {enabled|disabled}]` comando nel ["Riferimento al comando ONTAP"](#) contiene ulteriori informazioni su come abilitare/disabilitare il supporto per il thin provisioning T10 e su come abilitare il thin provisioning SCSI T10 su una LUN.

## Configurare le opzioni di provisioning dei volumi

È possibile configurare un volume per il thin provisioning, il thick provisioning o il provisioning semi-thick.

### A proposito di questa attività

Impostazione di `-space-slo` opzione a. `thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- il 100% dello spazio richiesto per le sovrascritture è riservato. Non è possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione

Impostazione di `-space-slo` opzione a. `semi-thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- Nessuno spazio riservato per le sovrascritture. È possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione.
- L'eliminazione automatica degli snapshot è attivata.

### Fase

1. Configurare le opzioni di provisioning dei volumi:

```
volume create -vserver vserver_name -volume volume_name -aggregate  
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Il `-space-guarantee` l'opzione predefinita è `none` Per sistemi AFF e volumi DP non AFF. In caso contrario, l'impostazione predefinita è `volume`. Per i volumi FlexVol esistenti, utilizzare `volume modify` per configurare le opzioni di provisioning.

Il seguente comando configura vol1 su SVM vs1 per il thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee none
```

Il seguente comando configura vol1 su SVM vs1 per il thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

Il seguente comando configura vol1 su SVM vs1 per il provisioning semi-spesso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

## Opzioni di configurazione del volume SAN

È necessario impostare diverse opzioni sul volume contenente il LUN. Il modo in cui si impostano le opzioni del volume determina la quantità di spazio disponibile per le LUN del volume.

### Crescita automatica

È possibile attivare o disattivare la crescita automatica. Se si attiva, la funzione di crescita automatica consente a ONTAP di aumentare automaticamente le dimensioni del volume fino a un massimo di dimensioni predeterminate. Per supportare la crescita automatica del volume, deve essere disponibile spazio nell'aggregato contenente. Pertanto, se si attiva la funzione di crescita automatica, è necessario monitorare lo spazio libero nell'aggregato contenente e aggiungerne di più quando necessario.

Impossibile attivare l'autogrow per supportare la creazione di snapshot. Se si tenta di creare uno snapshot e lo spazio sul volume non è sufficiente, la creazione dello snapshot non riesce, anche con la funzione di crescita automatica attivata.

Se la funzione di crescita automatica è disattivata, le dimensioni del volume rimangono invariate.

### Riduzione automatica

È possibile attivare o disattivare la riduzione automatica. Se la si attiva, la funzione di riduzione automatica consente a ONTAP di ridurre automaticamente le dimensioni complessive di un volume quando la quantità di spazio consumata nel volume diminuisce una soglia predeterminata. Ciò aumenta l'efficienza dello storage attivando i volumi per liberare automaticamente lo spazio libero inutilizzato.

### Eliminazione automatica di Snapshot

L'eliminazione automatica degli snapshot elimina automaticamente gli snapshot quando si verifica una delle seguenti situazioni:

- Il volume è quasi pieno.
- Lo spazio di riserva dell'istantanea è quasi pieno.
- Lo spazio riservato di sovrascrittura è pieno.

È possibile configurare l'eliminazione automatica degli snapshot per eliminare gli snapshot dal meno recente al più recente o dal più recente al meno recente. L'eliminazione automatica delle snapshot non elimina le snapshot collegate a snapshot in volumi clonati o LUN.

Se il tuo volume necessita di spazio aggiuntivo e hai abilitato sia l'autogrow che l'autodidem dello snapshot, per impostazione predefinita, ONTAP tenta di acquisire lo spazio necessario attivando prima l'autogrow. Se non viene acquisito spazio sufficiente attraverso l'espansione automatica, viene attivata la funzione di eliminazione automatica dello snapshot.

### **Riserva di Snapshot**

Snapshot Reserve definisce la quantità di spazio nel volume riservato agli snapshot. Lo spazio allocato alla riserva snapshot non può essere utilizzato per altri scopi. Se viene utilizzato tutto lo spazio allocato per la riserva snapshot, gli snapshot iniziano a occupare spazio aggiuntivo sul volume.

### **Requisito per lo spostamento di volumi in ambienti SAN**

Prima di spostare un volume contenente LUN o spazi dei nomi, è necessario soddisfare determinati requisiti.

- Per i volumi contenenti una o più LUN, è necessario disporre di almeno due percorsi per LUN (LIF) connessi a ciascun nodo del cluster.

In questo modo si eliminano i singoli punti di errore e si consente al sistema di sopravvivere ai guasti dei componenti.

- Per i volumi contenenti spazi dei nomi, il cluster deve eseguire ONTAP 9.6 o versione successiva.

Lo spostamento del volume non è supportato per le configurazioni NVMe che eseguono ONTAP 9.5.

### **Considerazioni per l'impostazione della riserva frazionale**

La riserva frazionale, detta anche *riserva di sovrascrittura LUN*, consente di disattivare la riserva di sovrascrittura per i LUN e i file con spazio riservato in un volume FlexVol. In questo modo è possibile massimizzare l'utilizzo dello storage, ma se l'ambiente viene influenzato negativamente da operazioni di scrittura non riuscite a causa della mancanza di spazio, è necessario comprendere i requisiti imposti da questa configurazione.

L'impostazione della riserva frazionale viene espressa in percentuale; gli unici valori validi sono 0 e 100 percentuale. L'impostazione della riserva frazionale è un attributo del volume.

Impostazione della riserva frazionale a 0 aumenta l'utilizzo dello storage. Tuttavia, un'applicazione che accede ai dati che risiedono nel volume potrebbe riscontrare un'interruzione dei dati se il volume non dispone di spazio libero, anche se la garanzia del volume è impostata su `volume`. Tuttavia, con una configurazione e un utilizzo corretti del volume, è possibile ridurre al minimo il rischio di errori di scrittura. ONTAP offre una garanzia di scrittura "Best effort" per i volumi con riserva frazionale impostata su 0 quando *tutti* i seguenti requisiti sono soddisfatti:

- La deduplica non è in uso
- La compressione non è in uso
- I file secondari FlexClone non sono in uso

- Tutti i file FlexClone e i LUN FlexClone sono abilitati per l'eliminazione automatica

Questa non è l'impostazione predefinita. È necessario attivare esplicitamente l'eliminazione automatica, al momento della creazione o modificando il file FlexClone o il LUN FlexClone dopo la creazione.

- L'offload delle copie di ODX e FlexClone non è in uso
- La garanzia del volume è impostata su `volume`
- La prenotazione dello spazio del file o del LUN è `enabled`
- Volume Snapshot Reserve (Riserva snapshot volume) è impostato su 0
- L'eliminazione automatica dello snapshot del volume `enabled` ha un livello di impegno di `destroy`, un elenco di eliminazione di `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr` e un trigger di `volume`

Questa impostazione garantisce inoltre che i file FlexClone e le LUN FlexClone vengano cancellati quando necessario.

Si noti che se la velocità di modifica è elevata, in rari casi l'eliminazione automatica dello snapshot potrebbe fallire, con conseguente esaurimento dello spazio del volume, anche con l'utilizzo di tutte le impostazioni di configurazione sopra richieste.

Inoltre, puoi utilizzare facoltativamente la funzionalità di crescita automatica dei volumi per ridurre la probabilità che gli snapshot di volume debbano essere eliminati automaticamente. Se si attiva la funzione di crescita automatica, è necessario monitorare lo spazio libero nell'aggregato associato. Se l'aggregato diventa abbastanza pieno da impedire la crescita del volume, è probabile che vengano eliminati più snapshot man mano che lo spazio libero del volume si esaurisce.

Se non si riesce a soddisfare tutti i requisiti di configurazione sopra indicati ed è necessario assicurarsi che il volume non esaurisca lo spazio, è necessario impostare la riserva frazionale del volume su 100. Ciò richiede più spazio libero in anticipo, ma garantisce che le operazioni di modifica dei dati avranno successo anche quando le tecnologie sopra elencate sono in uso.

Il valore predefinito e i valori consentiti per l'impostazione della riserva frazionale dipendono dalla garanzia del volume:

Garanzia di volume	Riserva frazionaria predefinita	Valori consentiti
Volume	100	0, 100
Nessuno	0	0, 100

## Gestione dello spazio lato host SAN

In un ambiente in cui è utilizzato il thin provisioning, la gestione dello spazio sul lato host completa il processo di gestione dello spazio dal sistema di storage liberato nel file system host.

Un file system host contiene metadati per tenere traccia di quali blocchi sono disponibili per memorizzare nuovi dati e quali blocchi contengono dati validi che non devono essere sovrascritti. Questi metadati vengono memorizzati nella LUN o nello spazio dei nomi. Quando un file viene cancellato nel file system host, i metadati del file system vengono aggiornati per contrassegnare i blocchi del file come spazio libero. Lo spazio libero

totale del file system viene quindi ricalcolato per includere i blocchi appena liberati. Nel sistema di storage, questi aggiornamenti dei metadati non appaiono diversi da qualsiasi altra scrittura eseguita dall'host. Pertanto, il sistema di storage non è a conoscenza di eventuali eliminazioni.

In questo modo si crea una discrepanza tra la quantità di spazio libero indicata dall'host e la quantità di spazio libero indicata dal sistema di storage sottostante. Ad esempio, si supponga di disporre di un LUN da 200 GB appena fornito assegnato all'host dal sistema storage. Sia l'host che il sistema di storage riportano 200 GB di spazio libero. L'host scrive quindi 100 GB di dati. A questo punto, sia l'host che il sistema di storage riportano 100 GB di spazio utilizzato e 100 GB di spazio inutilizzato.

Quindi, si eliminano 50 GB di dati dall'host. A questo punto, l'host segnalerà 50 GB di spazio utilizzato e 150 GB di spazio inutilizzato. Tuttavia, il sistema di storage riporta 100 GB di spazio utilizzato e 100 GB di spazio inutilizzato.

La gestione dello spazio sul lato host utilizza diversi metodi per riconciliare la differenza di spazio tra l'host e il sistema di storage.

### **Gestione semplificata degli host con SnapCenter**

È possibile utilizzare il software SnapCenter per semplificare alcune delle attività di gestione e protezione dei dati associate allo storage iSCSI e FC. SnapCenter è un pacchetto di gestione opzionale per host Windows e UNIX.

Puoi utilizzare il software SnapCenter per creare facilmente dischi virtuali a partire dai pool di storage che possono essere distribuiti tra diversi sistemi storage e per automatizzare i task di provisioning dello storage e semplificare il processo di creazione di snapshot e cloni a partire da snapshot coerenti con i dati dell'host.

Per ulteriori informazioni su, consultare la documentazione dei prodotti NetApp "[SnapCenter](#)".

#### **Link correlati**

["Attivare l'allocazione dello spazio ONTAP per i protocolli SAN"](#)

### **A proposito di igroups**

I gruppi di iniziatori (igroups) sono tabelle di nomi di host WWPN del protocollo FC o di nodi host iSCSI. È possibile definire igroups e mapparli alle LUN per controllare quali iniziatori hanno accesso alle LUN.

In genere, si desidera che tutte le porte iniziatore dell'host o gli iniziatori software abbiano accesso a un LUN. Se si utilizza un software multipathing o si dispone di host in cluster, ogni porta iniziatore o iniziatore software di ciascun host in cluster necessita di percorsi ridondanti verso la stessa LUN.

È possibile creare igroups che specifichino quali iniziatori hanno accesso alle LUN prima o dopo la creazione delle LUN, ma è necessario creare igroups prima di poter mappare una LUN a un igroup.

I gruppi iniziatori possono avere più iniziatori e più igroups possono avere lo stesso iniziatore. Tuttavia, non è possibile mappare un LUN a più igroups con lo stesso iniziatore. Un iniziatore non può essere un membro di igroups di diversi ostype.

### **Esempio di come gli igroups forniscono l'accesso al LUN**

È possibile creare più igroups per definire quali LUN sono disponibili per gli host. Ad esempio, se si dispone di un cluster host, è possibile utilizzare igroups per garantire che LUN specifiche siano visibili a un solo host del cluster o a tutti gli host del cluster.

La seguente tabella illustra come quattro igroups consentono l'accesso alle LUN per quattro diversi host che accedono al sistema di storage. Gli host in cluster (Host3 e Host4) sono entrambi membri dello stesso igroup (group3) e possono accedere alle LUN mappate a questo igroup. L'igroup denominato group4 contiene le WWPN di Host4 per memorizzare informazioni locali che non sono destinate al partner.

Host con HBA WWPN, IQN o EUI	igroups	WWPN, IQN, EUI aggiunti a igroups	LUN mappati a igroups
Host 1, percorso singolo (iSCSI software initiator)  iqn.1991-05.com.microsoft:host1	gruppo 1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host2, multipath (due HBA)  10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	gruppo 2	10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, multipath, in cluster con host 4  10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02	gruppo 3	10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun3
Host4, multipath, in cluster (non visibile all'host 3)  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	gruppo 4	10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4  /vol/vol2/qtrees1/lun5

## Specificare le WWPN dell'iniziatore e i nomi dei nodi iSCSI per un igroup

È possibile specificare i nomi dei nodi iSCSI e le WWPN degli iniziatori quando si crea un igroup oppure aggiungerli in un secondo momento. Se si sceglie di specificare i nomi dei nodi iSCSI e le WWPN dell'iniziatore quando si crea il LUN, è possibile rimuoverli in un secondo momento, se necessario.

Seguire le istruzioni nella documentazione delle utility host per ottenere le WWPN e per trovare i nomi dei nodi iSCSI associati a un host specifico. Per gli host che eseguono il software ESX, utilizzare Virtual Storage Console.

## Vantaggi dell'utilizzo di un ambiente SAN virtualizzato

La creazione di un ambiente virtualizzato utilizzando le macchine virtuali di storage

(SVM) e le LIF consente di espandere l'ambiente SAN a tutti i nodi del cluster.

- Gestione distribuita

È possibile accedere a qualsiasi nodo della SVM per amministrare tutti i nodi di un cluster.

- Maggiore accesso ai dati

Con MPIO e ALUA, puoi accedere ai tuoi dati attraverso qualsiasi LIF iSCSI o FC attiva per SVM.

- Accesso LUN controllato

Se si utilizzano SLM e portsets, è possibile limitare le LIF che un iniziatore può utilizzare per accedere alle LUN.

## Migliorare le performance di VMware VAAI per gli host ESX

ONTAP supporta alcune API vStorage VMware per l'integrazione degli array (VAAI) quando l'host ESX esegue ESX 4.1 o versioni successive. Queste funzionalità consentono di trasferire le operazioni dall'host ESX al sistema storage e aumentare il throughput di rete. L'host ESX attiva automaticamente le funzioni nell'ambiente corretto.

La funzione VAAI supporta i seguenti comandi SCSI:

- EXTENDED\_COPY

Questa funzione consente all'host di avviare il trasferimento dei dati tra le LUN o all'interno di una LUN senza coinvolgere l'host nel trasferimento dei dati. Ciò consente di risparmiare i cicli della CPU ESX e di aumentare il throughput di rete. La funzione di copia estesa, nota anche come "offload delle copie", viene utilizzata in scenari come la clonazione di una macchina virtuale. Quando viene richiamata dall'host ESX, la funzione di offload delle copie copia i dati all'interno del sistema di storage piuttosto che passare attraverso la rete host. L'offload della copia trasferisce i dati nei seguenti modi:

- All'interno di un LUN
- Tra LUN all'interno di un volume
- Tra LUN su diversi volumi all'interno di una macchina virtuale per lo storage (SVM)
- Tra LUN su SVM diverse all'interno di un cluster se questa funzione non può essere richiamata, l'host ESX utilizza automaticamente i comandi di LETTURA e SCRITTURA standard per l'operazione di copia.

- WRITE\_SAME

Questa funzionalità consente di trasferire il lavoro di scrittura di un modello ripetuto, ad esempio tutti gli zeri, a un array di storage. L'host ESX utilizza questa funzionalità in operazioni come lo zero-filling di un file.

- COMPARE\_AND\_WRITE

Questa funzionalità ignora alcuni limiti di concorrenza per l'accesso ai file, che accelerano le operazioni come l'avvio delle macchine virtuali.

## Requisiti per l'utilizzo dell'ambiente VAAI

Le funzionalità VAAI fanno parte del sistema operativo ESX e vengono richiamate automaticamente dall'host ESX una volta configurato l'ambiente corretto.

I requisiti ambientali sono i seguenti:

- L'host ESX deve eseguire ESX 4.1 o versione successiva.
- Il sistema storage NetApp che ospita il datastore VMware deve eseguire ONTAP.
- (Solo offload delle copie) l'origine e la destinazione dell'operazione di copia VMware devono essere ospitati sullo stesso sistema di storage all'interno dello stesso cluster.



La funzione di offload delle copie attualmente non supporta la copia dei dati tra gli archivi dati VMware ospitati su sistemi storage diversi.

## Determinare se le funzionalità VAAI sono supportate da ESX

Per verificare se il sistema operativo ESX supporta le funzionalità VAAI, è possibile controllare il client vSphere o utilizzare qualsiasi altro mezzo per accedere all'host. Per impostazione predefinita, ONTAP supporta i comandi SCSI.

È possibile controllare le impostazioni avanzate dell'host ESX per determinare se le funzioni VAAI sono attivate. La tabella indica i comandi SCSI corrispondenti ai nomi dei controlli ESX.

Comando SCSI	Nome del controllo ESX (funzione VAAI)
COPIA_ESTESA	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARE_AND_WRITE	HardwareAcceleratedLocking

## Scaricamento copia SAN

### ODX (Microsoft Offloaded Data Transfer)

Microsoft Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento diretto dei dati all'interno di un dispositivo di storage o tra dispositivi di storage compatibili senza trasferire i dati attraverso il computer host.

VMware e Microsoft supportano le operazioni di offload delle copie per aumentare le performance e il throughput di rete. È necessario configurare il sistema in modo che soddisfi i requisiti degli ambienti dei sistemi operativi VMware e Windows per utilizzare le rispettive funzioni di offload delle copie.

Quando si utilizza VMware e Microsoft Copy Offload in ambienti virtualizzati, è necessario allineare le LUN. Le LUN non allineate possono compromettere le prestazioni. ["Scopri di più sui LUN non allineati"](#).

ONTAP supporta ODX per i protocolli SMB e SAN.

Nei trasferimenti di file non ODX, i dati vengono letti dall'origine e trasferiti attraverso la rete all'host. L'host

trasferisce i dati di nuovo sulla rete alla destinazione. Nel trasferimento di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione senza passare attraverso l'host.

Poiché le copie con offload di ODX vengono eseguite direttamente tra origine e destinazione, si ottengono significativi vantaggi in termini di performance se le copie vengono eseguite nello stesso volume, inclusi tempo di copia più rapido per le stesse copie del volume, utilizzo ridotto di CPU e memoria sul client e utilizzo ridotto della larghezza di banda di i/o di rete. Se le copie sono tra i volumi, potrebbe non esserci un aumento significativo delle performance rispetto alle copie basate su host.

Per gli ambienti SAN, ODX è disponibile solo quando è supportato sia dall'host che dal sistema storage. I computer client che supportano ODX e che hanno ODX abilitato automaticamente e in modo trasparente utilizzano il trasferimento di file offload durante lo spostamento o la copia dei file. ODX viene utilizzato indipendentemente dal fatto che si trascinino i file tramite Esplora risorse o si utilizzino comandi di copia dei file dalla riga di comando o che un'applicazione client avvii richieste di copia dei file.

### **Requisiti per l'utilizzo di ODX**

Se si intende utilizzare ODX per gli offload delle copie, è necessario conoscere le considerazioni sul supporto dei volumi, i requisiti di sistema e i requisiti di funzionalità software.

Per utilizzare ODX, il sistema deve disporre di quanto segue:

- ONTAP

ODX viene attivato automaticamente nelle versioni supportate di ONTAP.

- Volume di origine minimo di 2 GB

Per ottenere prestazioni ottimali, il volume di origine deve essere superiore a 260 GB.

- Supporto di ODX sul client Windows

ODX è supportato in Windows Server 2012 o versioni successive e in Windows 8 o versioni successive. La matrice di interoperabilità contiene le informazioni più recenti sui client Windows supportati.

["Tool di matrice di interoperabilità NetApp"](#)

- Supporto dell'applicazione di copia per ODX

L'applicazione che esegue il trasferimento dei dati deve supportare ODX. Le operazioni applicative che supportano ODX includono:

- Operazioni di gestione di Hyper-V, come la creazione e la conversione di hard disk virtuali (VHD), la gestione di snapshot e la copia di file tra macchine virtuali
- Operazioni di Esplora risorse
- Comandi di copia di Windows PowerShell
- Comandi di copia del prompt dei comandi di Windows la Microsoft TechNet Library contiene ulteriori informazioni sulle applicazioni ODX supportate su server e client Windows.
- Se si utilizzano volumi compressi, la dimensione del gruppo di compressione deve essere 8K.

Le dimensioni del gruppo di compressione 32K non sono supportate.

ODX non funziona con i seguenti tipi di volume:

- Volumi di origine con capacità inferiori a 2 GB
- Volumi di sola lettura
- "Volumi FlexCache"



ODX è supportato sui volumi di origine FlexCache.

- "Volumi con provisioning semi-spessi"

#### Requisiti speciali per i file di sistema

È possibile eliminare i file ODX trovati in qtree. Non rimuovere o modificare altri file di sistema ODX a meno che non sia stato richiesto dal supporto tecnico.

Quando si utilizza la funzione ODX, esistono file di sistema ODX in ogni volume del sistema. Questi file consentono la rappresentazione point-in-time dei dati utilizzati durante il trasferimento ODX. I seguenti file di sistema si trovano nel livello root di ogni volume che contiene LUN o file in cui sono stati scaricati i dati:

- `.copy-offload` (una directory nascosta)
- `.tokens` (file sotto il nascosto `.copy-offload` directory)

È possibile utilizzare `copy-offload delete-tokens -path dir_path -node node_name` Comando per eliminare un qtree contenente un file ODX.

#### Casi di utilizzo per ODX

È necessario conoscere i casi di utilizzo per l'utilizzo di ODX su SVM in modo da poter determinare in quali circostanze ODX offre vantaggi in termini di performance.

I server e i client Windows che supportano ODX utilizzano l'offload delle copie come metodo predefinito per copiare i dati tra server remoti. Se il server o il client Windows non supporta ODX o l'offload delle copie ODX non riesce in qualsiasi momento, l'operazione di copia o spostamento ritorna alle tradizionali operazioni di lettura e scrittura per l'operazione di copia o spostamento.

I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti ODX:

- Intra-volume

I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Intervolume, stesso nodo, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

- Tra cluster

Le LUN di origine e di destinazione si trovano su volumi diversi che si trovano su nodi diversi tra cluster. Questo è supportato solo per SAN e non per SMB.

Esistono alcuni casi di utilizzo speciali aggiuntivi:

- Con l'implementazione di ONTAP ODX, è possibile utilizzare ODX per copiare i file tra le condivisioni SMB e le unità virtuali FC o iSCSI collegate.

È possibile utilizzare Esplora risorse, la CLI di Windows o PowerShell, Hyper-V o altre applicazioni che supportano ODX per copiare o spostare i file senza problemi utilizzando l'offload delle copie ODX tra le condivisioni SMB e le LUN connesse, a condizione che le condivisioni SMB e le LUN si trovino sullo stesso cluster.

- Hyper-V offre alcuni casi di utilizzo aggiuntivi per l'offload delle copie ODX:
  - È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

- Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
- L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.



Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

## Scopri di più sullo scaricamento della copia NVMe

La funzione di offload della copia NVMe consente a un host NVMe di trasferire le operazioni di copia dalla propria CPU alla CPU del controller di archiviazione ONTAP . L'host può copiare i dati da uno spazio dei nomi NVMe a un altro, riservando le risorse della CPU per i carichi di lavoro delle applicazioni.

Supponiamo, ad esempio, di dover ribilanciare i carichi di lavoro di archiviazione per migliorare la distribuzione delle prestazioni. Ciò richiede la migrazione di dieci macchine virtuali (VM) contenenti 45 namespace NVMe con una dimensione media di 500 GB ciascuna. Ciò significa che è necessario copiare circa 22,5 TB di dati. Invece di utilizzare la propria CPU per la migrazione dei dati, l'host può utilizzare l'offload della copia NVMe per evitare di ridurre le risorse della CPU per i carichi di lavoro delle applicazioni durante la copia dei dati.

### Supporto e limitazioni dell'offload della copia NVMe

L'offload della copia NVMe è supportato a partire da ONTAP 9.18.1. ONTAP non può avviare l'offload della copia NVMe; deve essere supportato e avviato dall'host.

Le seguenti limitazioni si applicano alle operazioni di copia offload NVMe con ONTAP:

- La dimensione massima supportata per l'operazione di copia è 16 MB.
- I dati possono essere migrati solo tra namespace NVMe all'interno dello stesso sottosistema.
- I dati possono essere migrati solo tra nodi nella stessa coppia HA.

## Amministrazione SAN

### Provisioning SAN

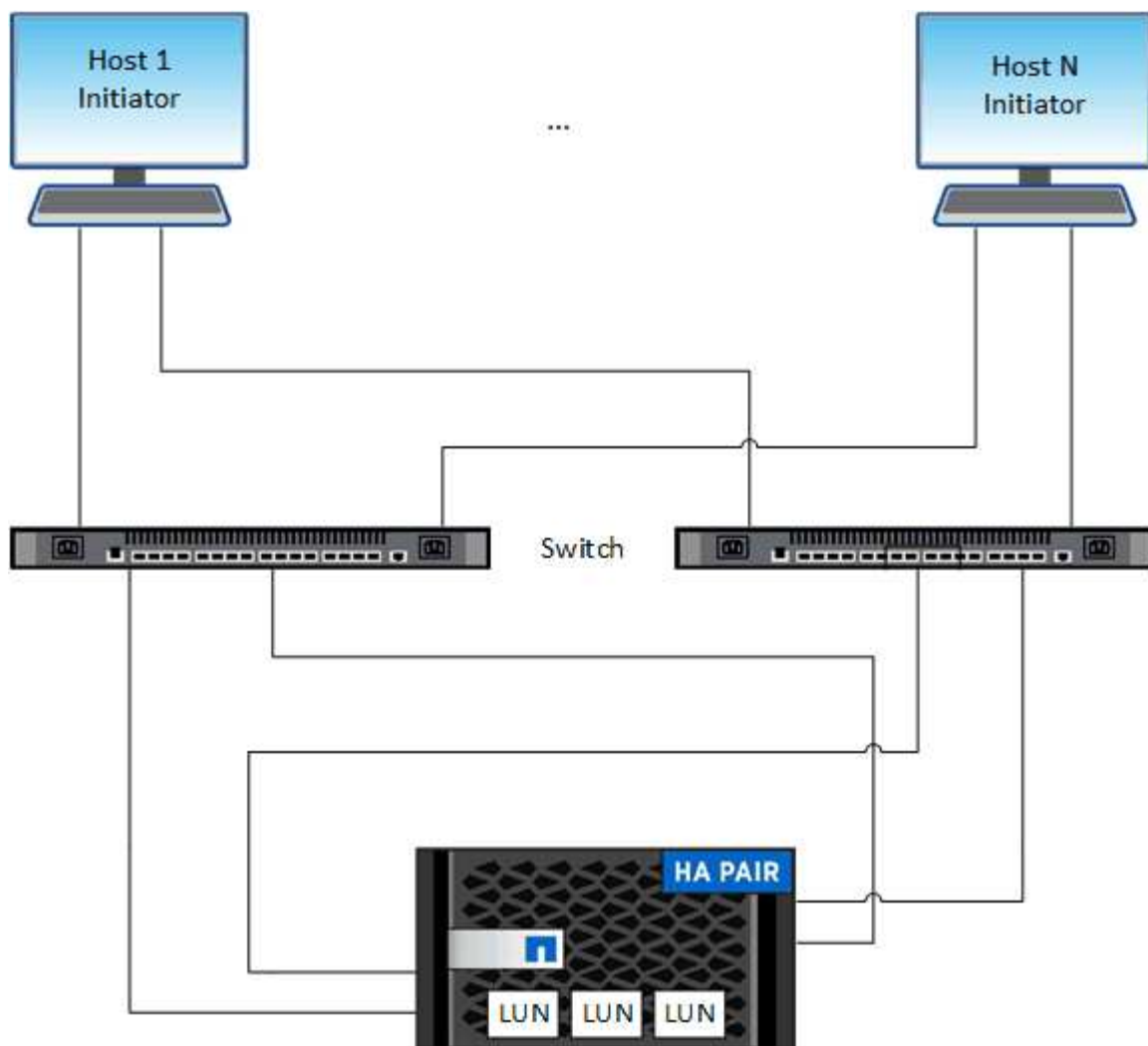
#### Panoramica sulla gestione SAN

Il contenuto di questa sezione illustra come configurare e gestire gli ambienti SAN con l'interfaccia a riga di comando (CLI) di ONTAP e Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione di sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), consultare i seguenti argomenti:

- ["Protocollo iSCSI"](#)
- ["Protocollo FC/FCoE"](#)

È possibile utilizzare i protocolli iSCSI e FC per fornire storage in un ambiente SAN.



Con iSCSI e FC, le destinazioni di storage sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. Si creano LUN e quindi le si associano ai gruppi di iniziatori (igroups). I gruppi di iniziatori sono tabelle di WWP host FC e nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN.

Le destinazioni FC si connettono alla rete tramite switch FC e adattatori lato host e sono identificate da nomi di porte mondiali (WWPN). Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN).

#### Per ulteriori informazioni

Se si dispone di un sistema di archiviazione ASA R2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 o ASA A20), consultare la ["Documentazione del sistema di storage ASA R2"](#).

#### Ulteriori informazioni sulle configurazioni degli array SAN all-flash

Gli array SAN all-flash NetApp (ASA) sono disponibili a partire da ONTAP 9,7. Gli ASA sono soluzioni solo SAN all-flash basate su piattaforme NetApp AFF comprovate.

Le piattaforme ASA includono quanto segue:

- ASA A150

- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800



A partire da ONTAP 9.16.0, un'esperienza ONTAP semplificata specifica per i clienti solo SAN è disponibile sui sistemi ASA R2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 o ASA A20). Se si dispone di un sistema ASA R2, consultare la ["Documentazione del sistema ASA R2"](#).

Le piattaforme ASA utilizzano Active-Active simmetrico per il multipathing. Tutti i percorsi sono attivi/ottimizzati, quindi in caso di failover dello storage, l'host non deve attendere che la transizione ALUA dei percorsi di failover riprenda l'i/O. In questo modo si riduce il tempo di failover.

### Configurare un ASA

Gli All-Flash SAN Array (ASA) seguono la stessa procedura di configurazione dei sistemi non ASA.

System Manager guida l'utente attraverso le procedure necessarie per inizializzare il cluster, creare un Tier locale, configurare i protocolli e eseguire il provisioning dello storage per ASA.

[Inizia subito a configurare il cluster di ONTAP.](#)

### Impostazioni e utility dell'host ASA

Le impostazioni dell'host per la configurazione degli array SAN all-flash (ASA) sono identiche a quelle di tutti gli altri host SAN.

È possibile scaricare ["Software NetApp host Utilities"](#) per gli host specifici dal sito di supporto.

### Metodi per identificare un sistema ASA

È possibile identificare un sistema ASA utilizzando Gestione di sistema o l'interfaccia a riga di comando (CLI) di ONTAP.

- **Dalla dashboard di System Manager:** Fare clic su **Cluster > Overview** e selezionare il nodo di sistema.

La **PERSONALITÀ** viene visualizzata come **All-Flash SAN Array**.

- **Dalla CLI:** Immettere il `san config show` comando.

Il valore dell'array SAN all-flash restituisce il valore vero per i sistemi ASA.

Ulteriori informazioni su `san config show` nella ["Riferimento al comando ONTAP"](#).

### Informazioni correlate

- ["Report tecnico 4968: Integrità e disponibilità dei dati degli array NetApp All-SAN"](#)
- ["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#)

## Configurare gli switch per FCoE

È necessario configurare gli switch per FCoE prima che il servizio FC possa essere eseguito sull'infrastruttura Ethernet esistente.

### Prima di iniziare

- La configurazione SAN deve essere supportata.

Per ulteriori informazioni sulle configurazioni supportate, consultare ["Tool di matrice di interoperabilità NetApp"](#).

- È necessario installare un Unified Target Adapter (UTA) sul sistema storage.

Se si utilizza un UTA2, è necessario impostarlo su cna modalità.

- Sull'host deve essere installato un adattatore di rete convergente (CNA).

### Fasi

1. Utilizzare la documentazione dello switch per configurare gli switch per FCoE.
2. Verificare che le impostazioni DCB di ogni nodo nel cluster siano state configurate correttamente.

```
run -node node1 -command dcb show
```

Le impostazioni DCB sono configurate sullo switch. Se le impostazioni non sono corrette, consultare la documentazione dello switch.

3. Verificare che l'accesso FCoE funzioni quando lo stato online della porta di destinazione FC è `true`.

```
fcip adapter show -fields node,adapter,status,state,speed,fabric-  
established,physical-protocol
```

Se lo stato in linea della porta di destinazione FC è `false`, consultare la documentazione dello switch.

### Informazioni correlate

- ["Tool di matrice di interoperabilità NetApp"](#)
- ["Report tecnico di NetApp 3800: Guida all'implementazione end-to-end Fibre Channel over Ethernet \(FCoE\)"](#)
- ["Cisco MDS 9000 NX-OS e SAN-OS Software Configuration Guide"](#)
- ["Prodotti Brocade"](#)

### Requisiti di sistema

La configurazione dei LUN implica la creazione di un LUN, la creazione di un igroup e la mappatura del LUN all'igroup. Il sistema deve soddisfare determinati prerequisiti prima di poter configurare le LUN.

- La matrice di interoperabilità deve elencare la configurazione SAN come supportata.

- L'ambiente SAN deve soddisfare i limiti di configurazione del controller e dell'host SAN specificati nella ["NetApp Hardware Universe"](#) Per la versione del software ONTAP in uso.
- È necessario installare una versione supportata delle utility host.

La documentazione relativa alle utility host fornisce ulteriori informazioni.

- È necessario disporre di LIF SAN nel nodo proprietario del LUN e nel partner ha del nodo proprietario.

#### Informazioni correlate

- ["Tool di matrice di interoperabilità NetApp"](#)
- ["Configurazione host SAN ONTAP"](#)
- ["Report tecnico di NetApp 4017: Best Practice SAN Fibre Channel"](#)

#### Cosa fare prima di creare un LUN

Prima di iniziare a configurare i LUN nel cluster, è necessario rivedere le linee guida relative alle LUN.

#### Perché le dimensioni effettive del LUN variano leggermente

Per quanto riguarda le dimensioni dei LUN, è necessario conoscere quanto segue.

- Quando si crea un LUN, le dimensioni effettive del LUN potrebbero variare leggermente in base al tipo di sistema operativo del LUN. Il tipo di sistema operativo LUN non può essere modificato dopo la creazione del LUN.
- Se si crea un LUN con le dimensioni massime del LUN, tenere presente che le dimensioni effettive del LUN potrebbero essere leggermente inferiori. ONTAP arrotonda il limite per essere leggermente inferiore.
- I metadati per ogni LUN richiedono circa 64 KB di spazio nell'aggregato contenente. Quando si crea un LUN, è necessario assicurarsi che l'aggregato contenente disponga di spazio sufficiente per i metadati del LUN. Se l'aggregato non contiene spazio sufficiente per i metadati del LUN, alcuni host potrebbero non essere in grado di accedere al LUN.

#### Linee guida per l'assegnazione degli ID LUN

In genere, l'ID LUN predefinito inizia con 0 e viene assegnato in incrementi di 1 per ogni LUN mappato aggiuntivo. L'host associa l'ID LUN alla posizione e al nome del percorso del LUN. L'intervallo di numeri ID LUN validi dipende dall'host. Per informazioni dettagliate, consultare la documentazione fornita con le utility host.

#### Linee guida per la mappatura delle LUN in igroups

- È possibile mappare un LUN solo una volta su un igroup.
- Come Best practice, è necessario mappare un LUN a un solo iniziatore specifico attraverso l'igroup.
- È possibile aggiungere un singolo iniziatore a più igroups, ma l'iniziatore può essere mappato a un solo LUN.
- Non è possibile utilizzare lo stesso ID LUN per due LUN mappati allo stesso igroup.
- È necessario utilizzare lo stesso tipo di protocollo per igroups e set di porte.

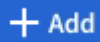
## Verificare e aggiungere la licenza FC o iSCSI del protocollo

Prima di abilitare l'accesso a blocchi per una macchina virtuale di storage (SVM) con FC o iSCSI, è necessario disporre di una licenza. Le licenze FC e iSCSI sono incluse in "ONTAP uno".

### Esempio 1. Fasi

#### System Manager

Se non si dispone di ONTAP ONE, verificare e aggiungere la licenza FC o iSCSI con Gestione sistema ONTAP (9,7 e versioni successive).

1. In System Manager, selezionare **Cluster > Settings > Licenses** (Cluster > Impostazioni > licenze)
2. Se la licenza non è presente nell'elenco, selezionare  e immettere la chiave di licenza.
3. Selezionare **Aggiungi**.

#### CLI

Se non si dispone di ONTAP ONE, verificare e aggiungere la licenza FC o iSCSI con la CLI ONTAP.

1. Verificare di disporre di una licenza attiva per FC o iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Se non si dispone di una licenza attiva per FC o iSCSI, aggiungere il codice di licenza.

```
license add -license-code <your_license_code>
```

## Eseguire il provisioning dello storage SAN

Questa procedura crea nuovi LUN su una VM di storage esistente che ha già configurato il protocollo FC o iSCSI.

### A proposito di questa attività

Questa procedura si applica ai sistemi FAS, AFF e ASA. Se hai un sistema ASA r2 (ASAA1K, ASAA90, ASA

A70, ASA A50, ASA A30, ASA A20 o ASA C30), segui ["questi passaggi"](#) per predisporre il tuo spazio di archiviazione. I sistemi ASA R2 forniscono un'esperienza ONTAP semplificata, specifica per i clienti solo SAN.

Se è necessario creare una nuova VM di storage e configurare il protocollo FC o iSCSI, vedere ["Configurare una SVM per FC"](#) oppure ["Configurare una SVM per iSCSI"](#).

Se la licenza FC non è abilitata, le LIF e le SVM sembrano essere in linea ma lo stato operativo è inattivo.

I LUN vengono visualizzati sull'host come dispositivi disco.



L'ALUA (Asymmetric Logical Unit Access) è sempre abilitato durante la creazione del LUN. Non è possibile modificare l'impostazione ALUA.

Per ospitare gli iniziatori, è necessario utilizzare lo zoning initiator singolo per tutte le LIF FC nella SVM.

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. Puoi disabilitare la QoS o scegliere un criterio QoS personalizzato durante il processo di provisioning o in un secondo momento.

## Esempio 2. Fasi


### System Manager

Creare LUN per fornire storage a un host SAN utilizzando il protocollo FC o iSCSI con Gestione di sistema di ONTAP (9.7 e versioni successive).

Per completare questa attività utilizzando System Manager Classic (disponibile con la versione 9,7 e precedenti), fare riferimento alla ["Configurazione iSCSI per Red Hat Enterprise Linux"](#)

### Fasi

1. Installare l'appropriato ["Utility host SAN"](#) sul proprio host.
2. In System Manager, fare clic su **Storage > LUN**, quindi su **Add**.
3. Inserire le informazioni richieste per creare il LUN.
4. È possibile fare clic su **altre opzioni** per eseguire una delle seguenti operazioni, a seconda della versione di ONTAP in uso.

Opzione	Disponibile a partire da
<ul style="list-style-type: none"><li>• Assegnare il criterio QoS ai LUN anziché al volume padre<ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; Storage and Optimization</b></li><li>◦ Selezionare <b>Performance Service Level</b>.</li><li>◦ Per applicare il criterio QoS ai singoli LUN anziché all'intero volume, selezionare <b>Applica questi limiti di performance a ogni LUN</b>.</li></ul><p>Per impostazione predefinita, i limiti di performance vengono applicati a livello di volume.</p></li></ul>	ONTAP 9.10.1
<ul style="list-style-type: none"><li>• Creare un nuovo gruppo di iniziatori utilizzando i gruppi di iniziatori esistenti<ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; INFORMAZIONI HOST</b></li><li>◦ Selezionare <b>New Initiator group using existing initiator groups</b> (nuovo gruppo iniziatore che utilizza</li></ul><div><p>Il tipo di sistema operativo per un igroup contenente altri igroup non può essere modificato dopo che è stato creato.</p></div></li></ul>	ONTAP 9.9.1
<ul style="list-style-type: none"><li>• Aggiungere una descrizione all'igroup o all'iniziatore host<p>La descrizione funge da alias per igroup o host initiator.</p><ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; INFORMAZIONI HOST</b></li></ul></li></ul>	ONTAP 9.9.1

- Creare il LUN su un volume esistente

ONTAP 9.9.1

Per impostazione predefinita, viene creata una nuova LUN in un nuovo volume.

- **Altre opzioni > Aggiungi LUN**
- Selezionare **LUN correlati al gruppo**.

- Disattivare QoS o scegliere un criterio QoS personalizzato

ONTAP 9.8

- **Altre opzioni > Storage and Optimization**
- Selezionare **Performance Service Level**.



In ONTAP 9.9.1 e versioni successive, se selezioni una policy QoS personalizzata, puoi anche selezionare il posizionamento manuale su un Tier locale specifico.

5. Per gli switch FC, eseguire la zona degli switch FC in base al numero WWPN. Utilizzare una zona per iniziatore e includere tutte le porte di destinazione in ciascuna zona.

6. Scopri le LUN sul tuo host.

Per VMware vSphere, utilizzare Virtual Storage Console (VSC) per rilevare e inizializzare le LUN.

7. Inizializzare le LUN e, facoltativamente, creare file system.

8. Verificare che l'host sia in grado di scrivere e leggere i dati sul LUN.

## CLI

Creare LUN per fornire storage a un host SAN utilizzando il protocollo FC o iSCSI con l'interfaccia CLI ONTAP.

1. Verificare di disporre di una licenza per FC o iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Se non si dispone di una licenza per FC o iSCSI, utilizzare `license add` comando.

```
license add -license-code <your_license_code>
```

3. Abilitare il servizio di protocollo su SVM:

**Per iSCSI:**

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

**Per FC:**

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Creare due LIF per le SVM su ciascun nodo:

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp supporta almeno un LIF iSCSI o FC per nodo per ogni SVM che fornisce dati. Tuttavia, per la ridondanza sono necessari due LIFS per nodo. Per iSCSI, si consiglia di configurare un minimo di due LIF per nodo in reti Ethernet separate.

5. Verificare che i file LIF siano stati creati e che il loro stato operativo sia *online*:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Crea le tue LUN:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

Il nome del LUN non può superare i 255 caratteri e non può contenere spazi.



L'opzione NVFAIL viene attivata automaticamente quando viene creata una LUN in un volume.

7. Crea i tuoi igroups:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Mappare i LUN a igroups:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. Verificare che i LUN siano configurati correttamente:

```
lun show -vserver <svm_name>
```

10. Facoltativamente, ["Creare un set di porte e associarlo a un igroup"](#).

11. Seguire i passaggi nella documentazione dell'host per abilitare l'accesso a blocchi su host specifici.

12. Utilizzare le utility host per completare la mappatura FC o iSCSI e rilevare le LUN sull'host.

### Informazioni correlate

- ["Panoramica sull'amministrazione SAN"](#)
- ["Configurazione host SAN ONTAP"](#)
- ["Visualizzare e gestire i gruppi SAN Initiator in System Manager"](#)
- ["Report tecnico di NetApp 4017: Best Practice SAN Fibre Channel"](#)

## Provisioning NVMe

### Panoramica di NVMe

È possibile utilizzare il protocollo NVMe (non-volatile Memory Express) per fornire storage in un ambiente SAN. Il protocollo NVMe è ottimizzato per le performance con lo storage a stato solido.

Per NVMe, le destinazioni di storage sono chiamate namespace. Uno spazio dei nomi NVMe è una quantità di storage non volatile che può essere formattata in blocchi logici e presentata a un host come dispositivo a blocchi standard. È possibile creare spazi dei nomi e sottosistemi, quindi mappare gli spazi dei nomi ai sottosistemi, in modo simile al modo in cui i LUN vengono forniti e mappati a igroups per FC e iSCSI.

Le destinazioni NVMe sono connesse alla rete attraverso un'infrastruttura FC standard utilizzando switch FC o un'infrastruttura TCP standard utilizzando switch Ethernet e adattatori lato host.

Il supporto per NVMe varia in base alla versione di ONTAP in uso. Vedere ["Supporto e limitazioni NVMe"](#) per ulteriori informazioni.

### Che cos'è NVMe

Il protocollo NVMe (nonvolatile memory express) è un protocollo di trasporto utilizzato per accedere a supporti di storage non volatili.

NVMe over Fabrics (NVMeoF) è un'estensione di NVMe definita dalle specifiche che consente la comunicazione basata su NVMe su connessioni diverse da PCIe. Questa interfaccia consente di collegare enclosure di storage esterne a un server.

NVMe è progettato per fornire un accesso efficiente ai dispositivi di storage costruiti con memoria non volatile, dalla tecnologia flash alle tecnologie di memoria persistente dalle performance più elevate. Pertanto, non presenta le stesse limitazioni dei protocolli di storage progettati per i dischi rigidi. I dispositivi flash e a stato solido (SSD) sono un tipo di memoria non volatile (NVM). NVM è un tipo di memoria che mantiene il contenuto durante un'interruzione dell'alimentazione. NVMe è un modo per accedere a tale memoria.

I vantaggi di NVMe includono maggiori velocità, produttività, throughput e capacità per il trasferimento dei dati. Le caratteristiche specifiche includono:

- NVMe è progettato per avere fino a 64 mila code.

Ciascuna coda può avere fino a 64 mila comandi simultanei.

- NVMe è supportato da più fornitori di hardware e software
- NVMe è più produttivo grazie alle tecnologie Flash che consentono tempi di risposta più rapidi
- NVMe consente più richieste di dati per ogni "request" inviata all'SSD.

NVMe richiede meno tempo per decodificare una "request" e non richiede il blocco dei thread in un programma multithread.

- NVMe supporta funzionalità che impediscono i colli di bottiglia a livello di CPU e consentono un'elevata scalabilità con l'espansione dei sistemi.

#### Informazioni sugli spazi dei nomi NVMe

Uno spazio dei nomi NVMe è una quantità di memoria non volatile (NVM) che può essere formattata in blocchi logici. Gli spazi dei nomi vengono utilizzati quando una macchina virtuale di storage viene configurata con il protocollo NVMe e sono l'equivalente dei LUN per i protocolli FC e iSCSI.

Uno o più spazi dei nomi vengono forniti e connessi a un host NVMe. Ogni namespace può supportare blocchi di varie dimensioni.

Il protocollo NVMe fornisce l'accesso agli spazi dei nomi attraverso più controller. Utilizzando i driver NVMe, supportati dalla maggior parte dei sistemi operativi, gli spazi dei nomi dei dischi a stato solido (SSD) vengono visualizzati come dispositivi a blocchi standard su cui i file system e le applicazioni possono essere implementati senza alcuna modifica.

Un NSID (Namespace ID) è un identificatore utilizzato da un controller per fornire l'accesso a uno spazio dei nomi. Quando si imposta l'NSID per un host o un gruppo di host, è anche possibile configurare l'accessibilità a un volume da parte di un host. Un blocco logico può essere mappato solo a un singolo gruppo host alla volta e un dato gruppo host non dispone di NSID duplicati.

#### Informazioni sui sottosistemi NVMe

Un sottosistema NVMe include uno o più controller NVMe, spazi dei nomi, porte del sottosistema NVM, un supporto di storage NVM e un'interfaccia tra il controller e il supporto di storage NVM. Quando si crea uno spazio dei nomi NVMe, per impostazione predefinita, non viene mappato a un sottosistema. È inoltre possibile scegliere di mappare un sottosistema nuovo o esistente.

#### Informazioni correlate

- Impara a ["Eseguire il provisioning dello storage NVMe"](#) utilizzare i sistemi ASA, AFF e FAS
- Impara a ["mappatura di un namespace NVMe a un sottosistema"](#) sui sistemi ASA AFF e FAS.
- ["Configurare gli host SAN e i client cloud"](#)

- Imparare a ["Provisioning dello storage SAN"](#) utilizzare i sistemi storage ASA R2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 o ASA A20).

## Requisiti di licenza NVMe

A partire da ONTAP 9.5 è necessaria una licenza per supportare NVMe. Se NVMe è attivato in ONTAP 9.4, viene concesso un periodo di valutazione di 90 giorni per l'acquisizione della licenza dopo l'aggiornamento a ONTAP 9.5.

È possibile attivare la licenza utilizzando il seguente comando:

```
system license add -license-code NVMe_license_key
```

## Configurazione, supporto e limitazioni NVMe

A partire da ONTAP 9.4, la ["NVMe \(non-volatile Memory Express\)"](#) il protocollo è disponibile per gli ambienti SAN. FC-NVMe utilizza le stesse procedure di configurazione fisica e di zoning delle reti FC tradizionali, ma consente una maggiore larghezza di banda, IOPS aumentati e latenza ridotta rispetto a FC-SCSI.

Il supporto e le limitazioni di NVMe variano in base alla versione di ONTAP, alla piattaforma e alla configurazione. Per ulteriori informazioni sulla configurazione specifica, consultare la ["Tool di matrice di interoperabilità NetApp"](#). Per i limiti supportati, vedere ["Hardware Universe"](#).



Il numero massimo di nodi per cluster è disponibile in Hardware Universe in **combinazione di piattaforme supportate**.

## Configurazione

- Puoi configurare la tua configurazione NVMe utilizzando un singolo fabric o multi-fabric.
- È necessario configurare una LIF di gestione per ogni SVM che supporti SAN.
- 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 NetApp"](#).

- 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.

Un fabric può essere costituito da uno o più switch e i controller di storage possono essere collegati a più switch.

## Caratteristiche

Le seguenti funzionalità NVMe sono supportate in base alla tua versione di ONTAP.

Inizio con ONTAP...	NVMe supporta
9.17.1	<ul style="list-style-type: none"> <li>• Accesso host NVMe/FC e NVMe/TCP con sincronizzazione attiva SnapMirror per carichi di lavoro VMware.</li> </ul>

9.15.1	<ul style="list-style-type: none"> <li>• Configurazioni IP MetroCluster a quattro nodi su NVMe/TCP</li> </ul>
9.14.1	<ul style="list-style-type: none"> <li>• Impostazione della priorità dell'host nel sottosistema (QoS a livello di host)</li> </ul>
9.12.1	<ul style="list-style-type: none"> <li>• Configurazioni IP MetroCluster a quattro nodi su NVMe/FC</li> <li>• Le configurazioni MetroCluster non sono supportate per le reti NVMe front-end prima di ONTAP 9.12.1.</li> <li>• Le configurazioni MetroCluster non sono supportate su NVMe/TCP.</li> </ul>
9.10.1	<a href="#">Ridimensionamento di uno spazio dei nomi</a>
9.9.1	<ul style="list-style-type: none"> <li>• La coesistenza di namespace e LUN nello stesso volume</li> </ul>
9.8	<ul style="list-style-type: none"> <li>• Coesistenza del protocollo</li> </ul> <p>I protocolli SCSI, NAS e NVMe possono esistere sulla stessa Storage Virtual Machine (SVM).</p> <p>Prima di ONTAP 9,8, NVMe può essere l'unico protocollo sulla SVM.</p>
9.6	<ul style="list-style-type: none"> <li>• blocchi da 512 byte e blocchi da 4096 byte per namespace</li> </ul> <p>4096 è il valore predefinito. 512 deve essere utilizzato solo se il sistema operativo host non supporta blocchi da 4096 byte.</p> <ul style="list-style-type: none"> <li>• Spostamento del volume con spazi dei nomi mappati</li> </ul>
9.5	<ul style="list-style-type: none"> <li>• Failover/giveback coppia ha multipath</li> </ul>

## Protocolli

Sono supportati i seguenti protocolli NVMe.

Protocollo	Inizio con ONTAP...	Consentito da...
TCP	9.10.1	Predefinito
FC	9.4	Predefinito

A partire da ONTAP 9.8, è possibile configurare i protocolli SCSI, NAS e NVMe sulla stessa macchina virtuale

per lo storage (SVM).

In ONTAP 9.7 e versioni precedenti, NVMe può essere l'unico protocollo su SVM.

### Spazi dei nomi

Quando si utilizzano gli namespace NVMe, devi essere consapevole di quanto segue:

- Per ONTAP 9.15.1 e versioni precedenti, ONTAP non supporta il comando di gestione DataSet (disallocare) NVMe con NVMe per il recupero dello spazio.
- Non è possibile utilizzare SnapRestore per ripristinare uno spazio dei nomi da una LUN o viceversa.
- La garanzia di spazio per gli spazi dei nomi è la stessa della garanzia di spazio del volume contenente.
- Non è possibile creare un namespace in una transizione di volumi da Data ONTAP 7-Mode.
- Gli spazi dei nomi non supportano quanto segue:
  - Ridenominazione
  - Spostamento tra volumi
  - Copia inter-volume
  - Copia su richiesta

### Ulteriori limitazioni

**Le seguenti funzioni di ONTAP non sono supportate dalle configurazioni NVMe:**

- Virtual Storage Console
- Prenotazioni persistenti

**Quanto segue si applica solo ai nodi che eseguono ONTAP 9.4:**

- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- Il servizio NVMe deve essere creato prima della creazione di NVMe LIF.

### Informazioni correlate

["Best practice per LE SAN moderne"](#)

### Configurare una VM di storage per NVMe

Se si desidera utilizzare il protocollo NVMe su un nodo, è necessario configurare la SVM in modo specifico per NVMe.


### Prima di iniziare

Gli adattatori FC o Ethernet devono supportare NVMe. Gli adattatori supportati sono elencati nella ["NetApp Hardware Universe"](#).

### Esempio 3. Fasi

#### System Manager

Configurazione di una VM di storage per NVMe con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare NVMe su una nuova VM di storage	Per configurare NVMe su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>NVMe</b> per il protocollo di accesso*.</li><li>4. Selezionare <b>Enable NVMe/FC</b> or <b>Enable NVMe/TCP</b> and <b>Save</b>.</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi fare clic su  accanto al protocollo NVMe.</li><li>4. Selezionare <b>Enable NVMe/FC</b> or <b>Enable NVMe/TCP</b> and <b>Save</b>.</li></ol>

#### CLI

Configurare una VM di storage per NVMe con l'interfaccia utente di ONTAP.

1. Se non si desidera utilizzare una SVM esistente, crearne una:

```
vserver create -vserver <SVM_name>
```

- a. Verificare che la SVM sia stata creata:

```
vserver show
```

2. Verificare che nel cluster siano installati adattatori compatibili con NVMe o TCP:

Per NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

Per TCP:

```
network port show
```

Ulteriori informazioni su `network port show` nella ["Riferimento al comando ONTAP"](#).

3. Se si utilizza ONTAP 9.7 o versioni precedenti, rimuovere tutti i protocolli da SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi, fcp, nfs, cifs, ndmp
```

A partire da ONTAP 9.8, non è necessario rimuovere altri protocolli quando si aggiunge NVMe.

4. Aggiungere il protocollo NVMe a SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Se si utilizza ONTAP 9.7 o versioni precedenti, verificare che NVMe sia l'unico protocollo consentito su SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe deve essere l'unico protocollo visualizzato in `allowed protocols` colonna.

6. Creare il servizio NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Verificare che il servizio NVMe sia stato creato:

```
vserver nvme show -vserver <SVM_name>
```

La `Administrative Status SVM` deve essere elencata come `up`. Ulteriori informazioni su `up` nella ["Riferimento al comando ONTAP"](#).

8. Creare una LIF NVMe/FC:

- Per ONTAP 9.9.1 o versione precedente, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-role data -data-protocol fc-nvme -home-node <home_node> -home  
-port <home_port>
```

- Per ONTAP 9.10.1 o versioni successive, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- Per ONTAP 9.10.1 o versioni successive, TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

## 9. Creare una LIF NVMe/FC sul nodo partner ha:

- Per ONTAP 9.9.1 o versione precedente, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Per ONTAP 9.10.1 o versioni successive, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

- Per ONTAP 9.10.1 o versioni successive, TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. Verificare che le LIF NVMe/FC siano state create:

```
network interface show -vserver <SVM_name>
```

11. Creare un volume sullo stesso nodo di LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate  
<aggregate_name> -size <volume_size>
```

Se viene visualizzato un messaggio di avviso relativo al criterio di efficienza automatica, è possibile ignorarlo in modo sicuro.

## Eeguire il provisioning dello storage NVMe

Utilizza questi passaggi per creare namespace ed eseguire il provisioning dello storage per qualsiasi host NVMe supportato su una VM di storage esistente.

### A proposito di questa attività

Questa procedura si applica ai sistemi FAS, AFF e ASA. Se hai un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), segui ["questi passaggi"](#) per predisporre il tuo spazio di archiviazione. I sistemi ASA R2 forniscono un'esperienza ONTAP semplificata, specifica per i clienti solo SAN.

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

### Prima di iniziare

La VM di storage deve essere configurata per NVME e il trasporto FC o TCP deve essere già impostato.

## System Manager

Utilizzando Gestione di sistema di ONTAP (9.7 e versioni successive), creare spazi dei nomi per fornire lo storage utilizzando il protocollo NVMe.

### Fasi

1. In System Manager, fare clic su **Storage > NVMe Namespaces**, quindi fare clic su **Add**.

Per creare un nuovo sottosistema, fare clic su **altre opzioni**.

2. Se si utilizza ONTAP 9.8 o versione successiva e si desidera disattivare la qualità del servizio o scegliere un criterio di qualità del servizio personalizzato, fare clic su **altre opzioni**, quindi in **archiviazione e ottimizzazione** selezionare **livello di servizio delle prestazioni**.
3. Zone your FC switch by WWPN (zone switch FC in base al numero WWPN Utilizzare una zona per iniziatore e includere tutte le porte di destinazione in ciascuna zona).
4. Sul tuo host, scopri i nuovi spazi dei nomi.
5. Inizializzare lo spazio dei nomi e formattarlo con un file system.
6. Verificare che l'host sia in grado di scrivere e leggere i dati sullo spazio dei nomi.

### CLI

Utilizzando l'interfaccia CLI di ONTAP, creare spazi dei nomi per fornire storage utilizzando il protocollo NVMe.

Questa procedura crea uno spazio dei nomi e un sottosistema NVMe su una VM di storage esistente già configurata per il protocollo NVMe, quindi mappa lo spazio dei nomi al sottosistema per consentire l'accesso ai dati dal sistema host.

Per configurare la VM di storage per NVMe, vedere ["Configurare una SVM per NVMe"](#).

### Fasi

1. Verificare che la SVM sia configurata per NVMe:

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

NVMe dovrebbe essere visualizzato sotto `allowed-protocols` colonna.

2. Creare lo spazio dei nomi NVMe:



Il volume a cui si fa riferimento con il `-path` parametro deve già esistere oppure è necessario crearne uno prima di eseguire questo comando.

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size  
<size_of_namespace> -ostype <OS_type>
```

3. Creare il sottosistema NVMe:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem  
<name_of_subsystem> -ostype <OS_type>
```

Il nome del sottosistema NVMe rileva la distinzione tra maiuscole e minuscole. Deve contenere da 1 a 96 caratteri. Sono consentiti caratteri speciali.

4. Verificare che il sottosistema sia stato creato:

```
vserver nvme subsystem show -vserver <svm_name>
```

Il nvme il sottosistema deve essere visualizzato sotto Subsystem colonna.

5. Ottenere l'NQN dall'host.
6. Aggiungere l'NQN host al sottosistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mappare lo spazio dei nomi nel sottosistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem  
<subsystem_name> -path <path>
```

Uno spazio dei nomi può essere mappato solo a un singolo sottosistema.

8. Verificare che lo spazio dei nomi sia mappato al sottosistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

Il sottosistema deve essere elencato come Attached subsystem.

## Mappare uno spazio dei nomi NVMe in un sottosistema

L'associazione di un namespace NVMe a un sottosistema consente l'accesso ai dati dall'host. È possibile mappare un namespace NVMe a un sottosistema quando si esegue il provisioning dello storage oppure è possibile farlo dopo che è stato eseguito il provisioning dello storage.

A partire da ONTAP 9.17.1, se si utilizza una configurazione ActiveSync SnapMirror, è possibile aggiungere una SVM a un host come server virtuale prossimale durante l'aggiunta dell'host a un sottosistema NVMe. I percorsi ottimizzati per un namespace in un sottosistema NVMe vengono pubblicati su un host solo dalla SVM configurata come server virtuale prossimale.

A partire da ONTAP 9.14.1, è possibile assegnare priorità all'allocazione delle risorse per host specifici. Per impostazione predefinita, quando un host viene aggiunto al sottosistema NVMe, viene assegnata una priorità regolare. È possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per modificare manualmente la priorità predefinita da normale ad alta. Agli host assegnati una priorità alta viene assegnato un numero maggiore di code i/o e profondità di coda.



Se si desidera assegnare una priorità elevata a un host aggiunto a un sottosistema in ONTAP 9.13.1 o versioni precedenti, è possibile farlo [modificare la priorità dell'host](#).

## Prima di iniziare

Lo spazio dei nomi e il sottosistema devono essere già creati. Per creare uno spazio dei nomi e un sottosistema, vedere ["Eseguire il provisioning dello storage NVMe"](#).

## Mappa uno spazio dei nomi NVMe

### Fasi

1. Ottenere l'NQN dall'host.
2. Aggiungere l'NQN host al sottosistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Se si desidera modificare la priorità predefinita dell'host da normale ad alta, utilizzare l' `-priority high` opzione. Questa opzione è disponibile a partire da ONTAP 9.14.1. Ulteriori informazioni su `vserver nvme subsystem host add` nella ["Riferimento al comando ONTAP"](#).

Se si desidera aggiungere un SVM come `proximal-vserver` a un host durante l'aggiunta dell'host a un sottosistema NVMe in una configurazione di sincronizzazione attiva SnapMirror, è possibile utilizzare `-proximal-vservers` Opzione. Questa opzione è disponibile a partire da ONTAP 9.17.1. È possibile aggiungere l'SVM di origine o di destinazione, o entrambe. L'SVM in cui si esegue questo comando è quella predefinita.

3. Mappare lo spazio dei nomi nel sottosistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem  
<subsystem_name> -path <path>
```

Uno spazio dei nomi può essere mappato solo a un singolo sottosistema. Ulteriori informazioni su `vserver nvme subsystem map add` nella ["Riferimento al comando ONTAP"](#).

4. Verificare che lo spazio dei nomi sia mappato al sottosistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

Il sottosistema deve essere elencato come `Attached subsystem`. Ulteriori informazioni su `vserver nvme namespace show` nella ["Riferimento al comando ONTAP"](#).

## Gestire le LUN

### Modificare il gruppo di criteri QoS LUN

A partire da ONTAP 9.10.1, è possibile utilizzare System Manager per assegnare o rimuovere criteri di qualità del servizio (QoS) su più LUN contemporaneamente.



Se il criterio QoS è assegnato a livello di volume, deve essere modificato a livello di volume. È possibile modificare il criterio QoS a livello di LUN solo se è stato originariamente assegnato a livello di LUN.

#### Fasi

1. In System Manager, fare clic su **Storage > LUN**.
2. Selezionare il LUN o i LUN che si desidera modificare.

Se si modificano più LUN alla volta, le LUN devono appartenere alla stessa Storage Virtual Machine (SVM). Se si selezionano LUN che non appartengono alla stessa SVM, l'opzione per modificare il gruppo di criteri QoS non viene visualizzata.

3. Fare clic su **More** (Altro) e selezionare **Edit QoS Policy Group** (Modifica gruppo policy QoS).

### Convertire un LUN in uno spazio dei nomi

A partire da ONTAP 9.11.1, è possibile utilizzare l'interfaccia CLI di ONTAP per convertire un LUN esistente in uno spazio dei nomi NVMe.

#### Prima di iniziare

- Il LUN specificato non deve avere mappe esistenti per un igroup.
- La LUN non deve trovarsi in una SVM configurata MetroCluster o in una relazione di sincronizzazione attiva SnapMirror.
- Il LUN non deve essere un endpoint del protocollo o un endpoint del protocollo.
- Il LUN non deve avere un prefisso diverso da zero e/o un flusso di suffissi diverso da zero.
- Il LUN non deve far parte di uno snapshot o della relazione di destinazione di SnapMirror come LUN di sola lettura.

#### Fase

1. Convertire una LUN in un namespace NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```


### Portare un LUN offline

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione di sistema per disattivare le LUN. Prima di ONTAP 9.10.1, è necessario utilizzare l'interfaccia utente di ONTAP per disattivare le LUN.

## System Manager

### Fasi

1. In System Manager, fare clic su **Storage>LUN**.
2. Portare una singola LUN o più LUN offline

Se si desidera...	Eeguire questa operazione...
Portare una singola LUN offline	Accanto al nome del LUN, fare clic su  e selezionare <b>Take Offline</b> .
Portare più LUN offline	<ol style="list-style-type: none"><li>1. Selezionare i LUN che si desidera disattivare.</li><li>2. Fare clic su <b>More</b> (Altro) e selezionare <b>take Offline</b> (non in linea).</li></ol>

### CLI

Quando si utilizza l'interfaccia CLI, è possibile scollegare un solo LUN alla volta.

### Fase

1. Portare il LUN offline:

```
lun offline <lun_name> -vserver <SVM_name>
```

## Ridimensionare un LUN in ONTAP

È possibile aumentare o diminuire le dimensioni di un LUN.

### A proposito di questa attività

Questa procedura si applica ai sistemi FAS, AFF e ASA. Se hai un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), segui ["questi passaggi"](#) per aumentare le dimensioni di un'unità di stoccaggio. I sistemi ASA R2 forniscono un'esperienza ONTAP semplificata, specifica per i clienti solo SAN.



Impossibile ridimensionare le LUN Solaris.

### Aumentare le dimensioni di un LUN

Le dimensioni del LUN possono variare a seconda della versione di ONTAP in uso.

Versione di ONTAP	Dimensione massima del LUN
ONTAP 9.12.1P2 e versioni successive	128 TB per piattaforme AFF, FAS e ASA


ONTAP 9.8 e versioni successive	<ul style="list-style-type: none"> <li>• 128 TB per le piattaforme ASA (All-Flash SAN Array)</li> <li>• 16 TB per piattaforme non ASA</li> </ul>
ONTAP 9.5, 9.6, 9.7	16 TB
ONTAP 9.4 o versioni precedenti	10 volte la dimensione del LUN originale, ma non superiore a 16 TB, che corrisponde alla dimensione massima del LUN. Ad esempio, se si crea un LUN da 100 GB, è possibile farlo crescere solo fino a 1,000 GB. La dimensione massima effettiva del LUN potrebbe non essere esattamente di 16 TB. ONTAP arrotonda il limite per essere leggermente inferiore.

Non è necessario portare il LUN offline per aumentare le dimensioni. Tuttavia, dopo aver aumentato le dimensioni, è necessario eseguire nuovamente la scansione del LUN sull'host per consentire all'host di riconoscere la modifica delle dimensioni.

#### Esempio 4. Fasi

##### System Manager

Aumenta le dimensioni di un LUN con Gestione di sistema di ONTAP (9.7 e versioni successive).

1. In System Manager, fare clic su **Storage > LUN**.
2. Fare clic su  e selezionare **Modifica**.
3. In **Storage and Optimization** (Storage e ottimizzazione), aumentare le dimensioni del LUN e di **Save** (Salva).

##### CLI

Aumentare le dimensioni di un LUN con l'interfaccia CLI di ONTAP.

1. Aumentare le dimensioni del LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

Ulteriori informazioni su `lun resize` nella ["Riferimento al comando ONTAP"](#).

2. Verificare l'aumento delle dimensioni del LUN:

```
lun show -vserver <SVM_name>
```

Le operazioni ONTAP arrotondano la dimensione massima effettiva del LUN, in modo che sia leggermente inferiore al valore previsto. Inoltre, le dimensioni effettive del LUN potrebbero variare leggermente in base al tipo di sistema operativo del LUN. Per ottenere il valore esatto ridimensionato, eseguire i seguenti comandi in modalità avanzata:

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+

Ulteriori informazioni su `lun show` nella ["Riferimento al comando ONTAP"](#).

1. Eseguire nuovamente la scansione del LUN sull'host.
2. Seguire la documentazione dell'host per rendere visibile la dimensione del LUN appena creato al file system host.

### Ridurre le dimensioni di un LUN

Prima di ridurre le dimensioni di un LUN, l'host deve migrare i blocchi contenenti i dati del LUN nel limite delle dimensioni del LUN più piccole. È necessario utilizzare uno strumento come SnapCenter per garantire che il LUN venga ridotto correttamente senza troncature i blocchi contenenti dati LUN. Si sconsiglia di ridurre manualmente le dimensioni del LUN.

Una volta ridotte le dimensioni del LUN, ONTAP notifica automaticamente all'iniziatore che le dimensioni del LUN sono diminuite. Tuttavia, potrebbero essere necessari ulteriori passaggi sull'host per il riconoscimento delle nuove dimensioni del LUN. Consultare la documentazione dell'host per informazioni specifiche sulla riduzione delle dimensioni della struttura del file host.

### Spostare un LUN

È possibile spostare un LUN tra i volumi all'interno di una macchina virtuale di storage (SVM), ma non è possibile spostare un LUN tra le SVM. Le LUN spostate tra i volumi all'interno di una SVM vengono spostate immediatamente e senza perdita di connettività.

#### Prima di iniziare

Se il LUN utilizza la mappa LUN selettiva (SLM, Selective LUN Map), è necessario farlo ["Modificare l'elenco dei nodi di reporting SLM"](#) Includere il nodo di destinazione e il partner ha prima di spostare la LUN.

#### A proposito di questa attività

Le funzionalità di efficienza dello storage, come deduplica, compressione e compattazione, non vengono mantenute durante uno spostamento del LUN. Devono essere riapplicati una volta completato lo spostamento del LUN.

La data Protection tramite snapshot si verifica a livello di volume. Pertanto, quando si sposta un LUN, questo rientra nello schema di protezione dei dati del volume di destinazione. Se non sono stati creati snapshot per il volume di destinazione, gli snapshot del LUN non vengono creati. Inoltre, tutti gli snapshot della LUN rimangono nel volume originale fino all'eliminazione di tali snapshot.

Non è possibile spostare un LUN nei seguenti volumi:

- Un volume di destinazione SnapMirror
- Il volume root SVM

Non è possibile spostare i seguenti tipi di LUN:

- LUN creata da un file

- LUN in stato NVFail
- Un LUN che si trova in una relazione di condivisione del carico
- Un LUN di classe protocollo-endpoint

Quando i nodi di un cluster si trovano su versioni diverse ONTAP , è possibile spostare una LUN tra volumi su nodi diversi solo se l'origine si trova su una versione successiva a quella di destinazione. Ad esempio, se il nodo del volume di origine si trova su ONTAP 9.15.1 e il nodo del volume di destinazione si trova su ONTAP 9.16.1, non è possibile spostare la LUN. È possibile spostare le LUN tra volumi su nodi che si trovano sulla stessa versione ONTAP .



Per i LUN Solaris os\_TYPE di 1 TB o superiore, l'host potrebbe riscontrare un timeout durante lo spostamento del LUN. Per questo tipo di LUN, è necessario smontare il LUN prima di iniziare lo spostamento.


## Esempio 5. Fasi

### System Manager

Spostamento di un LUN con Gestore di sistema di ONTAP (9.7 e versioni successive).

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per creare un nuovo volume quando si sposta una singola LUN. In ONTAP 9.8 e 9.9.1, il volume su cui si sposta il LUN deve esistere prima di iniziare lo spostamento del LUN.

#### Fasi

1. In System Manager, fare clic su **Storage>LUN**.
2. Fare clic con il pulsante destro del mouse sul LUN che si desidera spostare, quindi fare clic su  e selezionare **Sposta LUN**.

In ONTAP 9.10.1, selezionare per spostare il LUN su **un volume esistente** o su **nuovo volume**.

Se si sceglie di creare un nuovo volume, fornire le specifiche del volume.

3. Fare clic su **Sposta**.

### CLI

Spostare un LUN con l'interfaccia utente di ONTAP.

1. Spostare il LUN:

```
lun move start
```

Durante un breve periodo di tempo, il LUN è visibile sia sul volume di origine che su quello di destinazione. Questo è previsto e viene risolto al termine del trasferimento.

2. Tenere traccia dello stato dello spostamento e verificare che il completamento sia stato completato correttamente:

```
lun move show
```

### Informazioni correlate

- ["Mappa LUN selettiva"](#)

### Elimina LUN

È possibile eliminare un LUN da una macchina virtuale di storage (SVM) se non è più necessario il LUN.

### Prima di iniziare

Il LUN deve essere dismappato dal relativo igroup prima di poterlo eliminare.

#### Fasi

1. Verificare che l'applicazione o l'host non stia utilizzando il LUN.
2. Dismappare il LUN dall'igroup:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<LUN_name> -igroup <igroup_name>
```

3. Eliminare il LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Verificare che il LUN sia stato eliminato:

```
lun show -vserver <SVM_name>
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol16/lun8	online	mapped	windows	10.00GB

## Cosa fare prima di copiare le LUN

Prima di copiare un LUN, è necessario essere a conoscenza di alcuni elementi.

Gli amministratori dei cluster possono copiare un LUN tra le macchine virtuali di storage (SVM) all'interno del cluster utilizzando `lun copy` comando. Gli amministratori dei cluster devono stabilire la relazione di peering della macchina virtuale di storage (SVM) utilizzando `vserver peer create` Prima di eseguire un'operazione di copia del LUN tra SVM. Lo spazio nel volume di origine deve essere sufficiente per un clone del SIS.

I LUN delle snapshot possono essere utilizzati come LUN di origine per il `lun copy` comando. Quando si copia un LUN mediante il `lun copy` comando, la copia LUN è immediatamente disponibile per l'accesso in lettura e scrittura. Il LUN di origine rimane invariato grazie alla creazione di una copia del LUN. Sia il LUN di origine che la copia del LUN esistono come LUN univoci con numeri di serie LUN diversi. Le modifiche apportate al LUN di origine non si riflettono nella copia del LUN e le modifiche apportate alla copia del LUN non si riflettono nel LUN di origine. La mappatura LUN del LUN di origine non viene copiata nel nuovo LUN; la copia del LUN deve essere mappata.

La data Protection tramite snapshot si verifica a livello di volume. Pertanto, se si copia un LUN in un volume diverso dal volume del LUN di origine, il LUN di destinazione rientra nello schema di protezione dei dati del volume di destinazione. Se non sono stati creati snapshot per il volume di destinazione, non vengono create snapshot della copia LUN.

La copia delle LUN è un'operazione senza interruzioni.

Non è possibile copiare i seguenti tipi di LUN:

- LUN creata da un file
- LUN in stato NVFAIL
- Un LUN che si trova in una relazione di condivisione del carico
- Un LUN di classe protocollo-endpoint

Ulteriori informazioni su `lun copy` nella ["Riferimento al comando ONTAP"](#).

## Esaminare lo spazio configurato e utilizzato di un LUN

Conoscere lo spazio configurato e lo spazio effettivo utilizzato per le LUN può aiutare a determinare la quantità di spazio che può essere recuperato durante la rigenerazione dello spazio, la quantità di spazio riservato contenente dati e la dimensione totale configurata rispetto alla dimensione effettiva utilizzata per una LUN.

### Fase

1. Visualizzare lo spazio configurato rispetto allo spazio effettivo utilizzato per un LUN:

```
lun show
```

L'esempio seguente mostra lo spazio configurato rispetto allo spazio effettivo utilizzato dalle LUN nella SVM (Storage Virtual Machine) vs3:

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

vserver	path	size	space-reserve	size-used
vs3	/vol/vol0/lun1	50.01GB	disabled	25.00GB
vs3	/vol/vol0/lun1_backup	50.01GB	disabled	32.15GB
vs3	/vol/vol0/lun2	75.00GB	disabled	0B
vs3	/vol/volospace/lun0	5.00GB	enabled	4.50GB

4 entries were displayed.

Ulteriori informazioni su `lun show` nella ["Riferimento al comando ONTAP"](#).

## Controllo e monitoraggio delle performance i/o per le LUN utilizzando la QoS dello storage

È possibile controllare le prestazioni di input/output (i/o) alle LUN assegnando LUN ai gruppi di criteri Storage QoS. È possibile controllare le performance di i/o per garantire che i carichi di lavoro raggiungano specifici obiettivi di performance o per ridurre il carico di lavoro che ha un impatto negativo su altri carichi di lavoro.

### A proposito di questa attività

I gruppi di policy applicano un limite massimo di throughput (ad esempio, 100 MB/s). È possibile creare un gruppo di criteri senza specificare un throughput massimo, che consente di monitorare le performance prima di controllare il carico di lavoro.

È inoltre possibile assegnare le macchine virtuali di storage (SVM) con volumi FlexVol e LUN ai gruppi di

policy.

Tenere presente i seguenti requisiti relativi all'assegnazione di un LUN a un gruppo di criteri:

- Il LUN deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri.

Specificare la SVM quando si crea il gruppo di criteri.

- Se si assegna un LUN a un gruppo di criteri, non è possibile assegnare il volume o la SVM contenente il LUN a un gruppo di criteri.

Per ulteriori informazioni sull'utilizzo di Storage QoS, consultare ["Riferimento per l'amministrazione del sistema"](#).

## Fasi

1. Utilizzare `qos policy-group create` per creare un gruppo di criteri.

Ulteriori informazioni su `qos policy-group create` nella ["Riferimento al comando ONTAP"](#).

2. Utilizzare `lun create` o il `lun modify` con il `-qos-policy-group` Parametro per assegnare un LUN a un gruppo di criteri.

Ulteriori informazioni su `lun` nella ["Riferimento al comando ONTAP"](#).

3. Utilizzare `qos statistics` comandi per visualizzare i dati delle performance.
4. Se necessario, utilizzare `qos policy-group modify` comando per regolare il limite massimo di throughput del gruppo di criteri.

Ulteriori informazioni su `qos policy-group modify` nella ["Riferimento al comando ONTAP"](#).

## Strumenti disponibili per monitorare efficacemente le LUN

Sono disponibili strumenti che consentono di monitorare efficacemente le LUN ed evitare di esaurire lo spazio disponibile.

- Active IQ Unified Manager è uno strumento gratuito che ti consente di gestire tutto lo storage in tutti i cluster del tuo ambiente.
- System Manager è un'interfaccia utente grafica integrata in ONTAP che consente di gestire manualmente le esigenze di storage a livello di cluster.
- OnCommand Insight offre una singola vista dell'infrastruttura storage e consente di impostare il monitoraggio automatico, gli avvisi e i report quando LUN, volumi e aggregati stanno esaurendo lo spazio di storage.

## Funzionalità e limitazioni delle LUN in transizione

In un ambiente SAN, è necessario un'interruzione del servizio durante la transizione di un volume 7-Mode a ONTAP. Per completare la transizione, è necessario spegnere gli host. Dopo la transizione, è necessario aggiornare le configurazioni host prima di poter iniziare a fornire i dati in ONTAP

È necessario pianificare una finestra di manutenzione durante la quale è possibile arrestare gli host e

completare la transizione.

I LUN che sono stati trasferiti da Data ONTAP in 7-Mode a ONTAP presentano alcune funzionalità e restrizioni che influiscono sul modo in cui è possibile gestire i LUN.

Con i LUN in transizione è possibile effettuare le seguenti operazioni:

- Visualizzare il LUN utilizzando `lun show` comando
- Visualizzare l'inventario delle LUN in transizione dal volume 7-Mode utilizzando `transition 7-mode show` comando
- Ripristina un volume da uno snapshot 7-Mode

Il ripristino del volume trasferisce tutti i LUN acquisiti nello snapshot

- Ripristina una singola LUN da uno snapshot 7-Mode utilizzando il `snapshot restore-file` comando
- Crea un clone di una LUN in una snapshot 7-Mode
- Ripristina una serie di blocchi da una LUN acquisita in una snapshot 7-Mode
- Creare un FlexClone del volume utilizzando un'istantanea 7-Mode

Non è possibile eseguire le seguenti operazioni con LUN in transizione:

- Accesso ai cloni delle LUN con backup degli snapshot acquisiti nel volume

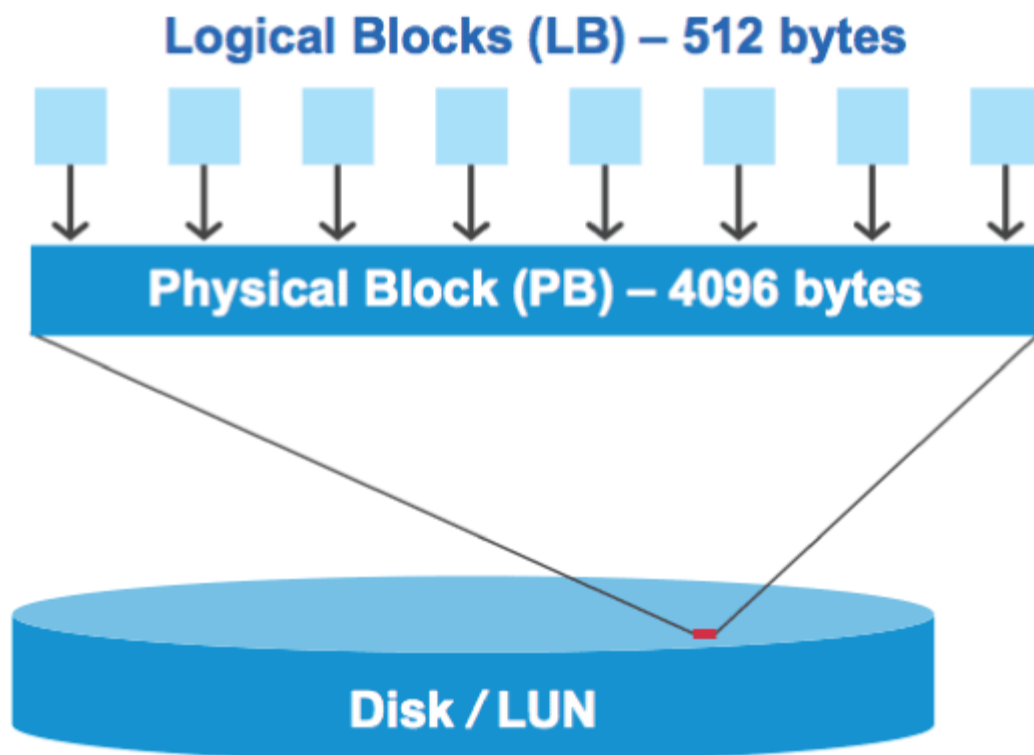
#### Informazioni correlate

- ["Transizione basata sulla copia"](#)
- ["lun show"](#)

#### Panoramica dei disallineamenti i/o sui LUN allineati correttamente

ONTAP potrebbe segnalare disallineamenti i/o su LUN correttamente allineati. In generale, questi avvisi di disallineamento possono essere ignorati se si è certi che il LUN sia correttamente configurato e che la tabella di partizione sia corretta.

I LUN e i dischi rigidi forniscono lo storage come blocchi. Poiché la dimensione del blocco per i dischi sull'host è di 512 byte, i LUN presentano blocchi di tale dimensione all'host, utilizzando blocchi di dimensioni maggiori da 4 KB per memorizzare i dati. Il blocco di dati a 512 byte utilizzato dall'host viene definito blocco logico. Il blocco di dati da 4 KB utilizzato dal LUN per memorizzare i dati viene definito blocco fisico. Ciò significa che ogni blocco fisico da 4 KB contiene otto blocchi logici da 512 byte.



Il sistema operativo host può avviare un'operazione di i/o in lettura o scrittura in qualsiasi blocco logico. Le operazioni di i/o vengono considerate allineate solo quando iniziano dal primo blocco logico del blocco fisico. Se un'operazione di i/o inizia in un blocco logico che non è anche l'inizio di un blocco fisico, l'i/o viene considerato disallineato. ONTAP rileva automaticamente il disallineamento e lo segnala sul LUN. Tuttavia, la presenza di i/o disallineati non significa necessariamente che anche il LUN sia disallineato. È possibile che i/o disallineati vengano segnalati su LUN allineati correttamente.

Se hai bisogno di ulteriori indagini, consulta il ["Knowledge Base NetApp : come identificare gli IO non allineati sulle LUN?"](#)

Per ulteriori informazioni sugli strumenti per la correzione dei problemi di allineamento, consultare la seguente documentazione: +

- ["Windows Unified host Utilities 7.1"](#)
- ["Provisioning della documentazione dello storage SAN"](#)

#### Ottenere l'allineamento i/o utilizzando i tipi di sistema operativo LUN

Per ONTAP 9,7 o versioni precedenti, è necessario utilizzare il LUN ONTAP consigliato `ostype` Valore che si avvicina maggiormente al sistema operativo per ottenere l'allineamento i/o con lo schema di partizionamento del sistema operativo.

Lo schema di partizione utilizzato dal sistema operativo host è un importante fattore che contribuisce ai disallineamenti i/o. Alcune LUN ONTAP `ostype` i valori utilizzano uno speciale offset noto come "prefix" per consentire l'allineamento dello schema di partizione predefinito utilizzato dal sistema operativo host.



In alcuni casi, potrebbe essere necessaria una tabella di partizione personalizzata per ottenere l'allineamento i/o. Tuttavia, per `ostype` valori con un valore "prefix" maggiore di 0, Una partizione personalizzata potrebbe creare un i/o disallineato

Per ulteriori informazioni sui LUN forniti in ONTAP 9.7 o versioni precedenti, vedere ["Knowledge Base NetApp : come identificare gli IO non allineati sulle LUN"](#) .



Per impostazione predefinita, i nuovi LUN con provisioning in ONTAP 9,8 o versioni successive dispongono di un prefisso e di una dimensione del suffisso pari a zero per tutti i tipi di sistema operativo LUN. Per impostazione predefinita, l'i/o deve essere allineato con il sistema operativo host supportato.

#### Considerazioni speciali sull'allineamento i/o per Linux

Le distribuzioni Linux offrono un'ampia gamma di modi per utilizzare un LUN, tra cui dispositivi raw per database, diversi gestori di volumi e file system. Non è necessario creare partizioni su un LUN se utilizzato come dispositivo raw o come volume fisico in un volume logico.

Per RHEL 5 e versioni precedenti e SLES 10 e versioni precedenti, se il LUN verrà utilizzato senza un gestore di volumi, è necessario partizionare il LUN in modo che una partizione inizi con un offset allineato, ovvero un settore che è anche un multiplo di otto blocchi logici.

#### Considerazioni sull'allineamento i/o speciali per i LUN Solaris

È necessario considerare diversi fattori quando si determina se utilizzare `solaris ostype` o il `solaris_efi` tipo di sistema operativo.

Vedere ["Guida all'installazione e all'amministrazione di Solaris host Utilities"](#) per informazioni dettagliate.

#### Le LUN di avvio ESX riportano un disallineamento

Le LUN utilizzate come LUN di boot ESX vengono in genere segnalate da ONTAP come disallineate. ESX crea più partizioni sul LUN di boot, rendendo molto difficile l'allineamento. Le LUN di boot ESX disallineate non sono generalmente un problema di performance perché la quantità totale di i/o disallineati è ridotta. Presupponendo che il LUN sia stato correttamente configurato con VMware `ostype`, non è necessaria alcuna azione.

#### Informazioni correlate

["Allineamento partizione/disco del file system delle macchine virtuali guest per VMware vSphere, altri ambienti virtuali e sistemi di storage NetApp"](#)

#### Modi per risolvere i problemi quando i LUN passano offline

Quando non è disponibile spazio per le scritture, le LUN passano offline per preservare l'integrità dei dati. Le LUN possono esaurire lo spazio e andare offline per diversi motivi, oltre a diversi modi per risolvere il problema.

Se...	È possibile...
Aggregato pieno	<ul style="list-style-type: none"><li>• Aggiungere altri dischi.</li><li>• Utilizzare <code>volume modify</code> comando per ridurre un volume con spazio disponibile.</li><li>• Se si dispone di volumi con garanzia di spazio che dispongono di spazio disponibile, impostare la garanzia di spazio del volume su <code>none</code> con <code>volume modify</code> comando.</li></ul>

Se...	È possibile...
Il volume è pieno ma c'è spazio disponibile nell'aggregato contenente	<ul style="list-style-type: none"> <li>• Per i volumi di garanzia dello spazio, utilizzare <code>volume modify</code> per aumentare le dimensioni del volume.</li> <li>• Per i volumi con thin provisioning, utilizzare <code>volume modify</code> per aumentare le dimensioni massime del volume.</li> </ul> <p>Se la crescita automatica del volume non è attivata, utilizzare <code>volume modify -autogrow -mode</code> per attivarlo.</p> <ul style="list-style-type: none"> <li>• Elimina manualmente le snapshot con il <code>volume snapshot delete</code> comando oppure utilizza il comando <code>volume snapshot autodelete modify</code> per eliminarle automaticamente.</li> </ul>

#### Informazioni correlate

["Gestione di dischi e Tier locali \(aggregato\)"](#)

["Gestione dello storage logico"](#)

#### Eseguire il troubleshooting dei LUN iSCSI non visibili sull'host

I LUN iSCSI vengono visualizzati come dischi locali per l'host. Se i LUN del sistema di storage non sono disponibili come dischi sull'host, verificare le impostazioni di configurazione.

Impostazione di configurazione	Cosa fare
Cablaggio	Verificare che i cavi tra l'host e il sistema di storage siano collegati correttamente.
Connettività di rete	<p>Verificare che vi sia una connettività TCP/IP tra l'host e il sistema di storage.</p> <ul style="list-style-type: none"> <li>• Dalla riga di comando del sistema storage, eseguire il ping delle interfacce host utilizzate per iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> </li> <li>• Dalla riga di comando dell'host, eseguire il ping delle interfacce del sistema di storage utilizzate per iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> </li> </ul>

Impostazione di configurazione	Cosa fare
Requisiti di sistema	Verificare che i componenti della configurazione siano qualificati. Inoltre, verificare di disporre del livello corretto del service pack del sistema operativo host (OS), della versione initiator, della versione di ONTAP e di altri requisiti di sistema. La matrice di interoperabilità contiene i requisiti di sistema più aggiornati.
Frame jumbo	Se si utilizzano frame jumbo nella configurazione, verificare che i frame jumbo siano attivati su tutti i dispositivi nel percorso di rete: La NIC Ethernet host, il sistema di storage e gli switch.
Stato del servizio iSCSI	Verificare che il servizio iSCSI sia concesso in licenza e avviato sul sistema storage.
Accesso initiator	Verificare che l'iniziatore sia connesso al sistema di storage. Se il <code>iscsi initiator show</code> l'output del comando indica che non sono stati registrati iniziatori. controllare la configurazione dell'iniziatore sull'host. Verificare inoltre che il sistema di storage sia configurato come destinazione dell'iniziatore.
Nomi dei nodi iSCSI (IQN)	Verificare di utilizzare i nomi dei nodi iniziatori corretti nella configurazione igroup. Sull'host, è possibile utilizzare i comandi e gli strumenti di initiator per visualizzare il nome del nodo di initiator. I nomi dei nodi iniziatori configurati nell'igroup e sull'host devono corrispondere.
Mappature LUN	Verificare che i LUN siano mappati a un igroup. Nella console del sistema di storage, è possibile utilizzare uno dei seguenti comandi: <ul style="list-style-type: none"> <li><code>lun mapping show</code> Visualizza tutti i LUN e gli igroups a cui sono associati.</li> <li><code>lun mapping show -igroup</code> Visualizza i LUN mappati a un igroup specifico.</li> </ul>
Le LIF iSCSI sono abilitate	Verificare che le interfacce logiche iSCSI siano attivate.

#### Informazioni correlate

- ["Tool di matrice di interoperabilità NetApp"](#)
- ["visualizzazione della mappatura del lun"](#)

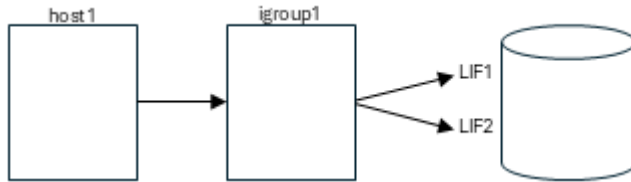
## Gestire igroups e portset

### Metodi per limitare l'accesso LUN con portset e igroups

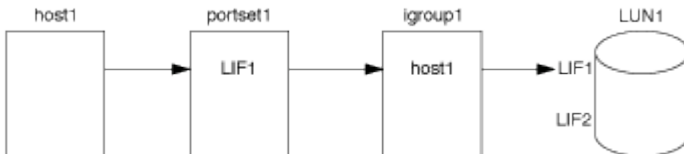
Oltre a utilizzare la mappa LUN selettiva (SLM), è possibile limitare l'accesso ai LUN tramite igroups e portset.

I portset possono essere utilizzati con SLM per limitare ulteriormente l'accesso di determinate destinazioni a determinati iniziatori. Quando si utilizza SLM con i portset, i LUN saranno accessibili sull'insieme di LIF nel portset sul nodo che possiede il LUN e sul partner ha di quel nodo.

Nell'esempio seguente, host1 non ha un portset. Senza un set di porte, host1 può accedere a LUN1 tramite LIF1 e LIF2.



È possibile limitare l'accesso a LUN1 utilizzando un portset. Nell'esempio seguente, host1 può accedere a LUN1 solo tramite LIF1. Tuttavia, host1 non può accedere a LUN1 tramite LIF2 perché LIF2 non è nel portset1.



#### Informazioni correlate

- [Mappa LUN selettiva](#)
- [Creare un portset e associarlo a un igroup](#)

#### Visualizza e gestisci GLI iniziatori SAN e igroups

È possibile utilizzare System Manager per visualizzare e gestire i gruppi di iniziatori (igroups) e gli iniziatori.

##### A proposito di questa attività

- I gruppi di iniziatori identificano gli host in grado di accedere a LUN specifiche sul sistema di storage.
- Una volta creati un gruppo iniziatore e un gruppo iniziatore, è possibile modificarli o eliminarli.
- Per gestire i gruppi di iniziatori SAN e gli iniziatori, è possibile eseguire le seguenti attività:
  - [\[view-manage-san-igroups\]](#)
  - [\[view-manage-san-inits\]](#)

#### Visualizzare e gestire i gruppi SAN Initiator

È possibile utilizzare System Manager per visualizzare un elenco di gruppi di iniziatori (igroups). Dall'elenco, è possibile eseguire operazioni aggiuntive.

##### Fasi

1. In System Manager, fare clic su **Hosts > SAN Initiator Groups** (host > gruppi iniziatori SAN).


Nella pagina viene visualizzato un elenco di gruppi di iniziatori (igroups). Se l'elenco è grande, è possibile visualizzare altre pagine dell'elenco facendo clic sui numeri di pagina nell'angolo inferiore destro della pagina.

Le colonne visualizzano varie informazioni su igroups. A partire da 9.11.1, viene visualizzato anche lo stato di connessione dell'igroup. Passare il mouse sugli avvisi di stato per visualizzare i dettagli.


2. (Facoltativo): È possibile eseguire le seguenti attività facendo clic sulle icone nell'angolo superiore destro dell'elenco:

- **Ricerca**
- **Scaricare** l'elenco.
- **Mostra o Nascondi** nell'elenco.
- **Filtra** i dati nell'elenco.

3. È possibile eseguire le operazioni dall'elenco:

- Fare clic  **Add** per aggiungere un igroup.
- Fare clic sul nome dell'igroup per visualizzare la pagina **Overview** che mostra i dettagli relativi all'igroup.

Nella pagina **Panoramica**, è possibile visualizzare i LUN associati all'igroup ed eseguire le operazioni per creare LUN e mappare i LUN. Fare clic su **All SAN Initiator** (tutti gli iniziatori SAN) per tornare all'elenco principale.

- Passare il mouse sull'igroup, quindi fare clic su  accanto al nome di un igroup per modificare o eliminare l'igroup.
- Passare il mouse sull'area a sinistra del nome dell'igroup, quindi selezionare la casella di controllo. Facendo clic su **+Aggiungi a gruppo iniziatore**, è possibile aggiungere tale igroup a un altro igroup.
- Nella colonna **Storage VM**, fare clic sul nome di una storage VM per visualizzarne i dettagli.

#### Visualizzare e gestire GLI iniziatori SAN

È possibile utilizzare System Manager per visualizzare un elenco di iniziatori. Dall'elenco, è possibile eseguire operazioni aggiuntive.

#### Fasi

1. In System Manager, fare clic su **Hosts > SAN Initiator Groups** (host > gruppi iniziatori SAN).

Nella pagina viene visualizzato un elenco di gruppi di iniziatori (igroups).

2. Per visualizzare gli iniziatori, attenersi alla seguente procedura:

- Fare clic sulla scheda **iniziatori FC** per visualizzare un elenco di iniziatori FC.
- Fare clic sulla scheda **iSCSI Initiators** per visualizzare un elenco di iniziatori iSCSI.

Le colonne visualizzano varie informazioni sugli iniziatori.

A partire da 9.11.1, viene visualizzato anche lo stato di connessione dell'iniziatore. Passare il mouse sugli avvisi di stato per visualizzare i dettagli.

3. (Facoltativo): È possibile eseguire le seguenti attività facendo clic sulle icone nell'angolo superiore destro dell'elenco:
  - **Cerca** l'elenco di iniziatori specifici.
  - **Scaricare** l'elenco.
  - **Mostra o Nascondi** nell'elenco.
  - **Filtra** i dati nell'elenco.

## Creare un igroup nidificato

A partire da ONTAP 9.9.1, è possibile creare un igroup composto da altri igroups esistenti.

1. In System Manager, fare clic su **host > SAN Initiator Groups**, quindi fare clic su **Add**.
2. Inserire i campi igroup **Name** (Nome) e **Description** (Descrizione).

La descrizione funge da alias igroup.

3. Selezionare **Storage VM** e **host Operating System**.



Il tipo di sistema operativo di un igroup nidificato non può essere modificato dopo la creazione dell'igroup.

4. In **Initiator Group Members** selezionare **Existing Initiator group**.

È possibile utilizzare **Search** per trovare e selezionare i gruppi iniziatori che si desidera aggiungere.

## Mappare igroups a più LUN

A partire da ONTAP 9.9.1, è possibile associare igroups a due o più LUN contemporaneamente.

1. In System Manager, fare clic su **Storage > LUN**.
2. Selezionare i LUN che si desidera mappare.
3. Fare clic su **More** (Altro), quindi su **Map to Initiator Groups** (Mappa ai gruppi di iniziatori)



Gli igroups selezionati vengono aggiunti ai LUN selezionati. Le mappature preesistenti non vengono sovrascritte.

## Creare un portset e associarlo a un igroup

Oltre all'utilizzo "[Mappa LUN selettiva \(SLM\)](#)", È possibile creare un portset e associare il portset a un igroup per limitare ulteriormente le LIF che possono essere utilizzate da un iniziatore per accedere a un LUN.

Se non si associa un portset a un igroup, tutti gli iniziatori nell'igroup possono accedere alle LUN mappate attraverso tutte le LIF sul nodo che possiede il LUN e il partner ha del nodo proprietario.

### Prima di iniziare

Devi avere almeno un LIF e un igroup.

A meno che non si utilizzino gruppi di interfacce, si consigliano due LIF per la ridondanza sia per iSCSI che per FC. Per i gruppi di interfacce si consiglia un solo LIF.

### A proposito di questa attività

È vantaggioso utilizzare i portset con SLM quando si dispone di più di due LIF su un nodo e si desidera limitare un determinato iniziatore a un sottoinsieme di LIF. Senza i portset, tutti gli iniziatori avranno accesso al LUN a tutte le destinazioni del nodo tramite il nodo proprietario del LUN e il partner ha del nodo proprietario.

## Esempio 6. Fasi

### System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per creare portset e associarli a igroups.

Se è necessario creare un portset e associarlo a un igroup in una release di ONTAP precedente alla 9.10.1, è necessario utilizzare la procedura CLI di ONTAP.

A partire da ONTAP 9.12.1, se non si dispone di un portset esistente, è necessario crearne il primo utilizzando la procedura ONTAP CLI.

1. In System Manager, fare clic su **Network > Overview > Portsets**, quindi fare clic su **Add**.
2. Inserire le informazioni relative al nuovo portset e fare clic su **Add** (Aggiungi).
3. Fare clic su **host > SAN Initiator Groups** (gruppi iniziatori SAN)
4. Per associare il portset a un nuovo igroup, fare clic su **Add** (Aggiungi).

Per associare il portset a un igroup esistente, selezionare l'igroup, fare clic su , quindi fare clic su **Modifica gruppo iniziatore**.

### Informazioni correlate

["Visualizza e gestisci gli iniziatori e gli igroups"](#)

### CLI

1. Creare un set di porte contenente le LIF appropriate:

```
portset create -vserver vservice_name -portset portset_name -protocol
protocol -port-name port_name
```

Se si utilizza FC, specificare `protocol` parametro as `fc`. Se si utilizza iSCSI, specificare `protocol` parametro as `iscsi`.

2. Collegare l'igroup al set di porte:

```
lun igroup bind -vserver vservice_name -igroup igroup_name -portset
portset_name
```

Ulteriori informazioni su `lun igroup bind` nella ["Riferimento al comando ONTAP"](#).

3. Verificare che i set di porte e i LIF siano corretti:

```
portset show -vserver vservice_name
```


Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1

## Gestire i portset


Oltre a "[Mappa LUN selettiva \(SLM\)](#)", È possibile utilizzare i portset per limitare ulteriormente le LIF che possono essere utilizzate da un iniziatore per accedere a un LUN.

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare le interfacce di rete associate ai portset ed eliminare i portset.

### Modificare le interfacce di rete associate a un portset

1. In System Manager, selezionare **Network > Overview > Portsets**.
2. Selezionare il portset che si desidera modificare , quindi selezionare **Modifica portset**.

### Eliminare un portset

1. In System Manager, fare clic su **Network > Overview > Portsets**.
2. Per eliminare un singolo portset, selezionarlo, quindi selezionare \*Elimina portset  \*.

Per eliminare più portset, selezionare i portset e fare clic su **Delete** (Elimina).

## Panoramica della mappa LUN selettiva

La mappa LUN selettiva (SLM) riduce il numero di percorsi dall'host al LUN. Con SLM, quando viene creata una nuova mappa LUN, la LUN è accessibile solo attraverso i percorsi sul nodo che possiede il LUN e il suo partner ha.

SLM consente la gestione di un singolo igroup per host e supporta anche operazioni di spostamento LUN senza interruzioni che non richiedono la manipolazione di portset o il remapping del LUN.

"[Portset](#)" Può essere utilizzato con SLM per limitare ulteriormente l'accesso di determinati target a determinati iniziatori. Quando si utilizza SLM con i portset, i LUN saranno accessibili sull'insieme di LIF nel portset sul nodo che possiede il LUN e sul partner ha di quel nodo.

SLM è attivato per impostazione predefinita su tutte le nuove mappe LUN.

### Determinare se SLM è attivato su una mappa LUN

Se l'ambiente in uso dispone di una combinazione di LUN creati in una release di ONTAP 9 e di LUN trasferiti da versioni precedenti, potrebbe essere necessario determinare se la mappa LUN selettiva (SLM) è attivata su un LUN specifico.

È possibile utilizzare le informazioni visualizzate nell'output di `lun mapping show -fields reporting-nodes, node` Per determinare se SLM è attivato sulla mappa LUN. Se SLM non è abilitato, nelle celle sotto la colonna "reporting-nodes" dell'output del comando viene visualizzato "-". Se SLM è attivato, l'elenco dei nodi visualizzato nella colonna "Nodes" viene duplicato nella colonna "reporting-Nodes".

Ulteriori informazioni su `lun mapping show` nella "[Riferimento al comando ONTAP](#)".

### Modificare l'elenco dei nodi di reporting SLM

Se si sposta un LUN o un volume contenente LUN in un'altra coppia ad alta disponibilità (ha) all'interno dello

stesso cluster, è necessario modificare l'elenco dei nodi di reporting della mappa LUN selettiva (SLM) prima di iniziare lo spostamento per garantire che vengano mantenuti i percorsi LUN attivi e ottimizzati.

## Fasi

1. Aggiungere il nodo di destinazione e il relativo nodo partner all'elenco dei nodi di reporting dell'aggregato o del volume:

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

Se si dispone di una convenzione di denominazione coerente, è possibile modificare più mappature LUN contemporaneamente utilizzando `igroup_prefix*` invece di `igroup_name`.

2. Eseguire nuovamente la scansione dell'host per rilevare i percorsi aggiunti di recente.
3. Se il sistema operativo lo richiede, aggiungere i nuovi percorsi alla configurazione MPIO (Multipath Network i/o).
4. Eseguire il comando per l'operazione di spostamento desiderata e attendere il completamento dell'operazione.
5. Verificare che l'i/o venga gestito tramite il percorso Active/Optimized:

```
lun mapping show -fields reporting-nodes
```

6. Rimuovere il proprietario del LUN precedente e il relativo nodo partner dall'elenco dei nodi di reporting:

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. Verificare che il LUN sia stato rimosso dalla mappa LUN esistente:

```
lun mapping show -fields reporting-nodes
```

8. Rimuovere eventuali voci di dispositivi obsolete per il sistema operativo host.
9. Modificare eventuali file di configurazione multipathing, se necessario.
10. Eseguire nuovamente la scansione dell'host per verificare la rimozione dei vecchi percorsi. + consultare la documentazione dell'host per istruzioni specifiche su come eseguire nuovamente la scansione degli host.

## Gestire il protocollo iSCSI

### Configura la tua rete per ottenere le migliori performance

Le reti Ethernet variano notevolmente in termini di performance. È possibile massimizzare le prestazioni della rete utilizzata per iSCSI selezionando valori di

configurazione specifici.

### **Fasi**

1. Collegare le porte host e storage alla stessa rete.

Si consiglia di collegarsi agli stessi switch. Il routing non deve mai essere utilizzato.

2. Selezionare le porte più veloci disponibili e dedicarle a iSCSI.

Le porte da 10 GbE sono le migliori. Le porte 1 GbE sono il minimo.

3. Disattiva il controllo di flusso Ethernet per tutte le porte.

Dovrebbe essere visualizzato ["Gestione della rete"](#) Per utilizzare la CLI per configurare il controllo di flusso della porta Ethernet.

4. Abilitare i frame jumbo (in genere MTU di 9000).

Tutti i dispositivi nel percorso dati, inclusi iniziatori, destinazioni e switch, devono supportare i frame jumbo. In caso contrario, l'abilitazione dei frame jumbo riduce notevolmente le performance di rete.

### **Configurare una SVM per iSCSI**

Per configurare una macchina virtuale di storage (SVM) per iSCSI, è necessario creare LIF per SVM e assegnare il protocollo iSCSI a tali LIF.


#### **A proposito di questa attività**

È necessario un minimo di un LIF iSCSI per nodo per ogni SVM che fornisce dati con il protocollo iSCSI. Per la ridondanza, è necessario creare almeno due LIF per nodo.

## Esempio 7. Fasi

### System Manager

Configurazione di una VM di storage per iSCSI con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare iSCSI su una nuova VM di storage	Per configurare iSCSI su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>iSCSI</b> per il protocollo di accesso*.</li><li>4. Fare clic su <b>Enable iSCSI</b> (attiva iSCSI) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + ogni nodo deve avere almeno due interfacce di rete.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi fare clic su  accanto al protocollo iSCSI.</li><li>4. Fare clic su <b>Enable iSCSI</b> (attiva iSCSI) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + ogni nodo deve avere almeno due interfacce di rete.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>

### CLI

Configurare una VM di storage per iSCSI con l'interfaccia CLI di ONTAP.

1. Abilitare le SVM per l'ascolto del traffico iSCSI:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Creare una LIF per le SVM su ciascun nodo da utilizzare per iSCSI:

- Per ONTAP 9.6 e versioni successive:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

- Per ONTAP 9.5 e versioni precedenti:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Verificare di aver configurato correttamente i file LIF:

```
network interface show -vserver vserver_name
```

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

4. Verificare che iSCSI sia attivo e in esecuzione e che l'IQN di destinazione per la SVM:

```
vserver iscsi show -vserver vserver_name
```

5. Dal tuo host, crea sessioni iSCSI sulle tue LIF.

#### Informazioni correlate

- ["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#)

#### Definire un metodo di policy di sicurezza per un iniziatore

È possibile definire un elenco di iniziatori e i relativi metodi di autenticazione. È inoltre possibile modificare il metodo di autenticazione predefinito applicabile agli iniziatori che non dispongono di un metodo di autenticazione definito dall'utente.

#### A proposito di questa attività

È possibile generare password univoche utilizzando gli algoritmi dei criteri di protezione del prodotto oppure specificare manualmente le password che si desidera utilizzare.



Non tutti gli iniziatori supportano password CHAP segrete esadecimali.

#### Fasi

1. Utilizzare `vserver iscsi security create` per creare un metodo di policy di sicurezza per un iniziatore.

```
vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. Seguire i comandi sullo schermo per aggiungere le password.

Crea un metodo di policy di sicurezza per Initiator iqn.1991-05.com.microsoft:host1 con nomi utente e password CHAP in entrata e in uscita.

#### Informazioni correlate

- [Come funziona l'autenticazione iSCSI](#)
- [Autenticazione CHAP](#)

#### Eliminare un servizio iSCSI per una SVM

È possibile eliminare un servizio iSCSI per una macchina virtuale di storage (SVM) se non è più necessario.

#### Prima di iniziare

Lo stato di amministrazione del servizio iSCSI deve essere "proprio d'" prima di poter eliminare un servizio iSCSI. È possibile spostare lo stato di amministrazione in basso con il ``vserver iscsi modify` comando.

#### Fasi

1. Utilizzare `vserver iscsi modify` Per arrestare l'i/o al LUN.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. Utilizzare `vserver iscsi delete` Comando per rimuovere il servizio iscsi dalla SVM.

```
vserver iscsi delete -vserver vs_1
```

3. Utilizzare `vserver iscsi show command` Per verificare che il servizio iSCSI sia stato eliminato da SVM.

```
vserver iscsi show -vserver vs1
```

### Per ulteriori informazioni, consultare la sezione relativa ai ripristini degli errori della sessione iSCSI

L'aumento del livello di ripristino degli errori di sessione iSCSI consente di ricevere informazioni più dettagliate sui ripristini degli errori iSCSI. L'utilizzo di un livello di ripristino degli errori superiore potrebbe causare una riduzione minore delle prestazioni della sessione iSCSI.

#### A proposito di questa attività

Per impostazione predefinita, ONTAP è configurato per utilizzare il livello di ripristino degli errori 0 per le sessioni iSCSI. Se si utilizza un iniziatore qualificato per il livello di ripristino degli errori 1 o 2, è possibile scegliere di aumentare il livello di ripristino degli errori. Il livello di ripristino degli errori di sessione modificato influisce solo sulle sessioni appena create e non sulle sessioni esistenti.

A partire da ONTAP 9.4, la `max-error-recovery-level` l'opzione non è supportata in `iscsi show` e `iscsi modify` comandi.

#### Fasi

1. Accedere alla modalità avanzata:

```
set -privilege advanced
```

2. Verificare l'impostazione corrente utilizzando `iscsi show` comando.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. Modificare il livello di ripristino degli errori utilizzando `iscsi modify` comando.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

### Registrare la SVM con un server iSNS

È possibile utilizzare `vserver iscsi isns` Comando per configurare la macchina virtuale di storage (SVM) per la registrazione con un server iSNS.

#### A proposito di questa attività

Il comando `vserver iscsi isns create` configura la SVM per la registrazione con il server iSNS. SVM non fornisce comandi che consentono di configurare o gestire il server iSNS. Per gestire il server iSNS, è possibile utilizzare gli strumenti di amministrazione del server o l'interfaccia fornita dal fornitore per il server iSNS.

## Fasi

1. Sul server iSNS, assicurarsi che il servizio iSNS sia attivo e disponibile per l'assistenza.
2. Creare la LIF di gestione SVM su una porta dati:

```
network interface create -vserver SVM_name -lif lif_name -role data -data
-protocol none -home-node home_node_name -home-port home_port -address
IP_address -netmask network_mask
```

Ulteriori informazioni su `network interface create` nella ["Riferimento al comando ONTAP"](#).

3. Creare un servizio iSCSI sulla SVM se non ne esiste già uno:

```
vserver iscsi create -vserver SVM_name
```

4. Verificare che il servizio iSCSI sia stato creato correttamente:

```
iscsi show -vserver SVM_name
```

5. Verificare che esista un percorso predefinito per SVM:

```
network route show -vserver SVM_name
```

6. Se non esiste un percorso predefinito per SVM, creare un percorso predefinito:

```
network route create -vserver SVM_name -destination destination -gateway
gateway
```

Ulteriori informazioni su `network route create` nella ["Riferimento al comando ONTAP"](#).

7. Configurare SVM per la registrazione con il servizio iSNS:

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

Sono supportate sia le famiglie di indirizzi IPv4 che IPv6. La famiglia di indirizzi del server iSNS deve essere uguale a quella della LIF di gestione SVM.

Ad esempio, non è possibile connettere un LIF di gestione SVM con un indirizzo IPv4 a un server iSNS con un indirizzo IPv6.

8. Verificare che il servizio iSNS sia in esecuzione:

```
vserver iscsi isns show -vserver SVM_name
```

9. Se il servizio iSNS non è in esecuzione, avviarlo:

```
vserver iscsi isns start -vserver SVM_name
```

## Risoluzione dei messaggi di errore iSCSI sul sistema di storage

Sono disponibili diversi messaggi di errore comuni relativi a iSCSI che è possibile visualizzare con `event log show` comando. Devi sapere cosa significano questi messaggi e cosa puoi fare per risolvere i problemi che identificano.

La seguente tabella contiene i messaggi di errore più comuni e le istruzioni per risolverli:

Messaggio	Spiegazione	Cosa fare
ISCSI: network interface identifier disabled for use; incoming connection discarded	Il servizio iSCSI non è abilitato sull'interfaccia.	È possibile utilizzare <code>iscsi interface enable</code> Per attivare il servizio iSCSI sull'interfaccia. Ad esempio:  <code>iscsi interface enable -vserver vs1 -lif lif1</code>
ISCSI: Authentication failed for initiator nodename	CHAP non è configurato correttamente per l'iniziatore specificato.	Controllare le impostazioni CHAP; non è possibile utilizzare lo stesso nome utente e password per le impostazioni in entrata e in uscita sul sistema di storage: <ul style="list-style-type: none"><li>• Le credenziali in entrata nel sistema di storage devono corrispondere alle credenziali in uscita sull'iniziatore.</li><li>• Le credenziali in uscita sul sistema di storage devono corrispondere alle credenziali in entrata sull'iniziatore.</li></ul>

Ulteriori informazioni su `event log show` nella ["Riferimento al comando ONTAP"](#).

### Attiva o disattiva il failover automatico della LIF iSCSI

Dopo l'upgrade a ONTAP 9.11.1 o versione successiva, dovresti attivare manualmente il failover LIF automatico su tutte le LIF iSCSI create in ONTAP 9.10.1 o versione precedente.

A partire da ONTAP 9.11.1, puoi abilitare il failover LIF automatico per LIF iSCSI su piattaforme di array SAN all-flash. In caso di failover dello storage, la LIF iSCSI viene automaticamente migrata dal nodo home o dalla porta al nodo partner di ha o alla porta, per poi tornare indietro una volta completato il failover. Oppure, se la porta per LIF iSCSI diventa guasta, la LIF viene migrata automaticamente a una porta funzionante nel suo nodo home corrente e quindi di nuovo alla porta originale una volta che la porta è nuovamente funzionante. Consente ai carichi di lavoro SAN in esecuzione su iSCSI di riprendere più rapidamente il servizio i/o dopo un failover.

In ONTAP 9.11.1 e versioni successive, per impostazione predefinita, le LIF iSCSI appena create vengono attivate per il failover automatico della LIF se si verifica una delle seguenti condizioni:

- Non ci sono LIF iSCSI nell'SVM
- Tutte le LIF iSCSI presenti nella SVM sono abilitate per il failover automatico della LIF

#### Attiva il failover automatico della LIF iSCSI

Per impostazione predefinita, le LIF iSCSI create in ONTAP 9.10.1 e versioni precedenti non sono abilitate per il failover automatico della LIF. Se nell'SVM sono presenti LIF iSCSI non abilitate per il failover automatico della LIF, nemmeno le LIF create di recente saranno abilitate per il failover automatico della LIF. Se il failover automatico della LIF non è abilitato e in caso di failover, la LIF iSCSI non migrerà.

Ulteriori informazioni su ["Failover e sconto della LIF"](#).

#### Fase

1. Attivazione del failover automatico per una LIF iSCSI:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover  
-policy sfo-partner-only -auto-revert true
```

Per aggiornare tutte le LIF iSCSI nella SVM, utilizza `-lif*` invece di `lif`.

#### Disattiva il failover automatico della LIF iSCSI

Se in precedenza hai abilitato il failover automatico di una LIF iSCSI creato in ONTAP 9.10.1 o versione precedente, puoi disabilitarlo.

#### Fase

1. Disattivare il failover automatico per una LIF iSCSI:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover  
-policy disabled -auto-revert false
```

Per aggiornare tutte le LIF iSCSI nella SVM, utilizza `-lif*` invece di `lif`.

#### Informazioni correlate

- ["Creare una LIF"](#)
- Manualmente ["Migrazione di una LIF"](#)
- Manualmente ["Ripristina una LIF nella porta home"](#)
- ["Configurare le impostazioni di failover su una LIF"](#)

## Gestire il protocollo FC

### Configurare una SVM per FC

Per configurare una SVM (Storage Virtual Machine) per FC, è necessario creare LIF per SVM e assegnare il protocollo FC a tali LIF.

**Prima di iniziare**

È necessario disporre di una licenza FC ("[Incluso con ONTAP One](#)") e deve essere attivata. In caso contrario, la licenza FC non è abilitata, le LIF e le SVM appariranno online, ma lo stato operativo sarà `down`. Il servizio FC deve essere abilitato affinché i tuoi LIF e SVM siano operativi. Per ospitare gli iniziatori, è necessario utilizzare lo zoning initiator singolo per tutte le LIF FC nella SVM.


**A proposito di questa attività**

NetApp supporta almeno un LIF FC per nodo per ogni SVM che fornisce dati con il protocollo FC. È necessario utilizzare due LIF per nodo e due fabric, con un LIF per nodo collegato. Ciò garantisce la ridondanza a livello di nodo e fabric.

## Esempio 8. Fasi

### System Manager

Configurazione di una VM di storage per iSCSI con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare FC su una nuova VM di storage	Per configurare FC su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>FC</b> per il protocollo di accesso*.</li><li>4. Fare clic su <b>Enable FC</b> (attiva FC). + le porte FC vengono assegnate automaticamente.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi fare clic su  accanto al protocollo FC.</li><li>4. Fare clic su <b>Enable FC</b> (attiva FC) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + le porte FC vengono assegnate automaticamente.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>

### CLI

1. Abilitare il servizio FC sulla SVM:

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. Creare due LIFF per le SVM su ciascun nodo che serve FC:

- Per ONTAP 9.6 e versioni successive:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol fcp -service-policy default-data-fcp -home-node node_name  
-home-port port_name -address ip_address -netmask netmask -status-admin  
up
```

- Per ONTAP 9.5 e versioni precedenti:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol fcp -home-node node_name -home-port port
```

3. Verificare che i file LIF siano stati creati e che il loro stato operativo sia online:

```
network interface show -vserver vserver_name lif_name
```

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

### Informazioni correlate

- ["Supporto NetApp"](#)
- ["Tool di matrice di interoperabilità NetApp"](#)

- [Considerazioni per le LIF negli ambienti SAN cluster](#)

## Eliminare un servizio FC per una SVM

È possibile eliminare un servizio FC per una macchina virtuale di storage (SVM) se non è più necessario.

### Prima di iniziare

Lo stato di amministrazione deve essere “dOwn” (proprio) prima di poter eliminare un servizio FC per una SVM. È possibile impostare lo stato di amministrazione su inattivo con `vserver fcp modify` o il `vserver fcp stop` comando.

### Fasi

1. Utilizzare `vserver fcp stop` Per arrestare l'i/o al LUN.

```
vserver fcp stop -vserver vs_1
```

2. Utilizzare `vserver fcp delete` Comando per rimuovere il servizio dalla SVM.

```
vserver fcp delete -vserver vs_1
```

3. Utilizzare `vserver fcp show` Per verificare che il servizio FC sia stato eliminato dalla SVM:

```
vserver fcp show -vserver vs_1
```

## Configurazioni MTU consigliate per jumbo frame FCoE

Per Fibre Channel over Ethernet (FCoE), i frame jumbo per la parte dell'adattatore Ethernet del CNA devono essere configurati a 9000 MTU. I frame jumbo per la parte dell'adattatore FCoE del CNA devono essere configurati a un valore superiore a 1500 MTU. Configurare i frame jumbo solo se gli switch iniziatori, di destinazione e tutti gli switch interventori supportano e sono configurati per i frame jumbo.

## Gestire il protocollo NVMe

### Avviare il servizio NVMe per una SVM

Prima di poter utilizzare il protocollo NVMe sulla macchina virtuale di storage (SVM), è necessario avviare il servizio NVMe sulla SVM.

### Prima di iniziare

NVMe deve essere consentito come protocollo sul sistema.

Sono supportati i seguenti protocolli NVMe:

Protocollo	A partire da ...	Consentito da...
TCP	ONTAP 9.10.1	Predefinito
FCP	ONTAP 9.4	Predefinito

## Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare che NVMe sia consentito come protocollo:

```
vserver nvme show
```

3. Creare il servizio del protocollo NVMe:

```
vserver nvme create
```

4. Avviare il servizio del protocollo NVMe su SVM:

```
vserver nvme modify -status -admin up
```

## Eliminare il servizio NVMe da una SVM

Se necessario, è possibile eliminare il servizio NVMe dalla macchina virtuale di storage (SVM).

## Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Arrestare il servizio NVMe su SVM:

```
vserver nvme modify -status -admin down
```

3. Eliminare il servizio NVMe:


```
vserver nvme delete
```

## Ridimensionare uno spazio dei nomi

A partire da ONTAP 9.10.1, è possibile utilizzare l'interfaccia utente di ONTAP per aumentare o ridurre le dimensioni di uno spazio dei nomi NVMe. È possibile utilizzare System Manager per aumentare le dimensioni di uno spazio dei nomi NVMe.

## Aumentare le dimensioni di uno spazio dei nomi

## System Manager

1. Fare clic su **Storage > NVMe Namespaces**.
2. Posizionare il puntatore del mouse sullo spazio dei nomi che si desidera aumentare, fare clic su , quindi su **Modifica**.
3. In **CAPACITY**, modificare le dimensioni dello spazio dei nomi.

## CLI

1. Immettere il seguente comando: `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

## Ridurre le dimensioni di uno spazio dei nomi

È necessario utilizzare l'interfaccia utente di ONTAP per ridurre le dimensioni di uno spazio dei nomi NVMe.

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Ridurre le dimensioni dello spazio dei nomi:

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

## Convertire uno spazio dei nomi in un LUN

A partire da ONTAP 9.11.1, puoi utilizzare l'interfaccia a riga di comando di ONTAP per convertire in LUN un namespace NVMe esistente.

### Prima di iniziare

- Lo spazio dei nomi NVMe specificato non deve avere mappe esistenti su un sottosistema.
- Lo spazio dei nomi non deve far parte di uno snapshot o della relazione di destinazione di SnapMirror come spazio dei nomi di sola lettura.
- Poiché gli spazi dei nomi NVMe sono supportati solo con specifiche piattaforme e schede di rete, questa funzione funziona solo con hardware specifico.

### Fasi

1. Inserisci il seguente comando per convertire un namespace NVMe in una LUN:

```
lun convert-from-namespace -vserver -namespace-path
```

Ulteriori informazioni su `lun convert-from-namespace` nella ["Riferimento al comando ONTAP"](#).

## Configura l'autenticazione in-band su NVMe

A partire da ONTAP 9.12.1 è possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per configurare l'autenticazione in-band (sicura), bidirezionale e unidirezionale tra un host e un controller NVMe sui protocolli NVMe/TCP e NVMe/FC utilizzando

l'autenticazione DH-HMAC-CHAP. A partire da ONTAP 9.14.1, l'autenticazione in banda può essere configurata in Gestione sistema.

Per impostare l'autenticazione in banda, ogni host o controller deve essere associato a una chiave DH-HMAC-CHAP che è una combinazione del NQN dell'host o del controller NVMe e di una password di autenticazione configurata dall'amministratore. Perché un host o un controller NVMe possa autenticare il proprio peer, deve conoscere la chiave associata al peer.

Nell'autenticazione unidirezionale, viene configurata una chiave segreta per l'host, ma non per il controller. Nell'autenticazione bidirezionale, viene configurata una chiave segreta sia per l'host che per il controller.

SHA-256 è la funzione hash predefinita e 2048-bit è il gruppo DH predefinito.

## System Manager

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per configurare l'autenticazione in-band creando o aggiornando un sottosistema NVMe, creando o clonando namespace NVMe o aggiungendo gruppi di coerenza con nuovi namespace NVMe.

### Fasi

1. In System Manager, fare clic su **host > sottosistema NVMe**, quindi su **Aggiungi**.
2. Aggiungere il nome del sottosistema NVMe e selezionare la VM di storage e il sistema operativo host.
3. Immettere l'NQN dell'host.
4. Selezionare **Usa autenticazione in banda** accanto a NQN host.
5. Fornire la password dell'host e la password del controller.

La chiave DH-HMAC-CHAP è una combinazione del NQN dell'host o del controller NVMe e di un segreto di autenticazione configurato dall'amministratore.

6. Selezionare la funzione hash preferita e il gruppo DH per ciascun host.

Se non si seleziona una funzione hash e un gruppo DH, SHA-256 viene assegnato come funzione hash predefinita e 2048 bit come gruppo DH predefinito.

7. In alternativa, fare clic su **Aggiungi** e ripetere la procedura come necessario per aggiungere altri host.
8. Fare clic su **Save** (Salva).
9. Per verificare che l'autenticazione in banda sia attivata, fare clic su **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

L'icona di una chiave trasparente accanto al nome host indica che la modalità unidirezionale è attivata. Un tasto opaco accanto al nome host indica che la modalità bidirezionale è attivata.

## CLI

### Fasi

1. Aggiungere l'autenticazione DH-HMAC-CHAP al sottosistema NVMe:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret
<authentication_host_secret> -dhchap-controller-secret
<authentication_controller_secret> -dhchap-hash-function <sha-
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
bit|8192-bit>
```

Ulteriori informazioni su `vserver nvme subsystem host add` nella ["Riferimento al comando ONTAP"](#).

2. Verificare che il protocollo di autenticazione DH-HMAC CHAP sia stato aggiunto all'host:

```
vserver nvme subsystem host show
```

```
[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

Ulteriori informazioni su `vserver nvme subsystem host show` nella ["Riferimento al comando ONTAP"](#).

3. Verificare che l'autenticazione CHAP DH-HMAC sia stata eseguita durante la creazione del controller NVMe:

```
vserver nvme subsystem controller show
```

```
[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode
```

#### Informazioni correlate

- ["Visualizza il controller del sottosistema nvme vserver"](#)

#### Disattiva l'autenticazione in banda su NVMe

Se è stata configurata l'autenticazione in banda su NVMe utilizzando DH-HMAC-CHAP, è possibile scegliere di disattivarla in qualsiasi momento.

Se si torna da ONTAP 9.12.1 o versione successiva a ONTAP 9.12.0 o versione precedente, è necessario disattivare l'autenticazione in banda prima di eseguire l'ripristino. Se l'autenticazione in banda mediante DH-HMAC-CHAP non è disattivata, l'operazione di revert avrà esito negativo.

## Fasi

1. Rimuovere l'host dal sottosistema per disattivare l'autenticazione DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

2. Verificare che il protocollo di autenticazione DH-HMAC-CHAP sia stato rimosso dall'host:

```
vserver nvme subsystem host show
```

3. Aggiungere nuovamente l'host al sottosistema senza autenticazione:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

## Impostare il canale sicuro TLS per NVMe/TCP

A partire da ONTAP 9.16.1, è possibile configurare il canale sicuro TLS per le connessioni NVMe/TCP. È possibile utilizzare System Manager o ONTAP CLI per aggiungere un nuovo sottosistema NVMe con TLS abilitato oppure abilitare TLS per un sottosistema NVMe esistente. ONTAP non supporta lo scarico dell'hardware TLS.

## System Manager

A partire da ONTAP 9.16.1, puoi usare System Manager per configurare TLS per connessioni NVMe/TCP creando o aggiornando un sottosistema NVMe, creando o clonando namespace NVMe o aggiungendo gruppi di coerenza con nuovi namespace NVMe.

### Fasi

1. In System Manager, fare clic su **host > sottosistema NVMe**, quindi su **Aggiungi**.
2. Aggiungere il nome del sottosistema NVMe e selezionare la VM di storage e il sistema operativo host.
3. Immettere l'NQN dell'host.
4. Selezionare **Richiedi TLS (Transport Layer Security)** accanto all'NQN dell'host.
5. Fornire la chiave precondivisa (PSK).
6. Fare clic su **Save** (Salva).
7. Per verificare che il canale sicuro TLS sia abilitato, selezionare **System Manager > hosts > NVMe Subsystem > Grid > Peek view**.

### CLI

#### Fasi

1. Aggiungere un host del sottosistema NVMe che supporti il canale sicuro TLS. È possibile fornire una chiave pre-condivisa (PSK) utilizzando `tls-configured-psk` discussione:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Verificare che l'host del sottosistema NVMe sia configurato per il canale sicuro TLS. Facoltativamente, è possibile utilizzare l' `'tls-key-type'` argomento per visualizzare solo gli host che utilizzano quel tipo di chiave:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Verificare che il controller host del sottosistema NVMe sia configurato per il canale sicuro TLS. Facoltativamente, è possibile utilizzare qualsiasi `tls-key-type` argomento, `tls-identity` o `tls-cipher` per visualizzare solo i controller che hanno gli attributi TLS:

```
vserver nvme subsystem controller show -vserver <svm_name>  
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type  
{none|configured} -tls-identity <text> -tls-cipher  
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

## Informazioni correlate

- ["sottosistema vserver nvme"](#)

## Disattiva il canale sicuro TLS per NVMe/TCP

A partire da ONTAP 9.16.1, è possibile configurare il canale sicuro TLS per le connessioni NVMe/TCP. Se è stato configurato un canale sicuro TLS per le connessioni NVMe/TCP, è possibile scegliere di disattivarlo in qualsiasi momento.

### Fasi

1. Rimuovere l'host dal sottosistema per disattivare il canale protetto TLS:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

2. Verificare che il canale protetto TLS sia rimosso dall'host:

```
vserver nvme subsystem host show
```

3. Aggiungere nuovamente l'host al sottosistema senza il canale protetto TLS:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

### Informazioni correlate

- ["host del sottosistema vserver nvme"](#)

## Modifica della priorità dell'host NVMe

A partire da ONTAP 9.14.1, è possibile configurare il sottosistema NVMe per assegnare priorità all'allocazione delle risorse per host specifici. Per impostazione predefinita, quando un host viene aggiunto al sottosistema, viene assegnata una priorità regolare. Agli host assegnati una priorità alta viene assegnato un numero maggiore di code i/o e profondità di coda.

È possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per modificare manualmente la priorità predefinita da normale ad alta. Per modificare la priorità assegnata a un host, è necessario rimuovere l'host dal sottosistema e quindi aggiungerlo nuovamente.

### Fasi

1. Verificare che la priorità dell'host sia impostata su regolare:

```
vserver nvme show-host-priority
```

Ulteriori informazioni su `vserver nvme show-host-priority` nella ["Riferimento al comando ONTAP"](#).

2. Rimuovere l'host dal sottosistema:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

Ulteriori informazioni su `vserver nvme subsystem host remove` nella ["Riferimento al comando ONTAP"](#).

3. Verificare che l'host sia stato rimosso dal sottosistema:

```
vserver nvme subsystem host show
```

Ulteriori informazioni su `vserver nvme subsystem host show` nella ["Riferimento al comando ONTAP"](#).

4. Aggiungere nuovamente l'host al sottosistema con priorità alta:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

Ulteriori informazioni su `vserver nvme subsystem host add` nella ["Riferimento al comando ONTAP"](#).

## Gestire il rilevamento automatico degli host dei controller NVMe/TCP in ONTAP

A partire da ONTAP 9.14.1, il rilevamento host dei controller che utilizzano il protocollo NVMe/TCP viene automatizzato per impostazione predefinita nei fabric basati su IP.

### Rilevamento automatico dell'host dei controller NVMe/TCP

Se in precedenza è stato disattivato il rilevamento automatico dell'host, ma le esigenze sono state modificate, è possibile riattivarlo.

#### Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Attivare il rilevamento automatico:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. Verificare che il rilevamento automatico dei controller NVMe/TCP sia attivato.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

### Disattiva il rilevamento automatico degli host dei controller NVMe/TCP

Se non è necessario che l'host rilevi automaticamente i controller NVMe/TCP e rilevi traffico multicast indesiderato sulla rete, disattivare questa funzionalità.

#### Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Disattiva rilevamento automatico:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. Verificare che il rilevamento automatico dei controller NVMe/TCP sia disattivato.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

### Disattiva l'identificatore della macchina virtuale dell'host NVMe in ONTAP

A partire da ONTAP 9.14.1, per impostazione predefinita, ONTAP supporta la capacità degli host NVMe/FC di identificare le macchine virtuali tramite un identificatore univoco e per gli host NVMe/FC di monitorare l'utilizzo delle risorse della macchina virtuale. Questo migliora il reporting e il troubleshooting sul lato host.

È possibile utilizzare bootarg per disattivare questa funzionalità. Vedi il ["Knowledge Base NetApp : come disabilitare l'identificatore della macchina virtuale host NVMe in ONTAP"](#) .

## Gestire i sistemi con adattatori FC

### Gestire i 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 di storage dispone di adattatori FC integrati che possono essere configurati come iniziatori o destinazioni. È anche possibile utilizzare schede adattatrici FC configurate come iniziatori o destinazioni. Gli iniziatori si collegano agli scaffali dei dischi back-end e, possibilmente, ad array di archiviazione esterni. I target si connettono solo agli switch FC. Sia le porte HBA di destinazione FC che la velocità della porta dello switch devono essere impostate sullo stesso valore e non devono essere impostate

su automatico.

## Informazioni correlate

["Configurazione SAN"](#)

### 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	<code>network fcp adapter show</code>
Modificare i parametri dell'adattatore di destinazione FC	<code>network fcp adapter modify</code>
Visualizza le informazioni sul traffico del protocollo FC	<code>run -node node_name sysstat -f</code>
Visualizza per quanto tempo il protocollo FC è in esecuzione	<code>run -node node_name uptime</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node node_name sysconfig -v adapter</code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node node_name sysconfig -ac</code>
Visualizzare una pagina man per un comando	<code>man &lt;command_name&gt;</code>

### 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	<code>run -node node_name storage show adapter</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node node_name sysconfig -v adapter</code>

Se si desidera...	Utilizzare questo comando...
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node <i>node_name</i> sysconfig -ac</code>

#### Comandi per la gestione degli adattatori FC integrati

Se si desidera...	Utilizzare questo comando...
Visualizza lo stato delle porte FC integrate	<code>run -node <i>node_name</i> system hardware unified-connect show</code>

#### Informazioni correlate

- ["adattatore fcp di rete"](#)

### Configurare gli adattatori FC

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 modalità target viene utilizzata per connettere le porte agli iniziatori FC. 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).

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.

#### Configurare gli adattatori FC per la modalità di destinazione

##### 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 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
```

Ulteriori informazioni su `network fcp adapter show` nella ["Riferimento al comando ONTAP"](#).

5. Porta online il tuo adattatore:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

## Configurare gli adattatori FC per la modalità Initiator

### 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
```

Ulteriori informazioni su `network interface delete` nella ["Riferimento al comando ONTAP"](#).

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
```

## Visualizzare le impostazioni dell'adattatore

È possibile utilizzare comandi specifici per visualizzare informazioni sugli adattatori FC/UTA.

## Adattatore di destinazione FC

### Fase

1. Utilizzare `network fcp adapter show` comando per visualizzare le informazioni sull'adattatore:  
`network fcp adapter show -instance -node node1 -adapter 0a`

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

Ulteriori informazioni su `network fcp adapter show` nella ["Riferimento al comando ONTAP"](#).

## Unified Target Adapter (UTA) X1143A-R6

### 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.

## 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.

Ulteriori informazioni su `network port delete` nella ["Riferimento al comando ONTAP"](#).

- 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
```

Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Speed (Mbps)
Status							
-----	-----	-----	-----	-----	-----	-----	
-----							
...							
e0i		Default	Default	down	1500	auto/10	-
e0f		Default	Default	down	1500	auto/10	-
...							

```
net-f8040-34::> ucadmin show
```

Admin	Node	Adapter	Current Mode	Current Type	Pending Mode	Pending 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
```

Ulteriori informazioni su `network port show` nella ["Riferimento al comando ONTAP"](#).

#### 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.

Ulteriori informazioni su `network fcp adapter show` nella ["Riferimento al comando ONTAP"](#).

#### Informazioni correlate

- ["interfaccia di rete"](#)

#### 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) di marchio Cisco sono elencati nel *Hardware Universe*.

#### Informazioni correlate

- ["NetApp Hardware Universe"](#)
- ["visualizzazione dell'adattatore fcp di rete"](#)

#### Configurazioni delle porte supportate per gli adattatori X1143A-R6

La modalità di destinazione FC è la configurazione predefinita per le porte dell'adattatore X1143A-R6. Tuttavia, le porte di questo adattatore possono essere configurate come porte Ethernet da 10 GB e FCoE o come porte FC da 16 GB.

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.

#### Informazioni correlate

["NetApp Hardware Universe"](#)

["Configurazione SAN"](#)

#### 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.

Ulteriori informazioni su `network fcp adapter show` nella ["Riferimento al comando ONTAP"](#).

## 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 le LIF per tutti i protocolli SAN

### Gestire le LIF per tutti i protocolli SAN

Gli initiator devono utilizzare multipath i/o (MPIO) e Asymmetric Logical Unit Access (ALUA) per la funzionalità di failover dei cluster in un ambiente SAN. In caso di guasto di un nodo, i file LIF non migrano né assumono gli indirizzi IP del nodo partner guasto. Il software MPIO, che utilizza ALUA sull'host, è invece responsabile della selezione dei percorsi appropriati per l'accesso LUN tramite LIF.

È necessario creare uno o più percorsi iSCSI da ciascun nodo di una coppia ha, utilizzando le interfacce logiche (LIF) per consentire l'accesso alle LUN servite dalla coppia ha. È necessario configurare una LIF di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.

La connessione diretta o l'utilizzo di switch Ethernet sono supportati per la connettività. Devi creare LIF per entrambi i tipi di connettività.

- È necessario configurare una LIF di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.  
È possibile configurare due LIF per nodo, uno per ciascun fabric utilizzato con FC e per separare le reti Ethernet per iSCSI.

Una volta create, le LIF possono essere rimosse dai set di porte, spostate in nodi diversi di una Storage Virtual Machine (SVM) ed eliminate.

### Informazioni correlate

- ["Panoramica sulla configurazione delle LIF"](#)
- ["Creare una LIF"](#)

## Configura una LIF NVMe in ONTAP

Quando si configurano le LIF NVMe, è necessario soddisfare alcuni requisiti.

### Prima di iniziare

NVMe deve essere supportato dall'adattatore FC su cui si crea la LIF. Gli adattatori supportati sono elencati nella ["Hardware Universe"](#).

## A proposito di questa attività

A partire da ONTAP 9.12.1 e versioni successive, puoi configurare due LIF NVMe per nodo su un massimo di 12 nodi. In ONTAP 9.11.1 e versioni precedenti, è possibile configurare due LIF NVMe per nodo su un massimo di due nodi.

Quando si crea una LIF NVMe si applicano le seguenti regole:

- NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare una LIF di gestione per ogni SVM che supporta LA SAN.
- Per ONTAP 9,5 e versioni successive, devi configurare una LIF NVMe sul nodo che contiene il namespace e sul partner ha del nodo.
- Solo per ONTAP 9.4:
  - Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
  - È possibile configurare un solo LIF dati NVMe per SVM.

## Fasi

### 1. Crea la LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVME/TCP è disponibile a partire da ONTAP 9.10.1 e versioni successive.

### 2. Verificare che la LIF sia stata creata:

```
network interface show -vserver <SVM_name>
```

Dopo la creazione, le LIF NVMe/TCP sono in attesa del rilevamento sulla porta 8009.

## Informazioni correlate

- ["interfaccia di rete"](#)

## Cosa fare prima di spostare UNA SAN LIF

È necessario eseguire uno spostamento LIF solo se si modifica il contenuto del cluster, ad esempio aggiungendo nodi al cluster o eliminando nodi dal cluster. Se si esegue un movimento LIF, non è necessario ridefinire la zona del fabric FC o creare nuove sessioni iSCSI tra gli host collegati del cluster e la nuova interfaccia di destinazione.

Non è possibile spostare UN LIF SAN utilizzando `network interface move` comando. Lo spostamento DELLA SAN LIF deve essere eseguito portando la LIF offline, spostando la LIF su un nodo o una porta home differente e quindi riportandola online nella nuova posizione. ALUA (Asymmetric Logical Unit Access) offre percorsi ridondanti e selezione automatica del percorso come parte di qualsiasi soluzione SAN ONTAP. Pertanto, non si verifica alcuna interruzione i/o quando la LIF viene portata offline per il movimento. L'host semplicemente riprova e sposta i/o in un altro LIF.

Grazie al movimento LIF, puoi effettuare le seguenti operazioni senza interruzioni:

- Sostituire una coppia ha di un cluster con una coppia ha aggiornata in modo trasparente per gli host che accedono ai dati LUN
- Aggiornare una scheda di interfaccia di destinazione
- Spostare le risorse di una macchina virtuale di storage (SVM) da un set di nodi in un cluster a un altro set di nodi nel cluster

### Rimuovere una LIF SAN da un set di porte

Se la LIF che si desidera eliminare o spostare si trova in un set di porte, è necessario rimuovere la LIF dal set di porte prima di poter eliminare o spostare la LIF.

#### A proposito di questa attività

È necessario eseguire il passaggio 1 della procedura seguente solo se una porta LIF è impostata. Non è possibile rimuovere l'ultimo LIF in un set di porte se il set di porte è associato a un gruppo di iniziatori. In caso contrario, è possibile iniziare con la fase 2 se sono presenti più LIF nella porta impostata.

#### Fasi

1. Se nella porta impostata è presente un solo LIF, utilizzare `lun igroup unbind` comando per disassociare il set di porte dal gruppo di iniziatori.



Quando si dislega un gruppo di iniziatori da un set di porte, tutti gli iniziatori del gruppo di iniziatori hanno accesso a tutte le LUN di destinazione mappate al gruppo di iniziatori su tutte le interfacce di rete.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

Ulteriori informazioni su `lun igroup unbind` nella ["Riferimento al comando ONTAP"](#).

2. Utilizzare `lun portset remove` Comando per rimuovere LIF dal set di porte.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Ulteriori informazioni su `lun portset remove` nella ["Riferimento al comando ONTAP"](#).

### Spostare UNA LIF SAN

Se un nodo deve essere portato offline, è possibile spostare un LIF SAN per conservare le informazioni di configurazione, ad esempio WWPN, ed evitare di eseguire il zoning dello switch fabric. Poiché un LIF SAN deve essere portato offline prima di essere spostato, il traffico host deve fare affidamento sul software di multipathing host per fornire un accesso senza interruzioni al LUN. È possibile spostare LE LIF SAN in qualsiasi nodo di un cluster, ma non è possibile spostare LE LIF SAN tra le macchine virtuali di storage (SVM).

#### Prima di iniziare

Se la LIF è membro di un set di porte, la LIF deve essere stata rimossa dalla porta impostata prima di poter spostare la LIF in un nodo diverso.

## A proposito di questa attività

Il nodo di destinazione e la porta fisica di un LIF che si desidera spostare devono trovarsi sullo stesso fabric FC o sulla stessa rete Ethernet. Se si sposta un LIF in un fabric diverso che non è stato correttamente zonato o si sposta un LIF in una rete Ethernet che non dispone di connettività tra iSCSI Initiator e destinazione, il LUN non sarà accessibile quando viene riportato online.

## Fasi

1. Visualizzare lo stato amministrativo e operativo della LIF:

```
network interface show -vserver vservice_name
```

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

2. Modificare lo stato del LIF in down (offline):

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin down
```

Ulteriori informazioni su `network interface modify` nella ["Riferimento al comando ONTAP"](#).

3. Assegnare alla LIF un nuovo nodo e una nuova porta:

```
network interface modify -vserver vservice_name -lif LIF_name -home-node node_name -home-port port_name
```

4. Modificare lo stato del LIF in up (online):

```
network interface modify -vserver vservice_name -lif LIF_name -status-admin up
```

Ulteriori informazioni su `up` nella ["Riferimento al comando ONTAP"](#).

5. Verificare le modifiche:

```
network interface show -vserver vservice_name
```

## Eliminare una LIF in un ambiente SAN

Prima di eliminare una LIF, assicurarsi che l'host connesso alla LIF possa accedere alle LUN attraverso un altro percorso.


### Prima di iniziare

Se il LIF che si desidera eliminare è membro di un set di porte, è necessario prima rimuovere il LIF dal set di porte prima di poter eliminare il LIF.

## System Manager

Eliminazione di una LIF con Gestione di sistema di ONTAP (9.7 e versioni successive).

### Fasi

1. In System Manager, fare clic su **rete > Panoramica**, quindi selezionare **interfacce di rete**.
2. Selezionare la VM di storage da cui si desidera eliminare la LIF.
3. Fare clic su  e selezionare **Elimina**.

### CLI

Eliminare un LIF con l'interfaccia utente di ONTAP.

### Fasi

1. Verificare il nome della LIF e la porta corrente da eliminare:

```
network interface show -vserver vs1
```

2. Eliminare la LIF:

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

Ulteriori informazioni su `network interface delete` nella ["Riferimento al comando ONTAP"](#).

3. Verificare di aver eliminato la LIF:

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Address/Mask	Node Port
Home			
-----	-----	-----	-----
vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

## Requisiti LIF SAN per l'aggiunta di nodi a un cluster

Quando si aggiungono nodi a un cluster, è necessario tenere presente alcune

considerazioni.

- Prima di creare LUN sui nuovi nodi, è necessario creare i file LIF appropriati.
- È necessario rilevare tali LIF dagli host in base alle specifiche dello stack host e del protocollo.
- È necessario creare LIF sui nuovi nodi in modo che i movimenti di LUN e volume siano possibili senza utilizzare la rete di interconnessione del cluster.

### **Configurare le LIF iSCSI in modo che restituisca FQDN per ospitare l'operazione di rilevamento di iSCSI SendTargets**

A partire da ONTAP 9, è possibile configurare le LIF iSCSI in modo che restituisca un nome di dominio completo (FQDN) quando un sistema operativo host invia un'operazione di rilevamento di iSCSI SendTargets. La restituzione di un FQDN è utile quando è presente un dispositivo NAT (Network Address Translation) tra il sistema operativo host e il servizio di storage.

#### **A proposito di questa attività**

Gli indirizzi IP su un lato del dispositivo NAT non hanno alcun significato dall'altro lato, ma gli FQDN possono avere un significato su entrambi i lati.



Il limite di interoperabilità del valore FQDN è di 128 caratteri su tutti i sistemi operativi host.

#### **Fasi**

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Configurare le LIF iSCSI per restituire FQDN:

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name  
-sendtargets_fqdn FQDN
```

Nell'esempio seguente, le LIF iSCSI sono configurate per restituire storagehost-005.example.com come FQDN.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn  
storagehost-005.example.com
```

3. Verificare che sendtargets sia l'FQDN:

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

In questo esempio, storagehost-005.example.com viene visualizzato nel campo di output sendtargets-fqdn.

```
cluster::vserver*> vs1 iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif          sendtargets-fqdn
-----
vs1      vs1_iscsi1  storagehost-005.example.com
vs1      vs1_iscsi2  storagehost-006.example.com
```

## Informazioni correlate

["Riferimento al comando ONTAP"](#)

## Attivare l’allocazione dello spazio ONTAP per i protocolli SAN

L’allocazione dello spazio ONTAP aiuta a impedire che le LUN o i namespace NVMe vengano portati offline se esauriscono lo spazio e consente agli host SAN di recuperare spazio.

Il supporto ONTAP per l’allocazione dello spazio si basa sul protocollo SAN e sulla versione di ONTAP in uso. A partire da ONTAP 9.16.1, l’allocazione dello spazio è abilitata per impostazione predefinita per i protocolli iSCSI, FC e NVMe per LUN appena creati e tutti i namespace.

Versione di ONTAP	Protocolli	L’allocazione dello spazio è...
9.16.1 o versione successiva	<ul style="list-style-type: none"> <li>• iSCSI</li> <li>• FC</li> <li>• NVMe</li> </ul>	Abilitata per impostazione predefinita per LUN appena creati e tutti i namespace
9.15.1	<ul style="list-style-type: none"> <li>• iSCSI</li> <li>• FC</li> </ul>	Attivata per impostazione predefinita per i LUN appena creati
	NVMe	Non supportato
9.14.1 e precedenti	<ul style="list-style-type: none"> <li>• iSCSI</li> <li>• FC</li> </ul>	Disattivata per impostazione predefinita per i LUN appena creati
	NVMe	Non supportato

Quando l’allocazione dello spazio è attivata:

- Se uno spazio LUN o namespace esaurisce, ONTAP comunica all’host che non è disponibile spazio libero per le operazioni di scrittura. Di conseguenza, LUN o namespace rimangono online e le operazioni di lettura continuano a essere gestite. A seconda della configurazione dell’host, l’host ritenta le operazioni di scrittura fino a quando non riesce o il filesystem host non viene messo offline. Le operazioni di scrittura riprendono quando ulteriore spazio libero diventa disponibile per LUN o namespace.

Se l’allocazione dello spazio non è abilitata, quando una LUN o uno spazio dei nomi esaurisce lo spazio, tutte le operazioni i/o non riescono e la LUN o lo spazio dei nomi vengono portati offline; il problema di spazio deve essere risolto per riprendere le normali operazioni. Potrebbe essere necessario eseguire nuovamente la scansione dei dispositivi LUN sull’host per ripristinare i percorsi e i dispositivi a uno stato

operativo.

- Un host può eseguire operazioni SCSI o NVME UNMAP (talvolta chiamate TRIM). Le operazioni di ANNULLAMENTO DELLA MAPPATURA consentono a un host di identificare blocchi di dati non più necessari perché non contengono più dati validi. L'identificazione avviene normalmente dopo l'eliminazione del file. Il sistema storage può quindi disallocare tali blocchi di dati in modo che lo spazio possa essere consumato altrove. Questa dislocazione migliora notevolmente l'efficienza complessiva dello storage, in particolare con file system con un elevato turnover dei dati.

### Prima di iniziare

L'abilitazione dell'allocazione dello spazio richiede una configurazione host in grado di gestire correttamente gli errori di allocazione dello spazio quando non è possibile completare una scrittura. Sfruttare SCSI o NVME UNMAP richiede una configurazione in grado di utilizzare il provisioning di blocchi logici, come definito nello standard SCSI SBC-3.

I seguenti host attualmente supportano il thin provisioning quando si attiva l'allocazione dello spazio:

- Citrix XenServer 6.5 e versioni successive
- VMware ESXi 5,0 e versioni successive
- Kernel Oracle Linux 6,2 UEK e versioni successive
- Red Hat Enterprise Linux 6.2 e versioni successive
- SUSE Linux Enterprise Server 11 e versioni successive
- Solaris 11,1 e versioni successive
- Windows

### A proposito di questa attività

Quando si aggiorna il cluster a ONTAP 9.15.1 o versioni successive, l'impostazione dell'allocazione dello spazio per tutte le LUN create prima dell'upgrade del software rimane invariata dopo l'upgrade, indipendentemente dal tipo di host. Ad esempio, se in ONTAP 9.13.1 è stato creato un LUN per un host VMware con allocazione dello spazio disattivata, l'allocazione dello spazio su tale LUN rimane disattivata dopo l'aggiornamento a ONTAP 9.15.1.

### Fasi

1. Attiva allocazione spazio:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>  
-space-allocation enabled
```

2. Verificare che l'allocazione dello spazio sia attivata:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>  
-fields space-allocation
```

3. Verificare che l'allocazione dello spazio sia attivata sul sistema operativo host.



Alcune configurazioni host, incluse alcune versioni di VMware ESXi, sono in grado di riconoscere automaticamente la modifica delle impostazioni e non richiedono l'intervento dell'utente. Altre configurazioni potrebbero richiedere una nuova scansione della periferica. Alcuni filesystem e gestori di volumi potrebbero richiedere impostazioni specifiche aggiuntive per abilitare il recupero dello spazio utilizzando SCSI UNMAP. Potrebbe essere necessario rimontare i file system o riavviare completamente il sistema operativo. Consultare la documentazione relativa all'host specifico.

## Configurazione host per host VMware ESXi 8.x e host NVMe successivi

Se si dispone di un host VMware che esegue ESXi 8.x o versione successiva con il protocollo NVMe, dopo aver attivato l'allocazione dello spazio in ONTAP, è necessario eseguire i seguenti passaggi sugli host.

### Fasi

1. Sull'host ESXi, verificare che il DSM sia disattivato:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

Il valore previsto è 0.

2. Abilitare il DSM NVMe:

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. Verificare che il DSM sia abilitato:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

Il valore previsto è 1.

### Link correlati

Ulteriori informazioni su ["Configurazione host NVMe-of per ESXi 8.x con ONTAP"](#).

## Combinazioni di configurazione di volume e file o LUN consigliate

### Panoramica delle combinazioni di configurazione di volume e file o LUN consigliate

Esistono combinazioni specifiche di configurazioni di volume e file o LUN FlexVol che è possibile utilizzare, a seconda dei requisiti di amministrazione e dell'applicazione. La comprensione dei vantaggi e dei costi di queste combinazioni può aiutarti a determinare la combinazione di configurazione del volume e del LUN più adatta al tuo ambiente.

Si consiglia di utilizzare le seguenti combinazioni di configurazione del volume e del LUN:

- File o LUN con spazio riservato con provisioning di volumi thick
- File o LUN non riservati in termini di spazio con provisioning di volumi thin
- File o LUN con spazio riservato con provisioning di volumi semi-spessi

È possibile utilizzare il thin provisioning SCSI sui LUN in combinazione con una qualsiasi di queste combinazioni di configurazione.

## **File o LUN con spazio riservato con provisioning di volumi thick**

### **Benefici:**

- Tutte le operazioni di scrittura all'interno dei file con spazio riservato sono garantite; non si verificheranno errori a causa dello spazio insufficiente.
- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.

### **Costi e limitazioni:**

- È necessario disporre di spazio sufficiente per l'aggregato in primo piano per supportare il volume con provisioning spesso.
- Lo spazio pari al doppio delle dimensioni del LUN viene allocato dal volume al momento della creazione del LUN.

## **File o LUN non riservati in termini di spazio con provisioning di volumi thin**

### **Benefici:**

- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.
- Lo spazio viene allocato solo quando viene utilizzato.

### **Costi e restrizioni:**

- Le operazioni di scrittura non sono garantite; possono fallire se il volume esaurisce lo spazio libero.
- È necessario gestire lo spazio libero nell'aggregato in modo efficace per evitare che l'aggregato esaurisca lo spazio libero.

## **File o LUN con spazio riservato con provisioning di volumi semi-spessi**

### **Benefici:**

Meno spazio viene riservato in anticipo rispetto al provisioning di volumi spessi e viene comunque fornita una garanzia di scrittura con il massimo sforzo.

### **Costi e restrizioni:**

- Con questa opzione, le operazioni di scrittura possono non riuscire.

È possibile ridurre questo rischio bilanciando correttamente lo spazio libero nel volume rispetto alla volatilità dei dati.

- Non puoi fare affidamento sulla conservazione di oggetti di data Protection come snapshot, file FlexClone e LUN.
- Non è possibile utilizzare le funzionalità di efficienza dello storage per la condivisione di blocchi di ONTAP che non possono essere eliminate automaticamente, tra cui deduplica, compressione e offload ODX/copia.

## **Determinare la combinazione di configurazione del volume e del LUN corretta per l'ambiente in uso**

Rispondendo ad alcune domande di base sull'ambiente in uso, è possibile determinare la migliore configurazione del volume FlexVol e del LUN per l'ambiente in uso.

### **A proposito di questa attività**

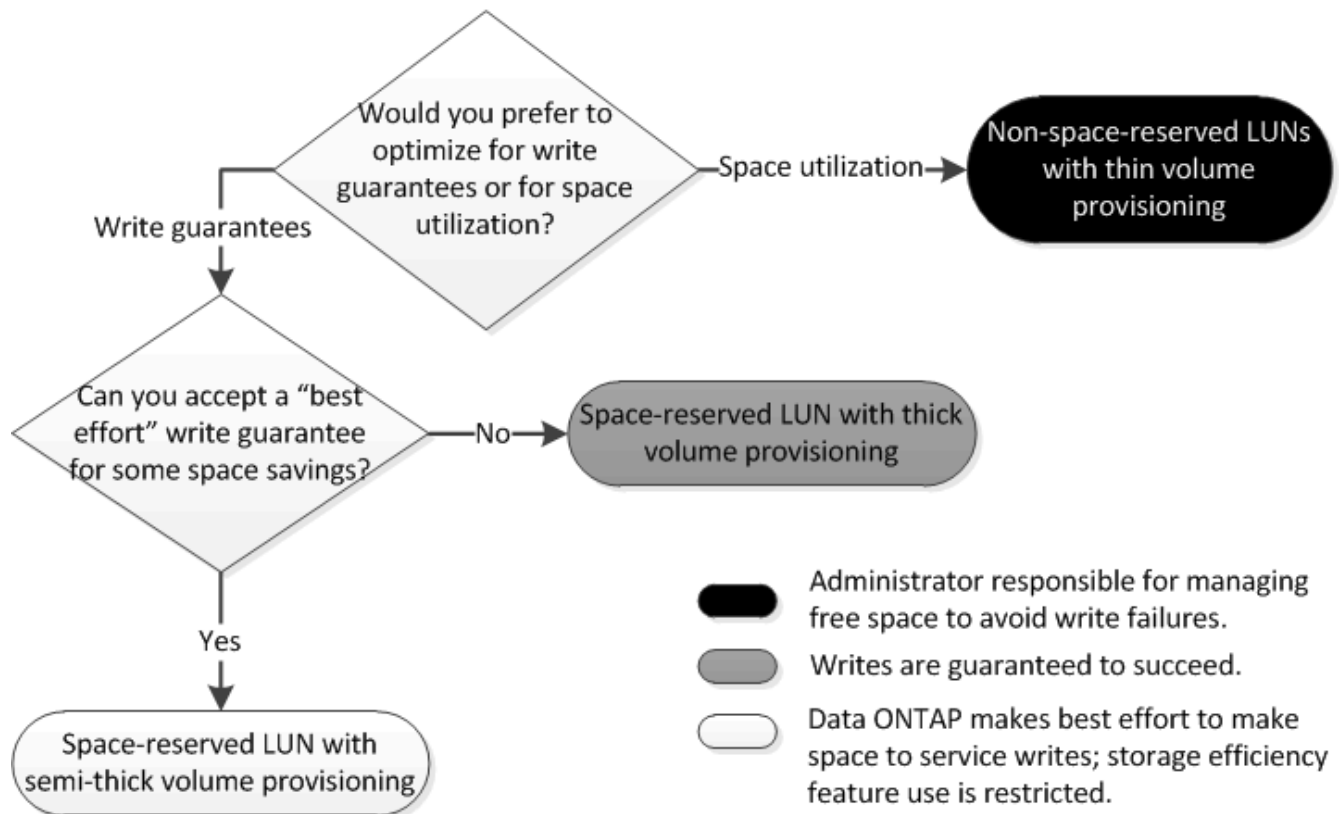
È possibile ottimizzare le configurazioni di LUN e volumi per il massimo utilizzo dello storage o per la sicurezza delle garanzie di scrittura. In base ai requisiti di utilizzo dello storage e alla capacità di monitorare e riempire rapidamente lo spazio libero, è necessario determinare il volume FlexVol e i volumi LUN appropriati per l'installazione.



Non è necessario un volume separato per ogni LUN.

#### Fase

1. Utilizzare la seguente struttura decisionale per determinare la combinazione di configurazione del volume e del LUN migliore per l'ambiente in uso:



#### Calcola il tasso di crescita dei dati per le LUN

È necessario conoscere il tasso di crescita dei dati LUN nel tempo per determinare se è necessario utilizzare LUN con spazio riservato o LUN senza spazio riservato.

#### A proposito di questa attività

Se hai un tasso di crescita dei dati costantemente elevato, le LUN riservate allo spazio potrebbero essere un'opzione migliore per te. Se si ha un basso tasso di crescita dei dati, è necessario prendere in considerazione LUN non riservate allo spazio.

Puoi utilizzare strumenti come OnCommand Insight per calcolare il tasso di crescita dei dati oppure puoi calcolarlo manualmente. I seguenti passaggi sono per il calcolo manuale.

#### Fasi

1. Impostare un LUN con spazio riservato.
2. Monitorare i dati sul LUN per un determinato periodo di tempo, ad esempio una settimana.

Assicurarsi che il periodo di monitoraggio sia sufficientemente lungo da formare un campione rappresentativo degli aumenti della crescita dei dati che si verificano regolarmente. Ad esempio, alla fine di ogni mese si potrebbe avere una notevole crescita dei dati.

3. Ogni giorno, registra in GB la crescita dei tuoi dati.
4. Al termine del periodo di monitoraggio, sommare i totali di ogni giorno, quindi dividere per il numero di giorni del periodo di monitoraggio.

Questo calcolo consente di ottenere il tasso medio di crescita.

### Esempio

In questo esempio, è necessario un LUN da 200 GB. Si decide di monitorare il LUN per una settimana e di registrare le seguenti modifiche giornaliere dei dati:

- Domenica: 20 GB
- Lunedì: 18 GB
- Martedì: 17 GB
- Mercoledì: 20 GB
- Giovedì: 20 GB
- Venerdì: 23 GB
- Sabato: 22 GB

In questo esempio, il tasso di crescita è  $(20+18+17+20+20+23+22) / 7 = 20$  GB al giorno.

### Impostazioni di configurazione per file o LUN con spazio riservato con volumi con thick provisioning

Questa combinazione di configurazione di file e volumi FlexVol o LUN offre la possibilità di utilizzare le tecnologie di efficienza dello storage e non richiede il monitoraggio attivo dello spazio libero, in quanto viene allocato spazio sufficiente in anticipo.

Le seguenti impostazioni sono necessarie per configurare un file o LUN con spazio riservato in un volume utilizzando il thick provisioning:

Impostazione del volume	Valore
Garanzia	Volume
Riserva frazionaria	100
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Attivato

### Impostazioni di configurazione per file non riservati allo spazio o LUN con volumi con thin provisioning

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede la minima quantità di storage da allocare in anticipo, ma richiede la gestione dello spazio libero attivo per evitare errori dovuti alla mancanza di spazio.

Le seguenti impostazioni sono necessarie per configurare un LUN o file non riservati allo spazio in un volume con thin provisioning:

Impostazione del volume	Valore
Garanzia	Nessuno
Riserva frazionaria	0
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Opzionale

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Disattivato

### Considerazioni aggiuntive

Quando il volume o l'aggregato esaurisce lo spazio, le operazioni di scrittura sul file o sul LUN possono avere esito negativo.

Se non si desidera monitorare attivamente lo spazio libero per il volume e l'aggregato, attivare la crescita automatica per il volume e impostare la dimensione massima del volume in base alle dimensioni dell'aggregato. In questa configurazione, è necessario monitorare attivamente lo spazio libero aggregato, ma non è necessario monitorare lo spazio libero nel volume.

### Impostazioni di configurazione per file o LUN con spazio riservato con provisioning di volumi semi-spessi

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede una quantità inferiore di storage da allocare in anticipo rispetto alla combinazione con provisioning completo, ma pone restrizioni sulle tecnologie di efficienza che è possibile utilizzare per il volume. Le sovrascritture vengono eseguite con il massimo sforzo per questa combinazione di configurazione.

Le seguenti impostazioni sono necessarie per configurare un LUN con spazio riservato in un volume utilizzando il provisioning semi-spessi:

Impostazione del volume	Valore
Garanzia	Volume
Riserva frazionaria	0
Riserva di Snapshot	0
Eliminazione automatica di Snapshot	On, con un livello di impegno di Destroy, un elenco Destroy che include tutti gli oggetti, il trigger impostato sul volume e tutti i LUN FlexClone e i file FlexClone abilitati per l'eliminazione automatica.
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Attivato

#### Restrizioni tecnologiche

Non è possibile utilizzare le seguenti tecnologie per l'efficienza dello storage dei volumi per questa combinazione di configurazione:

- Compressione
- Deduplica
- Offload delle copie di ODX e FlexClone
- LUN FlexClone e file FlexClone non contrassegnati per l'eliminazione automatica (cloni attivi)
- File secondari FlexClone
- Offload ODX/copia

#### Considerazioni aggiuntive

Quando si utilizza questa combinazione di configurazione, è necessario considerare i seguenti fatti:

- Quando il volume che supporta tale LUN ha poco spazio, i dati di protezione (LUN e file FlexClone, snapshot) vengono distrutti.
- Le operazioni di scrittura possono scadere e fallire quando il volume esaurisce lo spazio libero.

La compressione è attivata per impostazione predefinita per le piattaforme AFF. È necessario disattivare esplicitamente la compressione per qualsiasi volume per il quale si desidera utilizzare il provisioning semi-thick su una piattaforma AFF.

# Protezione dei dati SAN

## Scopri i metodi di protezione dei dati ONTAP per gli ambienti SAN

È possibile proteggere i dati creando copie di questi in modo che siano disponibili per il ripristino in caso di eliminazione accidentale, crash delle applicazioni, danneggiamento dei dati o disastro. A seconda delle esigenze di backup e protezione dei dati, ONTAP offre una vasta gamma di metodi che consentono di proteggere i dati.

### Sincronizzazione attiva di SnapMirror

A partire dalla disponibilità generale in ONTAP 9.9.1, fornisce l'obiettivo di tempo di ripristino zero (RTO zero) o il failover trasparente delle applicazioni (TAF) per consentire il failover automatico delle applicazioni business-critical negli ambienti SAN. SnapMirror Active Sync richiede l'installazione di ONTAP Mediator 1,2 in una configurazione con due cluster AFF o due cluster ASA (All-Flash SAN Array).

["Sincronizzazione attiva di SnapMirror"](#)

### Snapshot

Creazione, pianificazione e gestione manuale o automatica di backup multipli delle LUN grazie alle snapshot che utilizzano una quantità minima di spazio aggiuntivo sui volumi e che non comportano costi relativi alle performance. In caso di modifica o eliminazione accidentale dei dati del LUN, è possibile ripristinarli in maniera semplice e rapida da uno degli snapshot più recenti.

### LUN FlexClone (richiesta licenza FlexClone)

Fornisce copie scrivibili point-in-time di un'altra LUN in un volume attivo o in uno snapshot. Un clone e il suo padre possono essere modificati indipendentemente senza influire l'uno sull'altro.

### SnapRestore (licenza richiesta)

Permette di eseguire un recovery di dati veloce, efficiente in termini di spazio e su richiesta dalle snapshot su un intero volume. È possibile utilizzare SnapRestore per ripristinare un LUN a uno stato precedentemente conservato senza riavviare il sistema di storage.

### Copie mirrorate per la protezione dei dati (licenza SnapMirror richiesta)

Fornisce disaster recovery asincrono permettendoti di creare periodicamente snapshot di dati sul tuo volume, copiare tali snapshot su una rete locale o WAN in un volume partner, generalmente su un altro cluster e conservare tali snapshot. La copia mirror sul volume partner offre una rapida disponibilità e ripristino dei dati dal momento dell'ultimo snapshot, nel caso in cui i dati sul volume di origine siano corrotti o persi.

### Backup SnapVault (licenza SnapMirror richiesta)

Offre storage efficiente e conservazione a lungo termine dei backup. Le relazioni di SnapVault consentono di eseguire il backup di Snapshot selezionate di volumi su un volume di destinazione e di conservare i backup.

Se si eseguono backup su nastro e operazioni di archiviazione, è possibile eseguirli sui dati di cui è già stato eseguito il backup sul volume secondario SnapVault.

## SnapDrive per Windows o UNIX (licenza SnapDrive richiesta)

Configura l'accesso ai LUN, gestisce i LUN e gestisce le snapshot del sistema storage direttamente da host Windows o UNIX.

### Backup e ripristino su nastro nativo

Il supporto per la maggior parte delle unità a nastro esistenti è incluso in ONTAP, oltre a un metodo per i vendor di nastri per aggiungere dinamicamente il supporto per i nuovi dispositivi. ONTAP supporta anche il protocollo RMT (Remote Magnetic Tape), che consente il backup e il ripristino su qualsiasi sistema compatibile.

### Informazioni correlate

["Documentazione NetApp: SnapDrive per UNIX"](#) ["Documentazione NetApp: SnapDrive per Windows \(release correnti\)"](#) ["Protezione dei dati mediante backup su nastro"](#)

## Ripristinare una singola LUN da uno snapshot ONTAP

Puoi ripristinare una singola LUN da uno snapshot senza ripristinare l'intero volume che contiene la singola LUN. È possibile ripristinare il LUN in posizione o in un nuovo percorso nel volume. L'operazione ripristina solo la singola LUN senza influire su altri file o LUN nel volume. È anche possibile ripristinare i file con i flussi.

### Prima di iniziare

- È necessario disporre di spazio sufficiente sul volume per completare l'operazione di ripristino:
  - Se si sta ripristinando una LUN riservata allo spazio in cui la riserva frazionaria è pari a 0%, è necessario avere una dimensione pari a una volta quella della LUN ripristinata.
  - Se si sta ripristinando una LUN riservata allo spazio in cui la riserva frazionaria è del 100%, sono necessarie due volte le dimensioni della LUN ripristinata.
  - Se si sta ripristinando una LUN non riservata allo spazio, è necessario solo lo spazio effettivo utilizzato per la LUN ripristinata.

- È necessario creare uno snapshot del LUN di destinazione.

Se l'operazione di ripristino non riesce, il LUN di destinazione potrebbe essere troncato. In questi casi, è possibile utilizzare lo snapshot per evitare la perdita di dati.

- È necessario creare uno snapshot del LUN di origine.

In rari casi, il ripristino del LUN potrebbe non riuscire, lasciando inutilizzabile il LUN di origine. In questo caso, è possibile utilizzare lo snapshot per riportare il LUN allo stato appena prima del tentativo di ripristino.

- Il LUN di destinazione e il LUN di origine devono avere lo stesso tipo di sistema operativo.

Se il LUN di destinazione ha un tipo di sistema operativo diverso dal LUN di origine, l'host potrebbe perdere l'accesso ai dati al LUN di destinazione dopo l'operazione di ripristino.

### Fasi

1. Interrompere tutti gli accessi host al LUN dall'host.
2. Smontare il LUN sul proprio host in modo che l'host non possa accedere al LUN.

3. Dismappare il LUN:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

4. Determinare la snapshot su cui si desidera ripristinare il LUN:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Creare una snapshot del LUN prima di ripristinarlo:

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot_name>
```

6. Ripristinare il LUN specificato in un volume:

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot_name> -path <lun_path>
```

7. Seguire le istruzioni visualizzate.

8. Se necessario, portare il LUN online:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. Se necessario, rimappare il LUN:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

10. Dall'host, rimontare il LUN.

11. Riavviare l'accesso al LUN dall'host.

## Ripristino di tutte le LUN di un volume da una snapshot ONTAP

È possibile utilizzare il `volume snapshot restore` comando per ripristinare da uno snapshot tutti i LUN di un volume specifico.

### Fasi

1. Interrompere tutti gli accessi host alle LUN dall'host.

L'utilizzo di SnapRestore senza interrompere tutti gli accessi host alle LUN nel volume può causare la

corruzione dei dati e gli errori di sistema.

2. Smontare i LUN su tale host in modo che l'host non possa accedere ai LUN.
3. Dismappare le LUN:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

4. Determinare lo snapshot in cui si desidera ripristinare il volume:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

6. Ripristinare i dati:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot_name>
```

7. Seguire le istruzioni visualizzate.

8. Rimappare le LUN:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. Verificare che i LUN siano online:

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. Se le LUN non sono online, portarle online:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. Impostare i privilegi su admin:

```
set -privilege admin
```

12. Dall'host, rimontare i LUN.
13. Dall'host, riavviare l'accesso ai LUN.

## Proteggi i tuoi dati con le LUN di ONTAP FlexClone

Una LUN FlexClone è una copia scrivibile point-in-time di un altro LUN in un volume attivo o in uno snapshot. Il clone e il suo padre possono essere modificati indipendentemente senza influire l'uno sull'altro.

È possibile utilizzare LUN FlexClone per creare più copie di lettura/scrittura di un LUN.

### Motivi per creare LUN FlexClone

- È necessario creare una copia temporanea di un LUN a scopo di test.
- È necessario rendere disponibile una copia dei dati a utenti aggiuntivi senza fornire loro l'accesso ai dati di produzione.
- Si desidera creare un clone di un database per le operazioni di manipolazione e proiezione, conservando al contempo i dati originali in una forma inalterata.
- Si desidera accedere a un sottoinsieme specifico dei dati di un LUN (un volume logico o un file system specifico in un gruppo di volumi, O un file o un set di file specifico in un file system) e copiarlo nel LUN originale, senza ripristinare il resto dei dati nel LUN originale. Funziona su sistemi operativi che supportano contemporaneamente il montaggio di un LUN e di un clone del LUN. SnapDrive per UNIX supporta questa funzionalità con `snap connect` comando.
- Sono necessari più host DI boot SAN con lo stesso sistema operativo.

Un LUN FlexClone condivide inizialmente lo spazio con il LUN di origine. Per impostazione predefinita, il LUN FlexClone eredita l'attributo spazio-riservato del LUN padre. Ad esempio, se il LUN principale non è riservato allo spazio, anche il LUN FlexClone non è riservato per impostazione predefinita. Tuttavia, è possibile creare un LUN FlexClone non riservato allo spazio da un LUN padre che è riservato allo spazio.

Quando si clona una LUN, la condivisione dei blocchi avviene in background e non è possibile creare uno snapshot di un volume fino al termine della condivisione del blocco.

È necessario configurare il volume per attivare la funzione di eliminazione automatica del LUN FlexClone con `volume snapshot autodelete modify` comando. In caso contrario, se si desidera eliminare automaticamente i LUN FlexClone ma il volume non è configurato per l'eliminazione automatica di FlexClone, non viene eliminata alcuna LUN FlexClone.

Quando si crea un LUN FlexClone, la funzione di eliminazione automatica del LUN FlexClone viene disattivata per impostazione predefinita. È necessario abilitarlo manualmente su ogni LUN FlexClone prima che il LUN FlexClone possa essere cancellato automaticamente. Se si utilizza il provisioning di volumi semi-spessi e si desidera la garanzia di scrittura "Best effort" fornita da questa opzione, è necessario rendere disponibili *tutti* i LUN FlexClone per l'eliminazione automatica.



Quando si crea una LUN FlexClone da uno snapshot, la LUN viene automaticamente divisa dalla snapshot utilizzando un processo in background efficiente in termini di spazio, in modo che la LUN non continui a dipendere dalla snapshot o a consumare spazio aggiuntivo. Se la suddivisione in background non è stata completata e lo snapshot viene eliminato automaticamente, tale LUN FlexClone viene eliminato anche se è stata disattivata la funzione di eliminazione automatica FlexClone per tale LUN FlexClone. Una volta completata la suddivisione in background, il LUN FlexClone non viene eliminato anche se lo snapshot viene eliminato.

## Informazioni correlate

- ["Creare una LUN FlexClone"](#)
- ["Configurare un FlexVol volume per eliminare automaticamente i LUN FlexClone"](#)
- ["Impedisce l'eliminazione automatica di una LUN FlexClone"](#)

## Configurare e utilizzare i backup SnapVault in un ambiente SAN

### Informazioni sui backup ONTAP SnapVault in un ambiente SAN

La configurazione e l'utilizzo di SnapVault in un ambiente SAN sono molto simili alla configurazione e all'utilizzo in un ambiente NAS, ma il ripristino delle LUN in un ambiente SAN richiede alcune procedure speciali.

I backup di SnapVault contengono un set di copie di sola lettura di un volume di origine. In un ambiente SAN è sempre possibile eseguire il backup di interi volumi nel volume secondario SnapVault, non di singole LUN.

La procedura per la creazione e l'inizializzazione della relazione SnapVault tra un volume primario contenente LUN e un volume secondario che funge da backup SnapVault è identica alla procedura utilizzata con i volumi FlexVol utilizzati per i protocolli di file. Questa procedura è descritta in dettaglio in ["Protezione dei dati"](#).

È importante garantire che i LUN di cui viene eseguito il backup siano in uno stato coerente prima che le snapshot vengano create e copiate nel volume secondario SnapVault. L'automazione della creazione di snapshot con SnapCenter garantisce che i LUN di cui è stato eseguito il backup siano completi e utilizzabili dall'applicazione originale.

Esistono tre opzioni di base per il ripristino delle LUN da un volume secondario SnapVault:

- È possibile mappare un LUN direttamente dal volume secondario SnapVault e connettere un host al LUN per accedere al contenuto del LUN.

Il LUN è di sola lettura ed è possibile mappare solo lo snapshot più recente nel backup SnapVault. Le prenotazioni persistenti e altri metadati LUN vengono persi. Se lo si desidera, è possibile utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale, se ancora accessibile.

Il numero di serie del LUN è diverso da quello del LUN di origine.

- È possibile clonare qualsiasi snapshot nel volume secondario SnapVault in un nuovo volume di lettura/scrittura.

È quindi possibile mappare qualsiasi LUN del volume e connettere un host al LUN per accedere al contenuto del LUN. Se lo si desidera, è possibile utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale, se ancora accessibile.

- È possibile ripristinare l'intero volume contenente il LUN da qualsiasi snapshot nel volume secondario SnapVault.

Il ripristino dell'intero volume sostituisce tutte le LUN e tutti i file presenti nel volume. Tutte le nuove LUN create dopo la creazione dello snapshot vengono perse.

Le LUN mantengono la mappatura, i numeri di serie, gli UUID e le riserve persistenti.

## Accesso a una copia LUN in sola lettura da un backup ONTAP SnapVault

È possibile accedere a una copia di sola lettura di un LUN dall'ultimo snapshot in un backup SnapVault. L'ID LUN, il percorso e il numero di serie sono diversi dal LUN di origine e devono essere prima mappati. Le prenotazioni persistenti, le mappature LUN e gli igroups non vengono replicati nel volume secondario SnapVault.

### Prima di iniziare

- La relazione SnapVault deve essere inizializzata e lo snapshot più recente nel volume secondario SnapVault deve contenere il LUN desiderato.
- La macchina virtuale di storage (SVM) contenente il backup SnapVault deve disporre di una o più LIF con il protocollo SAN desiderato accessibile dall'host utilizzato per accedere alla copia del LUN.
- Se si prevede di accedere alle copie LUN direttamente dal volume secondario SnapVault, è necessario creare in anticipo i propri igroups sulla SVM SnapVault.

È possibile accedere a un LUN direttamente dal volume secondario SnapVault senza dover prima ripristinare o clonare il volume contenente il LUN.

### A proposito di questa attività

Se viene aggiunto un nuovo snapshot al volume secondario SnapVault mentre è stata mappata una LUN da uno snapshot precedente, il contenuto della LUN mappata cambia. Il LUN è ancora mappato con gli stessi identificatori, ma i dati vengono acquisiti dal nuovo snapshot. Se le dimensioni del LUN cambiano, alcuni host rilevano automaticamente la modifica delle dimensioni; gli host Windows richiedono una nuova scansione del disco per rilevare qualsiasi modifica delle dimensioni.

### Fasi

1. Elenca i LUN disponibili nel volume secondario di SnapVault.

```
lun show
```

In questo esempio, è possibile visualizzare i LUN originali nel volume primario srcvolA e le copie nel volume secondario SnapVault dstvolB:

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
-----	-----	-----	-----	-----	-----
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

```
6 entries were displayed.
```

Ulteriori informazioni su `lun show` nella ["Riferimento al comando ONTAP"](#).

2. Se il igroup per l'host desiderato non esiste già sulla SVM contenente il volume secondario SnapVault, creare un igroup.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol  
<protocol> -ostype <ostype> -initiator <initiator_name>
```

Questo comando crea un igroup per un host Windows che utilizza il protocollo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

3. Mappare la copia LUN desiderata all'igroup.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup  
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A  
-igroup temp_igroup
```

Ulteriori informazioni su `lun mapping create` nella ["Riferimento al comando ONTAP"](#).

4. Collegare l'host al LUN e accedere al contenuto del LUN come desiderato.

### Ripristinare una singola LUN da un backup ONTAP SnapVault

È possibile ripristinare una singola LUN in una nuova posizione o nella posizione originale. Puoi eseguire il ripristino da qualsiasi Snapshot nel volume secondario SnapVault. Per ripristinare il LUN nella posizione originale, ripristinarlo in una nuova posizione, quindi copiarlo.

#### Prima di iniziare

- La relazione SnapVault deve essere inizializzata e il volume secondario SnapVault deve contenere uno snapshot appropriato per il ripristino.
- La macchina virtuale di storage (SVM) contenente il volume secondario SnapVault deve disporre di una o più LIF con il protocollo SAN desiderato, accessibili dall'host utilizzato per accedere alla copia LUN.
- gli igroups devono già esistere sulla SVM SnapVault.

#### A proposito di questa attività

Il processo include la creazione di un clone del volume di lettura e scrittura da uno snapshot nel volume secondario SnapVault. È possibile utilizzare il LUN direttamente dal clone oppure, facoltativamente, copiare di nuovo il contenuto del LUN nella posizione originale del LUN.

Il LUN nel clone ha un percorso e un numero di serie diversi dal LUN originale. Le prenotazioni persistenti non vengono conservate.

## Fasi

1. Verificare il volume secondario che contiene il backup SnapVault.

```
snapmirror show
```

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

2. Identificare lo snapshot da cui si desidera ripristinare il LUN.

```
volume snapshot show
```

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. Creare un clone in lettura/scrittura dallo snapshot desiderato

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>  
-type <type> -parent-volume <parent_volume_name> -parent-snapshot  
<snapshot_name>
```

Il clone del volume viene creato nello stesso aggregato del backup di SnapVault. Lo spazio nell'aggregato deve essere sufficiente per memorizzare il clone.

```
cluster::> volume clone create -vserver vserverB
        -flexclone dstvolB_clone -type RW -parent-volume dstvolB
        -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Elenca i LUN nel clone del volume.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

Vserver	Path	State	Mapped	Type
vserverB	/vol/dstvolB_clone/lun_A	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_B	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_C	online	unmapped	windows

3 entries were displayed.

Ulteriori informazioni su `lun show` nella ["Riferimento al comando ONTAP"](#).

5. Se l'igroup per l'host desiderato non esiste già nella SVM contenente il backup di SnapVault, creare un igroup.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

Questo esempio crea un igroup per un host Windows che utilizza il protocollo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
        -protocol iscsi -ostype windows
        -initiator iqn.1991-05.com.microsoft:hostA
```

6. Mappare la copia LUN desiderata all'igroup.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
-path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

Ulteriori informazioni su `lun mapping create` nella ["Riferimento al comando ONTAP"](#).

7. Collegare l'host al LUN e accedere al contenuto del LUN, come desiderato.

Il LUN è di lettura/scrittura e può essere utilizzato al posto del LUN originale. Poiché il numero di serie del LUN è diverso, l'host lo interpreta come un LUN diverso dall'originale.

8. Utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale.

#### Informazioni correlate

- ["spettacolo snapmirror"](#)

#### Ripristino di tutte le LUN di un volume da un backup ONTAP SnapVault

Se è necessario ripristinare una o più LUN di un volume da un backup SnapVault, è possibile ripristinare l'intero volume. Il ripristino del volume influisce su tutti i LUN del volume.

#### Prima di iniziare

La relazione SnapVault deve essere inizializzata e il volume secondario SnapVault deve contenere uno snapshot appropriato per il ripristino.

#### A proposito di questa attività

Il ripristino di un intero volume riporta il volume allo stato in cui si trovava quando è stata creata la snapshot. Se al volume è stata aggiunta una LUN dopo lo snapshot, tale LUN viene rimosso durante il processo di ripristino.

Dopo il ripristino del volume, i LUN rimangono mappati agli igroups a cui sono stati mappati poco prima del ripristino. La mappatura LUN potrebbe essere diversa dalla mappatura al momento dello snapshot. Le riserve persistenti sulle LUN dei cluster host vengono mantenute.

#### Fasi

1. Arrestare i/o su tutti i LUN del volume.
2. Verificare il volume secondario che contiene il volume secondario SnapVault.

```
snapmirror show
```

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA		XDP vserverB:dstvolB	Snapmirrored	Idle	-	true	-

3. Identificare lo snapshot da cui si desidera eseguire il ripristino.

```
volume snapshot show
```

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB					
		snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. Specificare l'istantanea da utilizzare.

```
snapmirror restore -destination-path <destination_path> -source-path  
<source_path> -source-snapshot <snapshot_name>
```

La destinazione specificata per il ripristino è il volume originale su cui si sta eseguendo il ripristino.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA  
-source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010
```

```
Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on  
volume vserverA:src_volA will be deleted.  
Do you want to continue? {y|n}: y  
[Job 98] Job is queued: snapmirror restore from source  
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Se si condividono LUN in un cluster host, ripristinare le riserve persistenti sulle LUN dagli host interessati.

## Ripristino di un volume da un backup SnapVault

Nell'esempio seguente, il LUN denominato LUN\_D è stato aggiunto al volume dopo la creazione dello snapshot. Dopo aver ripristinato l'intero volume dallo snapshot, lun\_D non viene più visualizzato.

In `lun show` Output dei comandi, è possibile visualizzare i LUN nel volume primario srcvolA e le copie di sola lettura di tali LUN nel volume secondario SnapVault dstvolB. Nessuna copia di lun\_D nel backup di SnapVault.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA  
-source-path vserverB:dstvolB  
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than snapshot hourly.2013-02-11\_1205  
on volume vserverA:src\_volA will be deleted.  
Do you want to continue? {y|n}: y  
[Job 98] Job is queued: snapmirror restore from source  
"vserverB:dstvolB" for the snapshot daily.2013-02-10\_0010.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

Una volta ripristinato il volume dal volume secondario SnapVault, il volume di origine non contiene più lun\_D. Non è necessario rimappare le LUN nel volume di origine dopo il ripristino, perché sono ancora mappate.

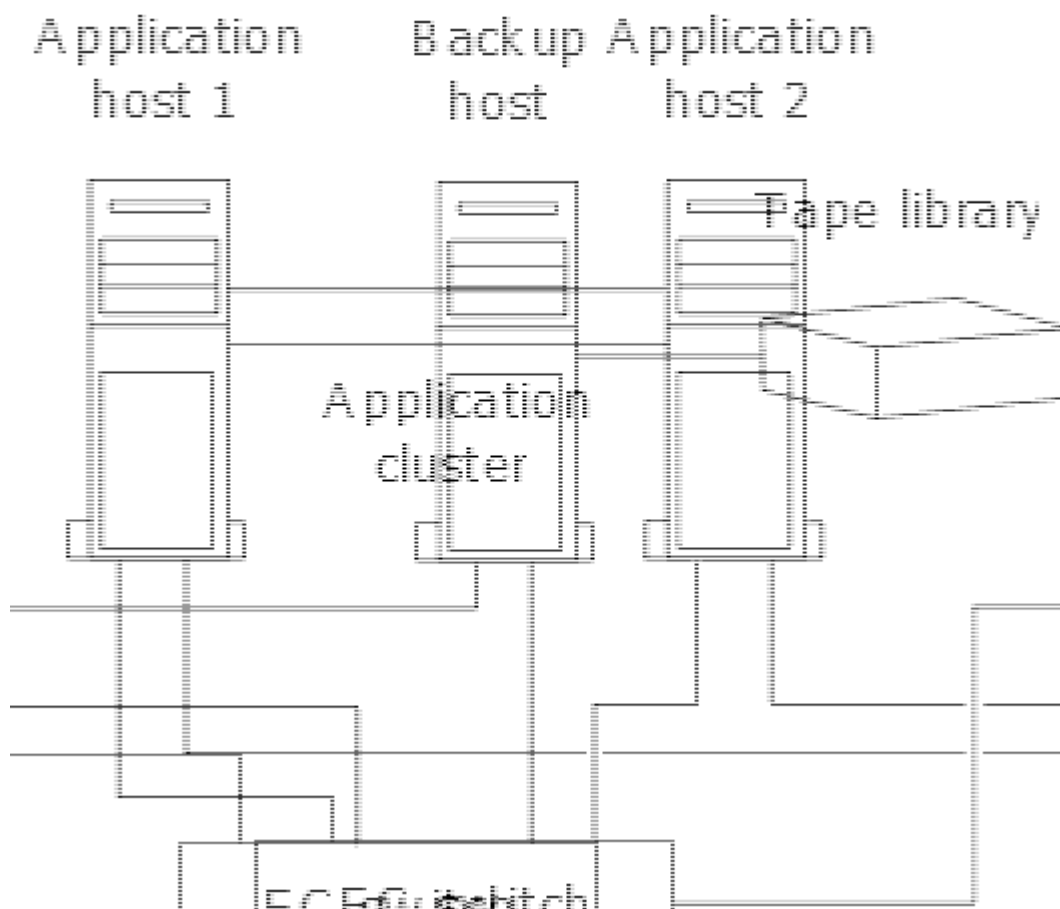
## Informazioni correlate

- "ripristino di snapmirror"
- "spettacolo snapmirror"

## Configurazione consigliata per collegare un sistema di backup host a ONTAP

È possibile eseguire il backup dei sistemi SAN su nastro attraverso un host di backup separato per evitare il peggioramento delle performance sull'host dell'applicazione.

È fondamentale che i dati SAN e NAS siano separati a scopo di backup. La figura seguente mostra la configurazione fisica consigliata per un sistema di backup host sul sistema di storage primario. È necessario configurare i volumi solo COME SAN. Le LUN possono essere limitate a un singolo volume oppure possono essere distribuite su più volumi o sistemi storage.



I volumi su un host possono essere costituiti da un singolo LUN mappato dal sistema di storage o da più LUN utilizzando un gestore di volumi, ad esempio VxVM sui sistemi HP-UX.

## Utilizzare un sistema di backup host per proteggere un LUN sul sistema di storage ONTAP

È possibile utilizzare un LUN clonato da uno snapshot come dati di origine per il sistema di backup host.

### Prima di iniziare

Un LUN di produzione deve esistere ed essere mappato a un igroup che includa il nome del nodo WWPN o Initiator del server applicazioni. Anche il LUN deve essere formattato e accessibile all'host

## Fasi

1. Salvare su disco il contenuto dei buffer del file system host.

È possibile utilizzare il comando fornito dal sistema operativo host oppure SnapDrive per Windows o SnapDrive per UNIX. Puoi anche scegliere di includere questo passo nello script di pre-elaborazione del backup SAN.

2. Creare una snapshot della LUN di produzione.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>  
-snapshot <snapshot> -comment <comment> -foreground false
```

3. Creare un clone della LUN di produzione.

```
volume file clone create -vserver <SMV_name> -volume <volume> -source  
-path <path> -snapshot-name <snapshot> -destination-path  
<destination_path>
```

4. Creare un igroup che includa il WWPN del server di backup.

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol  
<protocol> -ostype <os_type> -initiator <initiator>
```

5. Associare il clone LUN creato al passaggio 3 all'host di backup.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup>
```

È possibile scegliere di inserire questo passo nello script di post-elaborazione dell'applicazione DI backup SAN.

6. Individuare il nuovo LUN dall'host e rendere il file system disponibile all'host.

È possibile scegliere di inserire questo passo nello script di post-elaborazione dell'applicazione DI backup SAN.

7. Eseguire il backup dei dati nel clone LUN dall'host di backup su nastro utilizzando l'applicazione DI backup SAN.
8. Portare il clone LUN offline.

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. Rimuovere il clone del LUN.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. Rimuovere l'istantanea.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot  
<snapshot>
```

## 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.



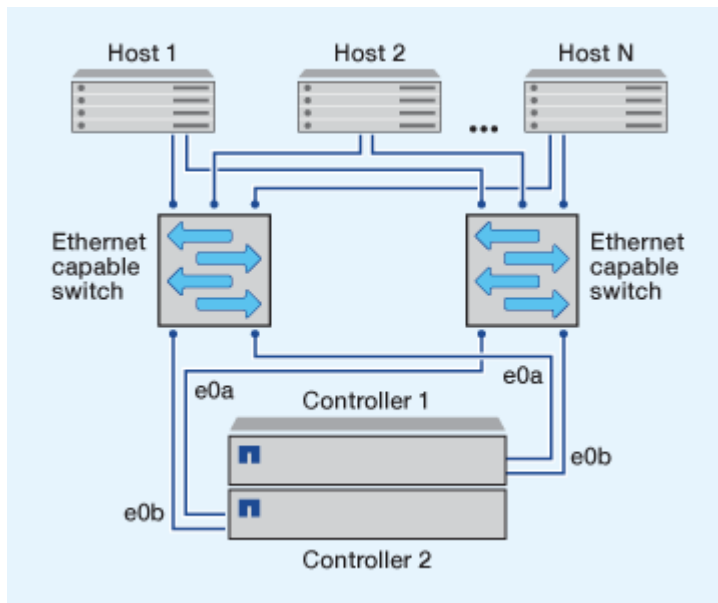
"**Configurazioni a nodo singolo**" sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

#### 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](#)".

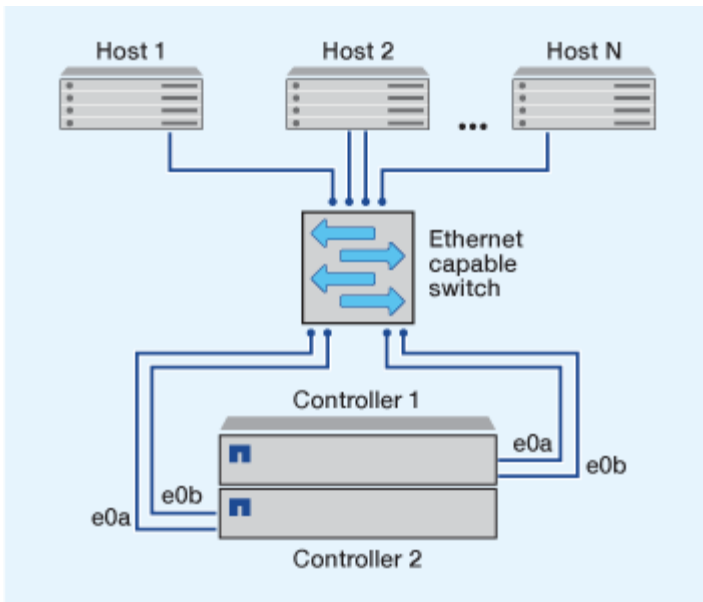
#### Configurazioni iSCSI multi-rete

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.



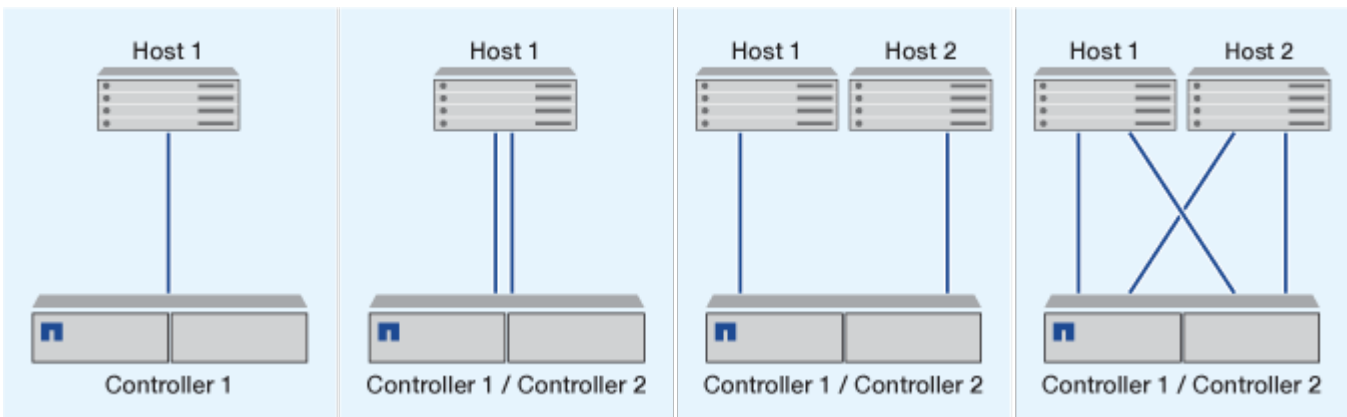
#### Configurazioni iSCSI a rete singola

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.

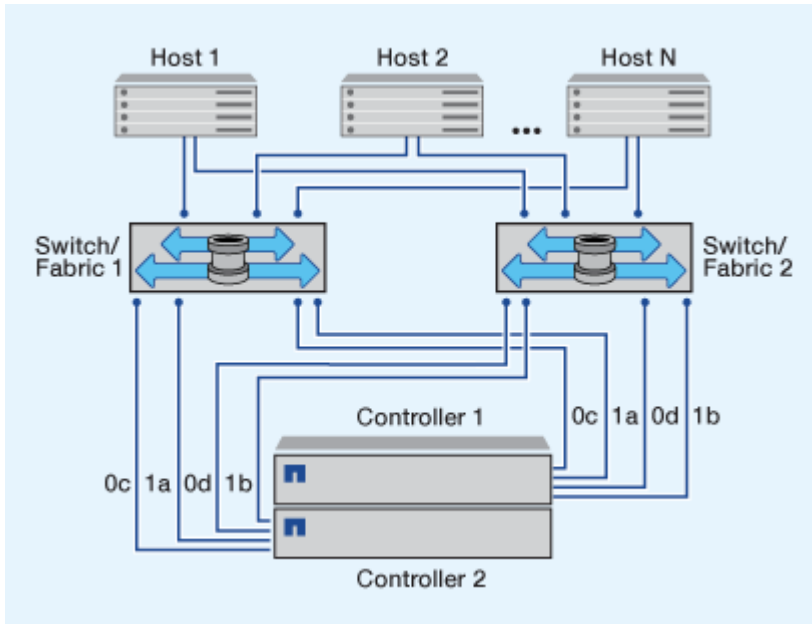
Più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere contemporaneamente ai controller di storage. Gli host richiedono l'installazione e la configurazione di una soluzione multipathing supportata. È possibile verificare i sistemi operativi e le soluzioni multipathing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

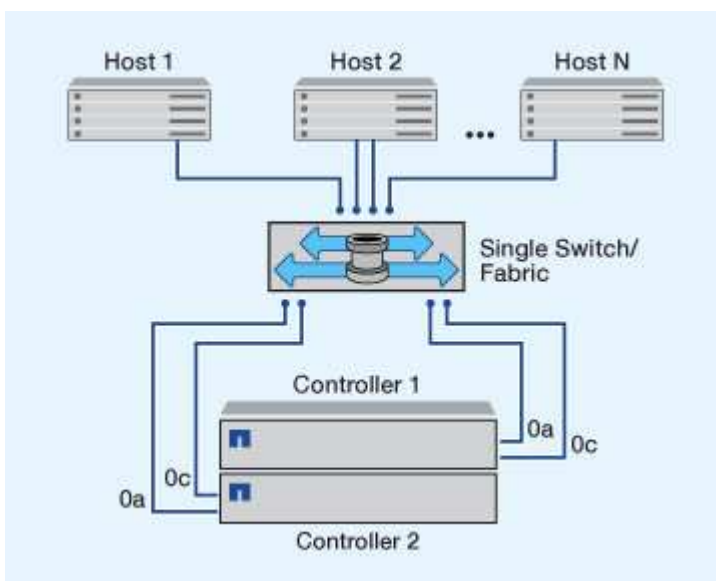


#### Configurazioni FC e FC-NVMe single-fabric

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
<ul style="list-style-type: none"><li>• FAS8200</li><li>• AFF A300</li></ul>	0g+0h	1: 0g 2: 0g, 0h

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte consigliate
<ul style="list-style-type: none"> <li>FAS2720</li> <li>FAS2750</li> <li>AFF A220</li> </ul>	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
<ul style="list-style-type: none"> <li>4 GB</li> <li>2 GB</li> <li>1 GB</li> </ul>	<ul style="list-style-type: none"> <li>8 GB</li> <li>4 GB</li> <li>2 GB</li> </ul>	<ul style="list-style-type: none"> <li>16 GB</li> <li>8 GB</li> <li>4 GB</li> </ul>	<ul style="list-style-type: none"> <li>32 GB</li> <li>16 GB</li> <li>8 GB</li> </ul>

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 nodel -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 nodel -adapter 0c -speed 16
```

5. Portare l'adattatore online:

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

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

```
network interface modify -vserver * -lif * { -home-node nodel -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	<code>network fcp adapter show</code>
Modificare i parametri dell'adattatore di destinazione FC	<code>network fcp adapter modify</code>

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni sul traffico del protocollo FC	<code>run -node <i>node_name</i> sysstat -f</code>
Visualizza per quanto tempo il protocollo FC è in esecuzione	<code>run -node <i>node_name</i> uptime</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node <i>node_name</i> sysconfig -ac</code>
Visualizzare una pagina man per un comando	<code>man <i>command_name</i></code>

#### 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	<code>run -node <i>node_name</i> storage show <i>adapter</i></code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node <i>node_name</i> sysconfig -ac</code>

#### Comandi per la gestione degli adattatori FC integrati

Se si desidera...	Utilizzare questo comando...
Visualizza lo stato delle porte FC integrate	<code>system node hardware unified-connect show</code>

#### 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.

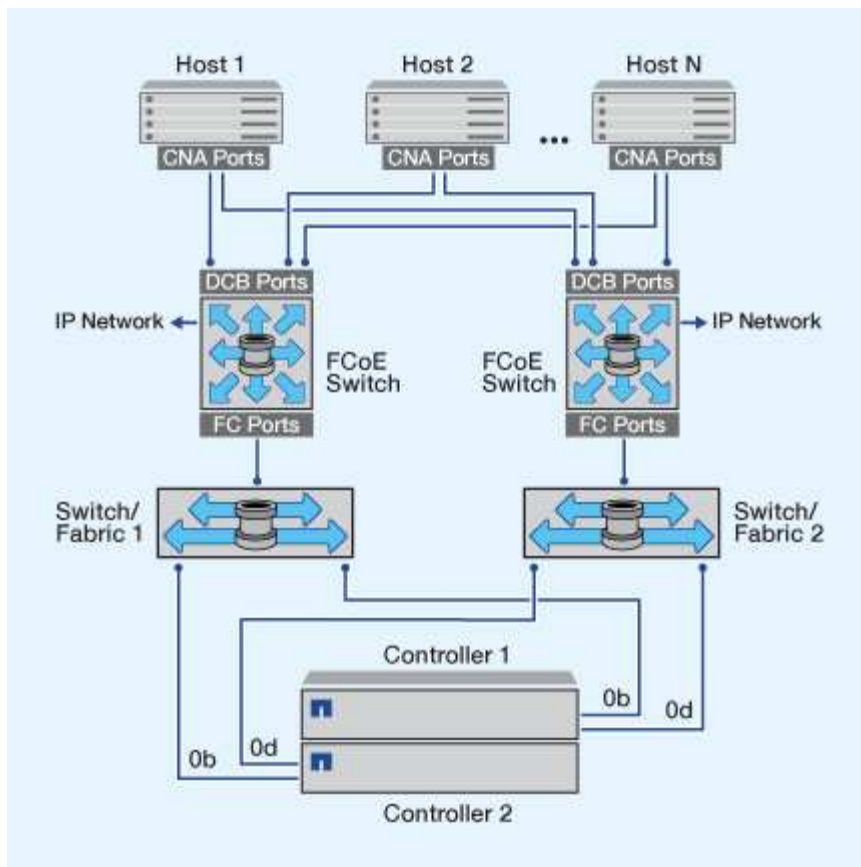
Le configurazioni FCoE richiedono switch Ethernet che supportano esplicitamente le funzionalità FCoE. Le configurazioni FCoE vengono validate attraverso lo stesso processo di interoperabilità e di garanzia della qualità degli switch FC. Le configurazioni supportate sono elencate nella matrice di interoperabilità.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

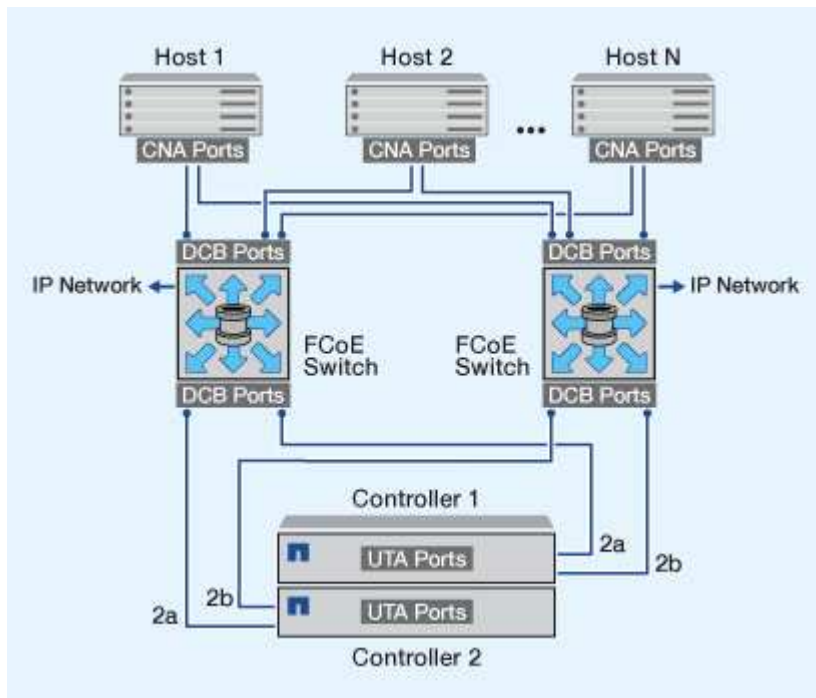
Utilizzando gli iniziatori FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha attraverso gli switch FCoE alle porte di destinazione FC. Lo switch FCoE deve anche disporre di porte FC. L'iniziatore FCoE host si connette sempre allo switch FCoE. Lo switch FCoE può connettersi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



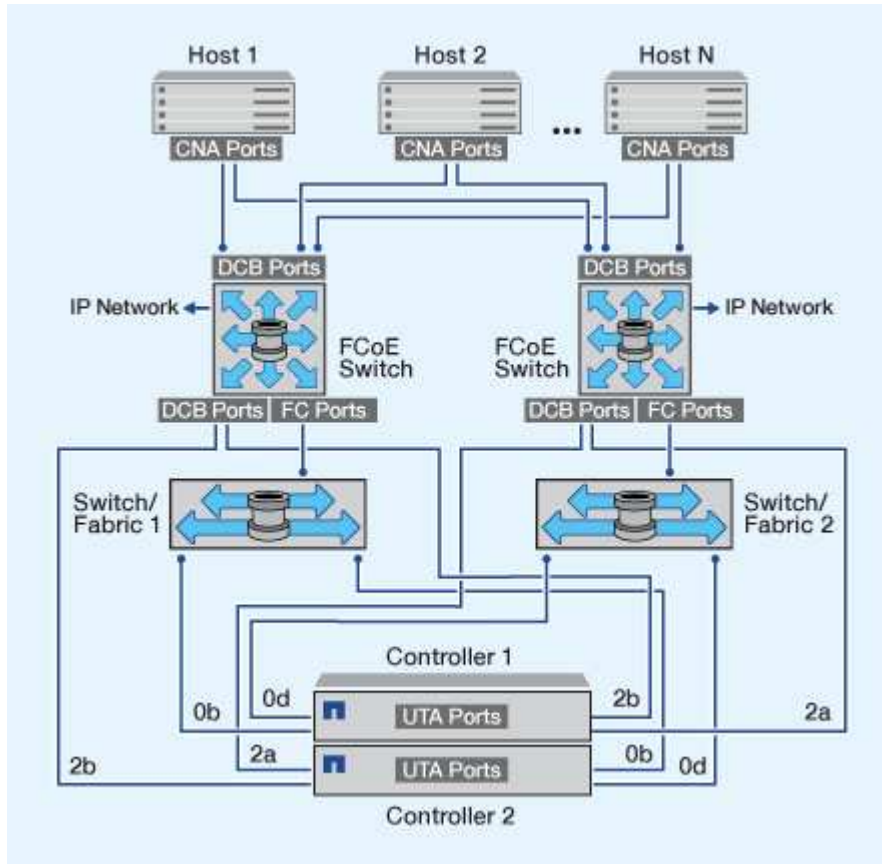
#### Iniziatore FCoE alla destinazione FCoE

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.



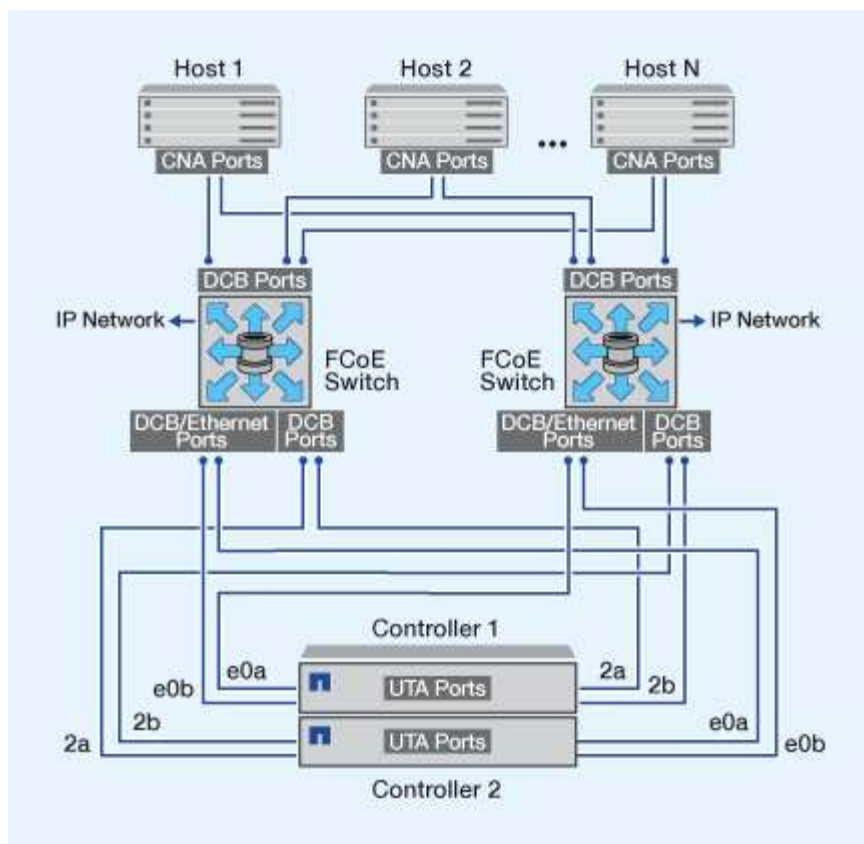
### Iniziatore FCoE per destinazioni FCoE e FC

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.



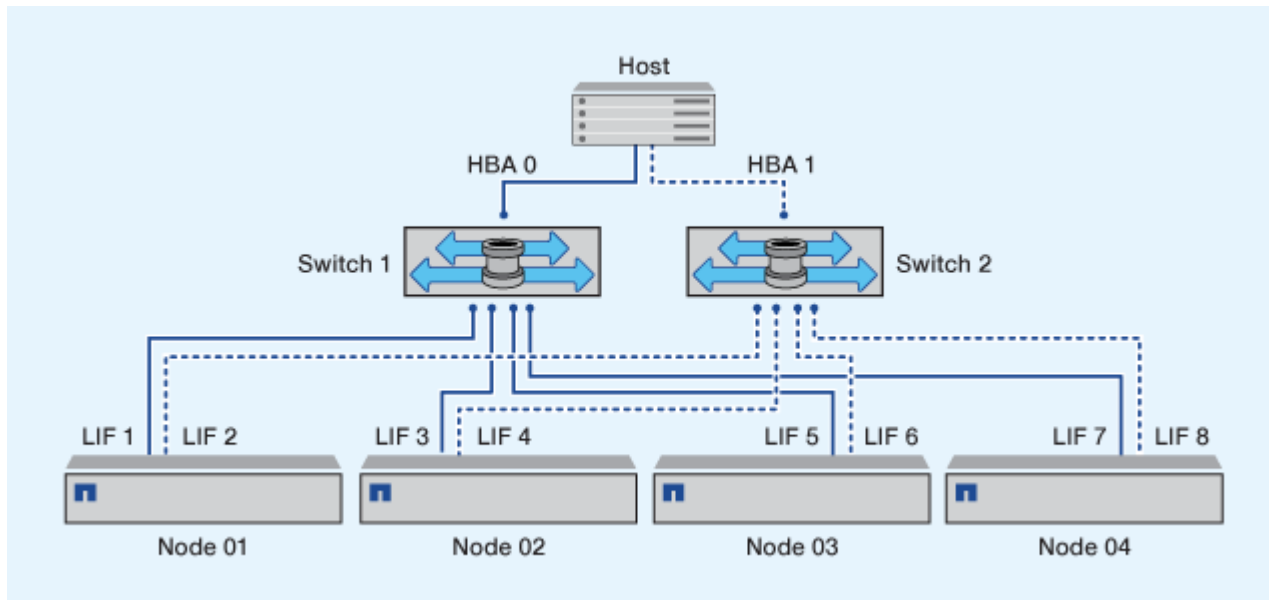
La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- 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 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.

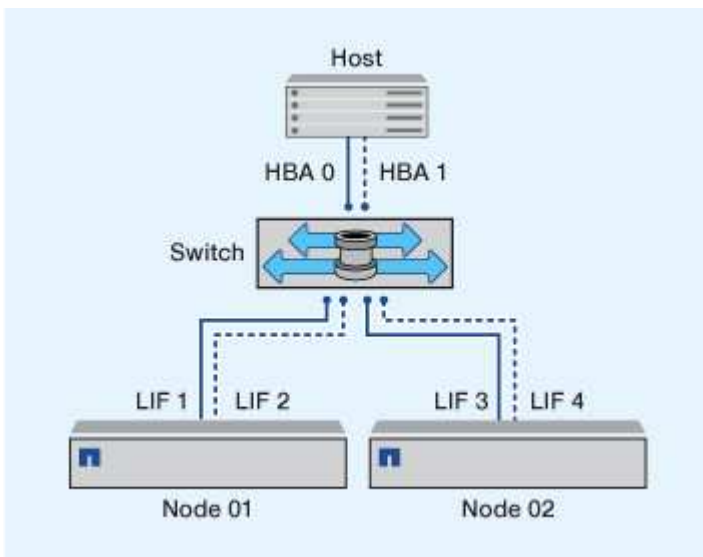
Nella figura seguente, l'host dispone di due iniziatori e sta eseguendo un software multipathing. Esistono due zone:



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 9. 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-pwvn 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 colleghino 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:

```
fcip 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 (ASAA1K, ASAA90, ASAA70, ASAA50, ASAA30, ASAA20 o ASAC30), 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	<ul style="list-style-type: none"><li>• NVMe/TCP</li><li>• NVMe/FC</li></ul>	12
9.10.1	<ul style="list-style-type: none"><li>• NVMe/TCP</li></ul>	2
9.9.1	<ul style="list-style-type: none"><li>• NVMe/FC</li></ul>	2
	<ul style="list-style-type: none"><li>• FC</li><li>• ISCSI</li></ul>	12
9.7	<ul style="list-style-type: none"><li>• FC</li><li>• ISCSI</li></ul>	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	<ul style="list-style-type: none"><li>• NVMe/TCP</li></ul>	2 nodi per cluster in configurazioni MetroCluster IP a quattro nodi
9.12.1	<ul style="list-style-type: none"><li>• NVMe/FC</li></ul>	2 nodi per cluster in configurazioni MetroCluster IP a quattro nodi
9.9.1	<ul style="list-style-type: none"><li>• FC</li><li>• ISCSI</li></ul>	4 nodi per cluster in configurazioni MetroCluster IP a 8 nodi
9.7	<ul style="list-style-type: none"><li>• FC</li><li>• ISCSI</li></ul>	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 WWPN. 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	<ul style="list-style-type: none"><li>• 7 per FC</li><li>• 5 per FCoE</li></ul>
Cisco	<ul style="list-style-type: none"><li>• 7 per FC</li><li>• Fino a 3 switch possono essere switch FCoE.</li></ul>

### 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 disuguaglianza 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.  $15 \times 128 = 1,920$ . 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.  $30 \times 128 = 3,840$ . 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  $15 \times 128 = 1,920$ .
  - 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)  $\times$  (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 =  $40,000 \times (.003) = 120$ .

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  $(10 \times 128) + (20 \times 32) = 1,920$ .

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

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

### 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/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/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 `/tgt-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\lpnids\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 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/qauccli
```

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

```

[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.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 COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

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

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

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

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

## Informazioni sul marchio commerciale

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