Gestione dei servizi iSCSI

ONTAP 9

NetApp
April 24, 2024

Sommario

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

A partire da ONTAP 9.1, i comandi di sicurezza iSCSI esistenti sono stati migliorati per 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
```

Che cos'è l'autenticazione CHAP

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.

Linee guida per l'utilizzo dell'autenticazione CHAP

Quando si utilizza l'autenticazione CHAP, seguire alcune linee guida.

- 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.

  Non è consentito un nome utente nullo.

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

  Le password possono essere valori esadecimali o stringhe. Per i valori esadecimali, inserire il valore con il prefisso "0x" o "0X". Non è consentita una password nulla.

> 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)

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.

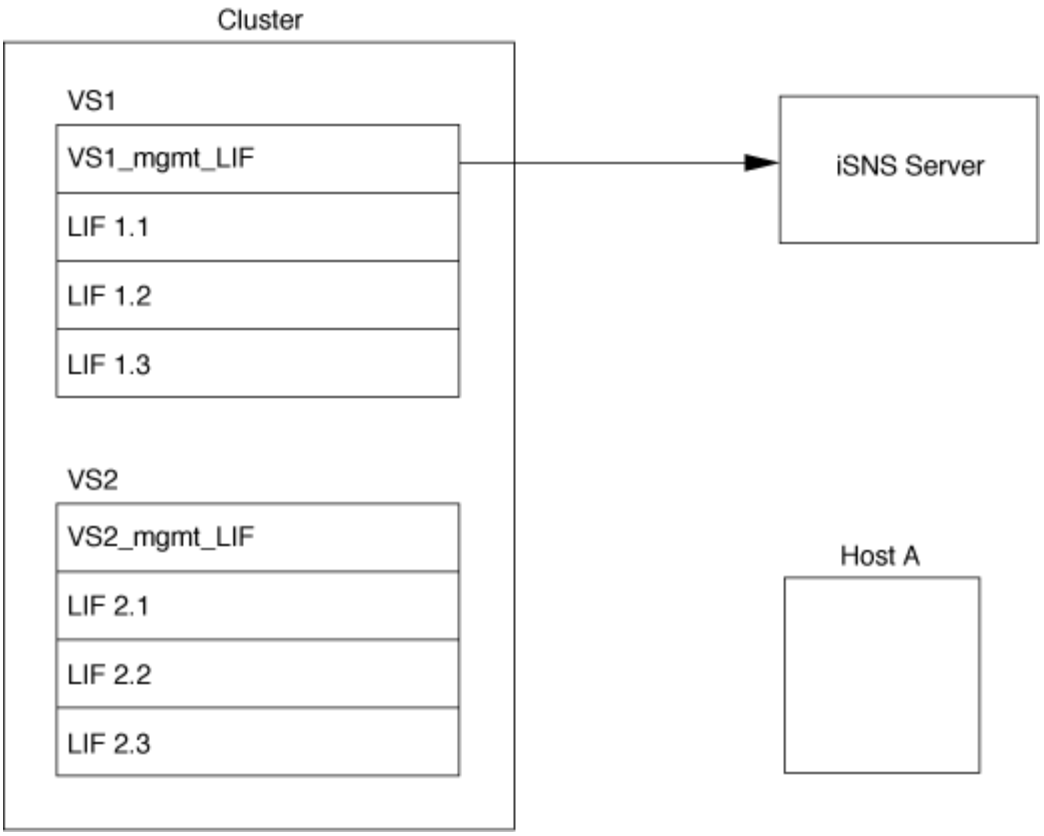
Il protocollo iSNS consente il rilevamento e la gestione automatizzati dei dispositivi iSCSI su una rete di storage IP. Un iniziatore iSCSI può eseguire query sul server iSNS per rilevare i dispositivi di destinazione iSCSI.

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

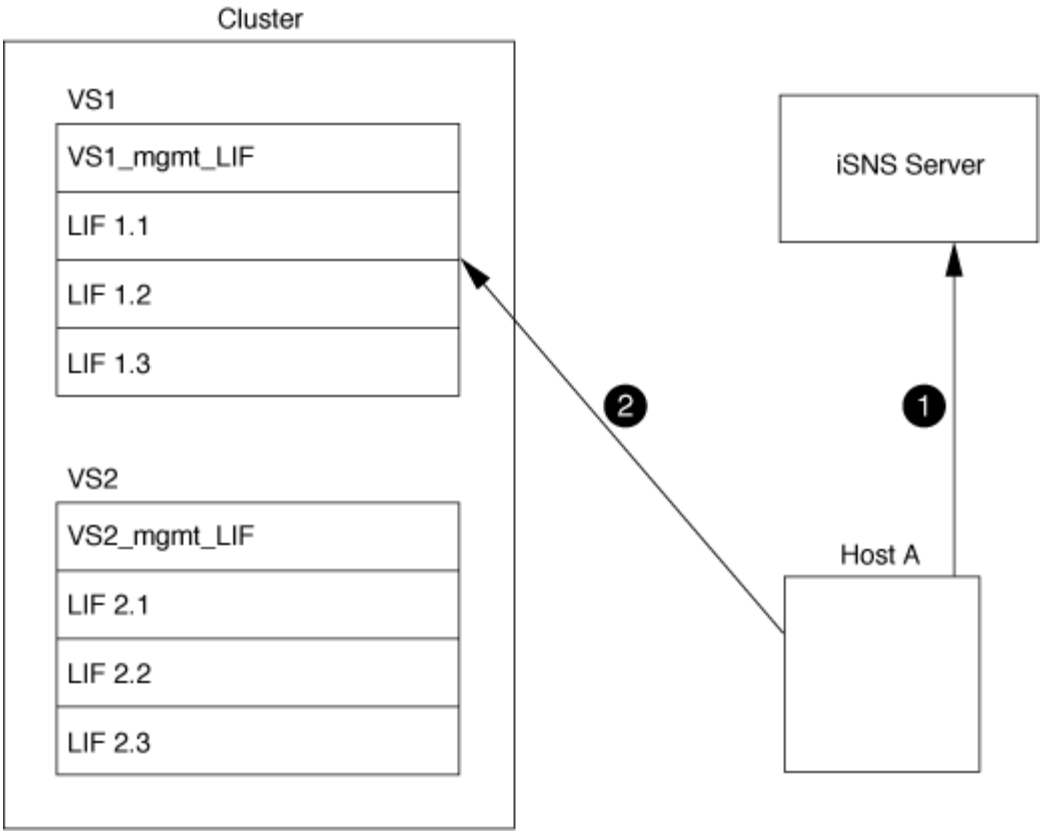
Come le SVM interagiscono con un server iSNS

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`

Comandi per la gestione di iSNS

ONTAP fornisce comandi per gestire il servizio iSNS.

Se si desidera…	Utilizzare questo comando…
Configurare un servizio iSNS	`vserver iscsi isns create`
Avviare un servizio iSNS	`vserver iscsi isns start`
Modificare un servizio iSNS	`vserver iscsi isns modify`
Visualizzare la configurazione del servizio iSNS	`vserver iscsi isns show`
Forzare un aggiornamento delle informazioni iSNS registrate	`vserver iscsi isns update`

Arrestare un servizio iSNS	`vserver iscsi isns stop`
Rimuovere un servizio iSNS	`vserver iscsi isns delete`
Visualizzare la pagina man per un comando	`man` *`command name`*

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.