Configurazione di iSCSI

E-Series Systems

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/it-it/e-series/config-linux/iscsi-verify-linux-config-support-task.html on March 22, 2024. Always check docs.netapp.com for the latest.

Sommario

Configurazione di iSCSI

Verificare che la configurazione Linux sia supportata

Per garantire un funzionamento affidabile, è necessario creare un piano di implementazione e utilizzare lo strumento matrice di interoperabilità NetApp (IMT) per verificare che l'intera configurazione sia supportata.

Fasi

1. Accedere alla "Tool di matrice di interoperabilità NetApp".
2. Fare clic sulla sezione **Ricerca soluzione**.
3. Nell'area **Protocols › SAN host**, fare clic sul pulsante **Add** (Aggiungi) accanto a **e-Series SAN host**.
4. Fare clic su **View Refine Search Criteria** (Visualizza criteri di ricerca raffinati).

   Viene visualizzata la sezione Criteri di ricerca più precisi. In questa sezione è possibile selezionare il protocollo applicabile e altri criteri per la configurazione, ad esempio sistema operativo, sistema operativo NetApp e driver host multipath.

5. Selezionare i criteri desiderati per la configurazione, quindi visualizzare gli elementi di configurazione compatibili applicabili.
6. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo prescritti nello strumento.

   Per informazioni dettagliate sulla configurazione scelta, fare clic sulla freccia a destra della pagina Visualizza configurazioni supportate.

Configurare gli indirizzi IP utilizzando DHCP

Per configurare le comunicazioni tra la stazione di gestione e lo storage array, utilizzare il protocollo DHCP (Dynamic host Configuration Protocol) per fornire gli indirizzi IP.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un server DHCP installato e configurato sulla stessa subnet delle porte di gestione dello storage.

A proposito di questa attività

Ogni array di storage dispone di un controller (simplex) o due controller (duplex) e ciascun controller dispone di due porte per la gestione dello storage. A ciascuna porta di gestione viene assegnato un indirizzo IP.

Le seguenti istruzioni si riferiscono a uno storage array con due controller (configurazione duplex).

Fasi

1. In caso contrario, collegare un cavo Ethernet alla stazione di gestione e alla porta di gestione 1 di ciascun controller (A e B).

   Il server DHCP assegna un indirizzo IP alla porta 1 di ciascun controller.

> Non utilizzare la porta di gestione 2 su entrambi i controller. La porta 2 è riservata al personale tecnico di NetApp.

> Se si scollega e si ricollega il cavo Ethernet o se lo storage array viene spento e riacceso, DHCP assegna nuovamente gli indirizzi IP. Questo processo si verifica fino a quando non vengono configurati gli indirizzi IP statici. Si consiglia di evitare di scollegare il cavo o di spegnere e riaccendere l'array.

Se lo storage array non riesce a ottenere gli indirizzi IP assegnati da DHCP entro 30 secondi, vengono impostati i seguenti indirizzi IP predefiniti:

- Controller A, porta 1: 169.254.128.101
- Controller B, porta 1: 169.254.128.102
- Subnet mask: 255.255.0.0

2. Individuare l'etichetta dell'indirizzo MAC sul retro di ciascun controller, quindi fornire all'amministratore di rete l'indirizzo MAC per la porta 1 di ciascun controller.

   L'amministratore di rete ha bisogno degli indirizzi MAC per determinare l'indirizzo IP di ciascun controller. Per connettersi al sistema di storage tramite il browser, sono necessari gli indirizzi IP.

Installare e configurare Linux Unified host Utilities

Gli strumenti delle utility host unificate di Linux consentono di gestire lo storage NetApp, incluse policy di failover e percorsi fisici.

Fasi

1. Utilizzare "Tool di matrice di interoperabilità NetApp" Per determinare la versione appropriata di Unified host Utilities da installare.

   Le versioni sono elencate in una colonna all'interno di ciascuna configurazione supportata.

2. Scaricare le Unified host Utilities da "Supporto NetApp".

> In alternativa, è possibile utilizzare l'utility SMdevices di SANtricity per eseguire le stesse funzioni dello strumento Unified host Utility. L'utility SMdevices è inclusa nel pacchetto SMutils. Il pacchetto SMutils è una raccolta di utility per verificare ciò che l'host vede dall'array di storage. È incluso nell'installazione del software SANtricity.

Installazione di SANtricity Storage Manager per SMcli (software SANtricity versione 11.53 o precedente)

Se si utilizza il software SANtricity versione 11.53 o precedente, è possibile installare il software Gestione archiviazione SANtricity sulla stazione di gestione per semplificare la gestione dell'array.

Gestione storage SANtricity include l'interfaccia a riga di comando (CLI) per ulteriori attività di gestione e l'agente di contesto host per l'invio delle informazioni di configurazione degli host ai controller degli array di storage attraverso il percorso i/O.

> Se si utilizza il software SANtricity 11.60 e versioni successive, non è necessario seguire questa procedura. La CLI sicura di SANtricity (SMcli) è inclusa nel sistema operativo SANtricity e può essere scaricata tramite Gestore di sistema di SANtricity. Per ulteriori informazioni su come scaricare SMcli tramite Gestione sistema di SANtricity, fare riferimento all'argomento *Download command line interface (CLI)* nella Guida in linea di Gestione sistema di SANtricity.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Software SANtricity 11.53 o precedente.
- Correggere i privilegi di amministratore o di superutente.
- Un sistema per il client di gestione dello storage SANtricity con i seguenti requisiti minimi:
  - **RAM**: 2 GB per Java Runtime Engine
  - **Spazio su disco**: 5 GB
  - **Sistema operativo/architettura**: Per informazioni su come determinare le versioni e le architetture dei sistemi operativi supportati, visitare il sito Web all'indirizzo "Supporto NetApp". Dalla scheda **Download**, andare al **Download › Gestione storage e-Series SANtricity**.

A proposito di questa attività

Questa attività descrive come installare SANtricity Storage Manager su entrambe le piattaforme, poiché sia Windows che Linux sono piattaforme comuni per le stazioni di gestione quando Linux viene utilizzato per l'host dati.

Fasi

1. Scaricare la versione del software SANtricity all'indirizzo "Supporto NetApp". Dalla scheda **Download**, andare al **Download › Gestione storage e-Series SANtricity**.
2. Eseguire il programma di installazione di SANtricity.

Windows	Linux
Fare doppio clic sul pacchetto di installazione SMIA*.exe per avviare l'installazione.	a. Accedere alla directory in cui si trova il pacchetto di installazione SMIA*.bin. b. Se il punto di montaggio temporaneo non dispone delle autorizzazioni di esecuzione, impostare `IATEMPDIR` variabile. Esempio: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Eseguire `chmod +x SMIA*.bin` per concedere l'autorizzazione di esecuzione al file. d. Eseguire `./SMIA*.bin` per avviare il programma di installazione.

3. Utilizzare l'installazione guidata per installare il software sulla stazione di gestione.

Accedere a Gestore di sistema di SANtricity e utilizzare l'installazione guidata

Per configurare lo storage array, è possibile utilizzare la procedura di installazione guidata in Gestore di sistema di SANtricity.

Gestore di sistema di SANtricity è un'interfaccia basata su web integrata in ogni controller. Per accedere all'interfaccia utente, puntare un browser verso l'indirizzo IP del controller. L'installazione guidata consente di iniziare a configurare il sistema.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Gestione fuori banda.
- Stazione di gestione per l'accesso a Gestore di sistema di SANtricity che include uno dei seguenti browser:

Browser	Versione minima
Google Chrome	89
Microsoft Edge	90
Mozilla Firefox	80
Safari	14

A proposito di questa attività

Gli utenti iSCSI hanno chiuso l'installazione guidata durante la configurazione di iSCSI.

La procedura guidata viene riavviata automaticamente quando si apre System Manager o si aggiorna il browser e viene soddisfatta almeno una delle seguenti condizioni:

- Non vengono rilevati pool e gruppi di volumi.
- Nessun carico di lavoro rilevato.
- Nessuna notifica configurata.

Fasi

1. Dal browser, immettere il seguente URL: `https://<DomainNameOrIPAddress>`

   `IPAddress` è l'indirizzo di uno dei controller degli array di storage.

   La prima volta che si apre Gestore di sistema di SANtricity su un array non configurato, viene visualizzato il prompt Set Administrator Password (Imposta password amministratore). La gestione degli accessi basata sui ruoli configura quattro ruoli locali: amministrazione, supporto, sicurezza e monitoraggio. Gli ultimi tre ruoli hanno password casuali che non possono essere indovinate. Dopo aver impostato una password per il ruolo di amministratore, è possibile modificare tutte le password utilizzando le credenziali di amministratore. Per ulteriori informazioni sui quattro ruoli utente locali, consultare la guida in linea disponibile nell'interfaccia utente di Gestore di sistema di SANtricity.

2. Immettere la password di System Manager per il ruolo di amministratore nei campi Set Administrator Password (Imposta password amministratore) e Confirm Password (Conferma password), quindi fare clic su **Set Password** (Imposta password).

   L'installazione guidata viene avviata se non sono configurati pool, gruppi di volumi, carichi di lavoro o notifiche.

3. Utilizzare l'installazione guidata per eseguire le seguenti operazioni:
   - **Verifica dell'hardware (controller e dischi)** — verifica del numero di controller e dischi nell'array di storage. Assegnare un nome all'array.
   - **Verifica di host e sistemi operativi** — verifica dei tipi di host e sistemi operativi a cui lo storage array può accedere.
   - **Accept Pools** — accettare la configurazione del pool consigliata per il metodo di installazione rapida. Un pool è un gruppo logico di dischi.
   - **Configura avvisi** — consente a System Manager di ricevere notifiche automatiche quando si verifica un problema con lo storage array.
   - **Enable AutoSupport** — monitora automaticamente lo stato dello storage array e invia le spedizioni al supporto tecnico.
4. Se non hai ancora creato un volume, creane uno dal **Storage › Volumes › Create › Volume**.

   Per ulteriori informazioni, consultare la guida in linea di Gestore di sistema di SANtricity.

Configurare il software multipath

Per fornire un percorso ridondante all'array di storage, è possibile configurare il software multipath.

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

- Per gli host Red Hat (RHEL), verificare che i pacchetti siano installati eseguendo `rpm -q device-mapper-multipath`.
- Per gli host SLES, verificare che i pacchetti siano installati eseguendo `rpm -q multipath-tools`.

Se il sistema operativo non è già stato installato, utilizzare i supporti forniti dal produttore del sistema operativo.

A proposito di questa attività

Il software multipath fornisce un percorso ridondante all'array di storage in caso di interruzione di uno dei percorsi fisici. Il software multipath presenta il sistema operativo con un singolo dispositivo virtuale che rappresenta i percorsi fisici attivi verso lo storage. Il software multipath gestisce anche il processo di failover che aggiorna il dispositivo virtuale.

Per le installazioni Linux si utilizza il tool DM-MP (Device mapper multipath). Per impostazione predefinita, DM-MP è disattivato in RHEL e SLES. Per abilitare i componenti DM-MP sull'host, attenersi alla seguente procedura.

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.

2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

```
# systemctl start multipathd
```

4. Salvare la versione del kernel eseguendo `uname -r` comando.

```
# uname -r
3.10.0-327.el7.x86_64
```

Queste informazioni verranno utilizzate quando si assegnano volumi all'host.

5. Attivare il `multipathd` daemon all'avvio.

```
systemctl enable multipathd
```

6. Ricostruire il `initramfs` o il `initrd` immagine nella directory /boot:

```
dracut --force --add multipath
```

7. Utilizzare "Creare l'host manualmente" procedura nella guida in linea per verificare se gli host sono definiti. Verificare che ogni impostazione del tipo di host sia basata sulle informazioni del kernel raccolte in fase 4.

> Il bilanciamento automatico del carico è disattivato per tutti i volumi mappati agli host che eseguono kernel 3.9 o versioni precedenti.

8. Riavviare l'host.

Impostare il file multipath.conf

Il file multipath.conf è il file di configurazione per il daemon multipath, multipath.

Il file multipath.conf sovrascrive la tabella di configurazione integrata per multipath.

> Per il sistema operativo SANtricity 8.30 e versioni successive, NetApp consiglia di utilizzare le impostazioni predefinite fornite.

Non sono richieste modifiche a /etc/multipath.conf.

Configurare gli switch

Gli switch vengono configurati in base alle raccomandazioni del vendor per iSCSI. Questi consigli possono includere sia direttive di configurazione che aggiornamenti del codice.

È necessario assicurarsi quanto segue:

- Sono disponibili due reti separate per l'alta disponibilità. Assicurarsi di isolare il traffico iSCSI per separare i segmenti di rete.
- È necessario attivare il controllo di flusso **da fine a fine**.
- Se appropriato, sono stati attivati i frame jumbo.

> Port channels/LACP non è supportato sulle porte switch del controller. LACP lato host non è consigliato; il multipathing offre gli stessi vantaggi e, in alcuni casi, benefici migliori.

Configurare il networking

È possibile configurare la rete iSCSI in diversi modi, a seconda dei requisiti di storage dei dati.

Rivolgersi all'amministratore di rete per suggerimenti sulla scelta della configurazione migliore per l'ambiente in uso.

Per configurare una rete iSCSI con ridondanza di base, collegare ciascuna porta host e una porta da ciascun controller a switch separati e partizionare ciascun set di porte host e porte controller su segmenti di rete o VLAN separati.

È necessario attivare il controllo di flusso hardware di invio e ricezione **end-to-end**. È necessario disattivare il controllo del flusso di priorità.

Se si utilizzano frame jumbo all'interno della SAN IP per motivi di performance, assicurarsi di configurare l'array, gli switch e gli host in modo che utilizzino frame jumbo. Consultare la documentazione del sistema operativo e dello switch per informazioni su come abilitare i frame jumbo sugli host e sugli switch. Per abilitare i frame jumbo sull'array, completare la procedura descritta in "Configurare il networking lato array".

> Molti switch di rete devono essere configurati con un numero superiore a 9,000 byte per l'overhead IP. Per ulteriori informazioni, consultare la documentazione dello switch.

Configurare il networking lato array

La GUI di Gestione di sistema di SANtricity consente di configurare il collegamento in rete iSCSI sul lato array.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- L'indirizzo IP o il nome di dominio di uno dei controller degli array di storage.
- Una password per la GUI di System Manager, RBAC (Role-Based Access Control) o LDAP e un servizio di directory configurato per l'accesso di sicurezza appropriato allo storage array. Per ulteriori informazioni sulla gestione degli accessi, consultare la guida in linea di Gestione di sistema SANtricity.

A proposito di questa attività

Questa attività descrive come accedere alla configurazione della porta iSCSI dalla pagina hardware di System Manager. È inoltre possibile accedere alla configurazione dal **sistema › Impostazioni › Configura porte iSCSI**.

Fasi

1. Dal browser, immettere il seguente URL: `https://<DomainNameOrIPAddress>`

   `IPAddress` è l'indirizzo di uno dei controller degli array di storage.

   La prima volta che si apre Gestore di sistema di SANtricity su un array non configurato, viene visualizzato il prompt Set Administrator Password (Imposta password amministratore). La gestione degli accessi basata sui ruoli configura quattro ruoli locali: amministrazione, supporto, sicurezza e monitoraggio. Gli ultimi tre ruoli hanno password casuali che non possono essere indovinate. Dopo aver impostato una password per il ruolo di amministratore, è possibile modificare tutte le password utilizzando le credenziali di amministratore. Per ulteriori informazioni sui quattro ruoli utente locali, consultare la guida in linea disponibile nell'interfaccia utente di Gestore di sistema di SANtricity.

2. Immettere la password di System Manager per il ruolo di amministratore nei campi Set Administrator Password (Imposta password amministratore) e Confirm Password (Conferma password), quindi fare clic su **Set Password** (Imposta password).

   L'installazione guidata viene avviata se non sono configurati pool, gruppi di volumi, carichi di lavoro o notifiche.

3. Chiudere l'installazione guidata.

   La procedura guidata verrà utilizzata in seguito per completare ulteriori attività di installazione.

4. Selezionare **hardware**.
5. Se la figura mostra i dischi, fare clic su **Mostra retro dello shelf**.

   Il grafico cambia per mostrare i controller invece dei dischi.

6. Fare clic sul controller con le porte iSCSI che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

7. Selezionare **Configure iSCSI ports** (Configura porte iSCSI).

   Viene visualizzata la finestra di dialogo Configure iSCSI Ports (Configura porte iSCSI).

8. Nell'elenco a discesa, selezionare la porta che si desidera configurare, quindi fare clic su **Avanti**.
9. Selezionare le impostazioni della porta di configurazione, quindi fare clic su **Avanti**.

   Per visualizzare tutte le impostazioni della porta, fare clic sul collegamento **Mostra altre impostazioni della porta** a destra della finestra di dialogo.

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità desiderata. Le opzioni visualizzate nell'elenco a discesa dipendono dalla velocità massima supportata dalla rete (ad esempio, 10 Gbps). Le schede di interfaccia host iSCSI da 25 GB opzionali disponibili sui controller non consentono la negoziazione automatica delle velocità. È necessario impostare la velocità di ciascuna porta su 10 GB o 25 GB. Tutte le porte devono essere impostate alla stessa velocità.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.
Porta TCP in ascolto (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

Se si seleziona **Enable IPv4** (attiva IPv4), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv4. Se si seleziona **Enable IPv6** (attiva IPv6*), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv6. Se sono state selezionate entrambe le opzioni, viene visualizzata prima la finestra di dialogo per le impostazioni IPv4, quindi dopo aver fatto clic su **Avanti**, viene visualizzata la finestra di dialogo per le impostazioni IPv6.

10. Configurare le impostazioni IPv4 e/o IPv6, automaticamente o manualmente. Per visualizzare tutte le impostazioni delle porte, fare clic sul collegamento **Mostra altre impostazioni** a destra della finestra di dialogo.

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router.

11. Fare clic su **fine**.
12. Chiudere System Manager.

Configurare la rete lato host

Per configurare la rete lato host, è necessario eseguire diversi passaggi.

A proposito di questa attività

È possibile configurare la rete iSCSI sul lato host impostando il numero di sessioni del nodo per percorso fisico, attivando i servizi iSCSI appropriati, configurando la rete per le porte iSCSI, creando associazioni faccie iSCSI e stabilendo le sessioni iSCSI tra iniziatori e destinazioni.

Nella maggior parte dei casi, è possibile utilizzare l'inbox software-initiator per iSCSI CNA/NIC. Non è necessario scaricare il driver, il firmware e il BIOS più recenti. Fare riferimento a. "Tool di matrice di interoperabilità NetApp" per determinare i requisiti del codice.

Fasi

1. Controllare `node.session.nr_sessions` variabile nel file /etc/iscsi/iscsid.conf per visualizzare il numero predefinito di sessioni per percorso fisico. Se necessario, modificare il numero predefinito di sessioni in una sessione.

```
node.session.nr_sessions = 1
```

2. Modificare il `node.session.timeo.replacement_timeout` variabile nel file /etc/iscsi/iscsid.conf in `20`, da un valore predefinito di `120`.

```
node.session.timeo.replacement_timeout = 20
```

3. In alternativa, è possibile impostare `node.startup = automatic` in /etc/iscsi/iscsid.conf prima di eseguire qualsiasi `iscsiadm` comandi per mantenere le sessioni dopo il riavvio.
4. Assicurarsi che `iscsid` e. `(open-)iscsi` i servizi sono attivati e abilitati per l'avvio.

```
# systemctl start iscsi
# systemctl start iscsid
# systemctl enable iscsi
# systemctl enable iscsid
```

5. Ottenere il nome dell'iniziatore IQN host, che verrà utilizzato per configurare l'host in un array.

```
# cat /etc/iscsi/initiatorname.iscsi
```

6. Configurare la rete per le porte iSCSI. Queste sono istruzioni di esempio per RHEL e SLES:

> Oltre alla porta di rete pubblica, gli iniziatori iSCSI devono utilizzare due o più NIC su segmenti privati o VLAN separati.

a. Determinare i nomi delle porte iSCSI utilizzando `ifconfig -a` comando.

b. Impostare l'indirizzo IP per le porte iSCSI Initiator. Le porte dell'iniziatore devono essere presenti sulla stessa sottorete delle porte di destinazione iSCSI.

Red Hat Enterprise Linux 7 e 8 (RHEL 7 e RHEL 8)

Creare il file di esempio `/etc/sysconfig/network-scripts/ifcfg-<NIC port>` con i seguenti contenuti.

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=<NIC port>
UUID=<unique UUID>
DEVICE=<NIC port>
ONBOOT=yes
IPADDR=192.168.xxx.xxx
PREFIX=24
NETMASK=255.255.255.0
NM_CONTROLLED=no
MTU=
```

Aggiunte opzionali per IPv6:

```
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=fdxx::192:168:xxxx:xxxx/32
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=eui64
```

Red Hat Enterprise Linux 9 (RHEL 9)

Utilizzare `nmtui` per attivare e modificare una connessione. Lo strumento genera un `<NIC port>.nmconnection` file all'interno di `/etc/NetworkManager/system-connections/`.

SUSE Linux Enterprise Server 12 e 15 (SLES 12 e SLES 15)

Creare il file di esempio `/etc/sysconfig/network/ifcfg-<NIC port>` con i seguenti contenuti.

```
IPADDR='192.168.xxx.xxx/24'
BOOTPROTO='static'
STARTMODE='auto'
```

Aggiunta opzionale per IPv6:

```
IPADDR_0='fdxx::192:168:xxxx:xxxx/32'
```

+

> Assicurarsi di impostare l'indirizzo per entrambe le porte iSCSI Initiator.

a. Riavviare i servizi di rete.

```
# systemctl restart network
```

b. Assicurarsi che il server Linux sia in grado di eseguire il ping di tutte le porte di destinazione iSCSI.

7. Stabilire le sessioni iSCSI tra iniziatori e destinazioni (quattro in totale) in base a uno dei due metodi.

a. (Facoltativo) quando si utilizza l'interfaccia ifaces, configurare le interfacce iSCSI creando due associazioni iface iSCSI.

```
# iscsiadm -m iface -I iface0 -o new
# iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v
<NIC port1>
```

```
# iscsiadm -m iface -I iface1 -o new
# iscsiadm -m iface -I iface1 -o update -n iface.net_ifacename -v
<NIC port2>
```

Per elencare le interfacce, utilizzare `iscsiadm -m iface`.

b. Individuare le destinazioni iSCSI. Salvare l'IQN (che sarà lo stesso per ogni rilevamento) nel foglio di lavoro per il passaggio successivo.

Metodo 1 (con ifache)

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port> -I iface0
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I iface0
```

Metodo 2 (senza ifache)

```
# iscsiadm -m discovery -t sendtargets -p
<target_ip_address>:<target_tcp_listening_port>
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260
```

L'IQN è simile al seguente:

```
iqn.1992-01.com.netapp:2365.60080e50001bf1600000000531d7be3
```

c. Creare la connessione tra gli iniziatori iSCSI e le destinazioni iSCSI.

Metodo 1 (con ifache)

```
# iscsiadm -m node -T <target_iqn> -p
<target_ip_address>:<target_tcp_listening_port> -I iface0 -l
# iscsiadm -m node -T iqn.1992-
01.com.netapp:2365.60080e50001bf1600000000531d7be3 -p
192.168.0.1:3260 -I iface0 -l
```

Metodo 2 (senza ifache)

```
# iscsiadm -m node -L all
```

a. Elencare le sessioni iSCSI stabilite sull'host.

```
# iscsiadm -m session
```

Verificare le connessioni di rete IP

Verificare le connessioni di rete IP (Internet Protocol) utilizzando i test ping per assicurarsi che host e array siano in grado di comunicare.

Fasi

1. Sull'host, eseguire uno dei seguenti comandi, a seconda che i frame jumbo siano abilitati:

   - Se i frame jumbo non sono abilitati, eseguire questo comando:

     ```
     ping -I <hostIP\> <targetIP\>
     ```

   - Se i frame jumbo sono abilitati, eseguire il comando ping con una dimensione del payload di 8,972 byte. Le intestazioni combinate IP e ICMP sono di 28 byte, che quando vengono aggiunte al payload equivale a 9,000 byte. L'interruttore -s imposta il `packet size` bit. Lo switch -d imposta l'opzione di debug. Queste opzioni consentono di trasmettere correttamente frame jumbo di 9,000 byte tra l'iniziatore iSCSI e la destinazione.

     ```
     ping -I <hostIP\> -s 8972 -d <targetIP\>
     ```

     In questo esempio, l'indirizzo IP di destinazione iSCSI è `192.0.2.8`.

```
#ping -I 192.0.2.100 -s 8972 -d 192.0.2.8
Pinging 192.0.2.8 with 8972 bytes of data:
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
Ping statistics for 192.0.2.8:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Problema A. `ping` Comando da ciascun indirizzo di iniziatore dell'host (l'indirizzo IP della porta Ethernet dell'host utilizzata per iSCSI) a ciascuna porta iSCSI del controller. Eseguire questa azione da ciascun server host nella configurazione, modificando gli indirizzi IP in base alle necessità.

   Se il comando non riesce (ad esempio, restituisce `Packet needs to be fragmented but DF set`), verificare le dimensioni MTU (supporto frame jumbo) per le interfacce Ethernet sul server host, sul controller storage e sulle porte dello switch.

Creare partizioni e filesystem

Poiché un nuovo LUN non dispone di partizione o file system quando l'host Linux lo rileva per la prima volta, è necessario formattare il LUN prima di poterlo utilizzare. In alternativa, è possibile creare un file system sul LUN.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un LUN rilevato dall'host.
- Un elenco dei dischi disponibili. (Per visualizzare i dischi disponibili, eseguire `ls` nella cartella /dev/mapper.)

A proposito di questa attività

È possibile inizializzare il disco come disco di base con una tabella di partizione GUID (GPT) o un record di boot master (MBR).

Formattare il LUN con un file system come ext4. Alcune applicazioni non richiedono questo passaggio.

Fasi

1. Recuperare l'ID SCSI del disco mappato emettendo `sanlun lun show -p` comando.

   L'ID SCSI è una stringa di 33 caratteri composta da cifre esadecimali, che iniziano con il numero 3. Se sono attivati nomi intuitivi, Device Mapper riporta i dischi come mpath invece che come ID SCSI.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
               Preferred Owner: Controller in Slot B
                 Current Owner: Controller in Slot B
                          Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
              Multipath Policy: round-robin 0
            Multipath Provider: Native
--------- ---------- ------- ------------
-----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
-----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Creare una nuova partizione secondo il metodo appropriato per la release del sistema operativo Linux.

   In genere, i caratteri che identificano la partizione di un disco vengono aggiunti all'ID SCSI (ad esempio, il numero 1 o p3).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Creare un file system sulla partizione.

   Il metodo per creare un file system varia a seconda del file system scelto.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Creare una cartella per montare la nuova partizione.

```
# mkdir /mnt/ext4
```

5. Montare la partizione.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verificare l’accesso allo storage sull’host

Prima di utilizzare il volume, verificare che l’host sia in grado di scrivere i dati nel volume e di leggerli nuovamente.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

1. Sull’host, copiare uno o più file nel punto di montaggio del disco.
2. Copiare di nuovo i file in un’altra cartella sul disco originale.
3. Eseguire `diff` per confrontare i file copiati con gli originali.

Al termine

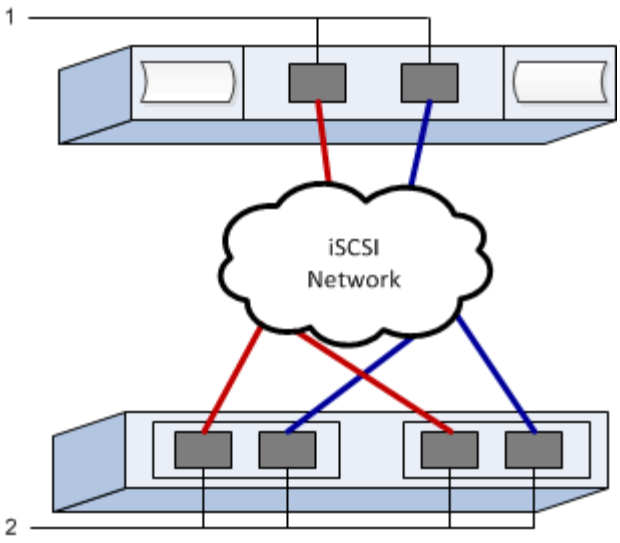
Rimuovere il file e la cartella copiati.

Registrare la configurazione iSCSI

È possibile generare e stampare un PDF di questa pagina, quindi utilizzare il seguente foglio di lavoro per registrare le informazioni di configurazione dello storage iSCSI. Queste informazioni sono necessarie per eseguire le attività di provisioning.

Configurazione consigliata

Le configurazioni consigliate sono costituite da due porte iniziatore e quattro porte di destinazione con una o più VLAN.



IQN di destinazione

N. didascalia	Connessione alla porta di destinazione	IQN
2	Porta di destinazione	

Nome host di mapping

N. didascalia	Informazioni sull'host	Nome e tipo
1	Nome host di mapping	
	Tipo di sistema operativo host	

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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