Utilizzare le soluzioni SANtricity

E-Series Systems

NetApp
March 22, 2024

This PDF was generated from https://docs.netapp.com/it-it/e-series/web-services-proxy/index.html on March 22, 2024. Always check docs.netapp.com for the latest.

Sommario

Utilizzare le soluzioni SANtricity

Proxy dei servizi Web

Panoramica dei proxy dei servizi web SANtricity

Il proxy dei servizi web SANtricity è un server API RESTful installato separatamente su un sistema host per gestire centinaia di sistemi storage NetApp e-Series nuovi e legacy. Il proxy include Gestore unificato di SANtricity, un'interfaccia basata su web che offre funzioni simili.

Panoramica dell'installazione

L'installazione e la configurazione di Web Services Proxy richiede i seguenti passaggi:

1. "Verifica dei requisiti di installazione e aggiornamento".
2. "Scaricare e installare il file proxy dei servizi Web".
3. "Accedere a API e Unified Manager".
4. "Configurare il proxy dei servizi Web".

Trova ulteriori informazioni

- Unified Manager — l'installazione del proxy include SANtricity Unified Manager, un'interfaccia basata su web che fornisce l'accesso alla configurazione ai più recenti sistemi storage e-Series ed EF-Series. Per ulteriori informazioni, consultare la guida in linea di Unified Manager, disponibile dalla relativa interfaccia utente o dal "Sito della documentazione del software SANtricity".
- Repository di GitHub — GitHub contiene un repository per la raccolta e l'organizzazione di script di esempio che illustrano l'utilizzo dell'API dei servizi web di NetApp SANtricity. Per accedere al repository, vedere "Esempi di NetApp WebServices".
- Representational state transfer (REST) — i servizi web sono un'API RESTful che fornisce l'accesso praticamente a tutte le funzionalità di gestione di SANtricity, in modo da avere familiarità con i concetti REST. Per ulteriori informazioni, vedere "Stili architettonici e progettazione di architetture software basate su rete".
- JavaScript Object Notation (JSON) — poiché i dati all'interno dei servizi Web sono codificati tramite JSON, dovresti avere familiarità con i concetti di programmazione JSON. Per ulteriori informazioni, vedere "Presentazione di JSON".

Scopri di più sui servizi Web

Panoramica dei servizi Web e di Unified Manager

Prima di installare e configurare il proxy dei servizi Web, leggere la panoramica dei servizi Web e di Gestione unificata di SANtricity.

Servizi Web

Web Services è un'API (Application Programming Interface) che consente di configurare, gestire e monitorare i sistemi storage NetApp e-Series ed EF-Series. Inviando richieste API, è possibile completare flussi di lavoro

come configurazione, provisioning e monitoraggio delle performance per i sistemi storage e-Series.

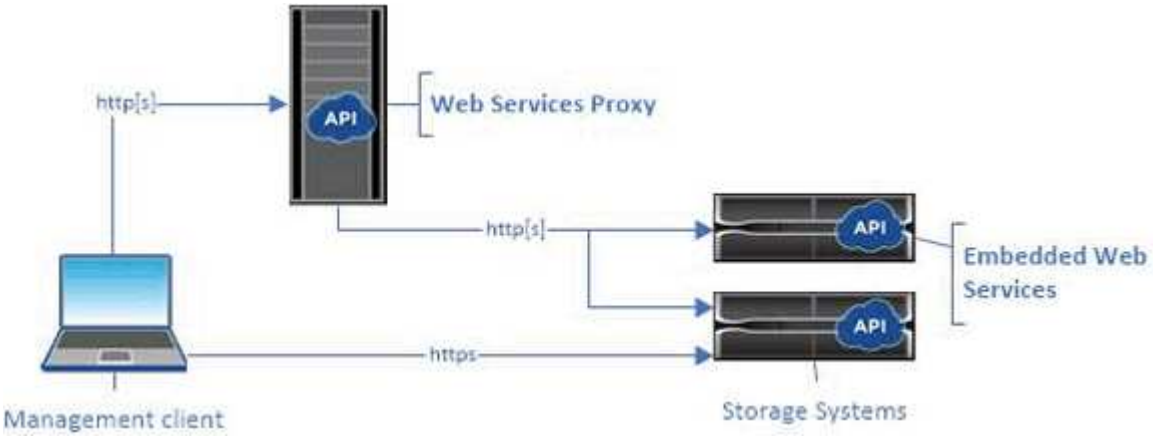
Quando si utilizza l'API dei servizi Web per gestire i sistemi storage, è necessario avere familiarità con quanto segue:

- JavaScript Object Notation (JSON): Poiché i dati all'interno dei servizi Web vengono codificati tramite JSON, è necessario conoscere i concetti di programmazione JSON. Per ulteriori informazioni, vedere "Presentazione di JSON".
- Representational state transfer (REST): I servizi Web sono un'API RESTful che fornisce accesso a quasi tutte le funzionalità di gestione di SANtricity, per cui dovresti avere familiarità con i concetti REST. Per ulteriori informazioni, vedere "Stili architettonici e progettazione di architetture software basate su rete".
- Concetti relativi ai linguaggi di programmazione: Java e Python sono i linguaggi di programmazione più comuni utilizzati con l'API dei servizi Web, ma qualsiasi linguaggio di programmazione in grado di effettuare richieste HTTP è sufficiente per l'interazione con l'API.

I servizi Web sono disponibili in due implementazioni:

- **Incorporato** — Un server API RESTful è incorporato in ciascun controller di un sistema storage E2800/EF280 con NetApp SANtricity 11.30 o versioni successive, E5700/EF570 con SANtricity 11.40 o versioni successive e EF300 o EF600 con SANtricity 11.60 o versioni successive. Non è richiesta alcuna installazione.
- **Proxy** — il proxy dei servizi web SANtricity è un server API RESTful installato separatamente su un server Windows o Linux. Questa applicazione basata su host è in grado di gestire centinaia di sistemi storage NetApp e-Series nuovi e legacy. In generale, è necessario utilizzare il proxy per le reti con più di 10 sistemi di storage. Il proxy è in grado di gestire numerose richieste in modo più efficiente rispetto all'API incorporata.

Il nucleo dell'API è disponibile in entrambe le implementazioni.



La seguente tabella fornisce un confronto tra il proxy e la versione integrata.

Considerazione	Proxy	Integrato
Installazione	Richiede un sistema host (Linux o Windows). Il proxy è disponibile per il download all'indirizzo "Sito di supporto NetApp" o su "DockerHub".	Non è richiesta alcuna installazione o abilitazione.

Considerazione	Proxy	Integrato
Sicurezza	Impostazioni di sicurezza minime per impostazione predefinita. Le impostazioni di sicurezza sono basse, in modo che gli sviluppatori possano iniziare a utilizzare l'API in modo rapido e semplice. Se lo si desidera, è possibile configurare il proxy con lo stesso profilo di protezione della versione integrata.	Impostazioni di protezione elevate per impostazione predefinita. Le impostazioni di sicurezza sono elevate perché l'API viene eseguita direttamente sui controller. Ad esempio, non consente l'accesso HTTP e disattiva tutti i protocolli di crittografia SSL e TLS precedenti per HTTPS.
Gestione centrale	Gestisce tutti i sistemi storage da un unico server.	Gestisce solo il controller su cui è incorporato.

Unified Manager

Il pacchetto di installazione del proxy include Unified Manager, un'interfaccia basata su web che fornisce l'accesso alla configurazione ai più recenti sistemi storage e-Series ed EF-Series, come E2800, E5700, EF300 ed EF600.

Da Unified Manager, è possibile eseguire le seguenti operazioni batch:

- Visualizzare lo stato di più sistemi storage da una vista centrale
- Scopri più sistemi storage nella tua rete
- Importa le impostazioni da un sistema storage a più sistemi
- Aggiornare il firmware per più sistemi storage

Compatibilità e limitazioni

L'utilizzo del proxy dei servizi Web è soggetto alle seguenti limitazioni e compatibilità.

Considerazione	Compatibilità o restrizione
Supporto HTTP	Il proxy dei servizi Web consente l'utilizzo di HTTP o HTTPS. (La versione integrata dei servizi Web richiede HTTPS per motivi di sicurezza).
Sistemi storage e firmware	Il proxy dei servizi Web è in grado di gestire tutti i sistemi storage e-Series, tra cui una combinazione di sistemi meno recenti e gli ultimi E2800, EF280, E5700, EF570, EF300, E sistemi della serie EF600.

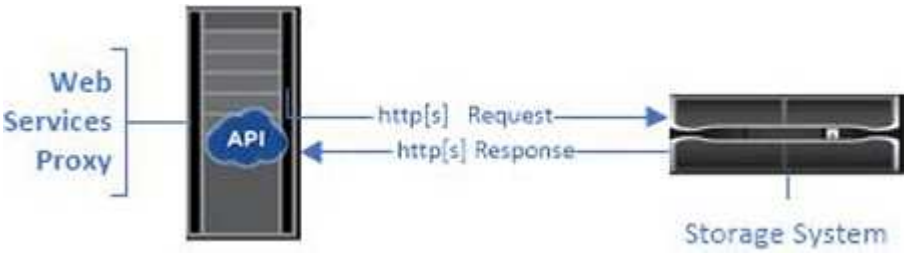
Considerazione	Compatibilità o restrizione
Supporto IP	Il proxy dei servizi Web supporta il protocollo IPv4 o IPv6. Il protocollo IPv6 potrebbe non funzionare quando il proxy dei servizi Web tenta di rilevare automaticamente l'indirizzo di gestione dalla configurazione del controller. Le possibili cause dell'errore includono problemi durante l'inoltro dell'indirizzo IP o l'attivazione di IPv6 sui sistemi storage ma non sul server.
NVSRAM file name limits	Il proxy dei servizi Web utilizza i nomi dei file NVSRAM per identificare accuratamente le informazioni sulla versione. Pertanto, non è possibile modificare I nomi dei file NVSRAM quando vengono utilizzati con il proxy dei servizi Web. Il proxy dei servizi Web potrebbe non riconoscere un file NVSRAM rinominato come file firmware valido.
Web di Symbol	Symbol Web è un URL nell'API REST. Consente di accedere a quasi tutte le chiamate Symbol. La funzione Symbol fa parte del seguente URL: `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` I sistemi storage disabilitati da Symbol sono supportati tramite il proxy dei servizi Web.

Nozioni di base sulle API

Nell'API dei servizi Web, le comunicazioni HTTP implicano un ciclo di richiesta-risposta.

Elementi URL nelle richieste

Indipendentemente dal linguaggio di programmazione o dallo strumento utilizzato, ogni chiamata all'API dei servizi Web ha una struttura simile, con un URL, un verbo HTTP e un'intestazione Accept.



Tutte le richieste includono un URL, come nell'esempio seguente, e contengono gli elementi descritti nella tabella.

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

Area	Descrizione
Trasporto HTTP `https://`	Il proxy dei servizi Web attiva l'utilizzo di HTTP o HTTPS. I servizi Web incorporati richiedono HTTPS per motivi di sicurezza.
URL di base e porta `webservices.name.com:8443`	Ogni richiesta deve essere instradata correttamente a un'istanza attiva dei servizi Web. È richiesto l'FQDN (Fully Qualified Domain Name) o l'indirizzo IP dell'istanza, insieme alla porta di ascolto. Per impostazione predefinita, i servizi Web comunicano tramite la porta 8080 (per HTTP) e la porta 8443 (per HTTPS). Per il proxy dei servizi Web, è possibile modificare entrambe le porte durante l'installazione del proxy o nel file wsconfig.xml. Il conflitto di porte è comune negli host del data center che eseguono varie applicazioni di gestione. Per i servizi Web incorporati, la porta sul controller non può essere modificata; per impostazione predefinita, la porta 8443 consente connessioni sicure.
Percorso API `devmgr/v2/storage-systems`	Viene inviata una richiesta a una risorsa REST o a un endpoint specifico all'interno dell'API dei servizi Web. La maggior parte degli endpoint è sotto forma di: `devmgr/v2/<resource>/[id]` Il percorso API è costituito da tre parti: • `devmgr` (Device Manager) è lo spazio dei nomi dell'API dei servizi Web. • `v2` Indica la versione dell'API a cui si accede. È anche possibile utilizzare `utils` per accedere agli endpoint di login. • `storage-systems` è una categoria all'interno della documentazione.

Verbi HTTP supportati

I verbi HTTP supportati includono GET, POST ed DELETE:

- Le richieste GET vengono utilizzate per le richieste di sola lettura.
- Le richieste POST vengono utilizzate per creare e aggiornare oggetti e anche per le richieste di lettura che potrebbero avere implicazioni sulla sicurezza.
- Le richieste DI ELIMINAZIONE vengono in genere utilizzate per rimuovere un oggetto dalla gestione, rimuovere completamente un oggetto o ripristinare lo stato dell'oggetto.

> Attualmente, l'API dei servizi Web non supporta PUT o PATCH. È invece possibile utilizzare POST per fornire le funzionalità tipiche di questi verbi.

Accettare le intestazioni

Quando si restituisce un corpo della richiesta, i servizi Web restituiscono i dati in formato JSON (se non diversamente specificato). Alcuni client richiedono per impostazione predefinita "text/html" o qualcosa di simile. In questi casi, l'API risponde con un codice HTTP 406, che indica che non è in grado di fornire dati in questo formato. Come Best practice, devi definire l'intestazione Accept come "application/json" per tutti i casi in cui ti aspetti che JSON sia il tipo di risposta. In altri casi in cui un corpo di risposta non viene restituito (ad esempio, DELETE), la fornitura dell'intestazione Accept non causa effetti indesiderati.

Risposte

Quando viene effettuata una richiesta all'API, una risposta restituisce due informazioni critiche:

- Codice di stato HTTP — indica se la richiesta ha avuto esito positivo.
- Corpo di risposta opzionale - di solito fornisce un corpo JSON che rappresenta lo stato della risorsa o di un corpo fornendo maggiori dettagli sulla natura di un guasto.

È necessario controllare il codice di stato e l'intestazione del tipo di contenuto per determinare l'aspetto del corpo della risposta risultante. Per i codici di stato HTTP 200-203 e 422, Web Services restituisce un corpo JSON con la risposta. Per altri codici di stato HTTP, i servizi Web generalmente non restituiscono un corpo JSON aggiuntivo, perché la specifica non lo consente (204) o perché lo stato è intuitivo. La tabella elenca i codici e le definizioni di stato HTTP comuni. Indica inoltre se le informazioni associate a ciascun codice HTTP vengono restituite in un corpo JSON.

Codice di stato HTTP	Descrizione	Corpo JSON
200 OK	Indica una risposta corretta.	Sì
201 creato	Indica che è stato creato un oggetto. Questo codice viene utilizzato in alcuni rari casi invece dello stato 200.	Sì
202 accettato	Indica che la richiesta è accettata per l'elaborazione come richiesta asincrona, ma è necessario effettuare una richiesta successiva per ottenere il risultato effettivo.	Sì

Codice di stato HTTP	Descrizione	Corpo JSON
203 informazioni non autorevoli	Simile a una risposta 200, ma i servizi Web non possono garantire che i dati siano aggiornati (ad esempio, al momento sono disponibili solo i dati memorizzati nella cache).	Sì
204 Nessun contenuto	Indica un'operazione riuscita, ma non esiste alcun corpo di risposta.	No
400 richiesta errata	Indica che il corpo JSON fornito nella richiesta non è valido.	No
401 non autorizzato	Indica che si è verificato un errore di autenticazione. Non sono state fornite credenziali oppure il nome utente o la password non sono validi.	No
403 proibita	Errore di autorizzazione, che indica che l'utente autenticato non dispone dell'autorizzazione per accedere all'endpoint richiesto.	No
404 non trovato	Indica che non è stato possibile individuare la risorsa richiesta. Questo codice è valido per API inesistenti o risorse inesistenti richieste dall'identificatore.	No
422 entità non elaborabile	Indica che la richiesta è generalmente ben formata, ma i parametri di input non sono validi oppure lo stato del sistema di storage non consente ai servizi Web di soddisfare la richiesta.	Sì
424 dipendenza non riuscita	Utilizzato in Web Services Proxy per indicare che il sistema di storage richiesto non è attualmente accessibile. Pertanto, i servizi Web non possono soddisfare la richiesta.	No
429 troppe richieste	Indica che è stato superato un limite di richiesta e che è necessario eseguire un nuovo processo in un secondo momento.	No

Script di esempio

GitHub contiene un repository per la raccolta e l'organizzazione di script di esempio che illustrano l'utilizzo dell'API dei servizi web NetApp SANtricity. Per accedere al repository, vedere "Esempi di NetApp WebServices".

Termini e concetti

I seguenti termini si applicano al proxy dei servizi Web.

Termine	Definizione
API	Un'API (Application Programming Interface) è un insieme di protocolli e metodi che consentono agli sviluppatori di comunicare con i dispositivi. L'API dei servizi Web viene utilizzata per comunicare con i sistemi storage e-Series.
ASUP	La funzione ASUP (AutoSupport) raccoglie i dati in un bundle di assistenza clienti e invia automaticamente il file di messaggio al supporto tecnico per la risoluzione dei problemi e l'analisi dei problemi in remoto.
Endpoint	Gli endpoint sono funzioni disponibili attraverso l'API. Un endpoint include un verbo HTTP e il percorso URI. Nei servizi Web, gli endpoint possono eseguire attività come il rilevamento di sistemi storage e la creazione di volumi.
Verbo HTTP	Un verbo HTTP è un'azione corrispondente per un endpoint, ad esempio il recupero e la creazione di dati. Nei servizi Web, i verbi HTTP includono POST, GET ed DELETE.
JSON	JavaScript Object Notation (JSON) è un formato di dati strutturato molto simile a XML, che utilizza un formato minimo e leggibile. I dati all'interno dei servizi Web vengono codificati tramite JSON.

Termine	Definizione
RIPOSO/riposo	REST (Representational state Transfer) è una specifica separata che definisce uno stile architettonico per un'API. Poiché la maggior parte delle API REST non rispetta completamente la specifica, vengono descritte come "reSTful" o "reST-like". In genere, un'API "reSTful" è indipendente dai linguaggi di programmazione e presenta le seguenti caratteristiche: • Basato su HTTP, che segue la semantica generale del protocollo • Produttore e consumatore di dati strutturati (JSON, XML, ecc.) • Orientato a oggetti (invece che orientato alle operazioni) I servizi Web sono un'API RESTful che fornisce l'accesso a quasi tutte le funzionalità di gestione di SANtricity.
sistema storage	Un sistema storage è un array e-Series, che include shelf, controller, dischi, software, e firmware.
API di Symbol	Symbol è un'API legacy per la gestione dei sistemi storage e-Series. L'implementazione sottostante dell'API dei servizi Web utilizza Symbol.
Servizi Web	I servizi Web sono API progettate da NetApp per consentire agli sviluppatori di gestire i sistemi storage e-Series. Esistono due implementazioni dei servizi Web: Incorporato nel controller e un proxy separato che può essere installato su Linux o Windows.

Installare e configurare

Verifica dei requisiti di installazione e aggiornamento

Prima di installare Web Services Proxy, esaminare i requisiti di installazione e le considerazioni sull'aggiornamento.

Requisiti di installazione

È possibile installare e configurare il proxy dei servizi Web su un sistema host Windows o Linux.

L'installazione del proxy include i seguenti requisiti.

Requisito	Descrizione
Limitazioni del nome host	Assicurarsi che il nome host del server in cui si desidera installare il proxy dei servizi Web contenga solo lettere ASCII, cifre numeriche e trattini (-). Questo requisito è dovuto a un limite di Java Keytool, utilizzato per generare un certificato autofirmato per il server. Se il nome host del server contiene altri caratteri, ad esempio un carattere di sottolineatura (_), il server Web non verrà avviato dopo l'installazione.
Sistemi operativi	È possibile installare il proxy sui seguenti sistemi operativi: • Linux • Windows Per un elenco completo dei sistemi operativi e della compatibilità del firmware, consultare "Tool di matrice di interoperabilità NetApp".
Linux: Considerazioni aggiuntive	Le librerie di base standard Linux (init-functions) sono necessarie per il corretto funzionamento del server Web. È necessario installare i pacchetti lsb/insserv per il sistema operativo in uso. Per ulteriori informazioni, consultare la sezione "pacchetti aggiuntivi richiesti" del file Readme.
Istanze multiple	È possibile installare solo un'istanza di Web Services Proxy su un server; tuttavia, è possibile installare il proxy su più server all'interno della rete.
Pianificazione della capacità	Il proxy dei servizi Web richiede uno spazio adeguato per la registrazione. Assicurarsi che il sistema soddisfi i seguenti requisiti di spazio disponibile su disco: • Spazio di installazione richiesto — 275 MB • Spazio minimo di registrazione — 200 MB • Memoria di sistema — 2 GB; lo spazio di heap è di 1 GB per impostazione predefinita È possibile utilizzare uno strumento di monitoraggio dello spazio su disco per verificare lo spazio disponibile su disco per lo storage persistente e la registrazione.
Licenza	Web Services Proxy è un prodotto standalone gratuito che non richiede una chiave di licenza. Tuttavia, si applicano i copyright e i termini del servizio applicabili. Se si installa il proxy in modalità grafica o console, è necessario accettare il Contratto di licenza con l'utente finale (EULA).

Considerazioni sull'upgrade

Se si esegue l'aggiornamento da una versione precedente, tenere presente che alcuni elementi vengono

conservati o rimossi.

- Per il proxy dei servizi Web, le impostazioni di configurazione precedenti vengono conservate. Queste impostazioni includono password utente, tutti i sistemi di storage rilevati, certificati server, certificati attendibili e configurazione del runtime del server.
- Per Unified Manager, tutti i file SANtricity OS precedentemente caricati nel repository vengono rimossi durante l'aggiornamento.

Installare o aggiornare il file proxy dei servizi Web

L'installazione comporta il download del file e l'installazione del pacchetto proxy su un server Linux o Windows. È inoltre possibile aggiornare il proxy seguendo queste istruzioni.

Scaricare i file proxy dei servizi Web

È possibile scaricare il file di installazione e il file Leggimi dalla pagina di download del software del sito del supporto NetApp.

Il pacchetto di download include Web Services Proxy e l'interfaccia di Unified Manager.

Fasi

1. Passare a. "Supporto NetApp - Download".
2. Selezionare **Proxy servizi web e-Series SANtricity**.
3. Seguire le istruzioni per scaricare il file. Assicurarsi di selezionare il pacchetto di download corretto per il server (ad esempio, EXE per Windows; BIN o RPM per Linux).
4. Scaricare il file di installazione sul server in cui si desidera installare il proxy e Unified Manager.

Installazione su server Windows o Linux

È possibile installare Web Services Proxy e Unified Manager utilizzando una delle tre modalità (grafica, console o silenzioso) oppure utilizzando un file RPM (solo Linux).

Prima di iniziare

- "Esaminare i requisiti di installazione".
- Assicurarsi di aver scaricato il file di installazione corretto (EXE per Windows; BIN per Linux) sul server in cui si desidera installare il proxy e Unified Manager.

Installazione in modalità grafica

È possibile eseguire l'installazione in modalità grafica per Windows o Linux. In modalità grafica, i prompt vengono visualizzati in un'interfaccia di tipo Windows.

Fasi

1. Accedere alla cartella in cui è stato scaricato il file di installazione.
2. Avviare l'installazione per Windows o Linux, come indicato di seguito:
    - Windows — fare doppio clic sul file di installazione:

      ```
      santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe
      ```

- Linux — eseguire il seguente comando: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

  Nei nomi dei file sopra indicati, `nn.nn.nn.nnnn` rappresenta il numero di versione.

Il processo di installazione viene avviato e viene visualizzata la schermata iniziale del proxy dei servizi Web NetApp SANtricity + Gestore unificato.

3. Seguire le istruzioni a schermo.

   Durante l'installazione, viene richiesto di attivare diverse funzioni e di inserire alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.

   > Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

4. Quando viene visualizzato il messaggio Webserver Started (Server Web avviato), fare clic su **OK** per completare l'installazione.

   Viene visualizzata la finestra di dialogo Installazione completata.

5. Fare clic sulle caselle di controllo se si desidera avviare Unified Manager o la documentazione API interattiva, quindi fare clic su **fine**.

Installazione in modalità console

È possibile eseguire l'installazione in modalità Console per Windows o Linux. In modalità Console, i prompt vengono visualizzati nella finestra del terminale.

Fasi

1. Eseguire il seguente comando: `<install filename> -i console`

   Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   > Per annullare l'installazione in qualsiasi momento durante il processo di installazione, digitare `QUIT` al prompt dei comandi.

   Viene avviato il processo di installazione e viene visualizzato il messaggio Avvio del programma di installazione — Introduzione.

2. Seguire le istruzioni a schermo.

   Durante l'installazione, viene richiesto di attivare diverse funzioni e di inserire alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.

   > Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

3. Una volta completata l'installazione, premere **Invio** per uscire dal programma di installazione.

Installazione in modalità silenziosa

È possibile eseguire l'installazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Eseguire il seguente comando: `<install filename> -i silent`

   Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Premere **Invio**.

   Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Installazione del comando RPM (solo Linux)

Per i sistemi Linux compatibili con il sistema di gestione dei pacchetti RPM, è possibile installare il proxy dei servizi Web utilizzando un file RPM opzionale.

Fasi

1. Scaricare il file RPM sul server in cui si desidera installare il proxy e Unified Manager.
2. Aprire una finestra terminale.
3. Immettere il seguente comando:

   ```
   rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   > Nel comando precedente, `nn.nn.nn.nnnn` rappresenta il numero di versione.

   Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Accedere a API e Unified Manager

I servizi Web includono la documentazione API, che consente di interagire direttamente con L'API REST. Include inoltre Unified Manager, un'interfaccia basata su browser per la gestione di più sistemi storage e-Series.

Accedere all'API dei servizi Web

Dopo aver installato Web Services Proxy, è possibile accedere alla documentazione API interattiva in un browser.

La documentazione API viene eseguita con ogni istanza dei servizi Web ed è disponibile anche in formato PDF statico dal sito del supporto NetApp. Per accedere alla versione interattiva, aprire un browser e immettere l'URL che indica la posizione dei servizi Web (un controller per la versione incorporata o un server per il proxy).

> L'API dei servizi Web implementa la specifica OpenAPI (originariamente chiamata specifica Swagger).

Per l'accesso iniziale, utilizzare le credenziali "admin". "Admin" è considerato un super amministratore con accesso a tutte le funzioni e i ruoli.

Fasi

1. Aprire un browser.
2. Inserire l'URL per l'implementazione del proxy o incorporato:

   - Integrato: `https://<controller>:<port>/devmgr/docs/`

     In questo URL, `<controller>` È l'indirizzo IP o FQDN del controller, e. `<port>` è il numero della porta di gestione del controller (il valore predefinito è 8443).

   - Proxy: `http[s]://<server>:<port>/devmgr/docs/`

     In questo URL, `<server>` È l'indirizzo IP o FQDN del server in cui è installato il proxy, e. `<port>` È il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o 8443 per HTTPS).

     > Se la porta di ascolto è già in uso, il proxy rileva il conflitto e richiede di scegliere un'altra porta di ascolto.

   La documentazione API viene aperta nel browser.

3. Una volta aperta la documentazione API interattiva, accedere al menu a discesa in alto a destra della pagina e selezionare **utils**.
4. Fare clic sulla categoria **Login** per visualizzare gli endpoint disponibili.
5. Fare clic sull'endpoint **POST: /Login**, quindi fare clic su **Provalo**.
6. Per il primo accesso, immettere admin come nome utente e password.
7. Fare clic su **Execute** (Esegui).
8. Per accedere agli endpoint per la gestione dello storage, andare al menu a discesa in alto a destra e selezionare **v2**.

   Vengono visualizzate le categorie di alto livello per gli endpoint. È possibile esplorare la documentazione API come descritto nella tabella.

Area	Descrizione
Menu a discesa	Nella parte superiore destra della pagina, un menu a discesa fornisce le opzioni per passare dalla versione 2 della documentazione API (V2), all'interfaccia dei simboli (Symbol V2) e alle utility API (utils) per l'accesso. Poiché la versione 1 della documentazione API era una versione preliminare e generalmente non disponibile, V1 non è incluso nel menu a discesa.

Area	Descrizione
Categorie	La documentazione API è organizzata in base a categorie di alto livello (ad esempio, amministrazione, configurazione). Fare clic su una categoria per visualizzare gli endpoint correlati.
Endpoint	Selezionare un endpoint per visualizzare i percorsi URL, i parametri richiesti, i corpi di risposta e i codici di stato che gli URL potrebbero restituire.
Provalo	Interagire direttamente con l'endpoint facendo clic su **Provalo**. Questo pulsante viene fornito in ciascuna vista espansa per gli endpoint. Quando si fa clic sul pulsante, vengono visualizzati i campi per l'immissione dei parametri (se applicabile). Immettere i valori e fare clic su **Esegui**. La documentazione interattiva utilizza JavaScript per inviare la richiesta direttamente all'API; non si tratta di una richiesta di test.

Accedere a Unified Manager

Dopo aver installato Web Services Proxy, è possibile accedere a Unified Manager per gestire più sistemi storage in un'interfaccia basata su web.

Per accedere a Unified Manager, aprire un browser e immettere l'URL che indica la posizione in cui è installato il proxy. Sono supportati i seguenti browser e versioni.

Browser	Versione minima
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

Fasi

1. Aprire un browser e immettere il seguente URL:

   ```
   http[s]://<server>:<port>/um
   ```

   In questo URL, `<server>` Rappresenta l'indirizzo IP o FQDN del server in cui è installato Web Services Proxy, e. `<port>` Rappresenta il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o

8443 per HTTPS).

Viene visualizzata la pagina di accesso a Unified Manager.

2. Per il primo accesso, immettere `admin` specificare il nome utente, quindi impostare e confermare una password per l'utente amministratore.

   La password può contenere fino a 30 caratteri. Per ulteriori informazioni su utenti e password, consultare la sezione Gestione degli accessi della guida in linea di Unified Manager.

Configurare il proxy dei servizi Web

È possibile modificare le impostazioni di Web Services Proxy per soddisfare i requisiti operativi e di performance specifici per il proprio ambiente.

Arrestare o riavviare il server Web

Il servizio Webserver viene avviato durante l'installazione e viene eseguito in background. Durante alcune attività di configurazione, potrebbe essere necessario arrestare o riavviare il servizio Webserver.

Fasi

1. Effettuare una delle seguenti operazioni:

   - Per Windows, accedere al menu **Avvio**, selezionare **Strumenti di amministrazione › servizi**, individuare **servizi Web NetApp SANtricity** e selezionare **Interrompi** o **Riavvia**.
   - Per Linux, scegliere il metodo per arrestare e riavviare il server Web per la versione del sistema operativo in uso. Durante l'installazione, una finestra di dialogo a comparsa indica quale demone è stato avviato. Ad esempio:

     ```
     web_services_proxy webserver installed and started. You can interact with it
     using systemctl start|stop|restart|status web_services_proxy.service
     ```

   Il metodo più comune per interagire con il servizio è l'utilizzo di `systemctl` comandi.

Risolvere i conflitti di porta

Se il proxy dei servizi Web è in esecuzione mentre un'altra applicazione è disponibile all'indirizzo o alla porta definiti, è possibile risolvere il conflitto di porte nel file wsconfig.xml.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere la seguente riga al file wsconfig.xml, in cui *n* è il numero della porta:

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   La tabella seguente mostra gli attributi che controllano le porte HTTP e le porte HTTPS.

Nome	Descrizione	Nodo padre	Attributi	Obbligatorio
config	Il nodo root per la configurazione	Nullo	Versione - la versione dello schema di configurazione è attualmente 1.0.	Sì
slport	La porta TCP in attesa delle richieste SSL. Il valore predefinito è 8443.	config	Clientauth	No
porta	La porta TCP in attesa della richiesta HTTP, per impostazione predefinita, è 8080.	config	-	No

3. Salvare e chiudere il file.
4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare il bilanciamento del carico e/o l'alta disponibilità

Per utilizzare il proxy dei servizi Web in una configurazione ad alta disponibilità (ha), è possibile configurare il bilanciamento del carico. In una configurazione ha, in genere, un singolo nodo riceve tutte le richieste mentre le altre sono in stand-by oppure le richieste sono bilanciate in base al carico su tutti i nodi.

Il proxy dei servizi Web può esistere in un ambiente ad alta disponibilità (ha), con la maggior parte delle API che funzionano correttamente indipendentemente dal destinatario della richiesta. I tag e le cartelle dei metadati sono due eccezioni, perché i tag e le cartelle vengono memorizzati in un database locale e non vengono condivisi tra le istanze di Web Services Proxy.

Tuttavia, in una piccola percentuale di richieste si verificano alcuni problemi di tempistica noti. In particolare, un'istanza del proxy può avere dati più recenti più velocemente di una seconda istanza per una piccola finestra. Il proxy dei servizi Web include una configurazione speciale che elimina questo problema di tempistica. Questa opzione non è attivata per impostazione predefinita, perché aumenta il tempo necessario per le richieste di servizio (per la coerenza dei dati). Per attivare questa opzione, è necessario aggiungere una proprietà a un file .INI (per Windows) o .SH (per Linux).

Fasi

1. Effettuare una delle seguenti operazioni:
   - Windows: Aprire il file appserver64.ini, quindi aggiungere `Dload-balance.enabled=true` proprietà.

     Ad esempio: `vmarg.7=-Dload-balance.enabled=true`
   - Linux: Aprire il file webserver.sh, quindi aggiungere `Dload-balance.enabled=true` proprietà.

     Ad esempio: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Salvare le modifiche.
3. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Disattiva il simbolo HTTPS

È possibile disattivare i comandi dei simboli (impostazione predefinita) e inviare comandi tramite una chiamata di procedura remota (RPC). Questa impostazione può essere modificata nel file wsconfig.xml.

Per impostazione predefinita, il proxy dei servizi Web invia i comandi dei simboli tramite HTTPS per tutti i sistemi storage della serie E2800 e E5700 con SANtricity OS versione 08.40 o successiva. I comandi Symbol inviati tramite HTTPS vengono autenticati nel sistema di storage. Se necessario, è possibile disattivare il supporto dei simboli HTTPS e inviare comandi tramite RPC. Ogni volta che viene configurato Symbol over RPC, tutti i comandi passivi al sistema di storage vengono abilitati senza autenticazione.

> Quando viene utilizzato Symbol over RPC, il proxy dei servizi Web non può connettersi ai sistemi con la porta di gestione dei simboli disattivata.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. In `devicemgt.symbolclientstrategy` sostituire `httpsPreferred` valore con `rpcOnly`.

   Ad esempio:

   ```
   <env key="devicemgt.symbolclientstrategy">rpcOnly</env>
   ```

3. Salvare il file.

Configurare la condivisione delle risorse tra origini

È possibile configurare la condivisione delle risorse tra origini (CORS), un meccanismo che utilizza intestazioni HTTP aggiuntive per fornire un'applicazione Web in esecuzione su un'origine per avere l'autorizzazione ad accedere a risorse selezionate da un server di origine diversa.

Il CORS viene gestito dal file cors.cfg che si trova nella directory di lavoro. La configurazione CORS è aperta per impostazione predefinita, pertanto l'accesso tra domini non è limitato.

Se non è presente alcun file di configurazione, CORS è aperto. Ma se il file cors.cfg è presente, viene utilizzato. Se il file cors.cfg è vuoto, non è possibile effettuare una richiesta CORS.

Fasi

1. Aprire il file cors.cfg che si trova nella directory di lavoro.
2. Aggiungere le righe desiderate al file.

   Ogni riga nel file di configurazione CORS è un modello di espressione regolare da abbinare. L'intestazione di origine deve corrispondere a una riga nel file cors.cfg. Se un modello di riga corrisponde all'intestazione di origine, la richiesta è consentita. Viene confrontata l'origine completa, non solo l'elemento host.

3. Salvare il file.

Le richieste vengono associate sull'host e in base al protocollo, ad esempio:

- Associare localhost a qualsiasi protocollo — `*localhost*`
- Corrispondenza localhost solo per HTTPS — `https://localhost*`

Disinstallare il proxy dei servizi Web

Per rimuovere Web Services Proxy e Unified Manager, è possibile utilizzare qualsiasi modalità (file grafico, console, silenzioso o RPM), indipendentemente dal metodo utilizzato per installare il proxy.

Disinstallazione della modalità grafica

È possibile eseguire la disinstallazione in modalità grafica per Windows o Linux. In modalità grafica, i prompt vengono visualizzati in un'interfaccia di tipo Windows.

Fasi

1. Avviare la disinstallazione per Windows o Linux, come indicato di seguito:
   - Windows — accedere alla directory che contiene il file di disinstallazione uninstall_web_Services_proxy. La directory predefinita si trova nel seguente percorso: C:/Program Files/NetApp/SANtricity Web Services Proxy/. Fare doppio clic `uninstall_web_services_proxy.exe`.

     In alternativa, è possibile accedere a **pannello di controllo › programmi › Disinstalla un programma**, quindi selezionare "Proxy dei servizi web NetApp SANtricity".

   - Linux — accedere alla directory che contiene il file di disinstallazione di Web Services Proxy. La directory predefinita si trova nella seguente posizione: `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i gui
   ```

   Viene visualizzata la schermata iniziale del proxy dei servizi Web di SANtricity.

3. Nella finestra di dialogo Disinstalla, fare clic su **Disinstalla**.

   Viene visualizzata la barra di avanzamento del programma di disinstallazione che mostra lo stato di avanzamento.

4. Quando viene visualizzato il messaggio Uninstall complete (disinstallazione completata), fare clic su **Done** (fine).

Disinstallazione della modalità console

È possibile eseguire la disinstallazione in modalità Console per Windows o Linux. In modalità Console, i prompt vengono visualizzati nella finestra del terminale.

Fasi

1. Accedere alla directory uninstall_web_Services_proxy.
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i console
   ```

Viene avviato il processo di disinstallazione.

3. Una volta completata la disinstallazione, premere **Invio** per uscire dal programma di installazione.

Disinstallazione in modalità silenziosa

È possibile eseguire la disinstallazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Accedere alla directory uninstall_web_Services_proxy.
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i silent
   ```

   Il processo di disinstallazione viene eseguito, ma nella finestra del terminale non vengono visualizzati messaggi o script di ritorno. Una volta disinstallato Web Services Proxy, viene visualizzato un prompt dei comandi nella finestra del terminale.

Disinstallazione del comando RPM (solo Linux)

È possibile utilizzare un comando RPM per disinstallare il proxy dei servizi Web da un sistema Linux.

Fasi

1. Aprire una finestra terminale.
2. Immettere la seguente riga di comando:

   ```
   rpm -e santricity_webservices
   ```

   > Il processo di disinstallazione potrebbe lasciare file che non facevano parte dell'installazione originale. Eliminare manualmente questi file per rimuovere completamente il proxy dei servizi Web.

Gestire l'accesso degli utenti in Web Services Proxy

È possibile gestire l'accesso degli utenti alle API dei servizi Web e a Unified Manager per motivi di sicurezza.

Panoramica della gestione degli accessi

La gestione degli accessi include accessi in base al ruolo, crittografia delle password, autenticazione di base e integrazione LDAP.

Accesso in base al ruolo

RBAC (role-based access control) associa gli utenti predefiniti ai ruoli. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità.

La tabella seguente descrive ciascun ruolo.

Ruolo	Descrizione
security.admin	SSL e gestione dei certificati.
storage.admin	Accesso completo in lettura/scrittura alla configurazione del sistema storage.
storage.monitor	Accesso in sola lettura per visualizzare i dati del sistema di storage.
support.admin	Accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).

Gli account utente predefiniti sono definiti nel file users.properties. È possibile modificare gli account utente modificando direttamente il file users.properties o utilizzando le funzioni di gestione degli accessi di Unified Manager.

La tabella seguente elenca gli accessi utente disponibili per il proxy dei servizi Web.

Accesso utente predefinito	Descrizione
amministratore	Un super amministratore che ha accesso a tutte le funzioni e include tutti i ruoli. Per Unified Manager, è necessario impostare la password al primo accesso.
storage	L'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
sicurezza	L'utente responsabile della configurazione della sicurezza. Questo utente include i seguenti ruoli: Security.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
supporto	L'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
monitorare	Un utente con accesso di sola lettura al sistema. Questo utente include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
rw (legacy per gli array meno recenti)	L'utente rw (lettura/scrittura) include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Accesso utente predefinito	Descrizione
ro (legacy per gli array meno recenti)	L'utente ro (sola lettura) include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Crittografia della password

Per ciascuna password, è possibile applicare un ulteriore processo di crittografia utilizzando la codifica della password SHA256 esistente. Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.

> Prima della versione 3.0 di Web Services Proxy, le password venivano crittografate solo tramite l'hashing SHA256. Tutte le password crittografate SHA256 esistenti con solo hash mantengono questa codifica e sono ancora valide nel file users.properties. Tuttavia, le password crittografate SHA256 solo con hash non sono sicure come quelle con crittografia SARTed SHA256.

Autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Questa impostazione può essere modificata nel file wsconfig.xml.

LDAP

Il protocollo LDAP (Lightweight Directory Access Protocol), un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti, è abilitato per il proxy dei servizi Web. L'integrazione LDAP consente l'autenticazione dell'utente e il mapping dei ruoli ai gruppi.

Per informazioni sulla configurazione della funzionalità LDAP, fare riferimento alle opzioni di configurazione nell'interfaccia di Unified Manager o nella sezione LDAP della documentazione API interattiva.

Configurare l'accesso dell'utente

È possibile gestire l'accesso degli utenti applicando una crittografia aggiuntiva alle password, impostando l'autenticazione di base e definendo l'accesso in base al ruolo.

Applicare crittografia aggiuntiva alle password

Per ottenere il massimo livello di sicurezza, è possibile applicare una crittografia aggiuntiva alle password utilizzando la codifica password SHA256 esistente.

Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.

Fasi

1. Aprire il file users.properties all'indirizzo:
   - (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Immettere nuovamente la password crittografata come testo normale.
3. Eseguire `securepasswds` Utilità della riga di comando per crittografare nuovamente la password o

semplicemente riavviare il proxy dei servizi Web. Questa utility viene installata nella directory di installazione principale del proxy dei servizi Web.

> In alternativa, è possibile utilizzare le password utente locali e cancellarle ogni volta che vengono modificate le password tramite Unified Manager.

Configurare l'autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Se lo si desidera, è possibile modificare tale impostazione nel file wsconfig.xml.

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Modificare la riga seguente nel file specificando false (non abilitato) o true (abilitato).

   Ad esempio: `<env key="enable-basic-auth">true</env>`

3. Salvare il file.
4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare l'accesso in base al ruolo

Per limitare l'accesso degli utenti a funzioni specifiche, è possibile modificare i ruoli specificati per ciascun account utente.

Web Services Proxy include RBAC (role-based access control), in cui i ruoli sono associati a utenti predefiniti. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità. È possibile modificare i ruoli assegnati agli account utente modificando direttamente il file users.properties.

> È inoltre possibile modificare gli account utente utilizzando Access Management in Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Fasi

1. Aprire il file users.properties, che si trova in:
   - (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Individuare la riga dell'account utente che si desidera modificare (storage, sicurezza, monitor, supporto, rw, o ro).

   > Non modificare l'utente admin. Si tratta di un super utente con accesso a tutte le funzioni.

3. Aggiungere o rimuovere i ruoli specificati, come desiderato.

   I ruoli includono:

   - Security.admin — SSL e gestione dei certificati.
   - Storage.admin — accesso completo in lettura/scrittura alla configurazione del sistema storage.

- Storage.monitor — accesso in sola lettura per visualizzare i dati del sistema di storage.
- Support.admin — accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).

> Il ruolo storage.monitor è necessario per tutti gli utenti, incluso l'amministratore.

4. Salvare il file.

Gestire la sicurezza e i certificati in Web Services Proxy

Per motivi di sicurezza in Web Services Proxy, è possibile specificare una designazione della porta SSL ed è possibile gestire i certificati. I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server.

Abilitare SSL

Il proxy dei servizi Web utilizza Secure Sockets Layer (SSL) per la protezione, che viene attivata durante l'installazione. È possibile modificare la designazione della porta SSL nel file wsconfig.xml.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere o modificare il numero della porta SSL, in modo simile all'esempio seguente:

```
<sslport clientauth="request">8443</sslport>
```

Risultato

Quando il server viene avviato con SSL configurato, il server cerca i file keystore e truststore.

- Se il server non trova un keystore, utilizza l'indirizzo IP del primo indirizzo IPv4 non loopback rilevato per generare un keystore e aggiungere un certificato autofirmato al keystore.
- Se il server non trova un truststore o non viene specificato, il server utilizza il keystore come truststore.

Ignora la convalida del certificato

Per supportare connessioni sicure, il proxy dei servizi Web convalida i certificati` dei sistemi di storage rispetto ai propri certificati attendibili. Se necessario, è possibile specificare che il proxy eluderà la convalida prima di connettersi ai sistemi di storage.

Prima di iniziare

- Tutte le connessioni del sistema di storage devono essere sicure.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy

- (Linux) — /opt/netapp/santricity_web_Services_proxy

2. Invio `true` in `trust.all.arrays` come mostrato nell'esempio:

```
<env key="trust.all.arrays">true</env>
```

3. Salvare il file.

Generare e importare un certificato di gestione host

I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server. Per generare e importare certificati CA (Certificate Authority) per il sistema host in cui è installato Web Services Proxy, è possibile utilizzare endpoint API.

Per gestire i certificati per il sistema host, eseguire le seguenti attività utilizzando l'API:

- Creare una richiesta di firma del certificato (CSR) per il sistema host.
- Inviare il file CSR a una CA, quindi attendere l'invio dei file di certificato.
- Importare i certificati firmati nel sistema host.

> È inoltre possibile gestire i certificati nell'interfaccia di Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile in Unified Manager.

Fasi

1. Accedere a. "Documentazione API interattiva".
2. Andare al menu a discesa in alto a destra e selezionare **v2**.
3. Espandere il collegamento **Administration** e scorrere verso il basso fino agli endpoint **/certificates**.
4. Generare il file CSR:
   a. Selezionare **POST:/certificates**, quindi selezionare **Try it out**.

      Il server Web rigenera un certificato autofirmato. È quindi possibile inserire informazioni nei campi per definire il nome comune, l'organizzazione, l'unità organizzativa, l'ID alternativo e altre informazioni utilizzate per generare la CSR.

   b. Aggiungere le informazioni richieste nel riquadro **Example Values** (valori di esempio) per generare un certificato CA valido, quindi eseguire i comandi.

      > Non chiamare di nuovo **POST:/certificates** o **POST:/certificates/reset**, altrimenti è necessario rigenerare la CSR. Quando si chiama **POST:/certificates** o **POST:/certificates/reset**, si sta generando un nuovo certificato autofirmato con una nuova chiave privata. Se si invia una CSR generata prima dell'ultimo ripristino della chiave privata sul server, il nuovo certificato di protezione non funziona. È necessario generare una nuova CSR e richiedere un nuovo certificato CA.

   c. Eseguire l'endpoint **GET:/certificates/server** per confermare che lo stato corrente del certificato è il certificato autofirmato con le informazioni aggiunte dal comando **POST:/certificates**.

      Il certificato del server (indicato dall'alias `jetty`) è ancora autofirmato a questo punto.

d. Espandere l'endpoint **POST:/certificates/export**, selezionare **provalo**, immettere un nome di file per il file CSR, quindi fare clic su **Esegui**.

5. Copiare e incollare `fileUrl` In una nuova scheda del browser per scaricare il file CSR, quindi inviare il file CSR a una CA valida per richiedere una nuova catena di certificati del server Web.
6. Quando la CA emette una nuova catena di certificati, utilizzare uno strumento di gestione dei certificati per suddividere i certificati server root, intermedi e Web, quindi importarli nel server proxy dei servizi Web:
   a. Espandere l'endpoint **POST:/sslconfig/server** e selezionare **Provalo**.
   b. Immettere un nome per il certificato CA root nel campo **alias**.
   c. Selezionare **false** nel campo **replaceMainServerCertificate**.
   d. Individuare e selezionare il nuovo certificato CA principale.
   e. Fare clic su **Execute** (Esegui).
   f. Verificare che il caricamento del certificato sia riuscito.
   g. Ripetere la procedura di caricamento del certificato CA per il certificato intermedio CA.
   h. Ripetere la procedura di caricamento del certificato per il nuovo file di certificato di sicurezza del server Web, ad eccezione di questa fase, selezionare **true** nell'elenco a discesa **replaceMainServerCertificate**.
   i. Verificare che l'importazione del certificato di sicurezza del server Web sia riuscita.
   j. Per confermare che i nuovi certificati root, intermedi e server web sono disponibili nel keystore, eseguire **GET:/certificates/server**.
7. Selezionare ed espandere l'endpoint **POST:/certificates/reload**, quindi selezionare **Try it out**. Quando richiesto, se si desidera riavviare entrambi i controller, selezionare **false**. ("vero" si applica solo nel caso di controller a doppio array). Fare clic su **Execute** (Esegui).

   L'endpoint **/certificates/reload** in genere restituisce una risposta http 202 corretta. Tuttavia, il ricaricamento dei certificati truststore e keystore del server Web crea una race condition tra il processo API e il processo di ricarica dei certificati del server Web. In rari casi, il ricaricamento del certificato del server Web può superare l'elaborazione dell'API. In questo caso, il ricaricamento sembra non riuscire anche se è stato completato correttamente. In tal caso, passare comunque alla fase successiva. Se il ricaricamento non è riuscito, anche il passaggio successivo non riesce.

8. Chiudere la sessione corrente del browser sul proxy dei servizi Web, aprire una nuova sessione del browser e verificare che sia possibile stabilire una nuova connessione sicura del browser al proxy dei servizi Web.

   Utilizzando una sessione di navigazione in incognito o privata, è possibile aprire una connessione al server senza utilizzare i dati salvati delle sessioni di navigazione precedenti.

Gestire i sistemi storage utilizzando Web Services Proxy

Per gestire i sistemi storage in rete, è necessario prima rilevarli e poi aggiungerli all'elenco di gestione.

Scopri i sistemi storage

È possibile impostare il rilevamento automatico o rilevare manualmente i sistemi storage.

Rilevare automaticamente i sistemi storage

È possibile specificare che i sistemi di storage vengano rilevati automaticamente in rete modificando le impostazioni nel file wsconfig.xml. Per impostazione predefinita, il rilevamento automatico IPv6 è disattivato e IPv4 è attivato.

Per aggiungere un sistema storage, è necessario fornire un solo indirizzo IP o DNS di gestione. Il server rileva automaticamente tutti i percorsi di gestione quando i percorsi non sono configurati o sono configurati e ruotabili.

> Se si tenta di utilizzare un protocollo IPv6 per rilevare automaticamente i sistemi storage dalla configurazione del controller dopo aver effettuato una connessione iniziale, il processo potrebbe non riuscire. Le possibili cause del guasto includono problemi durante l'inoltro dell'indirizzo IP o l'attivazione di IPv6 sui sistemi storage, ma non sul server.

Prima di iniziare

Prima di attivare le impostazioni di rilevamento IPv6, verificare che l'infrastruttura supporti la connettività IPv6 ai sistemi storage per mitigare eventuali problemi di connessione.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Nelle stringhe di ricerca automatica, modificare le impostazioni da `true` a. `false`, come desiderato. Vedere l'esempio seguente.

```
<env key="autodiscover.ipv6.enable">true</env>
```

> Quando i percorsi sono configurati, ma non configurati in modo che il server possa instradare verso gli indirizzi, si verificano errori di connessione intermittenti. Se non è possibile impostare gli indirizzi IP in modo che possano essere instradati dall'host, disattivare la funzione di rilevamento automatico (modificare le impostazioni su `false`).

3. Salvare il file.

Rilevare e aggiungere sistemi storage utilizzando endpoint API

È possibile utilizzare gli endpoint API per rilevare e aggiungere sistemi storage all'elenco gestito. Questa procedura crea una connessione di gestione tra il sistema di storage e l'API.

> Questa attività descrive come individuare e aggiungere sistemi storage utilizzando l'API REST, in modo da poter gestire questi sistemi nella documentazione API interattiva. Tuttavia, è possibile gestire i sistemi storage in Unified Manager, che offre un'interfaccia di facile utilizzo. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Prima di iniziare

Per i sistemi storage con SANtricity versione 11.30 e successive, l'interfaccia di gestione legacy per Symbol deve essere attivata nell'interfaccia di Gestore di sistema di SANtricity. In caso contrario, gli endpoint di rilevamento non riescono. Per trovare questa impostazione, aprire Gestione sistema e accedere al

Impostazioni › sistema › Impostazioni aggiuntive › interfaccia di gestione delle modifiche.

Fasi

1. Accedere a. "Documentazione API interattiva".
2. Scopri i sistemi storage come segue:
   a. Nella documentazione API, assicurarsi che sia selezionato **V2** nell'elenco a discesa, quindi espandere la categoria **Storage-Systems**.
   b. Fare clic sull'endpoint **POST: /Discovery**, quindi fare clic su **Provalo**.
   c. Inserire i parametri come descritto nella tabella.

IP startup IP finale	Sostituire la stringa con l'intervallo di indirizzi IP iniziale e finale per uno o più sistemi di storage in rete.
UseAgents	Impostare questo valore su: • Vero = utilizza agenti in-band per la scansione di rete. • Falso = non utilizzare agenti in-band per la scansione di rete.
ConnectionTimeout	Inserire i secondi consentiti per la scansione prima che la connessione si esaurisca.
MaxPortsToUse	Immettere un numero massimo di porte utilizzate per la scansione di rete.

   d. Fare clic su **Execute** (Esegui).

   Le azioni API vengono eseguite senza richieste dell'utente.

   Il processo di rilevamento viene eseguito in background.

   a. Assicurarsi che il codice restituisca 202.
   b. In **Response Body**, individuare il valore restituito per l'ID richiesta. Per visualizzare i risultati nel passaggio successivo, è necessario l'ID richiesta.
3. Visualizzare i risultati del rilevamento come segue:
   a. Fare clic sull'endpoint **GET: /Discovery**, quindi fare clic su **Provalo**.
   b. Inserire l'ID richiesta dal passaggio precedente. Se si lascia vuoto **ID richiesta**, l'endpoint passa per impostazione predefinita all'ultimo ID richiesta eseguito.

c. Fare clic su **Execute** (Esegui).

d. Assicurarsi che il codice restituisca 200.

e. Nel corpo della risposta, individuare l'ID richiesta e le stringhe per i sistemi di storage. Le stringhe sono simili all'esempio seguente:

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Annotare i valori per wwn, Label e ipAddresses. Sono necessari per il passaggio successivo.

4. Aggiungere i sistemi storage come segue:

a. Fare clic sull'endpoint **POST: /Storage-system**, quindi fare clic su **Provalo**.

b. Inserire i parametri come descritto nella tabella.

id
Immettere un nome univoco per il sistema di storage. È possibile inserire l'etichetta (visualizzata nella risposta per GET: /Discovery), ma il nome può essere qualsiasi stringa scelta. Se non si specifica un valore per questo campo, i servizi Web assegnano automaticamente un identificatore univoco.
ControllerAddresses
Inserire gli indirizzi IP visualizzati nella risposta per GET: /Discovery. Per i controller doppi, separare gli indirizzi IP con una virgola. Ad esempio: `"IP address 1","IP address 2"`
validare
Invio `true`, In modo da poter ricevere la conferma che i servizi Web possono connettersi al sistema di storage.
password
Inserire la password amministrativa per il sistema di storage.

wwn
Inserire il WWN del sistema di storage (visualizzato nella risposta per GET: /Discovery).

c. Rimuovi tutte le stringhe dopo `"enableTrace": true`, in modo che l'intero set di stringhe sia simile all'esempio seguente:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Fare clic su **Execute** (Esegui).

e. Assicurarsi che la risposta del codice sia 201, che indica che l'endpoint è stato eseguito correttamente.

   L'endpoint **Post: /Storage-Systems** viene messo in coda. È possibile visualizzare i risultati utilizzando l'endpoint **GET: /Storage-Systems** nella fase successiva.

5. Confermare l'aggiunta dell'elenco, come segue:

   a. Fare clic sull'endpoint **GET: /Storage-system**.

      Non sono richiesti parametri.

   b. Fare clic su **Execute** (Esegui).

   c. Assicurarsi che la risposta del codice sia 200, che indica che l'endpoint è stato eseguito correttamente.

   d. Nel corpo della risposta, cercare i dettagli del sistema di storage. I valori restituiti indicano che è stato aggiunto correttamente all'elenco degli array gestiti, in modo simile all'esempio seguente:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


Scalare il numero di sistemi storage gestiti

Per impostazione predefinita, l'API può gestire fino a 100 sistemi storage. Se è necessario gestire di più, è necessario superare i requisiti di memoria per il server.

Il server è impostato per utilizzare 512 MB di memoria. Per ogni 100 sistemi storage aggiuntivi della rete, aggiungere 250 MB a tale numero. Non aggiungere più memoria di quella fisicamente disponibile. Consente di aggiungere un numero sufficiente di componenti aggiuntivi per il sistema operativo e altre applicazioni.

> La dimensione predefinita della cache è 8,192 eventi. L'utilizzo approssimativo dei dati per la cache degli eventi MEL è di 1 MB per ogni 8,192 eventi. Pertanto, mantenendo le impostazioni predefinite, l'utilizzo della cache dovrebbe essere di circa 1 MB per un sistema storage.

> Oltre alla memoria, il proxy utilizza le porte di rete per ciascun sistema di storage. Linux e Windows considerano le porte di rete come handle di file. Come misura di sicurezza, la maggior parte dei sistemi operativi limita il numero di handle di file aperti che un processo o un utente può avere aperto contemporaneamente. In particolare negli ambienti Linux, dove le connessioni TCP aperte sono considerate come handle di file, il proxy dei servizi Web può facilmente superare questo limite. Poiché la correzione dipende dal sistema, fare riferimento alla documentazione del sistema operativo per informazioni su come aumentare questo valore.

Fasi

1. Effettuare una delle seguenti operazioni:
   - In Windows, accedere al file appserver64.init. Individuare la linea, `vmarg.3=-Xmx512M`
   - Su Linux, andare al file webserver.sh. Individuare la linea, `JAVA_OPTIONS="-Xmx512M"`
2. Per aumentare la memoria, sostituire `512` Con la memoria desiderata in MB.
3. Salvare il file.

Gestire il polling automatico per le statistiche del proxy dei servizi Web

È possibile configurare il polling automatico per tutte le statistiche di dischi e volumi sui sistemi storage rilevati.

Panoramica delle statistiche

Le statistiche forniscono informazioni sui tassi di raccolta dei dati e sulle performance dei sistemi storage.

Il proxy dei servizi Web consente di accedere ai seguenti tipi di statistiche:

- Statistiche raw — contatori totali per i punti dati al momento della raccolta dei dati. Le statistiche raw possono essere utilizzate per operazioni di lettura totali o operazioni di scrittura totali.
- Statistiche analizzate — informazioni calcolate per un intervallo. Esempi di statistiche analizzate sono le operazioni di input/output in lettura (IOPS) al secondo o il throughput in scrittura.

Le statistiche raw sono lineari, in genere richiedono almeno due punti di dati raccolti per ricavare da essi i dati utilizzabili. Le statistiche analizzate sono una derivazione delle statistiche raw, che forniscono metriche importanti. Molti valori che possono essere derivati dalle statistiche raw vengono visualizzati in un formato point-in-time utilizzabile nelle statistiche analizzate per maggiore comodità.

È possibile recuperare le statistiche raw indipendentemente dal fatto che il polling automatico sia attivato o meno. È possibile aggiungere `usecache=true` Stringa di query alla fine dell'URL per recuperare le statistiche memorizzate nella cache dall'ultimo polling. L'utilizzo dei risultati memorizzati nella cache aumenta notevolmente le performance del recupero delle statistiche. Tuttavia, più chiamate a una velocità uguale o inferiore alla cache dell'intervallo di polling configurata recuperano gli stessi dati.

Funzionalità delle statistiche

Il proxy dei servizi Web fornisce endpoint API che consentono il recupero di statistiche di controller e interfacce raw e analizzate da modelli hardware e versioni software supportati.

API Raw Statistics

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API delle statistiche analizzate

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Questi URL recuperano le statistiche analizzate dall'ultimo polling e sono disponibili solo quando il polling è attivato. Questi URL includono i seguenti dati input-output:

- Operazioni al secondo
- Throughput in megabyte al secondo
- Tempi di risposta in millisecondi

I calcoli si basano sulle differenze tra le iterazioni di polling statistiche, che sono le misure più comuni delle performance dello storage. Queste statistiche sono preferibili alle statistiche non analizzate.

> All'avvio del sistema, non esiste alcuna raccolta di statistiche precedente da utilizzare per calcolare le varie metriche, pertanto le statistiche analizzate richiedono almeno un ciclo di polling dopo l'avvio per restituire i dati. Inoltre, se i contatori cumulativi vengono ripristinati, il ciclo di polling successivo avrà numeri imprevedibili per i dati.

Configurare gli intervalli di polling

Per configurare gli intervalli di polling, modificare il file wsconfig.xml in modo da specificare un intervallo di polling in secondi.

> Poiché le statistiche sono memorizzate nella cache, potrebbe verificarsi un aumento di circa 1.5 MB di utilizzo della memoria per ciascun sistema di storage.

Prima di iniziare

- I sistemi storage devono essere rilevati dal proxy.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere la seguente riga all'interno di `<env-entries>` tag, in cui `n` indica il numero di secondi dell'intervallo tra le richieste di polling:

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Ad esempio, se si inserisce 60, il polling inizia a intervalli di 60 secondi. Ovvero, il sistema richiede l'avvio del polling 60 secondi dopo il completamento del periodo di polling precedente (indipendentemente dalla durata del periodo di polling precedente). Tutte le statistiche sono contrassegnate con l'ora esatta in cui sono state recuperate. Il sistema utilizza l'indicatore orario o la differenza temporale su cui basare il calcolo di 60 secondi.
3. Salvare il file.

Gestire AutoSupport utilizzando il proxy dei servizi Web

È possibile configurare ASUP (AutoSupport), che raccoglie i dati e li invia automaticamente al supporto tecnico per la risoluzione dei problemi e l'analisi dei problemi in remoto.

Panoramica di ASUP (AutoSupport)

La funzione ASUP (AutoSupport) trasmette automaticamente i messaggi a NetApp in base a criteri manuali e basati su pianificazione.

Ogni messaggio AutoSupport è un insieme di file di log, dati di configurazione, dati di stato e metriche delle performance. Per impostazione predefinita, AutoSupport trasmette i file elencati nella tabella seguente al team di supporto NetApp una volta alla settimana.

Nome file	Descrizione
x-headers-data.txt	Un file .txt contenente le informazioni dell'intestazione X.
manifest.xml	Un file .xml che descrive il contenuto del messaggio.
arraydata.xml	Un file .xml contenente l'elenco dei dati persistenti del client.
appserver-config.txt	Un file .txt contenente i dati di configurazione dell'application server.
wsconfig.txt	Un file .txt contenente i dati di configurazione del servizio Web.
host-info.txt	Un file .txt contenente informazioni sull'ambiente host.
server-logs.7z	Un file .7z contenente tutti i file di log del webserver disponibili.
client-info.txt	Un file .txt con coppie chiave/valore arbitrarie per contatori specifici dell'applicazione, ad esempio accessi a metodi e pagine web.
webservices-profile.json	Questi file contengono i dati del profilo WebServices e i dati statistici di monitoraggio Jersey. Per impostazione predefinita, le statistiche di monitoraggio Jersey sono attivate. È possibile attivarle e disattivarle nel file wsconfig.xml, come indicato di seguito: • Abilitare: `<env key="enable.jersey.statistics">true</env>` • Disattiva: `<env key="enable.jersey.statistics">false</env>`

Configurare AutoSupport

AutoSupport è attivato per impostazione predefinita al momento dell'installazione; tuttavia, è possibile modificare tale impostazione o i tipi di consegna.

Attiva o disattiva AutoSupport

La funzione AutoSupport viene attivata o disattivata durante l'installazione iniziale del proxy dei servizi Web, ma è possibile modificarla nel file ASUPConfig.

È possibile attivare o disattivare AutoSupport tramite il file ASUPConfig.xml, come descritto di seguito. In alternativa, è possibile attivare o disattivare questa funzione tramite l'API utilizzando **Configuration** e

POST/asup, quindi immettendo "true" o "false".

1. Aprire il file ASUPConfig.xml nella directory di lavoro.
2. Individuare le linee per <asupdata enable="Boolean_value" timestamp="timestamp">
3. Invio `true` (attiva) o. `false` (disattiva). Ad esempio:

```
<asupdata enabled="false" timestamp="0">
```

> La voce relativa all'indicatore data e ora è superflua.

4. Salvare il file.

Configurare il metodo di erogazione AutoSupport

È possibile configurare la funzione AutoSupport in modo che utilizzi i metodi di consegna HTTPS, HTTP o SMTP. HTTPS è il metodo di consegna predefinito.

1. Accedere al file ASUPConfig.xml nella directory di lavoro.
2. Nella stringa, `<delivery type="n">`, inserire 1, 2 o 3 come descritto nella tabella:

Valore	Descrizione
1	**HTTPS** (impostazione predefinita) <delivery type="1">
2	**HTTP** <delivery type="2">

3	**SMTP** — per configurare correttamente il tipo di recapito AutoSupport su SMTP, è necessario includere l'indirizzo del server di posta SMTP, insieme ai messaggi di posta elettronica dell'utente mittente e destinatario, come nell'esempio seguente:
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

Mirroring remoto del volume

Panoramica dei volumi di storage remoto

Utilizzare la funzione volumi di storage remoto SANtricity® per importare i dati da un dispositivo di storage remoto direttamente in un volume e-Series locale. Questa funzione consente di ottimizzare il processo di upgrade delle apparecchiature e offre funzionalità di migrazione dei dati per spostare i dati da dispositivi non-e-Series a sistemi e-Series.

Panoramica della configurazione

La funzione volumi di storage remoto è disponibile con Gestore di sistema SANtricity per gli ID dei sottomodello selezionati. Per utilizzare questa funzione, è necessario configurare un sistema di storage remoto e un sistema di storage e-Series per comunicare tra loro.

Utilizzare il seguente flusso di lavoro:

1. "Esaminare requisiti e limitazioni".
2. "Configurare l'hardware".
3. "Importa storage remoto".

Trova ulteriori informazioni

- Guida in linea, disponibile nell'interfaccia utente di System Manager o in "Sito della documentazione del software SANtricity".
- Per ulteriori informazioni tecniche sulla funzione Remote Storage Volumes (volumi storage remoti), consultare la "Report tecnico sui volumi di storage remoto".

Requisiti e restrizioni per lo storage remoto

Prima di configurare la funzione Remote Storage Volumes, esaminare i seguenti requisiti e limitazioni.

Requisiti hardware

Protocolli supportati

Per la versione iniziale della funzione Remote Storage Volumes, il supporto è disponibile solo per i protocolli iSCSI e IPv4.

Fare riferimento a. "Tool di matrice di interoperabilità NetApp" Per informazioni aggiornate sul supporto e sulla configurazione tra l'host e l'array e-Series (destinazione) utilizzato per la funzione Remote Storage Volumes.

Requisiti di sistema per lo storage

Il sistema storage e-Series deve includere:

- Due controller (modalità duplex)
- Connessioni iSCSI per i controller e-Series per comunicare con il sistema di storage remoto attraverso una o più connessioni iSCSI

- SANtricity OS 11.71 o superiore
- Funzione di storage remoto attivata nell'ID modello secondario (SMID)

Il sistema remoto può essere un sistema storage e-Series o un sistema di un altro vendor. Deve includere interfacce compatibili con iSCSI.

Requisiti di volume

I volumi utilizzati per le importazioni devono soddisfare i requisiti di dimensione, stato e altri criteri.

Volume di storage remoto

Il volume di origine di un'importazione viene chiamato "volume di storage remoto". Questo volume deve soddisfare i seguenti criteri:

- Non può far parte di un'altra importazione
- Deve avere uno stato online

Una volta avviata l'importazione, il firmware del controller crea un volume di storage remoto in background. A causa di questo processo in background, il volume di storage remoto non è gestibile in System Manager e può essere utilizzato solo per l'operazione di importazione.

Una volta creato, il volume di storage remoto viene trattato come qualsiasi altro volume standard sul sistema e-Series con le seguenti eccezioni:

- Può essere utilizzato come proxy per il dispositivo di storage remoto.
- Non può essere utilizzato come candidato per altre copie di volumi o snapshot.
- Impossibile modificare l'impostazione Data Assurance durante l'importazione.
- Non può essere mappato ad alcun host, perché sono riservati esclusivamente per l'operazione di importazione.

Ogni volume di storage remoto è associato a un solo oggetto di storage remoto; tuttavia, un oggetto di storage remoto può essere associato a più volumi di storage remoto. Il volume di storage remoto viene identificato in modo univoco utilizzando una combinazione di quanto segue:

- Identificatore dell'oggetto storage remoto
- Numero LUN del dispositivo di storage remoto

Candidati al volume di destinazione

Il volume di destinazione è il volume di destinazione sul sistema e-Series locale.

Il volume di destinazione deve soddisfare i seguenti criteri:

- Deve essere un volume RAID/DDP.
- Deve avere una capacità uguale o superiore al volume di storage remoto.
- Deve avere una dimensione del blocco uguale a quella del volume di storage remoto.
- Deve avere uno stato valido (ottimale).
- Non è possibile avere alcuna delle seguenti relazioni: Copia del volume, copie Snapshot, mirroring asincrono o sincrono.

- Non è possibile eseguire operazioni di riconfigurazione: Espansione dinamica del volume, espansione dinamica della capacità, dimensione dinamica dei segmenti, migrazione dinamica del RAID, riduzione dinamica della capacità, O deframmentazione.
- Impossibile eseguire il mapping a un host prima dell'inizio dell'importazione (tuttavia, è possibile eseguire il mapping dopo l'avvio dell'importazione).
- Non è possibile attivare la funzione Flash Read cache (FRC).

System Manager verifica automaticamente questi requisiti nell'ambito della procedura guidata di importazione dello storage remoto. Per la selezione del volume di destinazione vengono visualizzati solo i volumi che soddisfano tutti i requisiti.

Restrizioni

La funzione di storage remoto presenta le seguenti restrizioni:

- Il mirroring deve essere disattivato.
- Il volume di destinazione sul sistema e-Series non deve disporre di snapshot.
- Il volume di destinazione sul sistema e-Series non deve essere mappato ad alcun host prima dell'avvio dell'importazione.
- Il provisioning delle risorse del volume di destinazione nel sistema e-Series deve essere disattivato.
- I mapping diretti del volume di storage remoto a uno o più host non sono supportati.
- Il proxy dei servizi Web non è supportato.
- I segreti CHAP iSCSI non sono supportati.
- SMcli non è supportato.
- VMware Datastore non è supportato.
- Quando è presente una coppia di importazione, è possibile aggiornare un solo sistema di storage alla volta nella coppia relazione/importazione.

Preparazione per le importazioni in produzione

È necessario eseguire un'importazione di test o "dry run" prima delle importazioni in produzione per verificare la corretta configurazione dello storage e del fabric.

Molte variabili possono influire sull'operazione di importazione e sui tempi di completamento. Per garantire che un'importazione in produzione sia riuscita e per ottenere una stima della durata, è possibile utilizzare queste importazioni di test per garantire che tutte le connessioni funzionino come previsto e che l'operazione di importazione venga completata in un periodo di tempo appropriato. È quindi possibile apportare modifiche per ottenere i risultati desiderati prima di avviare l'importazione in produzione.

Configurare l'hardware per i volumi di storage remoto

Il sistema storage e-Series deve essere configurato per comunicare con il sistema storage remoto attraverso il protocollo iSCSI supportato.

Configurare il dispositivo di storage remoto e l'array e-Series

Prima di passare a Gestione sistema di SANtricity per configurare la funzione volumi di storage remoto, procedere come segue:

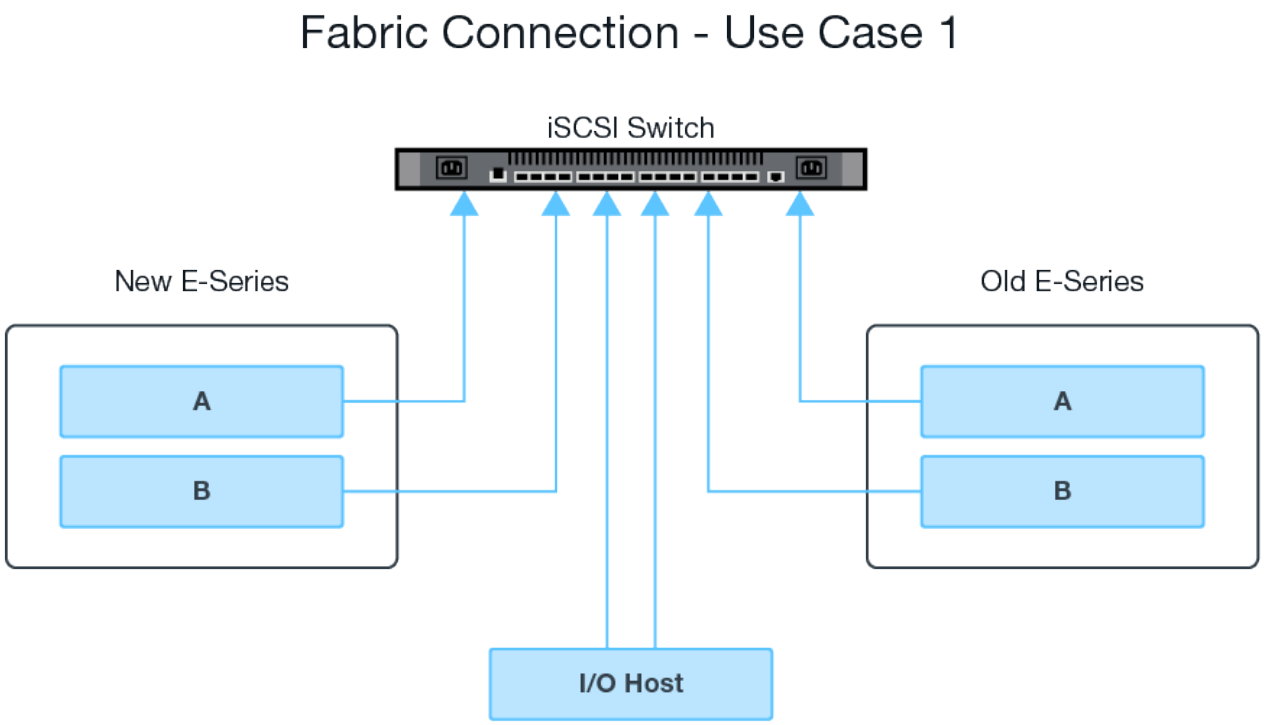
1. Stabilire manualmente una connessione cablata tra il sistema e-Series e il sistema di storage remoto in modo che i due sistemi possano essere configurati per comunicare tramite iSCSI.
2. Configurare le porte iSCSI in modo che il sistema e-Series e il sistema di storage remoto possano comunicare correttamente tra loro.
3. Ottenere l'IQN del sistema e-Series.
4. Rendere il sistema e-Series visibile al sistema di storage remoto. Se il sistema di storage remoto è un sistema e-Series, creare un host utilizzando l'IQN del sistema e-Series di destinazione come informazione di connessione per la porta host.
5. Se il dispositivo di storage remoto è in uso da un host/applicazione:
   - Arrestare i/o sul dispositivo di storage remoto.
   - Dismappare/smontare il dispositivo di storage remoto.
6. Mappare il dispositivo di storage remoto all'host definito per il sistema di storage e-Series.
7. Ottenere il numero LUN del dispositivo utilizzato per la mappatura.

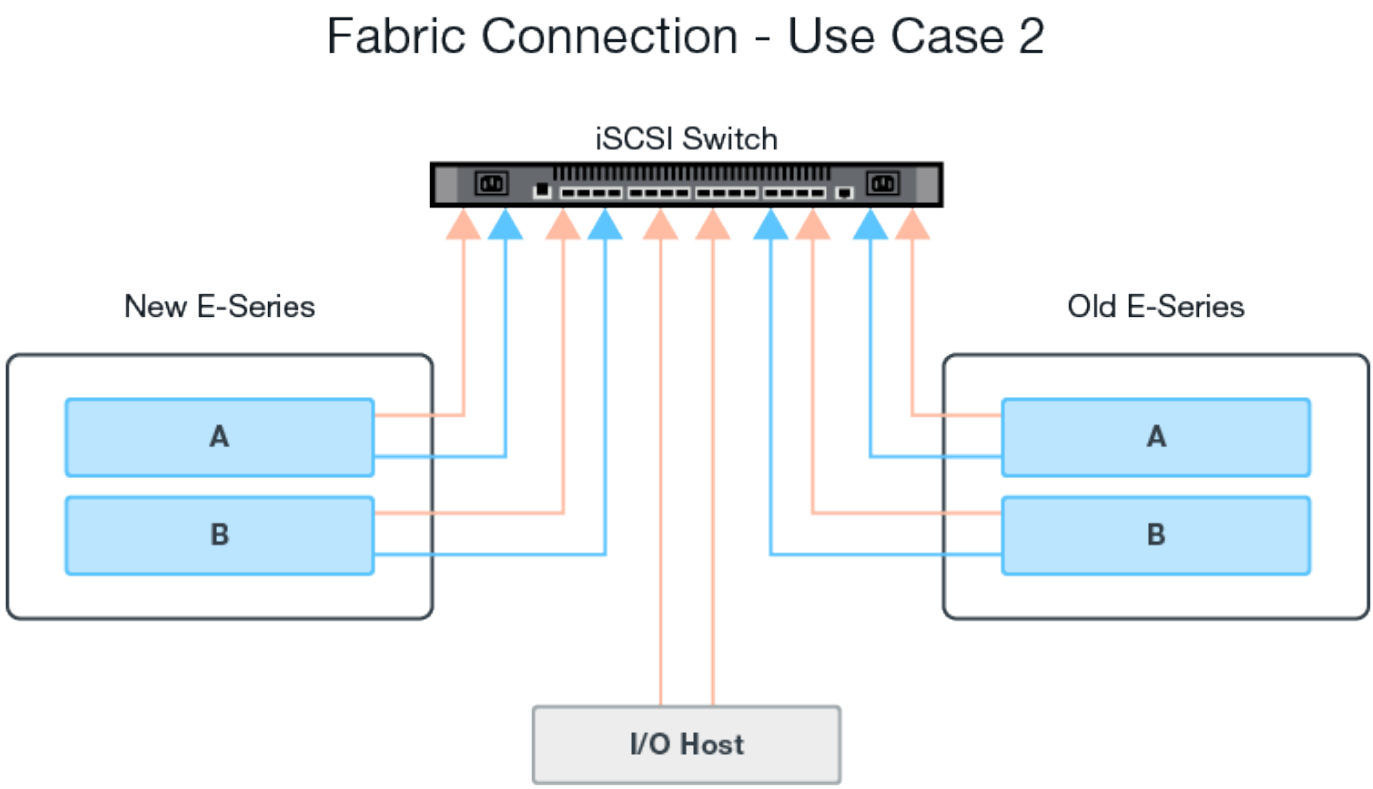
> Consigliato: Eseguire il backup del volume di origine remoto prima di avviare il processo di importazione.

Cablare gli array di storage

Nell'ambito del processo di configurazione, gli array di storage e l'host i/o devono essere cablati all'interfaccia compatibile con iSCSI.

I seguenti diagrammi forniscono esempi di come collegare i sistemi in modo che eseguano operazioni Remote Storage Volume su una connessione iSCSI.





Configurare le porte iSCSI

È necessario configurare le porte iSCSI per garantire la comunicazione tra la destinazione (array di storage locale e-Series) e l'origine (array di storage remoto).

Le porte iSCSI possono essere configurate in più modi in base alla subnet. Di seguito sono riportati alcuni esempi su come configurare le porte iSCSI per l'utilizzo con la funzione Remote Storage Volumes.

Fonte A.	Fonte B	Destinazione A	Destinazione B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

Fonte A.	Fonte B	Destinazione A	Destinazione B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

Importa storage remoto

Per avviare un'importazione dello storage da un sistema remoto a un sistema storage e-Series locale, utilizzare la procedura guidata di importazione dello storage remoto nell'interfaccia utente di Gestore di sistema di SANtricity.

Di cosa hai bisogno

- Il sistema storage e-Series deve essere configurato per comunicare con il sistema storage remoto. Vedere "Configurare l'hardware".

- Per il sistema di storage remoto, raccogliere le seguenti informazioni:
  - IQN iSCSI
  - Indirizzi IP iSCSI
  - Numero LUN del dispositivo di storage remoto (volume di origine)
- Per il sistema storage e-Series locale, creare o selezionare un volume da utilizzare per l'importazione dei dati. Il volume di destinazione deve soddisfare i seguenti requisiti:
  - Corrisponde alle dimensioni del blocco del dispositivo di storage remoto (il volume di origine).
  - Ha una capacità uguale o superiore al dispositivo di storage remoto.
  - Ha uno stato di ottimale ed è disponibile. Per un elenco completo dei requisiti, vedere "Requisiti e limitazioni".
- Consigliato: Eseguire il backup dei volumi sul sistema di storage remoto prima di avviare il processo di importazione.

A proposito di questa attività

In questa attività, viene creata una mappatura tra il dispositivo di storage remoto e un volume sul sistema di storage e-Series locale. Al termine della configurazione, viene avviata l'importazione.

> Poiché molte variabili possono influire sull'operazione di importazione e sui tempi di completamento, è necessario eseguire prima importazioni di "test" più piccole. Utilizzare questi test per assicurarsi che tutte le connessioni funzionino come previsto e che l'operazione di importazione venga completata in un intervallo di tempo appropriato.

Fasi

1. Da Gestione sistema di SANtricity, fare clic su **Storage > Storage remoto**.
2. Fare clic su **Importa storage remoto**.

   Viene visualizzata una procedura guidata per l'importazione dello storage remoto.

3. Nella fase 1a del pannello Configure Source (Configura origine), immettere le informazioni di connessione.

   a. Nel campo **Nome**, immettere il nome del dispositivo di storage remoto.

   b. Sotto **iSCSI Connection properties** (Proprietà connessione iSCSI), immettere quanto segue per il dispositivo di storage remoto: IQN, indirizzo IP e numero di porta (il valore predefinito è 3260).

      Se si desidera aggiungere un'altra connessione iSCSI, fare clic su **+Aggiungi un altro indirizzo IP** per includere un indirizzo IP aggiuntivo per lo storage remoto. Al termine, fare clic su **Avanti**.

   Dopo aver fatto clic su Next (Avanti), viene visualizzata la fase 1b del pannello Configure Source (Configura origine).

4. Nel campo **LUN**, selezionare il LUN di origine desiderato per il dispositivo di storage remoto, quindi fare clic su **Avanti**.

   Viene visualizzato il pannello Configure Target (Configura destinazione) che visualizza i volumi candidati da utilizzare come destinazione per l'importazione. Alcuni volumi non vengono visualizzati nell'elenco dei candidati a causa delle dimensioni dei blocchi, della capacità o della disponibilità dei volumi.

5. Dalla tabella, selezionare un volume di destinazione nel sistema storage e-Series. Se necessario, utilizzare il dispositivo di scorrimento per modificare la priorità di importazione. Fare clic su **Avanti**. Confermare

l'operazione nella finestra di dialogo successiva digitando `continue`, Quindi fare clic su **continua**.

Se il volume di destinazione ha una capacità superiore a quella del volume di origine, tale capacità aggiuntiva non viene segnalata all'host connesso al sistema e-Series. Per utilizzare la nuova capacità, è necessario eseguire un'operazione di espansione del file system sull'host dopo il completamento dell'operazione di importazione e la disconnessione.

Dopo aver confermato la configurazione nella finestra di dialogo, viene visualizzato il pannello Review (Revisione).

6. Dalla schermata Review (Revisione), verificare che le impostazioni relative al dispositivo di storage remoto, alla destinazione e all'importazione siano corrette. Fare clic su **fine** per completare la creazione dello storage remoto.

   Viene visualizzata un'altra finestra di dialogo che chiede se si desidera avviare un'altra importazione.

7. Se necessario, fare clic su **Sì** per creare un'altra importazione di storage remoto. Facendo clic su Yes (Sì) si torna alla fase 1a del pannello Configure Source (Configura origine), in cui è possibile selezionare la configurazione esistente o aggiungerne una nuova. Se non si desidera creare un'altra importazione, fare clic su **No** per uscire dalla finestra di dialogo.

   Una volta avviato il processo di importazione, l'intero volume di destinazione viene sovrascritto con i dati copiati. Se l'host scrive nuovi dati nel volume di destinazione durante questo processo, tali nuovi dati vengono propagati nuovamente al dispositivo remoto (volume di origine).

8. Visualizzare l'avanzamento dell'operazione nella finestra di dialogo View Operations (Visualizza operazioni) sotto il pannello Remote Storage (archiviazione remota).

   Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del sistema di storage remoto, dall'impostazione della priorità per l'importazione e dalla quantità di carico i/o su entrambi i sistemi storage e sui volumi associati. Una volta completata l'importazione, il volume locale è un duplicato del dispositivo di storage remoto.

9. Quando si è pronti a interrompere la relazione tra i due volumi, selezionare **Disconnect** nell'oggetto di importazione dalla vista Operations in Progress (operazioni in corso). Una volta disconnessa la relazione, le prestazioni del volume locale tornano alla normalità e non sono più influenzate dalla connessione remota.

Gestire l'avanzamento dell'importazione

Una volta avviato il processo di importazione, è possibile visualizzare e intraprendere azioni in merito.

Per ogni operazione di importazione, la pagina Operations in Progress (operazioni in corso) visualizza una percentuale di completamento e il tempo rimanente stimato. Le azioni includono la modifica della priorità di importazione, l'interruzione e la ripresa delle operazioni e la disconnessione dall'operazione.

> È inoltre possibile visualizzare le operazioni in corso dalla home page (**Home > Mostra operazioni in corso**).

Fasi

1. In Gestore di sistema di SANtricity, accedere alla pagina Storage remoto e selezionare **Visualizza operazioni**.

Viene visualizzata la finestra di dialogo Operations in Progress (operazioni in corso).

2. Se lo si desidera, utilizzare i collegamenti nella colonna Actions (azioni) per interrompere e riprendere, modificare la priorità o disconnettersi da un'operazione.
   - **Cambia priorità** – selezionare **Cambia priorità** per modificare la priorità di elaborazione di un'operazione in corso o in sospeso. Applicare una priorità all'operazione, quindi fare clic su **OK**.
   - **Stop** – selezionare **Stop** per sospendere la copia dei dati dal dispositivo di storage remoto. La relazione tra la coppia di importazione è ancora intatta ed è possibile selezionare **Riprendi** quando si è pronti per continuare l'operazione di importazione.
   - **Riprendi** – selezionare **Riprendi** per avviare un processo interrotto o non riuscito da dove è stato interrotto. Quindi, applicare una priorità all'operazione di ripresa, quindi fare clic su **OK**.

     L'operazione di ripresa **non** riavvia l'importazione dall'inizio. Se si desidera riavviare il processo dall'inizio, selezionare **Disconnect** (Disconnetti), quindi ricreare l'importazione mediante la procedura guidata di importazione dello storage remoto.
   - **Disconnect** – selezionare **Disconnect** per interrompere la relazione tra i volumi di origine e di destinazione per un'operazione di importazione interrotta, completata o non riuscita.

Modificare le impostazioni di connessione dello storage remoto

È possibile modificare, aggiungere o eliminare le impostazioni di connessione per qualsiasi configurazione di storage remoto tramite l'opzione View/Edit Settings (Visualizza/Modifica impostazioni).

Le modifiche apportate alle proprietà della connessione influiscono sulle importazioni in corso. Per evitare interruzioni, apportare modifiche alle proprietà della connessione solo quando le importazioni non sono in esecuzione.

Fasi

1. Dalla schermata archiviazione remota di Gestione sistema SANtricity, selezionare l'oggetto di archiviazione remota desiderato nella sezione Result list (elenco risultati).
2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la schermata Remote Storage Settings (Impostazioni storage remoto).
3. Fare clic sulla scheda **Connection Properties** (Proprietà connessione).

   Vengono visualizzati l'indirizzo IP configurato e le impostazioni della porta per l'importazione dello storage remoto.
4. Eseguire una delle seguenti operazioni:
   - **Edit** (Modifica) – fare clic su **Edit** (Modifica) accanto alla voce corrispondente per l'oggetto storage remoto. Inserire l'indirizzo IP e/o le informazioni sulla porta modificati nei campi.
   - **Aggiungi** – fare clic su **Aggiungi**, quindi inserire il nuovo indirizzo IP e le informazioni sulla porta nei campi forniti. Fare clic su **Aggiungi** per confermare, quindi la nuova connessione viene visualizzata nell'elenco degli oggetti di storage remoto.
   - **Delete** (Elimina) – selezionare la connessione desiderata dall'elenco, quindi fare clic su **Delete** (Elimina). Confermare l'operazione digitando `delete` Nel campo fornito, quindi fare clic su **Delete** (Elimina). La connessione viene rimossa dall'elenco degli oggetti di storage remoto.

5. Fare clic su **Save** (Salva).

   Le impostazioni di connessione modificate vengono applicate all'oggetto storage remoto.

Rimuovere l'oggetto storage remoto

Una volta completata l'importazione, è possibile rimuovere un oggetto di storage remoto se non si desidera più copiare i dati tra i dispositivi locali e remoti.

Fasi

1. Assicurarsi che nessuna importazione sia associata all'oggetto di storage remoto che si intende rimuovere.
2. Dalla schermata archiviazione remota di Gestione sistema SANtricity, selezionare l'oggetto di archiviazione remota desiderato nella sezione Result list (elenco risultati).
3. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Conferma rimozione connessione storage remoto.

4. Confermare l'operazione digitando `remove` Quindi fare clic su **Rimuovi**.

   L'oggetto Remote Storage selezionato viene rimosso.

Plug-in di storage per vCenter

Panoramica dello Storage Plugin per vCenter

Il plug-in di storage SANtricity per vCenter offre una gestione integrata degli array di storage e-Series dall'interno di una sessione del client VMware vSphere.

Attività disponibili

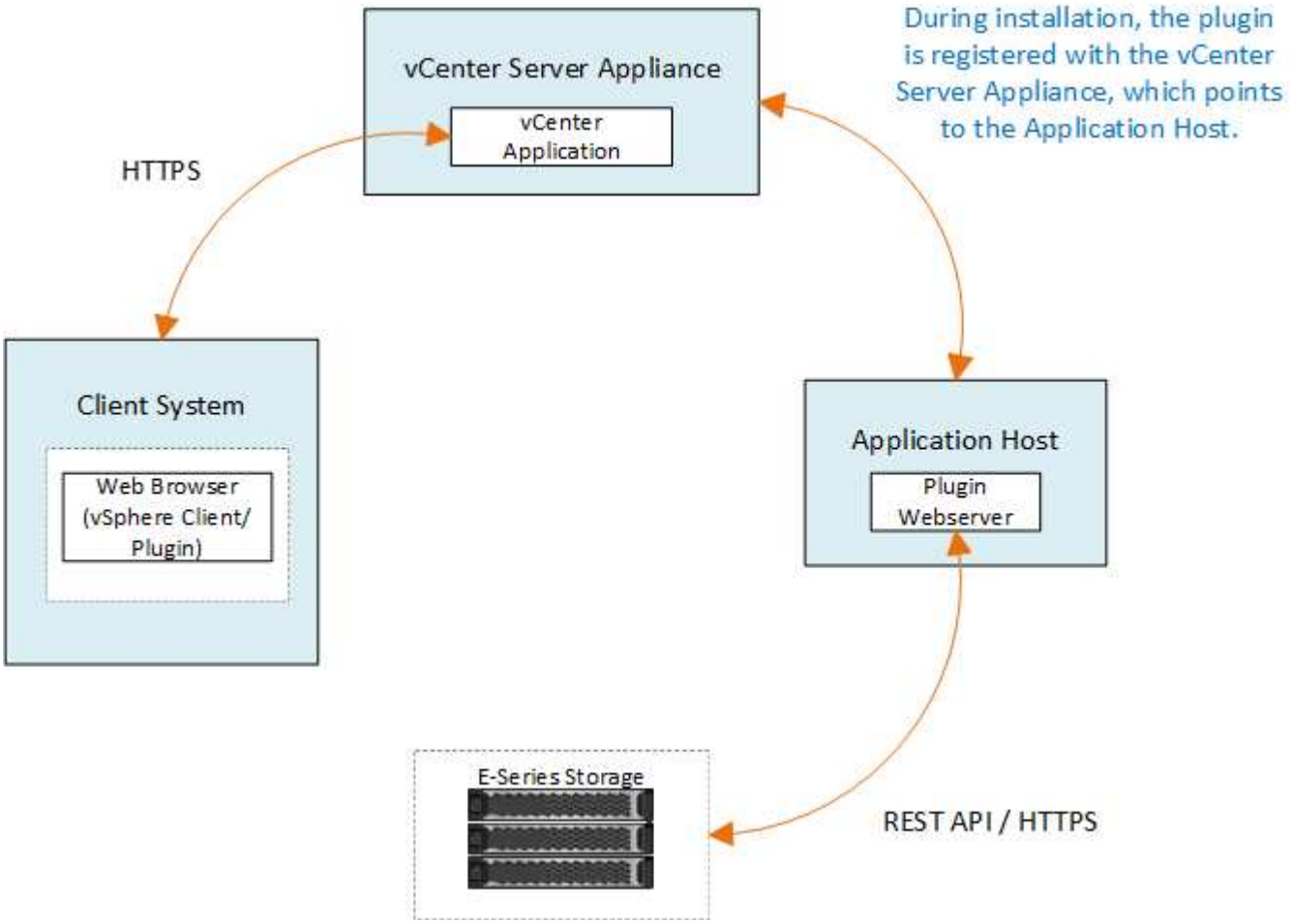
È possibile utilizzare il plug-in per eseguire le seguenti operazioni:

- Visualizzare e gestire gli array di storage rilevati in rete.
- Eseguire operazioni batch su gruppi di più array di storage.
- Eseguire gli aggiornamenti sul sistema operativo del software.
- Importare le impostazioni da uno storage array a un altro.
- Configurare volumi, cache SSD, host, cluster di host, pool, e gruppi di volumi.
- Avviare l'interfaccia di System Manager per ulteriori attività di gestione su un array.

> Il plug-in non sostituisce direttamente l'interfaccia di System Manager, integrata in ciascun controller per uno storage array. System Manager offre funzionalità di gestione aggiuntive; se lo si desidera, è possibile aprire System Manager selezionando un array di storage nella vista principale del plug-in e facendo clic su **Launch**.

Il plug-in richiede un'appliance VMware vCenter Server implementata nell'ambiente VMware e un host dell'applicazione per installare ed eseguire il webserver plug-in.

Fare riferimento alla figura seguente per ulteriori informazioni sulle comunicazioni nell'ambiente vCenter.



Panoramica dell'interfaccia

Quando si accede al plug-in, la pagina principale si apre su **Manage - All** (Gestisci - tutto). Da questa pagina è possibile visualizzare e gestire tutti gli array di storage rilevati nella rete.

Barra laterale di navigazione

La barra laterale di navigazione visualizza quanto segue:

- **Gestisci** — rileva gli array di storage nella tua rete, avvia System Manager per un array, importa le impostazioni da un array a più array, gestisci i gruppi di array, aggiorna il sistema operativo SANtricity ed esegui il provisioning dello storage.
- **Certificate Management** — Gestione dei certificati per l'autenticazione tra browser e client.
- **Operations** — consente di visualizzare l'avanzamento delle operazioni batch, ad esempio l'importazione di impostazioni da un array a un altro.

> Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.

- **Supporto** — Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

Browser supportati

È possibile accedere allo Storage Plugin per vCenter da diversi tipi di browser. Sono supportati i seguenti browser e versioni.

- Google Chrome 89 o versione successiva
- Mozilla Firefox 80 o versione successiva
- Microsoft Edge 90 o versione successiva

Ruoli e autorizzazioni degli utenti

Per accedere alle attività nel plug-in di storage per vCenter, l'utente deve disporre dei permessi di lettura/scrittura. Per impostazione predefinita, tutti gli ID utente VMware vCenter definiti non dispongono di autorizzazioni per eseguire le attività nel plug-in.

Panoramica della configurazione

La configurazione prevede i seguenti passaggi:

1. "Installare e registrare il plug-in".
2. "Configurare i permessi di accesso al plug-in".
3. "Accedere all'interfaccia del plug-in".
4. "Scopri gli array di storage".
5. "Eseguire il provisioning dello storage".

Trova ulteriori informazioni

Per ulteriori informazioni sulla gestione dei datastore nel client vSphere, vedere "Documentazione VMware vSphere".

Inizia subito

Verifica dei requisiti di installazione e aggiornamento

Prima di installare o aggiornare il plug-in di storage SANtricity per vCenter, esaminare i requisiti di installazione e le considerazioni sull'aggiornamento.

Requisiti di installazione

È possibile installare e configurare Storage Plugin per vCenter su un sistema host Windows. L'installazione del plug-in include i seguenti requisiti.

Requisito	Descrizione
Versioni supportate	• Versioni supportate di VMware vCenter Server Appliance: 6.7U3J, 7.0U1, 7.0U2, 7.0U3 e 8.0. • Versione del sistema operativo NetApp SANtricity: 11.60.2 o superiore • Versioni degli host delle applicazioni supportate: Windows 2016, Windows 2019, Windows 2022. Per ulteriori informazioni sulla compatibilità, consultare "Tool di matrice di interoperabilità NetApp".

Requisito	Descrizione
Istanze multiple	È possibile installare solo un'istanza di Storage Plugin per vCenter su un host Windows e registrarla solo su un vCSA.
Pianificazione della capacità	Storage Plugin per vCenter richiede uno spazio adeguato per l'esecuzione e la registrazione. Assicurarsi che il sistema soddisfi i seguenti requisiti di spazio disponibile su disco: • Spazio di installazione richiesto: 275 MB • Spazio di storage: 275 MB + 200 MB (registrazione) • Memoria di sistema: 1.5 GB
Licenza	Lo Storage Plugin per vCenter è un prodotto standalone gratuito che non richiede una chiave di licenza. Tuttavia, si applicano i copyright e i termini del servizio applicabili.

Considerazioni sull'upgrade

Se si esegue l'aggiornamento da una versione precedente, tenere presente che il plug-in deve essere disregistrato da vCSA prima dell'aggiornamento.

- Durante l'aggiornamento, la maggior parte delle impostazioni di configurazione precedenti del plug-in vengono mantenute. Queste impostazioni includono password utente, tutti i sistemi di storage rilevati, certificati server, certificati attendibili e configurazione del runtime del server.
- Il processo di aggiornamento non conserva i file **vcenter.properties**, pertanto è necessario annullare la registrazione del plug-in prima dell'aggiornamento. Una volta completato l'aggiornamento, è possibile registrare nuovamente il plug-in nella vCSA.
- Tutti i file SANtricity OS precedentemente caricati nel repository vengono rimossi durante l'aggiornamento.

Installare o aggiornare il plug-in di storage per vCenter

Per installare Storage Plugin per vCenter e verificare la registrazione del plug-in, procedere come segue. È anche possibile aggiornare il plug-in seguendo queste istruzioni.

Verificare i prerequisiti per l'installazione

Assicurarsi che i sistemi soddisfino i requisiti di "Verifica dei requisiti di installazione e aggiornamento".

> Il processo di aggiornamento non conserva i file **vcenter.properties**. Se si esegue l'aggiornamento, è necessario annullare la registrazione del plug-in prima dell'aggiornamento. Una volta completato l'aggiornamento, è possibile registrare nuovamente il plug-in nella vCSA.

Installare il software del plug-in

Per installare il software del plug-in:

1. Copiare il file del programma di installazione nell'host che verrà utilizzato come server applicazioni, quindi accedere alla cartella in cui è stato scaricato il programma di installazione.

2. Fare doppio clic sul file di installazione:

   ```
   santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe
   ```

   Nel nome file sopra indicato, `nn.nn.nn.nnnn` rappresenta il numero di versione.

3. All'avvio dell'installazione, seguire le istruzioni visualizzate sullo schermo per attivare diverse funzioni e immettere alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.

   Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

   Durante l'installazione, viene richiesto di eseguire la convalida del certificato. Mantenere la casella di controllo selezionata se si desidera applicare la convalida del certificato tra il plug-in e gli array di storage. Con questa applicazione, i certificati dell'array di storage vengono verificati per essere considerati attendibili rispetto al plug-in. Se i certificati non sono attendibili, non è consentito aggiungerli al plug-in. Se si desidera eseguire l'override della convalida del certificato, deselezionare la casella di controllo in modo che tutti gli array di storage possano essere aggiunti al plug-in utilizzando certificati autofirmati. Per ulteriori informazioni sui certificati, consultare la guida in linea disponibile nell'interfaccia del plug-in.

4. Quando viene visualizzato il messaggio Webserver Started (Server Web avviato), fare clic su **OK** per completare l'installazione, quindi fare clic su **Done** (fine).
5. Verificare che il server applicazioni sia stato installato correttamente eseguendo il comando **Services.msc**.
6. Verificare che il servizio del server applicazioni (VCP), **plug-in storage NetApp SANtricity per vCenter**, sia stato installato e che il servizio sia stato avviato.

   Se necessario, è possibile modificare le impostazioni di convalida certificato e porta servizio Web dopo l'installazione. Dalla directory di installazione, aprire il file wsconfig.xml. Per rimuovere la convalida del certificato sugli array di storage, modificare `env` chiave, `trust.all.arrays`, a. `true`. Per modificare la porta dei servizi Web, modificare `sslport` valore sul valore della porta desiderato compreso tra 0 e 65535. Assicurarsi che il numero di porta utilizzato non sia vincolante per un altro processo. Al termine, salvare le modifiche e riavviare il server Web del plug-in. Se il valore della porta del webserver del plug-in viene modificato dopo la registrazione del plug-in in vCSA, è necessario annullare la registrazione e registrare nuovamente il plug-in in modo che vCSA stia comunicando al webserver del plug-in sulla porta modificata.

Registrare il plug-in con un'appliance vCenter Server

Una volta installato il software del plug-in, registrare il plug-in con un vCSA.

Il plug-in può essere registrato solo su una vCSA alla volta. Per effettuare la registrazione a un vCSA diverso, è necessario annullare la registrazione del plug-in dal vCSA corrente e disinstallarlo dall'host dell'applicazione. È quindi possibile reinstallare il plug-in e registrarlo sull'altro vCSA.

1. Aprire un prompt dalla riga di comando e accedere alla seguente directory:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Eseguire il file **vcenter-register.bat**:
```
vcenter-register.bat ^
-action registerPlugin ^
-vcenterHostname <vCenter FQDN> ^
-username <Administrator username> ^
```
3. Verificare che lo script sia stato eseguito correttamente.

I registri vengono salvati in `%install_dir%/working/logs/vc-registration.log`.

Verificare la registrazione del plug-in

Dopo aver installato il plug-in e aver eseguito lo script di registrazione, verificare che il plug-in sia stato registrato correttamente con vCenter Server Appliance.

1. Aprire il client vSphere sull'appliance vCenter Server.
2. Nella barra dei menu, selezionare **Administrator › Client Plugin**.
3. Assicurarsi che Storage Plugin per vCenter sia elencato come **Enabled**.

   Se il plug-in è elencato come Disabled (Disattivato) e viene visualizzato un messaggio di errore che indica che non è possibile comunicare con l'application server, verificare che il numero di porta definito per l'application server sia abilitato a passare attraverso eventuali firewall in uso. Il numero di porta TCP (Transmission Control Protocol) del server applicazioni predefinito è 8445.

Configurare i permessi di accesso al plug-in

È possibile configurare le autorizzazioni di accesso per lo Storage Plugin per vCenter, che include utenti, ruoli e privilegi.

Esaminare i privilegi vSphere richiesti

Per accedere al plug-in nel client vSphere, è necessario assegnare un ruolo con i privilegi vSphere appropriati. Gli utenti con il privilegio vSphere "Configura datastore" hanno accesso in lettura/scrittura al plug-in, mentre gli utenti con il privilegio "Sfoglia datastore" hanno accesso in sola lettura. Se un utente non dispone di questi privilegi, il plug-in visualizza il messaggio "privilegi insufficienti".

Tipo di accesso al plug-in	È richiesto il privilegio vSphere
Lettura/scrittura (configurazione)	Datastore.Configure
Sola lettura (visualizzazione)	Datastore.Browse

Configurare i ruoli di Storage Administrator

Per fornire privilegi di lettura/scrittura agli utenti dei plug-in, è possibile creare, clonare o modificare un ruolo. Per ulteriori informazioni sulla configurazione dei ruoli nel client vSphere, consultare il seguente argomento nel VMware Doc Center:

- "Creare un ruolo personalizzato"

Accedere alle azioni dei ruoli

1. Dalla home page di vSphere Client, selezionare **Administrator** dall'area di controllo degli accessi.

2. Fare clic su **Roles** nell'area di controllo degli accessi.
3. Eseguire una delle seguenti operazioni:
   - **Crea nuovo ruolo**: Fare clic sull'icona dell'azione **Crea ruolo**.
   - **Clone role**: Selezionare un ruolo esistente e fare clic sull'icona dell'azione **Clone role**.
   - **Modifica ruolo esistente**: Selezionare un ruolo esistente e fare clic sull'icona dell'azione **Modifica ruolo**.

> Il ruolo di amministratore non è modificabile.

Viene visualizzata la procedura guidata appropriata, a seconda della selezione precedente.

Creare un nuovo ruolo

1. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

2. Assegnare altri privilegi all'elenco, se necessario, quindi fare clic su **Avanti**.
3. Assegnare un nome al ruolo e fornire una descrizione.
4. Fare clic su **fine**.

Clonare un ruolo

1. Assegnare un nome al ruolo e fornire una descrizione.
2. Fare clic su **OK** per terminare la procedura guidata.
3. Selezionare il ruolo clonato dall'elenco, quindi fare clic su **Edit role** (Modifica ruolo).
4. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

5. Fare clic su **Avanti**.
6. Aggiornare il nome e la descrizione, se necessario.
7. Fare clic su **fine**.

Modificare un ruolo esistente

1. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

2. Fare clic su **Avanti**.
3. Aggiornare il nome o la descrizione, se necessario.
4. Fare clic su **fine**.

Impostare le autorizzazioni per vCenter Server Appliance

Dopo aver impostato i privilegi per un ruolo, è necessario aggiungere un'autorizzazione all'appliance vCenter Server. Questa autorizzazione consente a un determinato utente o gruppo di accedere al plug-in.

1. Dall'elenco a discesa del menu, selezionare **hosts and Clusters** (host e cluster).
2. Selezionare **vCenter Server Appliance** dall'area di controllo degli accessi.
3. Fare clic sulla scheda **Permissions**.
4. Fare clic sull'icona dell'azione **Add Permission**.
5. Selezionare il dominio e l'utente/gruppo appropriati.
6. Selezionare il ruolo creato che consente il privilegio del plug-in di lettura/scrittura.
7. Attivare l'opzione **propaga ai figli**, se necessario.
8. Fare clic su **OK**.

> È possibile selezionare un'autorizzazione esistente e modificarla per utilizzare il ruolo creato. **Tuttavia, tenere presente che il ruolo deve avere gli stessi privilegi insieme ai privilegi del plug-in di lettura/scrittura per evitare una regressione dei permessi.**

Per accedere al plug-in, è necessario accedere a vSphere Client con l'account utente che dispone dei privilegi di lettura/scrittura per il plug-in.

Per ulteriori informazioni sulla gestione delle autorizzazioni, consultare i seguenti argomenti in VMware Doc Center:

- "Gestione delle autorizzazioni per i componenti vCenter"
- "Best practice per ruoli e autorizzazioni"

Accedere e navigare nel plug-in di storage per vCenter

È possibile accedere allo Storage Plugin per vCenter per navigare nell'interfaccia utente.

1. Prima di accedere al plug-in, assicurarsi di utilizzare uno dei seguenti browser:
   - Google Chrome 89 o versione successiva
   - Mozilla Firefox 80 o versione successiva
   - Microsoft Edge 90 o versione successiva
2. Accedere al client vSphere con l'account utente che dispone dei privilegi di lettura/scrittura per il plug-in.
3. Dalla home page del client vSphere, fare clic su **plug-in di storage SANtricity per vCenter**.

   Il plug-in si apre all'interno di una finestra del client vSphere. La pagina principale del plugin si apre su **Manage-All**.

4. Accedi alle attività di gestione dello storage dalla barra laterale di navigazione a sinistra:
   - **Gestisci** – rileva gli array di storage nella tua rete, apri System Manager per un array, importa le impostazioni da un array a più array, gestisci i gruppi di array, aggiorna il software del sistema operativo e esegui il provisioning dello storage.
   - **Certificate Management** – Gestisci i certificati per l'autenticazione tra browser e client.
   - **Operazioni** – consente di visualizzare l'avanzamento delle operazioni batch, ad esempio

l'importazione di impostazioni da un array a un altro.

- **Supporto** – Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

> Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.

Rilevare gli array di storage nel plug-in

Per visualizzare e gestire le risorse di storage, è necessario utilizzare l'interfaccia Storage Plugin for vCenter per rilevare gli indirizzi IP degli array nella rete.

Prima di iniziare

- È necessario conoscere gli indirizzi IP di rete (o l'intervallo di indirizzi) degli array controller.
- Gli array di storage devono essere configurati e configurati correttamente, nonché conoscere le credenziali di accesso (nome utente e password).

Fase 1: Inserire gli indirizzi di rete per il rilevamento

Fasi

1. Dalla pagina Gestisci, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Immetti intervallo indirizzi di rete.

2. Effettuare una delle seguenti operazioni:
   - Per rilevare un array, selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage), quindi immettere l'indirizzo IP di uno dei controller dell'array di storage.
   - Per rilevare più array di storage, selezionare il pulsante di opzione **Discover all storage array in a network range** (rileva tutti gli array di storage all'interno di un intervallo di rete), quindi immettere l'indirizzo di rete iniziale e l'indirizzo di rete finale per eseguire la ricerca nella sottorete locale.

3. Fare clic su **Avvia rilevamento**.

   All'inizio del processo di rilevamento, la finestra di dialogo visualizza gli array di storage rilevati. Il completamento del processo di rilevamento potrebbe richiedere alcuni minuti.

   Se non vengono rilevati array gestibili, verificare che gli array di storage siano collegati correttamente alla rete e che gli indirizzi assegnati rientrino nell'intervallo. Fare clic su **New Discovery Parameters** (nuovi parametri di rilevamento) per tornare alla pagina Add/Discover (Aggiungi/rileva).

4. Selezionare la casella di controllo accanto a qualsiasi array di storage che si desidera aggiungere al dominio di gestione.

   Il sistema esegue un controllo delle credenziali su ogni array che si sta aggiungendo al dominio di gestione. Prima di procedere, potrebbe essere necessario risolvere eventuali problemi relativi ai certificati non attendibili.

5. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

   Se gli array di storage dispongono di certificati validi, passare a. Fase 3: Fornire le password.

   Se gli array di storage non dispongono di certificati validi, viene visualizzata la finestra di dialogo Risolvi certificati autofirmati. Passare a. Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento.

   Se si desidera importare i certificati firmati dalla CA, annullare la procedura guidata di rilevamento e fare

clic su **Certificate Management** (Gestione certificati) nel pannello a sinistra. Per ulteriori informazioni, consultare la guida in linea.

Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento

È necessario risolvere eventuali problemi di certificato prima di procedere con il processo di rilevamento.

1. Se viene visualizzata la finestra di dialogo Risolvi certificati autofirmati, esaminare le informazioni visualizzate per i certificati non attendibili. Per ulteriori informazioni, fare clic sui puntini di sospensione all'estremità della tabella e selezionare **View** (Visualizza) dal menu a comparsa.
2. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, fare clic su **Avanti**, quindi su **Sì** per confermare e passare alla finestra di dialogo successiva della procedura guidata. I certificati autofirmati sono contrassegnati come attendibili e gli array di storage vengono aggiunti al plug-in.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una.
3. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

Fase 3: Fornire le password

Come ultimo passaggio per il rilevamento, è necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

1. Per ogni array rilevato, inserire la password admin nei campi.
2. Fare clic su **fine**.

   Il sistema può impiegare diversi minuti per connettersi agli array di storage specificati. Al termine del processo, gli array di storage vengono aggiunti al dominio di gestione e associati al gruppo selezionato (se specificato).

Eseguire il provisioning dello storage nel plug-in

Per eseguire il provisioning dello storage, è necessario creare volumi, assegnare volumi agli host e assegnare volumi agli archivi dati.

Fase 1: Creazione di volumi

I volumi sono container di dati che gestiscono e organizzano lo spazio di storage sull'array di storage. È possibile creare volumi dalla capacità di storage disponibile sull'array di storage, che consente di organizzare le risorse del sistema. Il concetto di "volumi" è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso rapido.

I volumi sono l'unico livello di dati visibile agli host. In un ambiente SAN, i volumi vengono mappati ai LUN (Logical Unit Number). Queste LUN conservano i dati utente accessibili mediante uno o più protocolli di accesso host supportati dallo storage array.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › Volumes** (Crea[volumi]).

Viene visualizzata la finestra di dialogo Select host (Seleziona host).

4. Dall'elenco a discesa, selezionare un host o un cluster host specifico al quale assegnare i volumi oppure scegliere di assegnare l'host o il cluster host in un secondo momento.
5. Per continuare la sequenza di creazione del volume per l'host o il cluster host selezionato, fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro). Un carico di lavoro contiene volumi con caratteristiche simili, ottimizzati in base al tipo di applicazione supportata dal carico di lavoro. È possibile definire un carico di lavoro o selezionare i carichi di lavoro esistenti.

6. Effettuare una delle seguenti operazioni:
   - Selezionare l'opzione **Create Volumes for a existing workload** (Crea volumi per un carico di lavoro esistente), quindi selezionare il carico di lavoro dall'elenco a discesa.
   - Selezionare l'opzione **Create a new workload** (Crea nuovo carico di lavoro) per definire un nuovo carico di lavoro per un'applicazione supportata o per altre applicazioni, quindi attenersi alla seguente procedura:
     i. Dall'elenco a discesa, selezionare il nome dell'applicazione per cui si desidera creare il nuovo workload. Selezionare una delle "altre" voci se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.
     ii. Immettere un nome per il carico di lavoro che si desidera creare.
7. Fare clic su **Avanti**. Se il carico di lavoro è associato a un tipo di applicazione supportato, inserire le informazioni richieste; in caso contrario, passare alla fase successiva.

   Viene visualizzata la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi). In questa finestra di dialogo vengono creati volumi da pool o gruppi di volumi idonei. Per ciascun pool e gruppo di volumi idonei, vengono visualizzati il numero di dischi disponibili e la capacità libera totale. Per alcuni carichi di lavoro specifici dell'applicazione, ciascun pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e la capacità libera rimanente in GiB. Per gli altri carichi di lavoro, la capacità proposta viene visualizzata quando si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

8. Prima di iniziare ad aggiungere volumi, leggere le linee guida riportate nella seguente tabella.

Campo	Descrizione
Capacità libera	Poiché i volumi vengono creati da pool o gruppi di volumi, il pool o il gruppo di volumi selezionato deve disporre di capacità libera sufficiente.

Campo	Descrizione
Data Assurance (da)	Per creare un volume abilitato da, la connessione host che si intende utilizzare deve supportare da. • Se si desidera creare un volume abilitato da, selezionare un pool o un gruppo di volumi che supporti da (cercare **Sì** accanto a "da" nella tabella dei candidati del pool e del gruppo di volumi). • Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi. LA protezione DA verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. La selezione di un pool o di un gruppo di volumi da-capable per il nuovo volume garantisce il rilevamento e la correzione degli errori. • Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.
Sicurezza dei dischi	Per creare un volume abilitato alla protezione, è necessario creare una chiave di sicurezza per l'array di storage. • Se si desidera creare un volume abilitato alla protezione, selezionare un pool o un gruppo di volumi che supporti la protezione (cercare **Sì** accanto a "abilitato alla protezione" nella tabella dei candidati del gruppo di volumi e del pool). • Le funzionalità di sicurezza dei dischi vengono presentate a livello di pool e gruppo di volumi. I dischi con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Un disco abilitato alla sicurezza crittografa i dati durante la scrittura e decrta i dati durante la lettura utilizzando una chiave di crittografia univoca. • Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
Provisioning delle risorse	Per creare un volume con provisioning di risorse, tutti i dischi devono essere dischi NVMe con l'opzione Deallocated o Unwritten Logical Block Error (DULBE).

9. Scegliere una di queste azioni a seconda che sia stato selezionato "Altro" o un carico di lavoro specifico dell'applicazione nella fase precedente:

   - **Altro** – fare clic su **Aggiungi nuovo volume** in ciascun pool o gruppo di volumi che si desidera utilizzare per creare uno o più volumi.
   - **Carico di lavoro specifico dell'applicazione** – fare clic su **Avanti** per accettare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato.

     Vengono visualizzati i seguenti campi.

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. La capacità in un pool viene allocata in incrementi di 4-GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Tipo di volume	Se si seleziona "carico di lavoro specifico dell'applicazione", viene visualizzato il campo Volume Type (tipo di volume). Indica il tipo di volume creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • da 512 a 512 byte • 4K – 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** – il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi con cache SSD**: È possibile specificare una dimensione dei segmenti 4 KiB per i volumi con cache SSD. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** – il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi del pool o del gruppo di volumi sono compatibili con la crittografia. Drive Security impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione Drive Security è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

10. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti**.
11. Nell'ultimo passaggio, esaminare un riepilogo dei volumi che si intende creare e apportare le modifiche necessarie. Per apportare modifiche, fare clic su **Indietro**. Quando si è soddisfatti della configurazione del volume, fare clic su **fine**.

Fase 2: Creazione dell'accesso host e assegnazione dei volumi

È possibile creare un host automaticamente o manualmente:

- **Automatico** — la creazione automatica dell'host per gli host basati su SCSI (non NVMe-of) viene avviata dall'HCA (host Context Agent). HCA è un'utility che è possibile installare su ciascun host collegato allo storage array. Ogni host su cui è installato l'HCA invia le informazioni di configurazione ai controller degli array di storage attraverso il percorso i/O. In base alle informazioni sull'host, i controller creano automaticamente l'host e le porte host associate e impostano il tipo di host. Se necessario, è possibile apportare ulteriori modifiche alla configurazione dell'host. Dopo che l'HCA ha eseguito il rilevamento automatico, l'host viene configurato automaticamente con i seguenti attributi:
  - Il nome host derivato dal nome di sistema dell'host.
  - Le porte di identificazione host associate all'host.
  - Il tipo di sistema operativo host dell'host.

> Il software host Context Agent per Linux e Windows è disponibile all'interno del sito "Supporto NetApp - Download".

> Gli host vengono creati come host standalone; l'HCA non crea o aggiunge automaticamente ai cluster di host.

- **Manuale** – durante la creazione manuale dell'host, è possibile associare gli identificatori delle porte host selezionandoli da un elenco o inserendoli manualmente. Dopo aver creato un host, è possibile assegnarvi dei volumi o aggiungerlo a un cluster host se si intende condividere l'accesso ai volumi.

Utilizzo di HCA per rilevare automaticamente l'host

È possibile consentire all'HCA (host Context Agent) di rilevare automaticamente gli host, quindi verificare che le informazioni siano corrette.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare **Storage › Hosts** (Storage[host]).

   La tabella elenca gli host creati automaticamente.

4. Verificare che le informazioni fornite dall'HCA siano corrette (nome, tipo di host, identificatori della porta host).
5. Per modificare le informazioni, selezionare l'host, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

Creazione manuale dell'host

Prima di iniziare

Leggi le seguenti linee guida:

- È necessario aver già aggiunto o rilevato gli array di storage all'interno dell'ambiente.
- È necessario definire le porte di identificazione host associate all'host.
- Assicurarsi di fornire lo stesso nome del nome di sistema assegnato all'host.
- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Fare clic sul **Create › host** (Crea[host]).

   Viene visualizzata la finestra di dialogo Create host (Crea host).

4. Selezionare le impostazioni per l'host in base alle esigenze.

Campo	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare il sistema operativo in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia host	(Facoltativo) se si dispone di più tipi di interfaccia host supportati sull'array di storage, selezionare il tipo di interfaccia host che si desidera utilizzare.

Campo	Descrizione
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare l'interfaccia i/o** — in genere, le porte host devono essere state registrate ed essere disponibili dall'elenco a discesa. È possibile selezionare gli identificatori della porta host dall'elenco. • **Aggiunta manuale** — se un identificatore di porta host non viene visualizzato nell'elenco, significa che la porta host non ha effettuato l'accesso. È possibile utilizzare un'utility HBA o l'utility iSCSI Initiator per individuare gli identificatori delle porte host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dall'utility (uno alla volta) nel campo host ports (Porte host). È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori associati all'host. Ciascun identificatore viene visualizzato nel campo host ports (Porte host). Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto.
Impostare CHAP Initiator secret	(Facoltativo) se si seleziona o si immette manualmente una porta host con un IQN iSCSI e si desidera richiedere a un host che tenta di accedere all'array di storage per l'autenticazione mediante il protocollo CHAP (Challenge Handshake Authentication Protocol), selezionare la casella di controllo **Set CHAP Initiator secret** (Imposta CHAP initiator secret). Per ogni porta host iSCSI selezionata o inserita manualmente, procedere come segue: • Immettere lo stesso segreto CHAP impostato su ciascun iniziatore host iSCSI per l'autenticazione CHAP. Se si utilizza l'autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di validarsi nell'array di storage e a un array di storage di validarsi nell'host), è necessario impostare anche il segreto CHAP per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lasciare vuoto il campo se non si richiede l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato è CHAP.

5. Fare clic su **Create** (Crea).
6. Per aggiornare le informazioni sull'host, selezionare l'host dalla tabella e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Una volta creato correttamente l'host, il sistema crea un nome predefinito per ciascuna porta host configurata per l'host (etichetta utente). L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per l'host IPT è `IPT_1`.

7. Quindi, è necessario assegnare un volume a un host o a un cluster di host in modo che possa essere utilizzato per le operazioni di i/O. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

8. Selezionare l'host o il cluster host a cui si desidera assegnare i volumi, quindi fare clic su **Assign Volumes**

(Assegna volumi).

Viene visualizzata una finestra di dialogo che elenca tutti i volumi che è possibile assegnare. È possibile ordinare qualsiasi colonna o digitare qualcosa nella casella Filter (filtro) per semplificare la ricerca di volumi specifici.

9. Selezionare la casella di controllo accanto a ciascun volume che si desidera assegnare oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
10. Fare clic su **Assegna** per completare l'operazione.

    Il sistema esegue le seguenti operazioni:

    - Il volume assegnato riceve il successivo numero LUN disponibile. L'host utilizza il numero LUN per accedere al volume.
    - Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host. Se applicabile, il volume di accesso configurato in fabbrica viene visualizzato anche negli elenchi dei volumi associati all'host.

Fase 3: Creazione di un datastore in vSphere Client

Per creare un datastore nel client vSphere, vedere "Creare un datastore VMFS nel client vSphere" Argomento di VMware Doc Center.

Aumentare la capacità del datastore esistente aumentando la capacità del volume

È possibile aumentare la capacità riportata (la capacità riportata agli host) di un volume utilizzando la capacità libera disponibile nel pool o nel gruppo di volumi.

Prima di iniziare

Assicurarsi che:

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associati al volume.
- Il volume è ottimale e non in alcun stato di modifica.
- Nel volume non sono in uso dischi hot spare. (Si applica solo ai volumi nei gruppi di volumi).

> L'aumento della capacità di un volume è supportato solo su alcuni sistemi operativi. Se si aumenta la capacità del volume su un sistema operativo host che non supporta l'espansione LUN, la capacità espansa non è utilizzabile e non è possibile ripristinare la capacità del volume originale.

Fasi

1. Accedere al plug-in in vSphere Client.
2. All'interno del plug-in, selezionare l'array di storage desiderato.
3. Fare clic su **Provisioning** e selezionare **Manage Volumes** (Gestisci volumi).
4. Selezionare il volume per il quale si desidera aumentare la capacità, quindi selezionare **aumenta capacità**.

   Viene visualizzata la finestra di dialogo Conferma aumento capacità.

5. Selezionare **Sì** per continuare.

Viene visualizzata la finestra di dialogo aumenta capacità riportata.

Questa finestra di dialogo visualizza la capacità corrente del volume riportata e la capacità libera disponibile nel gruppo di volumi o pool associato al volume.

6. Utilizzare la casella **aumenta capacità segnalata aggiungendo…** per aggiungere capacità alla capacità corrente disponibile indicata. È possibile modificare il valore della capacità in modo che venga visualizzato in megibyte (MiB), gibibyte (GiB) o tebibyte (TIB).
7. Fare clic su **aumenta**.
8. Visualizzare il pannello Recent Tasks (attività recenti) per l'avanzamento dell'operazione di aumento della capacità attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.
9. Una volta completata la capacità del volume, è necessario aumentare manualmente le dimensioni VMFS in modo che corrispondano come descritto nella "Aumentare la capacità del datastore VMFS nel client vSphere" Argomento di VMware Doc Center.

Aumentare la capacità del datastore esistente aggiungendo volumi

1. È possibile aumentare la capacità di un datastore aggiungendo volumi. Seguire la procedura descritta in Fase 1: Creazione di volumi.
2. Quindi, assegnare i volumi all'host desiderato per aumentare la capacità del datastore.

   Vedere "Aumentare la capacità del datastore VMFS nel client vSphere" Per ulteriori informazioni, consultare l'argomento di VMware Doc Center.

Visualizzare lo stato

È possibile visualizzare lo stato del sistema dal plugin Storage per vCenter o dal client vSphere.

1. Aprire il plug-in dal client vSphere.
2. Visualizzare lo stato dai seguenti pannelli:
   - **Stato array di storage** — Vai al pannello **Gestisci-tutto**. Per ogni array rilevato, la riga fornisce una colonna Status (Stato).
   - **Operazioni in corso** — fare clic su **operazioni** sul pannello laterale per visualizzare tutte le attività in esecuzione a lungo, ad esempio l'importazione delle impostazioni. È inoltre possibile visualizzare le operazioni a esecuzione prolungata dall'elenco a discesa Provisioning. Per ciascuna operazione elencata nella finestra di dialogo Operations in Progress (operazioni in corso), vengono visualizzate una percentuale di completamento e il tempo stimato rimanente per completare l'operazione. In alcuni casi, è possibile interrompere un'operazione o posizionarla con priorità più alta o più bassa. Se lo si desidera, utilizzare i collegamenti nella colonna Actions (azioni) per interrompere o modificare la priorità di un'operazione.

> Leggere tutto il testo di avviso fornito nelle finestre di dialogo, in particolare quando si interrompe un'operazione.

Le operazioni che potrebbero essere visualizzate per il plug-in sono elencate nella seguente tabella. È possibile che nell'interfaccia di System Manager vengano visualizzate operazioni aggiuntive.

Operazione	Stato possibile dell'operazione	Azioni da intraprendere
Creazione di volumi (solo volumi thick pool superiori a 64 TiB)	In corso	nessuno
Eliminazione del volume (solo volumi thick pool superiori a 64 TiB)	In corso	nessuno
Aggiungere capacità al pool o al gruppo di volumi	In corso	nessuno
Modificare un livello RAID per un volume	In corso	nessuno
Ridurre la capacità di un pool	In corso	nessuno
Verificare il tempo rimanente per un'operazione con formato di disponibilità istantanea (IAF) per i volumi del pool	In corso	nessuno
Controllare la ridondanza dei dati di un gruppo di volumi	In corso	nessuno
Inizializzare un volume	In corso	nessuno
Aumentare la capacità di un volume	In corso	nessuno
Modificare le dimensioni dei segmenti di un volume	In corso	nessuno

Gestire i certificati

Panoramica dei certificati

Gestione dei certificati nel plug-in di storage per vCenter consente di creare richieste di firma dei certificati (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Utilizzando Storage Plugin per vCenter, è possibile gestire i certificati per il browser su un sistema di gestione host e i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili.

Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

Sebbene i certificati firmati dalla CA forniscano una migliore protezione di sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), richiedono anche tariffe che possono essere costose se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

Certificati firmati

Un certificato firmato viene convalidato da un'autorità di certificazione (CA), un'organizzazione di terze parti fidata. I certificati firmati includono i dettagli sul proprietario dell'entità (in genere, un server o un sito Web), la data di emissione e scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando si apre un browser e si inserisce un indirizzo Web, il sistema esegue un processo di verifica dei certificati in background per determinare se si sta effettuando la connessione a un sito Web che include un certificato valido firmato dalla CA. In genere, un sito protetto con un certificato firmato include un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se si tenta di connettersi a un sito Web che non contiene un certificato firmato dalla CA, il browser visualizza un avviso che indica che il sito non è sicuro.

La CA esegue le operazioni necessarie per verificare l'identità dell'utente durante il processo dell'applicazione. Potrebbero inviare un'e-mail all'azienda registrata, verificare l'indirizzo aziendale ed eseguire una verifica HTTP o DNS. Una volta completato il processo applicativo, la CA invia i file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di attendibilità, come segue:

- **Root** — nella parte superiore della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedio** — i certificati intermedi si disconnettono dalla radice. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
- **Server** — nella parte inferiore della catena si trova il certificato del server, che identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di uno storage array richiede un certificato server separato.

Certificati autofirmati

Ogni controller dell'array di storage include un certificato preinstallato e autofirmato. Un certificato autofirmato è simile a un certificato firmato dalla CA, ad eccezione del fatto che è convalidato dal proprietario dell'entità anziché da una terza parte. Come un certificato firmato dalla CA, un certificato autofirmato contiene una propria chiave privata e garantisce inoltre che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client.

I certificati autofirmati non sono "attendibili" dai browser. Ogni volta che si tenta di connettersi a un sito Web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

Certificato di gestione

Quando si apre il plug-in, il browser tenta di verificare che l'host di gestione sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. È inoltre possibile ottenere certificati digitali firmati da una CA, in modo da non visualizzare più il messaggio di avviso.

Certificati attendibili

Durante una sessione di plug-in, potrebbero essere visualizzati ulteriori messaggi di sicurezza quando si tenta di accedere a un controller che non dispone di un certificato firmato dalla CA. In questo caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati dalla CA per i controller in modo che il plug-in possa autenticare le richieste dei client in entrata da questi controller.

USA certificati firmati dalla CA

È possibile ottenere e importare certificati con firma CA per un accesso sicuro al sistema di gestione che ospita lo Storage Plugin per vCenter.

L'utilizzo dei certificati firmati dalla CA è una procedura in tre fasi:

- Fase 1: Completare un file CSR.
- Fase 2: Inviare il file CSR.
- Fase 3: Importazione dei certificati di gestione.

Fase 1: Completare un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui è in esecuzione il plug-in. In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare il file CSR.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **completa CSR**.
3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città in cui si trova il sistema host o l'azienda.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova il sistema host o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.
4. Immettere le seguenti informazioni sul sistema host in cui è in esecuzione il plug-in:
   - **Nome comune** — l'indirizzo IP o il nome DNS del sistema host in cui è in esecuzione il plug-in. Assicurarsi che questo indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere al plug-in nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole.
   - **Nomi DNS alternativi** — se il nome comune è un nome DNS, immettere eventuali nomi DNS aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurarsi che le informazioni sull'host siano corrette. In caso contrario, i certificati restituiti dalla CA non avranno esito positivo quando si tenta di importarli.

6. Fare clic su **fine**.

Fase 2: Inviare il file CSR

Dopo aver creato un file CSR (Certificate Signing Request), il file CSR generato viene inviato a una CA per ricevere certificati di gestione firmati per il sistema che ospita il plug-in.

I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: .Pem, .crt, .cer o .key.

Fasi

1. Individuare il file CSR scaricato.

   La posizione della cartella del download dipende dal browser in uso.

2. Inviare il file CSR a una CA (ad esempio, VeriSign o DigiCert) e richiedere certificati firmati in formato PEM.

   Dopo aver inviato un file CSR alla CA, NON rigenerare un altro file CSR.

Ogni volta che si genera una CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi del sistema. Quando si ricevono i certificati firmati e li si importano, il sistema garantisce che sia la chiave privata che la chiave pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno ed è necessario richiedere nuovi certificati alla CA.

Fase 3: Importazione dei certificati di gestione

Una volta ricevuti i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui è installato il plug-in.

Prima di iniziare

- È necessario disporre dei certificati firmati dalla CA. Questi file includono il certificato di origine, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: Il certificato root, uno o più certificati intermedi e il certificato del server. È possibile utilizzare l'utility Windows certmgr per decomprimere i file (fare clic con il pulsante destro del mouse e selezionare **All Tasks › Export**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- È necessario copiare i file dei certificati nel sistema host in cui è in esecuzione il plug-in.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **Importa**.

   Viene visualizzata una finestra di dialogo per l'importazione dei file dei certificati.

3. Fare clic su **Browse** (Sfoglia) per selezionare prima i file dei certificati root e intermedi, quindi selezionare il certificato del server. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultato

I file vengono caricati e validati. Le informazioni sul certificato vengono visualizzate nella pagina Gestione certificati.

Reimpostare i certificati di gestione

Per il sistema di gestione che ospita lo Storage Plugin per vCenter, è possibile riportare il certificato di gestione allo stato originale autofirmato.

A proposito di questa attività

Questa attività elimina il certificato di gestione corrente dal sistema host in cui è in esecuzione Storage Plugin per vCenter. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Management**, selezionare **Reset**.

   Viene visualizzata la finestra di dialogo Conferma ripristino certificato di gestione.

3. Digitare reset nel campo, quindi fare clic su **Reset**.

   Dopo l'aggiornamento del browser, il browser potrebbe bloccare l'accesso al sito di destinazione e segnalare che il sito utilizza HTTP Strict Transport Security. Questa condizione si verifica quando si torna ai certificati autofirmati. Per eliminare la condizione che sta bloccando l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultato

Il sistema torna a utilizzare il certificato autofirmato dal server. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Importare certificati per gli array

Se necessario, è possibile importare i certificati per gli array di storage in modo che possano autenticarsi con il sistema che ospita lo Storage Plugin per vCenter. I certificati possono essere firmati da un'autorità di certificazione (CA) o autofirmati.

Prima di iniziare

Se si importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.

4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

   Il certificato viene caricato e validato.

Visualizzare i certificati

È possibile visualizzare informazioni riepilogative per un certificato, che includono l'organizzazione che utilizza il certificato, l'autorità che ha emesso il certificato, il periodo di validità e le impronte digitali (identificatori univoci).

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Per visualizzare ulteriori informazioni su un certificato, selezionare la relativa riga, selezionare i puntini di sospensione alla fine della riga, quindi fare clic su **Visualizza** o **Esporta**.

Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

Prima di iniziare

Per aprire il file esportato, è necessario disporre di un'applicazione per il visualizzatore dei certificati.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Selezionare un certificato dalla pagina, quindi fare clic sui puntini di sospensione alla fine della riga.
4. Fare clic su **Esporta**, quindi salvare il file del certificato.
5. Aprire il file nell'applicazione di visualizzazione dei certificati.

Eliminare i certificati attendibili

È possibile eliminare uno o più certificati non più necessari, ad esempio un certificato

scaduto.

Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.

> Tenere presente che l'eliminazione di un certificato root o intermedio può influire su più array di storage, poiché questi array possono condividere gli stessi file di certificato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.
3. Selezionare uno o più certificati nella tabella, quindi fare clic su **Elimina**.

   > La funzione Elimina non è disponibile per i certificati preinstallati.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

4. Confermare l'eliminazione, quindi fare clic su **Delete** (Elimina).

   Il certificato viene rimosso dalla tabella.

Risolvi i certificati non attendibili

Dalla pagina Certificate (certificato), è possibile risolvere i certificati non attendibili importando un certificato autofirmato dall'array di storage o importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

Prima di iniziare

Se si intende importare un certificato firmato dalla CA, assicurarsi che:

- È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
- La CA ha restituito file di certificato attendibili.
- I file dei certificati sono disponibili nel sistema locale.

A proposito di questa attività

I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura al plug-in, ma la connessione non viene confermata come sicura. Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti o revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.
4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

   Il certificato viene caricato e validato.

Gestire gli array

Panoramica sulla gestione degli array

Utilizzare la funzione Add/Discover per trovare e aggiungere gli array di storage che si desidera gestire nel plug-in Storage per vCenter. Dalla pagina Manage (Gestione), è possibile rinominare, rimuovere e fornire nuove password per gli array rilevati.

Considerazioni per il rilevamento degli array

Affinché il plug-in visualizzi e gestisca le risorse di storage, è necessario individuare gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare e aggiungere un singolo array o più array.

Array di storage multipli

Se si sceglie di rilevare più array, immettere un intervallo di indirizzi IP di rete e il sistema tenta di stabilire connessioni individuali a ciascun indirizzo IP dell'intervallo. Qualsiasi array di storage raggiunto correttamente viene visualizzato nel plug-in ed è possibile aggiungerlo al dominio di gestione.

Singolo storage array

Se si sceglie di rilevare un singolo array, immettere l'indirizzo IP singolo per uno dei controller nell'array di storage e aggiungerlo al dominio di gestione.

> Il plug-in rileva e visualizza solo il singolo indirizzo IP o indirizzo IP all'interno di un intervallo assegnato a un controller. Se a questi controller sono assegnati controller alternativi o indirizzi IP che non rientrano in questo singolo indirizzo IP o intervallo di indirizzi IP, il plug-in non li rileva o li visualizza. Tuttavia, una volta aggiunto lo storage array, tutti gli indirizzi IP associati vengono rilevati e visualizzati nella vista Manage (Gestione).

Credenziali dell'utente

Specificare la password di amministratore per ciascun array di storage che si desidera aggiungere.

Certificati

Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage rilevati stiano utilizzando certificati da un'origine attendibile. Il sistema utilizza due tipi di autenticazione basata su certificati per tutte le connessioni stabilite con il browser:

- **Certificati attendibili** — potrebbe essere necessario installare altri certificati attendibili forniti dall'autorità di certificazione se uno o entrambi i certificati del controller sono scaduti, revocati o mancanti nella relativa

catena.

- **Certificati autofirmati** — gli array possono anche utilizzare certificati autofirmati. Se si tenta di rilevare gli array senza importare certificati firmati, il plug-in fornisce un'ulteriore fase che consente di accettare il certificato autofirmato. Il certificato autofirmato dell'array di storage viene contrassegnato come attendibile e l'array di storage viene aggiunto al plug-in. Se le connessioni all'array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia del certificato di sicurezza dell'array di storage prima di aggiungere l'array di storage al plug-in.

Stato dello storage array

Quando si apre Storage Plugin per vCenter, viene stabilita la comunicazione con ciascun array di storage e viene visualizzato lo stato di ciascun array di storage.

Dalla pagina **Gestisci - tutto**, è possibile visualizzare lo stato dello storage array e lo stato della connessione dello storage array.

Stato	Indica
Ottimale	Lo storage array si trova in uno stato ottimale. Non ci sono problemi di certificato e la password è valida.
Password non valida	È stata fornita una password dello storage array non valida.
Certificato non attendibile	Una o più connessioni con lo storage array non sono attendibili perché il certificato HTTPS è autofirmato e non è stato importato oppure il certificato è firmato dalla CA e i certificati CA principali e intermedi non sono stati importati.
Richiede attenzione	Si è verificato un problema con lo storage array che richiede l'intervento dell'utente per correggerlo.
Blocco	Lo storage array si trova in uno stato bloccato.
Sconosciuto	Lo storage array non è mai stato contattato. Questo può accadere quando il plug-in si avvia e non è ancora entrato in contatto con lo storage array, oppure lo storage array non è in linea e non è mai stato contattato dall'avvio del plug-in.
Offline	Il plug-in aveva precedentemente contattato lo storage array, ma ora ha perso tutte le connessioni.

Interfaccia plug-in rispetto a System Manager

È possibile utilizzare Storage Plugin per vCenter per le attività operative di base sull'array di storage; tuttavia, in alcuni casi potrebbe essere necessario avviare System Manager per eseguire attività non disponibili nel plug-in.

System Manager è un'applicazione integrata nel controller dello storage array, collegata alla rete tramite una porta di gestione Ethernet. System Manager include tutte le funzioni basate su array.

La seguente tabella consente di decidere se utilizzare l'interfaccia del plug-in o l'interfaccia di System Manager per una specifica attività di array di storage.

Funzione	Interfaccia del plugin	Interfaccia di System Manager
Operazioni in batch su gruppi di array storage multipli	Sì	No Le operazioni vengono eseguite su un singolo array.
Aggiornamenti per il firmware del sistema operativo SANtricity	Sì. Uno o più array in un'operazione batch.	Sì. Solo array singolo.
Importa le impostazioni da un array a più array	Sì	No
Gestione dei cluster host e host (creazione, assegnazione di volumi, aggiornamento ed eliminazione)	Sì	Sì
Gestione di pool e gruppi di volumi (creazione, aggiornamento, attivazione della protezione ed eliminazione)	Sì	Sì
Gestione dei volumi (creazione, ridimensionamento, aggiornamento ed eliminazione)	Sì	Sì
Gestione della cache SSD (creazione, aggiornamento ed eliminazione)	Sì	Sì
Mirroring e gestione delle snapshot	No	Sì
Gestione dell'hardware (visualizzare lo stato del controller, configurare le connessioni delle porte, portare il controller offline, abilitare le hot spare, cancellare i dischi, ecc.)	No	Sì
Gestire gli avvisi (e-mail, SNMP e syslog)	No	Sì
Gestione delle chiavi di sicurezza	No	Sì
Gestione dei certificati per i controller	No	Sì
Gestione degli accessi per controller (LDAP, SAML, ecc.)	No	Sì
Gestione di AutoSupport	No	Sì

Scopri gli array di storage

Per visualizzare e gestire le risorse di storage nel plug-in Storage per vCenter, è necessario individuare gli indirizzi IP degli array nella rete.

Prima di iniziare

- È necessario conoscere gli indirizzi IP di rete (o l'intervallo di indirizzi) degli array controller.

- Gli array di storage devono essere configurati e configurati correttamente.
- Le password degli array di storage devono essere impostate utilizzando il riquadro Access Management di System Manager.

A proposito di questa attività

Il rilevamento degli array è una procedura a più fasi:

- Fase 1: Inserire gli indirizzi di rete per il rilevamento
- Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento
- Fase 3: Fornire le password

Fase 1: Inserire gli indirizzi di rete per il rilevamento

Come primo passo per il rilevamento degli array di storage, immettere un singolo indirizzo IP o un intervallo di indirizzi IP per la ricerca nella sottorete locale. La funzione Aggiungi/rileva consente di aprire una procedura guidata che guida l'utente nel processo di rilevamento.

Fasi

1. Dalla pagina **Gestisci**, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Immetti intervallo indirizzi di rete.

2. Effettuare una delle seguenti operazioni:
   - Per rilevare un array, selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage), quindi immettere l'indirizzo IP di uno dei controller dell'array di storage.
   - Per rilevare più array di storage, selezionare il pulsante di opzione **Discover all storage array in a network range** (rileva tutti gli array di storage all'interno di un intervallo di rete), quindi immettere l'indirizzo di rete iniziale e l'indirizzo di rete finale per eseguire la ricerca nella sottorete locale.
3. Fare clic su **Avvia rilevamento**.

   All'inizio del processo di rilevamento, la finestra di dialogo visualizza gli array di storage rilevati. Il completamento del processo di rilevamento potrebbe richiedere alcuni minuti.

   > Se non vengono rilevati array gestibili, verificare che gli array di storage siano collegati correttamente alla rete e che gli indirizzi assegnati rientrino nell'intervallo. Fare clic su **New Discovery Parameters** (nuovi parametri di rilevamento) per tornare alla pagina Add/Discover (Aggiungi/rileva).

4. Selezionare la casella di controllo accanto a qualsiasi array di storage che si desidera aggiungere al dominio di gestione.

   Il sistema esegue un controllo delle credenziali su ogni array che si sta aggiungendo al dominio di gestione. Prima di procedere, potrebbe essere necessario risolvere eventuali problemi relativi ai certificati non attendibili.

5. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.
6. Se gli array di storage dispongono di certificati validi, passare a. Fase 3: Fornire le password. Se uno degli array di storage non dispone di certificati validi, viene visualizzata la finestra di dialogo Risolvi certificati autofirmati; passare a. Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento. Se si desidera importare i certificati firmati dalla CA, annullare le finestre di dialogo di rilevamento e accedere a. "Importare certificati per gli array".

Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento

Se necessario, è necessario risolvere eventuali problemi di certificato prima di procedere con il processo di rilevamento.

Durante il rilevamento, se uno degli array di storage mostra lo stato "certificati non attendibili", viene visualizzata la finestra di dialogo Risolvi certificati autofirmati. In questa finestra di dialogo è possibile risolvere i certificati non attendibili oppure importare i certificati CA (vedere "Importare certificati per gli array").

Fasi

1. Se viene visualizzata la finestra di dialogo Risolvi certificati autofirmati, esaminare le informazioni visualizzate per i certificati non attendibili. Per ulteriori informazioni, fare clic sui puntini di sospensione all'estremità della tabella e selezionare **View** (Visualizza) dal menu a comparsa.
2. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, fare clic su **Avanti**, quindi su **Sì** per confermare e passare alla scheda successiva della procedura guidata. I certificati autofirmati verranno contrassegnati come attendibili e gli array di storage verranno aggiunti al plug-in.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una al plug-in.

Fase 3: Fornire le password

Come ultimo passaggio per il rilevamento, è necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

Fasi

1. Se in precedenza sono stati configurati gruppi per gli array, è possibile utilizzare il menu a discesa per selezionare un gruppo per gli array rilevati.
2. Per ogni array rilevato, inserire la password admin nei campi.
3. Fare clic su **fine**.

> Il sistema può impiegare diversi minuti per connettersi agli array di storage specificati.

Risultato

Gli array di storage vengono aggiunti al dominio di gestione e associati al gruppo selezionato (se specificato).

> È possibile utilizzare l'opzione Launch per aprire System Manager basato su browser per uno o più array di storage quando si desidera eseguire operazioni di gestione.

Rinominare l'array di storage

È possibile modificare il nome dello storage array visualizzato nella pagina Manage (Gestione) del plug-in Storage per vCenter.

Fasi

1. Nella pagina **Manage** (Gestisci), selezionare la casella di controllo a sinistra del nome dello storage array.
2. Selezionare i puntini di sospensione all'estrema destra della riga, quindi selezionare **Rename storage array** dal menu a comparsa.
3. Inserire il nuovo nome e fare clic su **Save** (Salva).

Modificare le password degli array di storage

È possibile aggiornare le password utilizzate per visualizzare e accedere agli array di storage nel plug-in Storage per vCenter.

Prima di iniziare

È necessario conoscere la password corrente per lo storage array, impostata in System Manager.

A proposito di questa attività

In questa attività, immettere la password corrente per un array di storage in modo da potervi accedere nel plug-in. Questo potrebbe essere necessario se la password dell'array è stata modificata in System Manager.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare uno o più array di storage.
2. Selezionare **operazioni non comuni › fornire password array di storage**.
3. Immettere la password o le password per ciascun array di storage, quindi fare clic su **Save** (Salva).

Rimuovere gli array di storage

È possibile rimuovere uno o più array di storage se non si desidera più gestirli dallo Storage Plugin per vCenter.

A proposito di questa attività

Non è possibile accedere a nessuno degli array di storage rimossi. Tuttavia, è possibile stabilire una connessione a uno degli array di storage rimossi puntando direttamente un browser all'indirizzo IP o al nome host.

La rimozione di uno storage array non influisce in alcun modo sullo storage array o sui relativi dati. Se uno storage array viene rimosso accidentalmente, può essere aggiunto di nuovo.

Fasi

1. Dalla pagina **Manage** (Gestione), selezionare uno o più array di storage da rimuovere.
2. Selezionare **operazioni non comuni › Rimuovi array di storage**.

   Lo storage array viene rimosso da tutte le viste dell'interfaccia del plugin.

Avviare System Manager

Per gestire un singolo array, utilizzare l'opzione di avvio per aprire Gestione di sistema di SANtricity in una nuova finestra del browser.

System Manager è un'applicazione integrata nel controller dello storage array, collegata alla rete tramite una porta di gestione Ethernet. System Manager include tutte le funzioni basate su array. Per accedere a System Manager, è necessario disporre di una connessione out-of-band a un client di gestione della rete con un browser Web.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare uno o più array di storage che si desidera gestire.
2. Fare clic su **Avvia**.

Il sistema apre una nuova scheda nel browser, quindi visualizza la pagina di accesso di System Manager.

3. Immettere il nome utente e la password, quindi fare clic su **Log in** (Accedi).

Importare le impostazioni

Panoramica delle impostazioni di importazione

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che consente di replicare le impostazioni di un singolo array di storage (l'origine) in più array (le destinazioni) nel plug-in Storage per vCenter.

Impostazioni disponibili per l'importazione

È possibile importare le seguenti configurazioni da un array a un altro:

- **Alerts** — metodi di avviso per inviare eventi importanti agli amministratori utilizzando la posta elettronica, un server syslog o un server SNMP.
- **AutoSupport** — funzionalità che monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.
- **Servizi di directory** — metodo di autenticazione dell'utente gestito tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.
- **Impostazioni di sistema** — configurazioni relative a:
  - Impostazioni di scansione dei supporti per un volume
  - Impostazioni SSD
  - Bilanciamento automatico del carico (non include il reporting sulla connettività host)
- **Configurazione dello storage** — configurazioni relative a:
  - Volumi (solo volumi thick e non repository)
  - Gruppi di volumi e pool
  - Assegnazioni dei dischi hot spare

Workflow di configurazione

Per importare le impostazioni, seguire questo flusso di lavoro:

1. Su uno storage array da utilizzare come origine, configurare le impostazioni utilizzando System Manager.
2. Sugli array di storage da utilizzare come destinazione, eseguire il backup della configurazione utilizzando System Manager.
3. Dall'interfaccia del plugin, accedere alla pagina **Manage** e importare le impostazioni.
4. Dalla pagina Operations (operazioni), esaminare i risultati dell'operazione Import Settings (Impostazioni di importazione).

Requisiti per la replica delle configurazioni di storage

Prima di importare una configurazione dello storage da uno storage array a un altro, esaminare i requisiti e le linee guida.

Shelf

- Gli shelf in cui risiedono i controller devono essere identici sugli array di origine e di destinazione.
- Gli shelf ID devono essere identici sugli array di origine e di destinazione.
- Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità (se il disco viene utilizzato nella configurazione, la posizione dei dischi inutilizzati non è importante).

Controller

- Il tipo di controller può essere diverso tra gli array di origine e di destinazione, ma il tipo di enclosure RBOD deve essere identico.
- L'HICS, incluse le funzionalità da dell'host, deve essere identico tra gli array di origine e di destinazione.
- L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
- Le impostazioni FDE non sono incluse nel processo di importazione.

Stato

- Gli array di destinazione devono essere nello stato ottimale.
- Non è necessario che l'array di origine sia nello stato ottimale.

Storage

- La capacità del disco può variare tra gli array di origine e di destinazione, a condizione che la capacità del volume sulla destinazione sia superiore a quella dell'origine. (Un array di destinazione potrebbe disporre di unità più recenti e di capacità maggiore che non sarebbero completamente configurate nei volumi dall'operazione di replica).
- Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.

Importare le impostazioni degli avvisi

È possibile importare configurazioni di avviso da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Gli avvisi vengono configurati in System Manager (**Impostazioni › Avvisi**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

È possibile selezionare avvisi e-mail, SNMP o syslog per l'operazione di importazione:

- **Avvisi via email** — Indirizzo del server di posta e indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — Nome di comunità e indirizzo IP per il server SNMP.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Email alerts** (Avvisi email), **SNMP alerts** (Avvisi SNMP) o **Syslog alerts** (Avvisi Syslog), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati per inviare avvisi agli amministratori tramite e-mail, SNMP o syslog.

Importa impostazioni AutoSupport

È possibile importare una configurazione AutoSupport da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- AutoSupport è configurato in Gestione sistema (**supporto › Centro di supporto**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Seleziona impostazioni, selezionare **AutoSupport**, quindi fare clic su **Avanti**.

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni AutoSupport dell'array di origine.

Importare le impostazioni dei servizi di directory

È possibile importare una configurazione di servizi di directory da un array di storage ad altri array di storage. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- I servizi di directory sono configurati in System Manager (**Impostazioni › Gestione accessi**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono il nome di dominio e l'URL di un server LDAP (Lightweight Directory

Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Directory Services** (servizi directory), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con gli stessi servizi di directory dell'array di origine.

Importare le impostazioni di sistema

È possibile importare le impostazioni di sistema da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Le impostazioni di sistema sono configurate in System Manager per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono le impostazioni di scansione dei supporti per un volume, le impostazioni SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **System** (sistema), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni di sistema dell'array di origine.

Importare le impostazioni di configurazione dello storage

È possibile importare la configurazione dello storage da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Lo storage viene configurato in System Manager per l'array di storage che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".
- Gli array di origine e di destinazione devono soddisfare i seguenti requisiti:
  - Gli shelf in cui risiedono i controller devono essere identici.
  - Gli ID degli shelf devono essere identici.
  - Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità.

    - Il tipo di enclosure RBOD deve essere identico.
    - L'HICS, incluse le funzionalità di Data Assurance dell'host, deve essere identico.
    - Gli array di destinazione devono essere nello stato ottimale.
    - La capacità del volume sull'array di destinazione è maggiore della capacità dell'array di origine.
- Hai compreso le seguenti restrizioni:
    - L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
    - Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.

A proposito di questa attività

Le impostazioni importate includono volumi configurati (solo volumi thick e non di repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Storage Configuration** (Configurazione archiviazione), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con la stessa configurazione dello storage dell'array di origine.

Gestire i gruppi di array

Panoramica dei gruppi di array

È possibile gestire l'infrastruttura fisica e virtualizzata nel plug-in di storage per vCenter

raggruppando un set di array di storage. È possibile raggruppare gli array di storage per semplificare l'esecuzione dei processi di monitoraggio o reporting.

Tipi di gruppi di array di storage:

- **Tutti i gruppi** — il gruppo tutti è il gruppo predefinito e include tutti gli array di storage rilevati nell'organizzazione. È possibile accedere al gruppo All dalla vista principale.
- **User-created group** — Un gruppo creato dall'utente include gli array di storage che si selezionano manualmente per aggiungere a quel gruppo. È possibile accedere ai gruppi creati dall'utente dalla vista principale.

Creare un gruppo di array di storage

È possibile creare gruppi di storage e quindi aggiungere array di storage ai gruppi. Il gruppo di storage definisce quali dischi forniscono lo storage che costituisce il volume.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Create storage array group** (Crea gruppo array di storage).
2. Nel campo **Nome**, digitare un nome per il nuovo gruppo.
3. Selezionare gli array di storage che si desidera aggiungere al nuovo gruppo.
4. Fare clic su **Create** (Crea).

Aggiungere array di storage al gruppo

È possibile aggiungere uno o più array di storage a un gruppo creato dall'utente.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo a cui si desidera aggiungere gli array di storage.
2. Selezionare **Manage Groups › Add storage array to group** (Gestisci gruppi[Aggiungi array di storage al gruppo]).
3. Selezionare gli array di storage che si desidera aggiungere al gruppo.
4. Fare clic su **Aggiungi**.

Rinominare il gruppo di array di storage

È possibile modificare il nome di un gruppo di array di storage quando il nome corrente non è più significativo o applicabile.

A proposito di questa attività

Tenere presenti queste linee guida.

- Un nome può essere composto da lettere, numeri e caratteri speciali come sottolineatura (_), trattino (-) e cancelletto (n.). Se si sceglie un altro carattere, viene visualizzato un messaggio di errore. Viene richiesto di scegliere un altro nome.
- Limitare il nome a 30 caratteri. Gli spazi iniziali e finali del nome vengono cancellati.

- Utilizzare un nome univoco e significativo, facile da comprendere e ricordare.
- Evitare nomi o nomi arbitrari che perderebbero rapidamente il loro significato in futuro.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo di array di storage che si desidera rinominare.
2. Selezionare **Manage Groups › Rename storage array group** (Gestisci gruppi[Rinomina gruppo array di storage])
3. Nel campo **Nome gruppo**, digitare un nuovo nome per il gruppo.
4. Fare clic su **Rinomina**.

Rimuovere gli array di storage dal gruppo

È possibile rimuovere uno o più array di storage gestiti da un gruppo se non si desidera più gestirli da un gruppo di storage specifico.

A proposito di questa attività

La rimozione degli array di storage da un gruppo non influisce in alcun modo sull'array di storage o sui relativi dati. Se lo storage array è gestito da System Manager, è comunque possibile gestirlo utilizzando il browser. Se uno storage array viene accidentalmente rimosso da un gruppo, può essere aggiunto di nuovo.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare il **Manage Groups (Gestisci gruppi) › Remove storage array from group** (Rimuovi array di storage dal gruppo).
2. Dal menu a discesa, selezionare il gruppo che contiene gli array di storage che si desidera rimuovere, quindi fare clic sulla casella di controllo accanto a ciascun array di storage che si desidera rimuovere dal gruppo.
3. Fare clic su **Rimuovi**.

Eliminare il gruppo di array di storage

È possibile rimuovere uno o più gruppi di array di storage non più necessari.

A proposito di questa attività

Questa operazione elimina solo il gruppo di array di storage. Gli array di storage associati al gruppo cancellato rimangono accessibili tramite la vista Manage All (Gestisci tutti) o qualsiasi altro gruppo a cui è associato.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Delete storage array group** (Elimina gruppo array di storage).
2. Selezionare uno o più gruppi di array di storage che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).

Aggiornare il software del sistema operativo

Panoramica sull'aggiornamento

Nel plug-in di storage per vCenter, è possibile gestire il software SANtricity e gli

aggiornamenti DI NVSRAM per più array di storage dello stesso tipo.

Workflow di upgrade

I seguenti passaggi forniscono un workflow di alto livello per l'esecuzione degli aggiornamenti software:

1. È possibile scaricare il file SANtricity OS più recente dal sito di supporto (un collegamento è disponibile nella pagina di supporto). Salvare il file sul sistema host di gestione (l'host in cui si accede al plug-in in un browser), quindi decomprimere il file.
2. Nel plug-in, è possibile caricare il file del software SANtricity OS e IL file NVSRAM nel repository (un'area del server in cui sono memorizzati i file).
3. Una volta caricati i file nel repository, è possibile selezionare il file da utilizzare nell'aggiornamento. Dalla pagina Aggiorna software SANtricity OS, selezionare il file del software del sistema operativo e IL file NVSRAM. Dopo aver selezionato un file software, in questa pagina viene visualizzato un elenco di array di storage compatibili. Selezionare quindi gli array di storage che si desidera aggiornare con il nuovo software. (Non è possibile selezionare array incompatibili).
4. È quindi possibile avviare un trasferimento e un'attivazione software immediati oppure scegliere di preparare i file per l'attivazione in un secondo momento. Durante il processo di aggiornamento, il plug-in esegue le seguenti operazioni:
   - Esegue un controllo dello stato degli array di storage per determinare se esistono condizioni che potrebbero impedire il completamento dell'aggiornamento. Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.
   - Trasferisce i file di aggiornamento a ciascun controller.
   - Riavvia i controller e attiva il nuovo software del sistema operativo, un controller alla volta. Durante l'attivazione, il file del sistema operativo esistente viene sostituito con il nuovo file.

> È inoltre possibile specificare che il software venga attivato in un secondo momento.

Considerazioni sull'upgrade

Prima di eseguire l'upgrade di più array di storage, esaminare le considerazioni chiave come parte della pianificazione.

Versioni correnti

È possibile visualizzare le versioni correnti del software SANtricity OS dalla pagina Gestione del plug-in di storage per vCenter per ciascun array di storage rilevato. La versione viene visualizzata nella colonna Software SANtricity OS. Il firmware del controller e LE informazioni SU NVSRAM sono disponibili in una finestra di dialogo a comparsa quando si fa clic sulla versione del sistema operativo in ciascuna riga.

Altri componenti che richiedono l'aggiornamento

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare il driver multipath/failover dell'host o il driver HBA in modo che l'host possa interagire correttamente con i controller. Per informazioni sulla compatibilità, fare riferimento a. "Tool di matrice di interoperabilità".

Controller doppi

Se uno storage array contiene due controller e si dispone di un driver multipath installato, lo storage array può continuare a elaborare l'i/o durante l'aggiornamento. Durante l'aggiornamento, si verifica la seguente

procedura:

1. Il controller A esegue il failover di tutti i LUN verso il controller B.
2. L'aggiornamento avviene sul controller A.
3. Il controller A riprende i LUN e tutti i LUN del controller B.
4. L'aggiornamento avviene sul controller B.

Al termine dell'aggiornamento, potrebbe essere necessario ridistribuire manualmente i volumi tra i controller per garantire che i volumi tornino al controller proprietario corretto.

Eseguire un controllo dello stato di salute prima dell'aggiornamento

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare. Il controllo dello stato di salute valuta i componenti dello storage array per assicurarsi che l'aggiornamento possa continuare.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › controllo stato pre-aggiornamento**.

   Viene visualizzata la finestra di dialogo Pre-Upgrade Health Check (verifica dello stato di salute pre-aggiornamento) che elenca tutti i sistemi storage rilevati.

2. Se necessario, filtrare o ordinare i sistemi storage nell'elenco, in modo da poter visualizzare tutti i sistemi che non sono attualmente nello stato ottimale.
3. Selezionare le caselle di controllo relative ai sistemi storage che si desidera eseguire attraverso il controllo dello stato di salute.
4. Fare clic su **Start**.

   L'avanzamento viene visualizzato nella finestra di dialogo durante l'esecuzione del controllo dello stato di salute.

5. Una volta completato il controllo dello stato di salute, fare clic sui puntini di sospensione (…) a destra di ciascuna riga per visualizzare ulteriori informazioni ed eseguire altre attività.

> Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.

Aggiornare il sistema operativo SANtricity

Aggiorna uno o più storage array con il software più recente e NVSRAM per assicurarti di disporre di tutte le funzionalità più recenti e delle correzioni dei bug. Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller.

Prima di iniziare

Assicurarsi che:

- I file più recenti del sistema operativo SANtricity sono disponibili sul sistema host in cui è in esecuzione il plug-in.
- Si sa se si desidera attivare l'aggiornamento software ora o in una versione successiva. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:
  - **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. Il failover dei controller durante l'attivazione potrebbe risultare inferiore al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — si consiglia di testare il nuovo software del sistema operativo su un array di storage prima di aggiornare i file su altri array di storage.

> **Rischio di perdita di dati o rischio di danni allo storage array** — non apportare modifiche allo storage array durante l'aggiornamento. Mantenere l'alimentazione dello storage array.

Fasi

1. Se l'array di storage contiene un solo controller o un driver multipath non è in uso, interrompere l'attività i/o dell'array di storage per evitare errori dell'applicazione. Se lo storage array dispone di due controller e si dispone di un driver multipath installato, non è necessario interrompere l'attività di i/O.
2. Dalla vista principale, selezionare **Gestisci**, quindi uno o più array di storage da aggiornare.
3. Selezionare **Upgrade Center › Upgrade › SANtricity OS › Software**.

   Viene visualizzata la pagina aggiornamento del software SANtricity OS.

4. Scaricare il pacchetto software SANtricity OS più recente dal sito del supporto sul computer locale.
   a. Fare clic su Aggiungi nuovo file al repository software
   b. Fare clic sul collegamento per trovare i download più recenti di SANtricity OS.
   c. Fare clic sul collegamento **Download Latest Release** (Scarica ultima versione).
   d. Seguire le istruzioni rimanenti per scaricare il file del sistema operativo e IL file NVSRAM sul computer locale.

   > Il firmware con firma digitale è richiesto nella versione 8.42 e successive. Se si tenta di scaricare il firmware senza firma, viene visualizzato un errore e il download viene interrotto.

5. Selezionare il file del software del sistema operativo e IL file NVSRAM che si desidera utilizzare per aggiornare i controller:

   a. Dal menu a discesa, selezionare il file del sistema operativo scaricato sul computer locale.

      Se sono disponibili più file, i file vengono ordinati dalla data più recente alla data più vecchia.

      > Il repository software elenca tutti i file software associati al plug-in. Se il file che si desidera utilizzare non viene visualizzato, fare clic sul collegamento **Add new file to software repository** (Aggiungi nuovo file al repository software) per accedere alla posizione in cui si trova il file del sistema operativo che si desidera aggiungere.

   a. Dal menu a discesa **Select an NVSRAM file** (Seleziona un file NVSRAM), selezionare il file del controller che si desidera utilizzare.

      Se sono presenti più file, i file vengono ordinati dalla data più recente alla data più vecchia.

6. Nella tabella Compatible Storage Array (matrice di storage compatibile), esaminare gli array di storage compatibili con il file software del sistema operativo selezionato, quindi selezionare gli array da aggiornare.
   - Gli array di storage selezionati nella vista Manage (Gestione) e compatibili con il file del firmware selezionato vengono selezionati per impostazione predefinita nella tabella Compatible Storage Array (array di storage compatibile).
   - Gli array di storage che non possono essere aggiornati con il file del firmware selezionato non sono selezionabili nella tabella degli array di storage compatibili, come indicato dallo stato **incompatibile**.
7. (Facoltativo) per trasferire il file software agli array di storage senza attivarli, selezionare la casella di controllo **trasferire il software del sistema operativo agli array di storage, contrassegnarlo come staged e attivarlo in un secondo momento**.
8. Fare clic su **Start**.
9. A seconda che si sia scelto di attivare ora o successivamente, eseguire una delle seguenti operazioni:
   - Tipo `TRANSFER` Per confermare che si desidera trasferire le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Transfer** (trasferimento). Per attivare il software trasferito, selezionare **Centro di aggiornamento › attiva software SANtricity OS a fasi**.
   - Tipo `UPGRADE` Per confermare che si desidera trasferire e attivare le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Upgrade** (Aggiorna).

     Il sistema trasferisce il file software a ciascun array di storage selezionato per l'aggiornamento, quindi attiva il file avviando un riavvio.

   Durante l'operazione di aggiornamento si verificano le seguenti azioni:

   - Durante il processo di aggiornamento viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa continuare.
   - Se un controllo dello stato di salute non riesce per un array di storage, l'aggiornamento si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'aggiornamento.
   - È possibile annullare l'operazione di aggiornamento dopo il controllo dello stato di salute prima dell'aggiornamento.
10. (Facoltativo) una volta completato l'aggiornamento, è possibile visualizzare un elenco degli aggiornamenti per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

    Il file viene salvato nella cartella Download del browser con il nome `upgrade_log-<date>. json`.

Attivare il software del sistema operativo in fasi

È possibile scegliere di attivare il file software immediatamente o attendere fino a un momento più comodo. Questa procedura presuppone che l'utente abbia scelto di attivare il file software in un secondo momento.

A proposito di questa attività

È possibile trasferire i file del firmware senza attivarli. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

- **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. I controller si riavviano e si eseguono il failover durante l'attivazione, pertanto le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.

> Non è possibile interrompere il processo di attivazione dopo l'avvio.

Fasi

1. Dalla vista principale, selezionare **Gestisci**. Se necessario, fare clic sulla colonna **Status** per ordinare, nella parte superiore della pagina, tutti gli array di storage con stato "OS Upgrade (waiting activation)" (aggiornamento del sistema operativo (in attesa di attivazione).
2. Selezionare uno o più array di storage per i quali si desidera attivare il software, quindi selezionare **Centro di aggiornamento › attiva software Staged SANtricity**.

   Durante l'operazione di aggiornamento si verificano le seguenti azioni:

   - Nell'ambito del processo di attivazione viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'attivazione possa continuare.
   - Se un controllo dello stato di salute non riesce per un array di storage, l'attivazione si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'attivazione.
   - È possibile annullare l'operazione di attivazione dopo il controllo dello stato di salute pre-aggiornamento.

     Una volta completato correttamente il controllo dello stato di salute prima dell'aggiornamento, si verifica l'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dello storage array e dai componenti che si stanno attivando.
3. (Facoltativo) una volta completata l'attivazione, è possibile visualizzare un elenco degli elementi attivati per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

   Il file viene salvato nella cartella Download del browser con il nome `activate_log-<date>. json`.

Software per sistemi operativi chiari e staged

È possibile rimuovere il software del sistema operativo in fasi per assicurarsi che una versione in sospeso non venga attivata inavvertitamente in un secondo momento. La rimozione del software del sistema operativo in fasi non influisce sulla versione corrente in esecuzione sugli array di storage.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › Cancella software SANtricity in fasi**.

   Viene visualizzata la finestra di dialogo Cancella software SANtricity a fasi che elenca tutti i sistemi storage

rilevati con software o NVSRAM in sospeso.

2. Se necessario, filtrare o ordinare i sistemi di storage nell'elenco, in modo da poter visualizzare tutti i sistemi che dispongono di software in fasi.
3. Selezionare le caselle di controllo relative ai sistemi storage con software in sospeso che si desidera eliminare.
4. Fare clic su **Cancella**.

   Lo stato dell'operazione viene visualizzato nella finestra di dialogo.

Gestire il repository software

È possibile visualizzare e gestire un repository software, che elenca tutti i file software associati allo Storage Plugin per vCenter.

Prima di iniziare

Se si utilizza il repository per aggiungere file SANtricity OS, assicurarsi che i file del sistema operativo siano disponibili sul sistema locale.

A proposito di questa attività

È possibile utilizzare l'opzione Gestisci repository software SANtricity OS per importare uno o più file del sistema operativo nel sistema host in cui è in esecuzione il plug-in. Puoi anche scegliere di eliminare uno o più file del sistema operativo disponibili nel repository software.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi **Centro di aggiornamento › Gestisci repository software SANtricity**.

   Viene visualizzata la finestra di dialogo Gestisci repository software SANtricity OS.

2. Eseguire una delle seguenti operazioni:
   - **Importazione:**
     i. Fare clic su **Importa**.
     ii. Fare clic su **Browse** (Sfoglia), quindi individuare il percorso in cui si trovano i file del sistema operativo che si desidera aggiungere. I file del sistema operativo hanno un nome file simile a. `N2800-830000-000.dlp`.
     iii. Selezionare uno o più file del sistema operativo da aggiungere, quindi fare clic su **Importa**.
   - **Elimina:**
     i. Selezionare uno o più file del sistema operativo che si desidera rimuovere dal repository software.
     ii. Fare clic su **Delete** (Elimina).

Risultato

Se è stata selezionata l'opzione di importazione, i file vengono caricati e validati. Se si seleziona Delete (Elimina), i file vengono rimossi dal repository software.

Eseguire il provisioning dello storage

Panoramica sul provisioning

Nel plug-in Storage per vCenter, è possibile creare container di dati, chiamati volumi, in modo che l'host possa accedere allo storage sull'array.

Tipi di volume e caratteristiche

I volumi sono container di dati che gestiscono e organizzano lo spazio di storage sull'array di storage.

È possibile creare volumi dalla capacità di storage disponibile sull'array di storage, che consente di organizzare le risorse del sistema. Il concetto di "volumi" è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso rapido.

I volumi sono l'unico livello di dati visibile agli host. In un ambiente SAN, i volumi vengono mappati ai LUN (Logical Unit Number). Queste LUN conservano i dati utente accessibili mediante uno o più protocolli di accesso host supportati dallo storage array, tra cui FC, iSCSI e SAS.

Ciascun volume di un pool o di un gruppo di volumi può avere le proprie caratteristiche individuali in base al tipo di dati che verranno memorizzati in esso. Alcune di queste caratteristiche includono:

- **Dimensione segmento** — Un segmento è la quantità di dati in kilobyte (KiB) che viene memorizzata su un disco prima che lo storage array passi al disco successivo nello stripe (gruppo RAID). La dimensione del segmento è uguale o inferiore alla capacità del gruppo di volumi. La dimensione del segmento è fissa e non può essere modificata per i pool.
- **Capacità** — consente di creare un volume dalla capacità libera disponibile in un pool o in un gruppo di volumi. Prima di creare un volume, il pool o il gruppo di volumi deve già esistere e disporre di capacità libera sufficiente per creare il volume.
- **Controller ownership** — tutti gli storage array possono avere uno o due controller. Su un array a controller singolo, il carico di lavoro di un volume viene gestito da un singolo controller. Su un array a controller doppio, un volume avrà un controller preferito (A o B) che "possiede" il volume. In una configurazione a controller doppio, la proprietà del volume viene regolata automaticamente utilizzando la funzione di bilanciamento automatico del carico per correggere eventuali problemi di bilanciamento del carico quando i carichi di lavoro si spostano tra i controller. Il bilanciamento automatico del carico fornisce il bilanciamento automatizzato del carico di lavoro i/o e garantisce che il traffico i/o in entrata dagli host sia gestito dinamicamente e bilanciato tra entrambi i controller.
- **Assegnazione del volume** — è possibile consentire agli host di accedere a un volume sia quando si crea il volume che in un secondo momento. Tutti gli accessi host vengono gestiti tramite un numero di unità logica (LUN). Gli host rilevano le LUN che, a loro volta, sono assegnate ai volumi. Se si assegna un volume a più host, utilizzare il software di clustering per assicurarsi che il volume sia disponibile per tutti gli host.

  Il tipo di host può avere limiti specifici sul numero di volumi a cui l'host può accedere. Tenere presente questa limitazione quando si creano volumi per l'utilizzo da parte di un determinato host.

- **Resource provisioning** — per gli array storage EF600 o EF300, è possibile specificare che i volumi vengano utilizzati immediatamente senza alcun processo di inizializzazione in background. Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati).
- **Descrivi name** — puoi assegnare un nome a un volume qualsiasi, ma ti consigliamo di renderlo descrittivo.

Durante la creazione del volume, a ciascun volume viene allocata la capacità e viene assegnato un nome, una

dimensione del segmento (solo gruppi di volumi), una proprietà del controller e un'assegnazione volume-a-host. I dati dei volumi vengono automaticamente bilanciati in base alle esigenze dei controller.

Capacità per i volumi

I dischi dell'array di storage forniscono la capacità fisica dello storage per i dati. Prima di iniziare a memorizzare i dati, è necessario configurare la capacità allocata in componenti logici noti come pool o gruppi di volumi. Questi oggetti storage vengono utilizzati per configurare, memorizzare, gestire e conservare i dati sull'array di storage.

Capacità di creare ed espandere volumi

È possibile creare volumi dalla capacità non assegnata o dalla capacità libera in un pool o un gruppo di volumi.

- Quando si crea un volume dalla capacità non assegnata, è possibile creare contemporaneamente un pool o un gruppo di volumi e il volume.
- Quando si crea un volume dalla capacità libera, si crea un volume aggiuntivo su un pool o un gruppo di volumi già esistente.dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere una corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

> L'interfaccia del plug-in non fornisce un'opzione per creare volumi thin.

Capacità dei volumi riportata

La capacità del volume riportata è uguale alla quantità di capacità dello storage fisico allocata. Deve essere presente l'intera quantità di capacità dello storage fisico. Lo spazio fisicamente allocato è uguale allo spazio riportato all'host.

Di norma, si imposta la capacità del volume indicata come capacità massima a cui si pensa che il volume crescerà. I volumi offrono performance elevate e prevedibili per le applicazioni, soprattutto perché tutta la capacità dell'utente viene riservata e allocata al momento della creazione.

Limiti di capacità

La capacità minima di un volume è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità dei dischi nel pool o nel gruppo di volumi.

Quando si aumenta la capacità di un volume segnalata, tenere presenti le seguenti linee guida:

- È possibile specificare fino a tre cifre decimali (ad esempio, 65.375 GiB).
- La capacità deve essere inferiore o uguale al massimo disponibile nel gruppo di volumi. Quando si crea un volume, viene preallocata una certa capacità aggiuntiva per la migrazione DSS (Dynamic Segment Size). La migrazione DSS è una funzione del software che consente di modificare le dimensioni dei segmenti di un volume.
- Alcuni sistemi operativi host supportano volumi superiori a 2 TIB (la capacità massima indicata è determinata dal sistema operativo host). Infatti, alcuni sistemi operativi host supportano fino a 128 volumi TIB. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Carichi di lavoro specifici dell'applicazione

Quando si crea un volume, si seleziona un carico di lavoro per personalizzare la configurazione dell'array di

storage per un'applicazione specifica.

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

Durante la creazione del volume, il sistema richiede di rispondere alle domande sull'utilizzo di un carico di lavoro. Ad esempio, se si creano volumi per Microsoft Exchange, viene chiesto quante cassette postali sono necessarie, quali sono i requisiti medi di capacità delle caselle postali e quante copie del database si desidera. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze. In alternativa, è possibile saltare questo passaggio nella sequenza di creazione del volume.

Tipi di carichi di lavoro

È possibile creare due tipi di carichi di lavoro: Specifici dell'applicazione e altri.

- **Specifico dell'applicazione** — quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.
  - Microsoft SQL Server
  - Server Microsoft Exchange
  - Applicazioni di videosorveglianza
  - VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

    È possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

- **Altri (o applicazioni senza supporto specifico per la creazione di volumi)** — Altri carichi di lavoro utilizzano una configurazione del volume che è necessario specificare manualmente quando si desidera creare un carico di lavoro non associato a un'applicazione specifica o se il sistema non dispone di ottimizzazione integrata per l'applicazione che si intende utilizzare sull'array di storage. Specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Viste delle applicazioni e dei workload

Per visualizzare applicazioni e carichi di lavoro, avviare System Manager. Da questa interfaccia è possibile visualizzare le informazioni associate a un carico di lavoro specifico dell'applicazione in due modi diversi:

- È possibile selezionare la scheda Applications & workload (applicazioni e carichi di lavoro) nel riquadro Volumes (volumi) per visualizzare i volumi dell'array di storage raggruppati per carico di lavoro e il tipo di applicazione a cui è associato il carico di lavoro.
- È possibile selezionare la scheda applicazioni e carichi di lavoro nel riquadro prestazioni per visualizzare le metriche delle performance (latenza, IOPS e MB) per gli oggetti logici. Gli oggetti sono raggruppati in base all'applicazione e al carico di lavoro associato. Raccogliendo questi dati sulle performance a intervalli

regolari, è possibile stabilire misurazioni di riferimento e analizzare i trend, che possono aiutare a indagare i problemi relativi alle performance di i/O.

Creare storage

Nel plug-in di storage per vCenter, è possibile creare lo storage creando prima un carico di lavoro per un tipo di applicazione specifico. In seguito, è possibile aggiungere capacità di storage al carico di lavoro creando volumi con caratteristiche di volume sottostanti simili.

Fase 1: Creazione di carichi di lavoro

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione.

A proposito di questa attività

Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

Il sistema consiglia una configurazione del volume ottimizzata solo per i seguenti tipi di applicazione:

- Microsoft SQL Server
- Server Microsoft Exchange
- Videosorveglianza
- VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › workload** (Crea[carico di lavoro]).

   Viene visualizzata la finestra di dialogo Create Application workload (Crea carico di lavoro applicazione).

4. Utilizzare l'elenco a discesa per selezionare il tipo di applicazione per cui si desidera creare il carico di lavoro, quindi digitare un nome per il carico di lavoro.
5. Fare clic su **Create** (Crea).

Fase 2: Creazione di volumi

È possibile creare volumi per aggiungere capacità di storage a un carico di lavoro specifico dell'applicazione e rendere visibili i volumi creati a un host o a un cluster host specifico.

A proposito di questa attività

La maggior parte dei tipi di applicazioni utilizza per impostazione predefinita una configurazione di volume definita dall'utente, mentre altri tipi hanno una configurazione smart applicata alla creazione di un volume. Ad esempio, se si creano volumi per un'applicazione Microsoft Exchange, viene chiesto quante cassette postali sono necessarie, quali sono i requisiti medi di capacità delle caselle postali e quante copie del database si

desidera. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze.

È possibile creare volumi dal **Provisioning › Gestisci volumi › Crea › volumi** o dal **Provisioning › Configura pool e gruppi di volumi › Crea › volumi**. La procedura è la stessa per entrambe le selezioni.

Il processo di creazione di un volume è una procedura a più fasi.

Fase 2a: Selezionare l'host per un volume

Nella prima fase, è possibile selezionare un host o un cluster host specifico per il volume oppure scegliere di assegnare l'host in un secondo momento.

Prima di iniziare

Assicurarsi che:

- Sono stati definiti host o cluster di host validi (andare al **Provisioning › Configure hosts**).
- Sono stati definiti gli identificatori delle porte host per l'host.
- La connessione host deve supportare Data Assurance (da) se si intende creare volumi abilitati da. Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

- Il sistema operativo di un host può avere limiti specifici sul numero di volumi a cui l'host può accedere. Tenere presente questa limitazione quando si creano volumi per l'utilizzo da parte di un determinato host.
- È possibile definire un'assegnazione per ciascun volume nell'array di storage.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un LUN univoco.
- Se si desidera accelerare il processo di creazione dei volumi, è possibile saltare la fase di assegnazione dell'host in modo che i volumi appena creati vengano inizializzati offline.

> L'assegnazione di un volume a un host non riesce se si tenta di assegnare un volume a un cluster di host che è in conflitto con un'assegnazione stabilita per un host nei cluster di host.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › Volumes** (Crea[volumi]).

   Viene visualizzata la finestra di dialogo Select host (Seleziona host).

4. Dall'elenco a discesa, selezionare un host o un cluster host specifico al quale assegnare i volumi oppure scegliere di assegnare l'host o il cluster host in un secondo momento.
5. Per continuare la sequenza di creazione del volume per l'host o il cluster host selezionato, fare clic su **Avanti.**

Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

Fase 2b: Selezionare un carico di lavoro per un volume

Nella seconda fase, selezionare un workload per personalizzare la configurazione dello storage array per un'applicazione specifica, ad esempio VMware.

A proposito di questa attività

Questa attività descrive come creare volumi per un carico di lavoro. In genere, un carico di lavoro contiene volumi con caratteristiche simili, ottimizzati in base al tipo di applicazione supportata dal carico di lavoro. È possibile definire un workload in questa fase oppure selezionare i workload esistenti.

Tenere presenti le seguenti linee guida:

- Quando si utilizza un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. È possibile rivedere la configurazione del volume consigliata, quindi modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi) (disponibile nella fase successiva).
- Quando si utilizzano altri tipi di applicazioni, è possibile specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi) (disponibile nella fase successiva).

Fasi

1. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **Create Volumes for a existing workload** (Crea volumi per un carico di lavoro esistente), quindi selezionare il carico di lavoro dall'elenco a discesa.
    - Selezionare l'opzione **Create a new workload** (Crea nuovo carico di lavoro) per definire un nuovo carico di lavoro per un'applicazione supportata o per "altre" applicazioni, quindi attenersi alla seguente procedura:
        - Dall'elenco a discesa, selezionare il nome dell'applicazione per cui si desidera creare il nuovo workload. Selezionare una delle "altre" voci se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.
        - Immettere un nome per il carico di lavoro che si desidera creare.
2. Fare clic su **Avanti**.
3. Se il carico di lavoro è associato a un tipo di applicazione supportato, inserire le informazioni richieste; in caso contrario, passare alla fase successiva.

Fase 2c: Aggiunta o modifica di volumi

Nel terzo passaggio, definire la configurazione del volume.

Prima di iniziare

- I pool o i gruppi di volumi devono disporre di capacità libera sufficiente.
- Il numero massimo di volumi consentito in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello di sistema di storage:
    - 2,048 volumi (serie EF600 ed E5700)
    - 1,024 volumi (EF300)

    - 512 volumi (serie E2800)
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.
    - Se si desidera creare un volume abilitato da, selezionare un pool o un gruppo di volumi che supporti da (cercare **Sì** accanto a "da" nella tabella dei candidati del pool e del gruppo di volumi).
    - Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi. LA protezione DA verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. La selezione di un pool o di un gruppo di volumi da-capable per il nuovo volume garantisce il rilevamento e la correzione degli errori.
    - Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.
- Per creare un volume abilitato alla protezione, è necessario creare una chiave di sicurezza per l'array di storage.
    - Se si desidera creare un volume abilitato per la protezione, selezionare un pool o un gruppo di volumi che supporti la protezione (cercare Sì accanto a "abilitato per la protezione" nella tabella dei candidati del pool e del gruppo di volumi).
    - Le funzionalità di sicurezza dei dischi vengono presentate a livello di pool e gruppo di volumi. I dischi con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Un disco abilitato alla sicurezza crittografa i dati durante la scrittura e decrta i dati durante la lettura utilizzando una chiave di crittografia univoca.
    - Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
- Per creare un volume con provisioning di risorse, tutti i dischi devono essere dischi NVMe con l'opzione Deallocated o Unwritten Logical Block Error (DULBE).

A proposito di questa attività

I volumi vengono creati da pool o gruppi di volumi idonei, visualizzati nella finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi). Per ciascun pool e gruppo di volumi idonei, vengono visualizzati il numero di dischi disponibili e la capacità libera totale.

Per alcuni carichi di lavoro specifici dell'applicazione, ciascun pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e la capacità libera rimanente in GiB. Per gli altri carichi di lavoro, la capacità proposta viene visualizzata quando si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

Fasi

1. Scegliere una di queste azioni in base alla selezione di un altro workload o di un workload specifico dell'applicazione nel passaggio precedente:
    - **Altro** — fare clic su **Aggiungi nuovo volume** in ogni pool o gruppo di volumi che si desidera utilizzare per creare uno o più volumi.

Dettagli campo

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • da 512 a 512 byte • 4K – 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi nel pool o nel gruppo di volumi sono protetti. Drive Security impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione Drive Security è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Campo	Descrizione
Provisioning delle risorse (solo EF300 e EF600)	**Yes** viene visualizzato accanto a "Resource Provisioned" (risorse fornite) solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

- **Carico di lavoro specifico dell'applicazione** — fare clic su **Avanti** per accettare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato.

Dettagli campo

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4-GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Tipo di volume	Il tipo di volume indica il tipo di volume creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • 512 — 512 byte • 4K — 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi nel pool o nel gruppo di volumi sono protetti. La sicurezza del disco impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione di sicurezza del disco è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Campo	Descrizione
Provisioning delle risorse (solo EF300 e EF600)	**Yes** viene visualizzato accanto a "Resource Provisioned" (risorse fornite) solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

2. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti**.

Fase 2d: Analisi della configurazione del volume

Nell'ultimo passaggio, viene esaminato un riepilogo dei volumi che si intende creare e vengono apportate le modifiche necessarie.

Fasi

1. Esaminare i volumi che si desidera creare. Per apportare modifiche, fare clic su **Indietro**.
2. Quando si è soddisfatti della configurazione del volume, fare clic su **fine**.

Al termine

- Nel client vSphere, creare datastore per i volumi.
- Eseguire tutte le modifiche del sistema operativo necessarie sull'host dell'applicazione in modo che le applicazioni possano utilizzare il volume.
- Eseguire il sistema basato su host `hot_add` o un'utility specifica del sistema operativo (disponibile presso un fornitore di terze parti), quindi eseguire `SMdevices` utility per correlare i nomi dei volumi con i nomi degli array di storage host.

  Il `hot_add` e a. `SMdevices` le utility sono incluse nel `SMutils` pacchetto. Il `SMutils` il pacchetto è un insieme di utility per verificare ciò che l'host vede dall'array di storage. È incluso nell'installazione del software SANtricity.

Aumentare la capacità di un volume

È possibile ridimensionare un volume per aumentarne la capacità indicata.

Prima di iniziare

Assicurarsi che:

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associati al volume.
- Il volume è ottimale e non in alcun stato di modifica.
- Nel volume non sono in uso dischi hot spare. (Si applica solo ai volumi nei gruppi di volumi).

A proposito di questa attività

Questa attività descrive come aumentare la capacità riportata (la capacità riportata agli host) di un volume utilizzando la capacità libera disponibile nel pool o nel gruppo di volumi. Assicurarsi di prendere in considerazione eventuali requisiti di capacità futuri per altri volumi in questo pool o gruppo di volumi.

L'aumento della capacità di un volume è supportato solo su alcuni sistemi operativi. Se si aumenta la capacità del volume su un sistema operativo host non supportato, la capacità espansa non è utilizzabile e non è possibile ripristinare la capacità del volume originale.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage che contiene i volumi che si desidera ridimensionare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il volume per il quale si desidera aumentare la capacità, quindi selezionare **aumenta capacità**.

   Viene visualizzata la finestra di dialogo Conferma aumento capacità.

4. Selezionare **Sì** per continuare.

   Viene visualizzata la finestra di dialogo aumenta capacità riportata. Questa finestra di dialogo visualizza la capacità corrente del volume riportata e la capacità libera disponibile nel gruppo di volumi o pool associato al volume.

5. Utilizzare la casella **aumenta capacità segnalata aggiungendo…** per aggiungere capacità alla capacità corrente disponibile indicata. È possibile modificare il valore della capacità in modo che venga visualizzato in megibyte (MiB), gibibyte (GiB) o tebibyte (TIB).
6. Fare clic su **aumenta**.

   La capacità del volume viene aumentata in base alla selezione effettuata. Tenere presente che questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Al termine

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Modificare le impostazioni di un volume

È possibile modificare le impostazioni di un volume, ad esempio il nome, l'assegnazione dell'host, la dimensione del segmento, la priorità di modifica, la memorizzazione nella cache, e così via.

Prima di iniziare

Assicurarsi che il volume che si desidera modificare sia nello stato ottimale.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera modificare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il volume che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Settings (Impostazioni volume). Le impostazioni di configurazione del volume selezionato vengono visualizzate in questa finestra di dialogo.

4. Selezionare la scheda **Basic** per modificare il nome del volume e l'assegnazione dell'host.

Dettagli campo

Impostazione	Descrizione
Nome	Visualizza il nome del volume. Modificare il nome di un volume quando il nome corrente non è più significativo o applicabile.
Capacità	Visualizza la capacità riportata e allocata per il volume selezionato.
Gruppo pool/Volume	Visualizza il nome e il livello RAID del pool o del gruppo di volumi. Indica se il pool o il gruppo di volumi sono abilitati per la protezione e la protezione.
Host	Visualizza l'assegnazione del volume. Si assegna un volume a un cluster host o host in modo che sia possibile accedervi per le operazioni di i/O. Questa assegnazione consente a un host o a un cluster di host di accedere a un determinato volume o a una serie di volumi in un array di storage. • **Assegnato a** — identifica l'host o il cluster di host che ha accesso al volume selezionato. • **LUN** — Un numero di unità logica (LUN) è il numero assegnato allo spazio degli indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi. Per le interfacce NVMe, questa colonna visualizza l'ID dello spazio dei nomi. Uno spazio dei nomi è uno storage NVM formattato per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che si riferisce a un volume nell'array di storage. L'ID dello spazio dei nomi è l'identificatore univoco del controller NVMe per lo spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.
Identificatori	Visualizza gli identificatori del volume selezionato. • WWID (World-wide identifier). Identificatore esadecimale univoco del volume. • Extended Unique Identifier (EUI). Un identificatore EUI-64 per il volume. • SSID (Subsystem Identifier). L'identificatore del sottosistema dell'array di storage di un volume.

5. Selezionare la scheda **Avanzate** per modificare le impostazioni di configurazione aggiuntive per un volume in un pool o in un gruppo di volumi.

Dettagli campo

Impostazione	Descrizione
Informazioni su applicazioni e carichi di lavoro	Durante la creazione dei volumi, è possibile creare carichi di lavoro specifici dell'applicazione o altri carichi di lavoro. Se applicabile, il nome del carico di lavoro, il tipo di applicazione e il tipo di volume vengono visualizzati per il volume selezionato. Se lo si desidera, è possibile modificare il nome del carico di lavoro.
Impostazioni della qualità del servizio	**Disable data assurance (Disattiva data assurance) in modo permanente** — questa impostazione viene visualizzata solo se il volume è abilitato per Data Assurance (da). DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. Utilizzare questa opzione per disattivare in modo permanente il da sul volume selezionato. Se disattivato, il da non può essere riattivato su questo volume. **Enable pre-Read Redundancy check** — questa impostazione viene visualizzata solo se il volume è un volume spesso. I controlli di ridondanza di pre-lettura determinano se i dati su un volume sono coerenti ogni volta che viene eseguita una lettura. Un volume con questa funzione attivata restituisce errori di lettura se i dati risultano incoerenti dal firmware del controller.
Proprietà del controller	Definisce il controller designato come controller principale o proprietario del volume. La proprietà del controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per l'i/o totale.

Impostazione	Descrizione
Dimensionamento dei segmenti	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti.** il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Priorità di modifica	Mostra l'impostazione della priorità di modifica, che viene visualizzata solo per i volumi in un gruppo di volumi. La priorità di modifica definisce il tempo di elaborazione allocato per le operazioni di modifica del volume in relazione alle prestazioni del sistema. È possibile aumentare la priorità di modifica del volume, anche se ciò potrebbe influire sulle prestazioni del sistema. Spostare le barre di scorrimento per selezionare un livello di priorità. **Modifica dei tassi di priorità** — il tasso di priorità più basso offre benefici alle prestazioni del sistema, ma l'operazione di modifica richiede più tempo. Il tasso di priorità più elevato è utile per l'operazione di modifica, ma le prestazioni del sistema potrebbero essere compromesse.
Caching	Mostra l'impostazione del caching, che è possibile modificare per influire sulle prestazioni i/o complessive di un volume.

Impostazione	Descrizione
Cache SSD	(Questa funzione non è disponibile sui sistemi storage EF600 o EF300). Mostra l'impostazione della cache SSD, che è possibile attivare sui volumi compatibili per migliorare le prestazioni di sola lettura. I volumi sono compatibili se condividono le stesse funzionalità di sicurezza del disco e di data assurance. La funzione SSD cache utilizza uno o più dischi a stato solido (SSD) per implementare una cache di lettura. Le performance applicative sono migliorate grazie ai tempi di lettura più rapidi per gli SSD. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. È sufficiente selezionare il volume che si desidera memorizzare nella cache, quindi il caching è automatico e dinamico.

6. Fare clic su **Save** (Salva).

Risultato

Le impostazioni del volume vengono modificate in base alle selezioni effettuate.

Aggiungere volumi al carico di lavoro

È possibile aggiungere volumi non assegnati a un carico di lavoro esistente o nuovo.

A proposito di questa attività

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera aggiungere.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

4. Selezionare **Aggiungi al carico di lavoro**.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

5. Eseguire una delle seguenti operazioni:
   - **Aggiungi volumi a un carico di lavoro esistente** — selezionare questa opzione per aggiungere volumi a un carico di lavoro esistente. Utilizzare l'elenco a discesa per selezionare un carico di lavoro. Il tipo di applicazione associato al carico di lavoro viene assegnato ai volumi aggiunti a questo carico di lavoro.
   - **Aggiungi volumi a un nuovo carico di lavoro** — selezionare questa opzione per definire un nuovo carico di lavoro per un tipo di applicazione e aggiungere volumi al nuovo carico di lavoro.
6. Selezionare **Avanti** per continuare con la sequenza di aggiunta al carico di lavoro.

   Viene visualizzata la finestra di dialogo Select Volumes (Seleziona volumi).

7. Selezionare i volumi che si desidera aggiungere al carico di lavoro.
8. Esaminare i volumi che si desidera aggiungere al carico di lavoro selezionato.
9. Quando si è soddisfatti della configurazione del carico di lavoro, fare clic su **fine**.

Modificare le impostazioni del carico di lavoro

È possibile modificare il nome di un workload e visualizzarne il tipo di applicazione associato.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage che contiene il carico di lavoro che si desidera modificare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

4. Selezionare il carico di lavoro che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Applications & workload Settings (Impostazioni applicazioni e carichi di lavoro).

5. (Facoltativo) modificare il nome del carico di lavoro fornito dall'utente.
6. Fare clic su **Save** (Salva).

Inizializzare i volumi

Un volume viene inizializzato automaticamente quando viene creato per la prima volta. Tuttavia, il Recovery Guru potrebbe consigliare di inizializzare manualmente un volume per eseguire il ripristino in seguito a determinate condizioni di errore.

Utilizzare questa opzione solo sotto la guida del supporto tecnico. È possibile selezionare uno o più volumi da inizializzare.

Prima di iniziare

- Tutte le operazioni di i/o sono state interrotte.
- Tutti i dispositivi o i file system sui volumi che si desidera inizializzare devono essere smontati.
- Il volume si trova in uno stato ottimale e non sono in corso operazioni di modifica sul volume.*attenzione: *Non è possibile annullare l'operazione dopo l'avvio. Tutti i dati del volume vengono cancellati. Non provare a eseguire questa operazione a meno che il Recovery Guru non lo suggerisca. Prima di iniziare questa procedura, contattare il supporto tecnico.

A proposito di questa attività

Quando si inizializza un volume, il volume mantiene le impostazioni relative a WWN, assegnazioni host, capacità allocata e capacità riservata. Inoltre, mantiene le stesse impostazioni di sicurezza e di Data Assurance (da).

Non è possibile inizializzare i seguenti tipi di volumi:

- Volume di base di un volume di snapshot
- Volume primario in una relazione mirror
- Volume secondario in relazione mirror
- Volume di origine in una copia del volume
- Volume di destinazione in una copia del volume
- Volume che ha già un'inizializzazione in corso

Questa procedura si applica solo ai volumi standard creati da pool o gruppi di volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera inizializzare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Initialize Volumes** (Altro[Inizializza volumi]).

   Viene visualizzata la finestra di dialogo Inizializza volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Selezionare uno o più volumi da inizializzare e confermare che si desidera eseguire l'operazione.

Risultati

Il sistema esegue le seguenti operazioni:

- Cancella tutti i dati dai volumi inizializzati.
- Cancella gli indici dei blocchi, il che fa sì che i blocchi non scritti vengano letti come se fossero riempiti a zero (il volume sembra essere completamente vuoto).

Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Ridistribuire i volumi

Ridistribuisci i volumi per spostarli di nuovo nei proprietari di controller preferiti. In genere, i driver multipath spostano i volumi dal proprietario del controller preferito quando si verifica un problema lungo il percorso dei dati tra l'host e l'array di storage.

Prima di iniziare

- I volumi che si desidera ridistribuire non sono in uso o si verificano errori di i/O.
- Un driver multipath viene installato su tutti gli host che utilizzano i volumi che si desidera ridistribuire, altrimenti si verificheranno errori di i/O. Se si desidera ridistribuire i volumi senza un driver multipath sugli host, tutte le attività di i/o sui volumi durante l'operazione di ridistribuzione devono essere interrotte per evitare errori dell'applicazione.

A proposito di questa attività

La maggior parte dei driver multipath host tenta di accedere a ciascun volume su un percorso verso il proprietario del controller preferito. Tuttavia, se questo percorso preferito non è disponibile, il driver multipath sull'host esegue il failover su un percorso alternativo. Questo failover potrebbe causare la modifica della proprietà del volume nel controller alternativo. Dopo aver risolto la condizione che ha causato il failover, alcuni host potrebbero spostare automaticamente la proprietà del volume nel proprietario del controller preferito, ma in alcuni casi potrebbe essere necessario ridistribuire manualmente i volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi da ridistribuire.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il **More › redistribuisci volumi**.

   Viene visualizzata la finestra di dialogo redistribuisci volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage il cui proprietario preferito del controller non corrisponde al proprietario corrente.

4. Selezionare uno o più volumi da ridistribuire e confermare che si desidera eseguire l'operazione.

Risultato

Il sistema sposta i volumi selezionati nei controller preferiti oppure viene visualizzata una finestra di dialogo ridistribuisci volumi non necessari.

Modificare la proprietà del controller di un volume

È possibile modificare la proprietà del controller preferito di un volume, in modo che l'i/o per le applicazioni host venga indirizzato attraverso il nuovo percorso.

Prima di iniziare

Se non si utilizza un driver multipath, tutte le applicazioni host che attualmente utilizzano il volume devono essere chiuse. Questa azione impedisce gli errori dell'applicazione quando il percorso di i/o cambia.

A proposito di questa attività

È possibile modificare la proprietà del controller per uno o più volumi in un pool o un gruppo di volumi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi per i quali si desidera modificare la proprietà del controller.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change ownership** (Altro[Modifica proprietà]).

   Viene visualizzata la finestra di dialogo Change Volume Ownership (Modifica proprietà volume). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Utilizzare l'elenco a discesa **Preferred Owner** (Proprietario preferito) per modificare il controller preferito per ciascun volume che si desidera modificare e confermare che si desidera eseguire l'operazione.

Risultati

- Il sistema modifica la proprietà del controller del volume. L'i/o al volume viene ora indirizzato attraverso questo percorso i/O.
- Il volume potrebbe non utilizzare il nuovo percorso i/o fino a quando il driver multipath non viene riconfigurato per riconoscere il nuovo percorso.

Questa operazione richiede in genere meno di cinque minuti.

Modificare le impostazioni della cache per un volume

È possibile modificare le impostazioni della cache di lettura e di scrittura per influire sulle

prestazioni i/o generali di un volume.

A proposito di questa attività

Quando si modificano le impostazioni della cache di un volume, tenere presenti le seguenti linee guida:

- Dopo aver aperto la finestra di dialogo Change cache Settings (Modifica impostazioni cache), potrebbe essere visualizzata un'icona accanto alle proprietà della cache selezionate. Questa icona indica che il controller ha temporaneamente sospeso le operazioni di caching. Questa azione potrebbe verificarsi quando una nuova batteria è in carica, quando un controller è stato rimosso o se il controller ha rilevato una mancata corrispondenza nelle dimensioni della cache. Una volta deselezionata la condizione, le proprietà della cache selezionate nella finestra di dialogo diventano attive. Se le proprietà della cache selezionate non diventano attive, contattare il supporto tecnico.
- È possibile modificare le impostazioni della cache per un singolo volume o per più volumi su un array di storage. È possibile modificare le impostazioni della cache per tutti i volumi contemporaneamente.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage contenente i volumi per i quali si desidera modificare le impostazioni della cache.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change cache settings** (Altro[Modifica impostazioni cache]).

   Viene visualizzata la finestra di dialogo Change cache Settings (Modifica impostazioni cache). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Selezionare la scheda **Basic** per modificare le impostazioni per il caching in lettura e il caching in scrittura.

   Dettagli campo

Impostazione della cache	Descrizione
Read Caching (cache lettura)	La cache di lettura è un buffer che memorizza i dati letti dai dischi. I dati di un'operazione di lettura potrebbero essere già presenti nella cache di un'operazione precedente, eliminando così la necessità di accedere ai dischi. I dati rimangono nella cache di lettura fino a quando non vengono scaricati.
Cache di scrittura	La cache di scrittura è un buffer che memorizza i dati dell'host che non sono ancora stati scritti sui dischi. I dati rimangono nella cache di scrittura fino a quando non vengono scritti sui dischi. Il caching in scrittura può aumentare le performance di i/O. La cache viene automaticamente scaricata dopo la disattivazione del caching in scrittura per un volume.

5. Selezionare la scheda **Advanced** (Avanzate) per modificare le impostazioni avanzate per i volumi spessi. Le impostazioni avanzate della cache sono disponibili solo per i volumi thick.

Dettagli campo

Impostazione	Descrizione
Precaricamento della cache di lettura dinamica	Dynamic cache Read Prefetch consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache durante la lettura dei blocchi di dati da un disco alla cache. Questo caching aumenta la possibilità che le future richieste di dati possano essere compilate dalla cache. Il prefetch dinamico della lettura della cache è importante per le applicazioni multimediali che utilizzano l'i/o sequenziale La velocità e la quantità di dati precaricati nella cache vengono regolate automaticamente in base alla velocità e alle dimensioni della richiesta dell'host. L'accesso casuale non fa sì che i dati vengano precaricati nella cache. Questa funzione non si applica quando il caching in lettura è disattivato.
Cache di scrittura senza batterie	L'impostazione Write Caching without batteries (cache di scrittura senza batterie) consente di continuare il caching in scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta del caching in scrittura senza batterie non è generalmente consigliata, in quanto i dati potrebbero andare persi in caso di interruzione dell'alimentazione. In genere, il caching in scrittura viene disattivato temporaneamente dal controller fino a quando le batterie non vengono caricate o non viene sostituita una batteria guasta. ATTENZIONE: **Possibile perdita di dati** — se si seleziona questa opzione e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione Write caching without batteries (cache di scrittura senza batterie).
Cache di scrittura con mirroring	Il caching in scrittura con mirroring si verifica quando i dati scritti nella memoria cache di un controller vengono scritti anche nella memoria cache dell'altro controller. Pertanto, se un controller si guasta, l'altro può completare tutte le operazioni di scrittura in sospeso. Il mirroring della cache di scrittura è disponibile solo se il caching di scrittura è attivato e sono presenti due controller. Il caching in scrittura con mirroring è l'impostazione predefinita alla creazione del volume.

6. Fare clic su **Save** (Salva) per modificare le impostazioni della cache.

Modificare le impostazioni di scansione dei supporti per un volume

Una scansione dei supporti è un'operazione in background che esegue la scansione di tutti i dati e delle informazioni di ridondanza nel volume. Utilizzare questa opzione per attivare o disattivare le impostazioni di scansione dei supporti per uno o più volumi o per modificare la durata della scansione.

Prima di iniziare

Comprendere quanto segue:

- Le scansioni dei supporti vengono eseguite continuamente a una velocità costante in base alla capacità da sottoporre a scansione e alla durata della scansione. Le scansioni in background possono essere temporaneamente sospese da un'attività in background con priorità più alta (ad esempio ricostruzione), ma vengono rieseguite alla stessa velocità costante.

- La scansione di un volume viene eseguita solo quando l'opzione di scansione dei supporti è attivata per l'array di storage e per quel volume. Se è attivata anche la verifica della ridondanza per quel volume, le informazioni di ridondanza nel volume verranno controllate per verificarne la coerenza con i dati, a condizione che il volume disponga di ridondanza. La scansione dei supporti con controllo della ridondanza è attivata per impostazione predefinita per ciascun volume al momento della creazione.
- Se durante la scansione si verifica un errore irreversibile del supporto, i dati verranno riparati utilizzando le informazioni di ridondanza, se disponibili.

  Ad esempio, le informazioni di ridondanza sono disponibili in volumi RAID 5 ottimali o in volumi RAID 6 ottimali o con un solo disco guasto. Se l'errore irreversibile non può essere riparato utilizzando le informazioni di ridondanza, il blocco di dati viene aggiunto al registro del settore illeggibile. Nel registro eventi vengono riportati errori del supporto correggibili e non correggibili.

- Se il controllo di ridondanza rileva un'incoerenza tra i dati e le informazioni di ridondanza, viene riportato nel registro eventi.

A proposito di questa attività

Le scansioni dei supporti rilevano e riparano gli errori dei supporti sui blocchi di dischi che vengono raramente letti dalle applicazioni. Ciò può impedire la perdita di dati in caso di guasto di un disco, poiché i dati dei dischi guasti vengono ricostruiti utilizzando le informazioni di ridondanza e i dati di altri dischi nel gruppo di volumi o nel pool.

È possibile eseguire le seguenti operazioni:

- Attivare o disattivare la scansione dei supporti in background per l'intero array di storage
- Modificare la durata della scansione per l'intero array di storage
- Attivare o disattivare la scansione dei supporti per uno o più volumi
- Attivare o disattivare il controllo di ridondanza per uno o più volumi

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage contenente i volumi per i quali si desidera modificare le impostazioni di scansione dei supporti.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change media scan settings** (Altro[Modifica impostazioni di scansione dei supporti]).

   Viene visualizzata la finestra di dialogo Change Drive Media Scan Settings (Modifica impostazioni scansione supporti unità). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Per attivare la scansione dei supporti, selezionare la casella di controllo **scansione supporti durante…**. La disattivazione della casella di controllo scansione supporti consente di sospendere tutte le impostazioni di scansione dei supporti.
5. Specificare il numero di giorni in cui si desidera eseguire la scansione del supporto.
6. Selezionare la casella di controllo **Media Scan** per ciascun volume su cui si desidera eseguire una scansione dei supporti. Il sistema attiva l'opzione Redundancy Check (controllo ridondanza) per ciascun volume su cui si sceglie di eseguire una scansione dei supporti. Se esistono singoli volumi per i quali non si desidera eseguire un controllo di ridondanza, deselezionare la casella di controllo **controllo di ridondanza**.
7. Fare clic su **Save** (Salva).

Risultato

Il sistema applica le modifiche alle scansioni dei supporti in background in base alla selezione effettuata.

Elimina volume

È possibile eliminare uno o più volumi per aumentare la capacità libera di un pool o di un gruppo di volumi.

Prima di iniziare

Sui volumi che si intende eliminare, assicurarsi che:

- Viene eseguito il backup di tutti i dati.
- All Input/Output (i/o) viene interrotto.
- Tutti i dispositivi e i file system vengono smontati.

A proposito di questa attività

In genere, i volumi vengono eliminati se sono stati creati con parametri o capacità errati o se non soddisfano più le esigenze di configurazione dello storage. L'eliminazione di un volume aumenta la capacità libera nel pool o nel gruppo di volumi.

> L'eliminazione di un volume causa la perdita di tutti i dati presenti su tali volumi.

Tenere presente che **non è possibile** eliminare un volume che presenta una delle seguenti condizioni:

- Il volume è in fase di inizializzazione.
- Il volume è in fase di ricostruzione.
- Il volume fa parte di un gruppo di volumi che contiene un disco sottoposto a un'operazione copyback.
- Il volume sta subendo un'operazione di modifica, ad esempio una modifica delle dimensioni dei segmenti, a meno che il volume non sia ora nello stato Failed (guasto).
- Il volume contiene qualsiasi tipo di prenotazione persistente.
- Il volume è un volume di origine o un volume di destinazione in un volume di copia con stato Pending (in sospeso), in Progress (in corso) o Failed (non riuscito).

> Quando un volume supera una determinata dimensione (attualmente 128 TB), l'operazione di eliminazione viene eseguita in background e lo spazio liberato potrebbe non essere immediatamente disponibile.

Fasi

1. Dalla pagina **Manage** (Gestione), selezionare l'array di storage che contiene i volumi che si desidera eliminare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Volumes.

4. Selezionare uno o più volumi da eliminare, quindi confermare che si desidera eseguire l'operazione.
5. Fare clic su **Delete** (Elimina).

Configurare gli host

Panoramica sulla creazione dell'host

Per gestire lo storage con Storage Plugin per vCenter, è necessario individuare o definire ciascun host della rete. Un host è un server che invia i/o a un volume su un array di storage.

Creazione automatica o manuale degli host

La creazione di un host è una delle operazioni necessarie per consentire all'array di storage di sapere quali host sono collegati e di consentire l'accesso i/o ai volumi. Un host può essere creato automaticamente o manualmente.

- **Automatico** — la creazione automatica dell'host per gli host basati su SCSI (non NVMe-of) viene avviata dall'HCA (host Context Agent). HCA è un'utility che è possibile installare su ciascun host collegato allo storage array. Ogni host su cui è installato l'HCA invia le informazioni di configurazione ai controller degli array di storage attraverso il percorso i/O. In base alle informazioni sull'host, i controller creano automaticamente l'host e le porte host associate e impostano il tipo di host. Se necessario, è possibile apportare ulteriori modifiche alla configurazione dell'host. Dopo che l'HCA ha eseguito il rilevamento automatico, l'host viene configurato automaticamente con i seguenti attributi:
  - Il nome host derivato dal nome di sistema dell'host.
  - Le porte di identificazione host associate all'host.
  - Il tipo di sistema operativo host dell'host.

> Gli host vengono creati come host standalone; l'HCA non crea o aggiunge automaticamente ai cluster di host.

- **Manuale** — durante la creazione manuale dell'host, è possibile associare gli identificatori delle porte host selezionandoli da un elenco o inserendoli manualmente. Dopo aver creato un host, è possibile assegnarvi dei volumi o aggiungerlo a un cluster host se si intende condividere l'accesso ai volumi.

Modalità di assegnazione dei volumi

Per consentire a un host di inviare i/o a un volume, è necessario assegnarvi il volume. È possibile selezionare un host o un cluster di host quando si crea un volume oppure assegnarlo in un secondo momento a un host o a un cluster di host. Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.

L'assegnazione di volumi agli host è flessibile e consente di soddisfare le esigenze di storage specifiche.

- **Host standalone, non parte di un cluster di host** — è possibile assegnare un volume a un singolo host. È possibile accedere al volume solo da un host.
- **Cluster di host** — è possibile assegnare un volume a un cluster di host. Tutti gli host del cluster host possono accedere al volume.
- **Host all'interno di un cluster di host** — è possibile assegnare un volume a un singolo host che fa parte di un cluster di host. Anche se l'host fa parte di un cluster di host, è possibile accedere al volume solo dal singolo host e non da altri host del cluster di host.

Quando vengono creati i volumi, i LUN (Logical Unit Number) vengono assegnati automaticamente. Il LUN funge da indirizzo tra l'host e il controller durante le operazioni di i/O. Una volta creato il volume, è possibile

modificare i LUN.

Creare l’accesso all’host

Per gestire lo storage con Storage Plugin per vCenter, è necessario individuare o definire ciascun host della rete.

A proposito di questa attività

Creando un host, si definiscono i parametri host per fornire la connessione allo storage array e l’accesso i/o ai volumi.

È possibile consentire all’HCA (host Context Agent) di rilevare automaticamente gli host, quindi verificare che le informazioni siano corrette selezionando **Visualizza/Modifica impostazioni** dalla pagina Configura host. Tuttavia, l’HCA non è disponibile su tutti i sistemi operativi supportati ed è necessario creare l’host manualmente.

Quando si crea un host, tenere presenti le seguenti linee guida:

- È necessario definire le porte di identificazione host associate all’host.
- Assicurarsi di fornire lo stesso nome del nome di sistema assegnato all’host.
- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Fare clic sul **Create › host** (Crea[host]).

   Viene visualizzata la finestra di dialogo Create host (Crea host).

4. Selezionare le impostazioni per l’host in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare il sistema operativo in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia host	(Facoltativo) se si dispone di più tipi di interfaccia host supportati sull'array di storage, selezionare il tipo di interfaccia host che si desidera utilizzare.
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare l'interfaccia i/o** — in genere, le porte host devono essere state registrate ed essere disponibili dall'elenco a discesa. È possibile selezionare gli identificatori della porta host dall'elenco. • **Aggiunta manuale** — se un identificatore di porta host non viene visualizzato nell'elenco, significa che la porta host non ha effettuato l'accesso. È possibile utilizzare un'utility HBA o l'utility iSCSI Initiator per individuare gli identificatori delle porte host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dall'utility (uno alla volta) nel campo host ports (Porte host). È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori associati all'host. Ciascun identificatore viene visualizzato nel campo host ports (Porte host). Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto.
Impostare CHAP Initiator secret	(Facoltativo) se si seleziona o si immette manualmente una porta host con un IQN iSCSI e si desidera richiedere a un host che tenta di accedere allo storage array per l'autenticazione mediante Challenge Handshake Authentication Protocol (CHAP), selezionare la casella di controllo "Set CHAP Initiator secret" (Imposta CHAP initiator secret). Per ogni porta host iSCSI selezionata o inserita manualmente, procedere come segue: • Immettere lo stesso segreto CHAP impostato su ciascun iniziatore host iSCSI per l'autenticazione CHAP. Se si utilizza l'autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di validarsi nell'array di storage e a un array di storage di validarsi nell'host), è necessario impostare anche il segreto CHAP per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lasciare vuoto il campo se non si richiede l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato è CHAP.

5. Fare clic su **Create** (Crea).
6. Per aggiornare le informazioni sull'host, selezionare l'host dalla tabella e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

Risultato

Una volta creato correttamente l'host, il sistema crea un nome predefinito per ciascuna porta host configurata per l'host (etichetta utente). L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per l'host IPT è `IPT_1`.

Al termine

È necessario assegnare un volume a un host in modo che possa essere utilizzato per le operazioni di i/O. Passare a. "Assegnare volumi agli host".

Creare un cluster host

Quando due o più host richiedono l'accesso i/o agli stessi volumi, è possibile creare un cluster host.

A proposito di questa attività

Tenere presenti queste linee guida quando si crea un cluster host:

- Questa operazione non viene avviata a meno che non siano disponibili due o più host per la creazione del cluster.
- Gli host nei cluster di host possono avere sistemi operativi diversi (eterogenei).
- Gli host NVMe nei cluster di host non possono essere misti con host non NVMe.
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.

  Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare **Create › host cluster** (Crea[cluster host]).

   Viene visualizzata la finestra di dialogo Create host Cluster (Crea cluster host).

4. Selezionare le impostazioni appropriate per il cluster host.

Impostazione	Descrizione
Nome	Digitare il nome del nuovo cluster host.
Selezionare gli host per condividere l'accesso al volume	Selezionare due o più host dall'elenco a discesa. Vengono visualizzati nell'elenco solo gli host che non fanno già parte di un cluster di host.

5. Fare clic su **Create** (Crea).

Se gli host selezionati sono collegati a tipi di interfaccia che hanno diverse funzionalità di Data Assurance (da), viene visualizzata una finestra di dialogo con il messaggio che da non sarà disponibile sul cluster host. Questa non disponibilità impedisce l'aggiunta di volumi abilitati da al cluster host. Selezionare **Sì** per continuare o **No** per annullare.

DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente all'array di storage di verificare la presenza di errori che potrebbero verificarsi quando i dati vengono spostati tra gli host e i dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Risultato

Il nuovo cluster di host viene visualizzato nella tabella con gli host assegnati nelle righe sottostanti.

Al termine

È necessario assegnare un volume a un cluster host in modo che possa essere utilizzato per le operazioni di i/O. Passare a. "Assegnare volumi agli host".

Assegnare volumi agli host

È necessario assegnare un volume a un host o a un cluster di host in modo che possa essere utilizzato per le operazioni di i/O.

Prima di iniziare

Tenere presenti queste linee guida quando si assegnano volumi agli host:

- È possibile assegnare un volume a un solo host o cluster di host alla volta.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un LUN univoco.
- Per i nuovi gruppi di volumi, se si attende la creazione e l'inizializzazione di tutti i volumi prima di assegnarli a un host, il tempo di inizializzazione del volume viene ridotto. Tenere presente che, una volta mappato un volume associato al gruppo di volumi, tutti i volumi torneranno all'inizializzazione più lenta.

A proposito di questa attività

L'assegnazione di un volume consente a un host o a un cluster di host di accedere a tale volume in un array di storage.

Durante questa attività vengono visualizzati tutti i volumi non assegnati, ma le funzioni per gli host con o senza Data Assurance (da) si applicano come segue:

- Per un host da-capable, è possibile selezionare i volumi che sono da-enabled o non da-enabled.
- Per un host che non supporta da, se si seleziona un volume abilitato da, viene visualizzato un avviso che indica che il sistema deve disattivare automaticamente da sul volume prima di assegnarlo all'host.

  L'assegnazione di un volume non riesce nelle seguenti condizioni:

- Vengono assegnati tutti i volumi.
- Il volume è già assegnato a un altro host o cluster di host. La possibilità di assegnare un volume non è disponibile nelle seguenti condizioni:
- Non esistono host o cluster di host validi.
- Non sono stati definiti identificatori di porta host per l'host.

- Sono state definite tutte le assegnazioni dei volumi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host a cui si desidera assegnare i volumi, quindi fare clic su **Assign Volumes** (Assegna volumi).

   Viene visualizzata una finestra di dialogo che elenca tutti i volumi che è possibile assegnare. È possibile ordinare qualsiasi colonna o digitare qualcosa nella casella Filter (filtro) per semplificare la ricerca di volumi specifici.

4. Selezionare la casella di controllo accanto a ciascun volume che si desidera assegnare oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
5. Fare clic su **Assegna** per completare l'operazione.

Risultati

Dopo aver assegnato correttamente uno o più volumi a un host o a un cluster di host, il sistema esegue le seguenti operazioni:

- Il volume assegnato riceve il successivo numero LUN disponibile. L'host utilizza il numero LUN per accedere al volume.
- Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host. Se applicabile, il volume di accesso configurato in fabbrica viene visualizzato anche negli elenchi dei volumi associati all'host.

Annullare l'assegnazione dei volumi

Se non è più necessario l'accesso i/o a un volume, è possibile annullare l'assegnazione dall'host o dal cluster host.

A proposito di questa attività

Tenere presenti queste linee guida quando si annulla l'assegnazione di un volume:

- Se si rimuove l'ultimo volume assegnato da un cluster host e il cluster host dispone anche di host con volumi assegnati specifici, assicurarsi di rimuovere o spostare tali assegnazioni prima di rimuovere l'ultima assegnazione per il cluster host.
- Se un cluster host, un host o una porta host viene assegnata a un volume registrato nel sistema operativo, è necessario annullare la registrazione prima di poter rimuovere questi nodi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host che si desidera modificare, quindi fare clic su **Annulla assegnazione volumi**.

Viene visualizzata una finestra di dialogo che mostra tutti i volumi attualmente assegnati.

4. Selezionare la casella di controllo accanto a ciascun volume che si desidera annullare l'assegnazione oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
5. Fare clic su **Annulla assegnazione**.

Risultati

- I volumi non assegnati sono disponibili per una nuova assegnazione.
- Fino a quando le modifiche non vengono configurate sull'host, il volume viene ancora riconosciuto dal sistema operativo host.

Modificare le impostazioni di un host

È possibile modificare il nome, il tipo di sistema operativo host e i cluster host associati per un host o un cluster host.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti dell'host.

4. Per modificare le proprietà dell'host, assicurarsi che la scheda **Proprietà** sia selezionata, quindi modificare le impostazioni in base alle esigenze.

   Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome dell'host fornito dall'utente. Specificare un nome per l'host.
Cluster host associato	È possibile scegliere una delle seguenti opzioni: • **None** — l'host rimane un host standalone. Se l'host è stato associato a un cluster host, il sistema rimuove l'host dal cluster. • **<Host Cluster>** — il sistema associa l'host al cluster selezionato.
Tipo di sistema operativo host	È possibile modificare il tipo di sistema operativo in esecuzione sull'host definito.

5. Per modificare le impostazioni delle porte, fare clic sulla scheda **host Ports** (Porte host), quindi modificare le impostazioni in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Porta host	È possibile scegliere una delle seguenti opzioni: • **Add** — utilizzare Add per associare un nuovo identificatore di porta host all'host. La lunghezza del nome dell'identificatore della porta host è determinata dalla tecnologia dell'interfaccia host. I nomi degli identificatori delle porte host Fibre Channel e Infiniband devono contenere 16 caratteri. I nomi degli identificatori delle porte host iSCSI hanno un massimo di 223 caratteri. La porta deve essere univoca. Un numero di porta già configurato non è consentito. • **Delete** — utilizzare Delete per rimuovere (disassociare) un identificatore di porta host. L'opzione Delete (Elimina) non rimuove fisicamente la porta host. Questa opzione rimuove l'associazione tra la porta host e l'host. A meno che non si rimuovano host bus adapter o iSCSI Initiator, la porta host viene ancora riconosciuta dal controller. ! Se si elimina un identificatore di porta host, questo non viene più associato a questo host. Inoltre, l'host perde l'accesso a uno qualsiasi dei volumi assegnati tramite questo identificatore di porta host.
Etichetta	Per modificare il nome dell'etichetta della porta, fare clic sull'icona **Modifica** (matita). Il nome dell'etichetta della porta deve essere univoco. Un nome di etichetta già configurato non è consentito.
Segreto CHAP	Viene visualizzato solo per gli host iSCSI. È possibile impostare o modificare il segreto CHAP per gli iniziatori (host iSCSI). Il sistema utilizza il metodo CHAP (Challenge Handshake Authentication Protocol), che convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa chiamata CHAP secret (segreto CHAP).

6. Fare clic su **Save** (Salva).

Eliminare l'host o il cluster host

È possibile rimuovere un host o un cluster di host in modo che i volumi non siano più associati a tale host.

A proposito di questa attività

Tenere presenti queste linee guida quando si elimina un host o un cluster host:

- Tutte le assegnazioni di volume specifiche vengono eliminate e i volumi associati sono disponibili per una nuova assegnazione.
- Se l'host fa parte di un cluster host che dispone di assegnazioni specifiche, il cluster host non viene influenzato. Tuttavia, se l'host fa parte di un cluster di host che non ha altre assegnazioni, il cluster di host e qualsiasi altro host o identificativo di porta host associato ereditano eventuali assegnazioni predefinite.

- Tutti gli identificatori di porta host associati all'host diventano indefiniti.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host che si desidera eliminare, quindi fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo di conferma.

4. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Se si elimina un host, il sistema esegue le seguenti operazioni:

- Elimina l'host e, se applicabile, lo rimuove dal cluster host.
- Rimuove l'accesso a tutti i volumi assegnati.
- Riporta i volumi associati a uno stato non assegnato.
- Restituisce gli identificatori di porta host associati all'host a uno stato non associato. Se si elimina un cluster host, il sistema esegue le seguenti operazioni:
  - Elimina il cluster host e gli host associati (se presenti).
  - Rimuove l'accesso a tutti i volumi assegnati.
  - Riporta i volumi associati a uno stato non assegnato.
  - Restituisce gli identificatori di porta host associati agli host a uno stato non associato.

Configurare pool e gruppi di volumi

Panoramica dei pool e dei gruppi di volumi

Per eseguire il provisioning dello storage nel plug-in di storage per vCenter, creare un pool o un gruppo di volumi che conterrà i dischi rigidi (HDD) o SSD (Solid state Disk) che si desidera utilizzare nell'array di storage.

Provisioning

L'hardware fisico viene fornito in componenti logici in modo che i dati possano essere organizzati e recuperati facilmente. Sono supportati due tipi di raggruppamenti:

- Piscine
- Gruppi di volumi

I pool e i gruppi di volumi sono le unità di storage di livello superiore in un array di storage: Suddividono la capacità dei dischi in divisioni gestibili. All'interno di queste divisioni logiche si trovano i singoli volumi o LUN in cui sono memorizzati i dati.

Quando viene implementato un sistema storage, il primo passo consiste nel presentare la capacità disponibile dei dischi ai vari host:

- Creazione di pool o gruppi di volumi con capacità sufficiente
- Aggiunta del numero di dischi necessari per soddisfare i requisiti di performance al pool o al gruppo di volumi
- Selezione del livello di protezione RAID desiderato (se si utilizzano gruppi di volumi) per soddisfare specifici requisiti di business

È possibile avere pool o gruppi di volumi sullo stesso sistema di storage, ma un'unità non può far parte di più di un pool o gruppo di volumi. I volumi presentati agli host per i/o vengono quindi creati utilizzando lo spazio nel pool o nel gruppo di volumi.

Piscine

I pool sono progettati per aggregare i dischi rigidi fisici in un ampio spazio di storage e fornire una protezione RAID avanzata per l'IT. Un pool crea molti set RAID virtuali dal numero totale di dischi assegnati al pool e distribuisce i dati in modo uniforme tra tutti i dischi partecipanti. In caso di perdita o aggiunta di un disco, il sistema ribilancia dinamicamente i dati su tutti i dischi attivi.

I pool funzionano come un altro livello RAID, virtualizzando l'architettura RAID sottostante per ottimizzare le performance e la flessibilità durante l'esecuzione di attività come la ricostruzione, l'espansione del disco e la gestione della perdita del disco. Il sistema imposta automaticamente il livello RAID a 6 in una configurazione 8+2 (otto dischi dati più due dischi di parità).

Corrispondenza dei dischi

È possibile scegliere tra HDD o SSD da utilizzare nei pool; tuttavia, come per i gruppi di volumi, tutti i dischi nel pool devono utilizzare la stessa tecnologia. I controller selezionano automaticamente i dischi da includere, quindi è necessario assicurarsi di disporre di un numero sufficiente di dischi per la tecnologia scelta.

Gestione dei dischi guasti

I pool hanno una capacità minima di 11 dischi; tuttavia, la capacità di un disco è riservata alla capacità di riserva in caso di guasto di un disco. Questa capacità di riserva è chiamata "capacità di conservazione".

Quando vengono creati i pool, viene preservata una certa quantità di capacità per l'utilizzo in caso di emergenza. Questa capacità è espressa in termini di un certo numero di dischi, ma l'implementazione effettiva è distribuita nell'intero pool di dischi. La quantità predefinita di capacità conservata si basa sul numero di dischi nel pool.

Una volta creato il pool, è possibile modificare il valore della capacità di conservazione su una capacità maggiore o minore oppure impostarlo su una capacità di conservazione non pari a 0 unità. La capacità massima che è possibile conservare (espressa come numero di dischi) è 10, ma la capacità disponibile potrebbe essere inferiore, in base al numero totale di dischi nel pool.

Gruppi di volumi

I gruppi di volumi definiscono il modo in cui la capacità viene assegnata ai volumi nel sistema di storage. I dischi sono organizzati in gruppi RAID e i volumi risiedono tra i dischi di un gruppo RAID. Pertanto, le impostazioni di configurazione dei gruppi di volumi identificano i dischi che fanno parte del gruppo e il livello RAID utilizzato.

Quando si crea un gruppo di volumi, i controller selezionano automaticamente le unità da includere nel gruppo. È necessario scegliere manualmente il livello RAID per il gruppo. La capacità del gruppo di volumi corrisponde al numero totale di dischi selezionati, moltiplicato per la capacità.

Corrispondenza dei dischi

Per le dimensioni e le prestazioni, è necessario associare le unità del gruppo di volumi. Se nel gruppo di volumi sono presenti dischi più piccoli e più grandi, tutti i dischi vengono riconosciuti come la capacità più piccola. Se nel gruppo di volumi sono presenti dischi più lenti e veloci, tutti i dischi vengono riconosciuti alla velocità più bassa. Questi fattori influiscono sulle performance e sulla capacità complessiva del sistema storage.

Non è possibile combinare diverse tecnologie di dischi (dischi HDD e SSD). RAID 3, 5 e 6 sono limitati a un massimo di 30 dischi. RAID 1 e RAID 10 utilizzano il mirroring, pertanto questi gruppi di volumi devono avere un numero pari di dischi.

Gestione dei dischi guasti

I gruppi di volumi utilizzano i dischi hot spare come standby nel caso in cui un disco si guasti in volumi RAID 1/10, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. Un'unità hot spare non contiene dati e aggiunge un altro livello di ridondanza all'array di storage.

Se un disco si guasta nell'array di storage, il disco hot spare viene sostituito automaticamente per il disco guasto senza richiedere uno swap fisico. Se il disco hot spare è disponibile quando si verifica un guasto, il controller utilizza i dati di ridondanza per ricostruire i dati dal disco guasto al disco hot spare.

Decidere se utilizzare pool o gruppi di volumi

Scegli un pool

- Se hai bisogno di una ricostruzione più rapida dei dischi e di un'amministrazione dello storage semplificata e/o di un carico di lavoro altamente casuale.
- Se si desidera distribuire i dati per ciascun volume in modo casuale su un set di dischi che compongono il pool.non è possibile impostare o modificare il livello RAID dei pool o dei volumi nei pool. I pool utilizzano il livello RAID 6.

Scegliere un gruppo di volumi

- Se hai bisogno della massima larghezza di banda del sistema, della possibilità di ottimizzare le impostazioni dello storage e di un carico di lavoro altamente sequenziale.
- Se si desidera distribuire i dati tra i dischi in base a un livello RAID. È possibile specificare il livello RAID quando si crea il gruppo di volumi.
- Se si desidera scrivere i dati per ciascun volume in sequenza nel set di dischi che compongono il gruppo di volumi.

> Poiché i pool possono coesistere con i gruppi di volumi, un array di storage può contenere sia pool che gruppi di volumi.

Creazione automatica e manuale del pool

A seconda della configurazione dello storage, è possibile consentire al sistema di creare pool automaticamente o manualmente. Un pool è un insieme di dischi raggruppati in modo logico.

Prima di creare e gestire i pool, consultare le sezioni seguenti per sapere come vengono creati automaticamente i pool e quando potrebbe essere necessario crearli manualmente.

Creazione automatica

Quando il sistema rileva una capacità non assegnata nell'array di storage, avvia la creazione automatica del pool quando il sistema rileva una capacità non assegnata in un array di storage. Viene richiesto automaticamente di creare uno o più pool o di aggiungere la capacità non assegnata a un pool esistente o a entrambi.

La creazione automatica del pool si verifica quando si verifica una di queste condizioni:

- I pool non esistono nell'array di storage e sono presenti dischi simili a sufficienza per creare un nuovo pool.
- Vengono aggiunte nuove unità a un array di storage che dispone di almeno un pool.ogni unità in un pool deve essere dello stesso tipo di unità (HDD o SSD) e avere capacità simile. Il sistema richiede di completare le seguenti attività:
- Creare un singolo pool se il numero di dischi di questi tipi è sufficiente.
- Creare più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
- Aggiungere le unità al pool esistente se un pool è già definito nell'array di storage e aggiungere nuove unità dello stesso tipo di disco al pool.
- Aggiungere i dischi dello stesso tipo al pool esistente e utilizzare gli altri tipi di dischi per creare pool diversi se i nuovi dischi sono di tipi diversi.

Creazione manuale

Se la creazione automatica non riesce a determinare la configurazione migliore, potrebbe essere necessario creare un pool manualmente. Questa situazione può verificarsi per uno dei seguenti motivi:

- I nuovi dischi potrebbero essere aggiunti a più di un pool.
- Uno o più dei nuovi candidati al pool possono utilizzare la protezione contro la perdita di shelf o la protezione contro la perdita di cassetto.
- Uno o più dei candidati attuali del pool non possono mantenere la protezione contro la perdita di shelf o lo stato di protezione contro la perdita di cassetto.è anche possibile creare un pool manualmente se si dispone di più applicazioni sull'array di storage e non si desidera che siano in concorrenza con le stesse risorse di disco. In questo caso, è possibile creare manualmente un pool più piccolo per una o più applicazioni. È possibile assegnare solo uno o due volumi invece di assegnare il carico di lavoro a un pool di grandi dimensioni con molti volumi attraverso i quali distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di un'applicazione specifica può consentire alle operazioni degli array di storage di funzionare più rapidamente, con meno conflitti.

Crea pool automaticamente

È possibile creare pool automaticamente quando il sistema rileva almeno 11 dischi non assegnati o rileva un disco non assegnato idoneo per un pool esistente. Un pool è un insieme di dischi raggruppati in modo logico.

Prima di iniziare

È possibile avviare la finestra di dialogo Configurazione automatica pool quando si verifica una delle seguenti condizioni:

- È stato rilevato almeno un disco non assegnato che può essere aggiunto a un pool esistente con tipi di disco simili.
- Sono stati rilevati undici (11) o più dischi non assegnati che possono essere utilizzati per creare un nuovo

pool (se non possono essere aggiunti a un pool esistente a causa di tipi di dischi diversi).

A proposito di questa attività

È possibile utilizzare la creazione automatica del pool per configurare facilmente tutte le unità non assegnate nell'array di storage in un unico pool e per aggiungere unità nei pool esistenti.

Tenere presente quanto segue:

- Quando si aggiungono dischi a un array di storage, il sistema rileva automaticamente i dischi e richiede di creare un singolo pool o più pool in base al tipo di disco e alla configurazione corrente.
- Se i pool sono stati precedentemente definiti, il sistema richiede automaticamente di aggiungere le unità compatibili a un pool esistente. Quando vengono aggiunte nuove unità a un pool esistente, il sistema ridistribuisce automaticamente i dati nella nuova capacità, che ora include le nuove unità aggiunte.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Per la creazione del pool, è necessario utilizzare tutti i dischi dell'array di storage.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare **More › Avvia configurazione automatica del pool**.

   La tabella dei risultati elenca i nuovi pool, i pool esistenti con le unità aggiunte o entrambi. Per impostazione predefinita, un nuovo pool viene denominato con un numero sequenziale.

   Si noti che il sistema esegue le seguenti operazioni:

   - Crea un singolo pool se il numero di dischi con lo stesso tipo di disco (HDD o SSD) è sufficiente e la capacità è simile.
   - Crea più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
   - Aggiunge le unità a un pool esistente se un pool è già definito nell'array di storage e si aggiungono nuove unità dello stesso tipo di disco al pool.
   - Aggiunge le unità dello stesso tipo di unità al pool esistente e utilizza gli altri tipi di unità per creare pool diversi se le nuove unità sono di tipi diversi di unità.
4. Per modificare il nome di un nuovo pool, fare clic sull'icona **Modifica** (la matita).
5. Per visualizzare ulteriori caratteristiche del pool, posizionare il cursore o toccare l'icona Dettagli (la pagina).

   Vengono visualizzate informazioni relative al tipo di disco, alla funzionalità di sicurezza, alla funzione di data assurance (da), alla protezione contro la perdita di shelf e alla protezione contro la perdita di cassetto.

   Per gli array di storage EF600 e EF300, vengono visualizzate anche le impostazioni relative al provisioning delle risorse e alle dimensioni dei blocchi di volume.

6. Fare clic su **Accept** (Accetta).

Creare il pool manualmente

È possibile creare un pool manualmente se l'installazione non soddisfa i requisiti per la configurazione automatica del pool. Un pool è un insieme di dischi raggruppati in modo

logico.

Prima di iniziare

- È necessario disporre di un minimo di 11 dischi con lo stesso tipo di disco (HDD o SSD).
- La protezione contro la perdita di shelf richiede che i dischi che compongono il pool si trovino in almeno sei diversi shelf di dischi e che non vi siano più di due dischi in un singolo shelf di dischi.
- La protezione contro la perdita di cassetto richiede che le unità che compongono il pool siano collocate in almeno cinque cassetti diversi e che il pool includa un numero uguale di shelf di dischi da ciascun cassetto.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Per la creazione del pool, è necessario utilizzare tutti i dischi dell'array di storage.

A proposito di questa attività

Durante la creazione del pool, determinerai le sue caratteristiche, come il tipo di disco, la funzionalità di sicurezza, la funzionalità di data assurance (da), la protezione contro la perdita di shelf e la protezione contro la perdita di cassetto.

Per gli array di storage EF600 e EF300, le impostazioni includono anche il provisioning delle risorse e le dimensioni dei blocchi di volume.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › Pool** (Crea[Pool])

   Viene visualizzata la finestra di dialogo Create Pool (Crea pool).

4. Digitare un nome per il pool.
5. (Facoltativo) se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   La tabella dei risultati elenca tutti i pool possibili che è possibile creare.

6. Selezionare il pool candidato che si desidera utilizzare in base alle seguenti caratteristiche, quindi fare clic su **Create** (Crea).

Dettagli campo

Caratteristica	Utilizzare
Capacità libera	Mostra la capacità libera del pool Candidate in GiB. Selezionare un pool candidato con la capacità adatta alle esigenze di storage dell'applicazione. Anche la capacità di conservazione (spare) viene distribuita in tutto il pool e non fa parte della capacità libera.
Totale dischi	Mostra il numero di dischi disponibili nel pool Candidate. Il sistema riserva automaticamente il maggior numero possibile di dischi per la capacità di conservazione (per ogni sei dischi in un pool, il sistema riserva un disco per la capacità di conservazione). Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti.
Dimensioni blocco unità (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che i dischi del pool possono scrivere. I valori possono includere: • 512 — dimensione del settore di 512 byte. • 4K — dimensione del settore di 4,096 byte.
Sicuro	Indica se il pool candidato è costituito interamente da dischi con funzionalità di protezione, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). • È possibile proteggere il pool con Drive Security, ma tutte le unità devono essere sicure per poter utilizzare questa funzione. • Se si desidera creare un pool solo FDE, cercare **Yes - FDE** nella colonna Secure-capable. Se si desidera creare un pool solo FIPS, cercare **Sì - FIPS** o **Sì - FIPS (misto)**. "Misto" indica una combinazione di dischi di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il pool funzionerà al livello di sicurezza inferiore (140-2). • È possibile creare un pool composto da dischi che possono essere o meno sicuri o che sono una combinazione di livelli di sicurezza. Se i dischi del pool includono dischi che non sono sicuri, non è possibile rendere il pool sicuro.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se il pool è protetto ed è stata creata una chiave di sicurezza, è possibile attivare la protezione selezionando la casella di controllo. L'unico modo per rimuovere Drive Security dopo averlo attivato è eliminare il pool e cancellare i dischi.

Caratteristica	Utilizzare
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo candidato del pool. DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. Se si desidera utilizzare da, selezionare un pool che supporti da. Questa opzione è disponibile solo se la funzione da è stata attivata. Un pool può contenere dischi che supportano da o non da, ma tutti i dischi devono essere in grado di utilizzare questa funzione.
Funzionalità di provisioning delle risorse (solo EF300 e EF600)	Mostra se il provisioning delle risorse è disponibile per questo candidato del pool. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.
Protezione contro la perdita di shelf	Mostra se è disponibile la protezione contro la perdita di shelf. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool se si verifica una perdita totale di comunicazione con un singolo shelf di dischi.
Protezione in caso di perdita del cassetto	Mostra se è disponibile la protezione contro le perdite dei cassetti, fornita solo se si utilizza uno shelf di dischi che contiene cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi in un pool se si verifica una perdita totale di comunicazione con un singolo cassetto in uno shelf di dischi.
Dimensioni dei blocchi di volume supportate (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per i volumi nel pool: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Creare un gruppo di volumi

È possibile creare un gruppo di volumi per uno o più volumi accessibili all'host. Un gruppo di volumi è un container per volumi con caratteristiche condivise, come il livello RAID e la capacità.

Prima di iniziare

Consultare le seguenti linee guida:

- È necessario almeno un disco non assegnato.
- Esistono dei limiti per quanto riguarda la capacità di un disco in un singolo gruppo di volumi. Questi limiti variano in base al tipo di host.
- Per attivare la protezione contro la perdita di scaffali/cassetti, è necessario creare un gruppo di volumi che utilizzi dischi posizionati in almeno tre shelf o cassetti, a meno che non si utilizzi RAID 1, dove due

shelf/cassetti sono il minimo.

- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Il sistema attualmente consente la selezione del disco nella funzione Advanced (Avanzate) quando si crea un gruppo di volumi.

Esaminare in che modo la scelta del livello RAID influisce sulla capacità risultante del gruppo di volumi.

- Se si seleziona RAID 1, è necessario aggiungere due dischi alla volta per assicurarsi che sia selezionata una coppia mirrorata. Il mirroring e lo striping (noto come RAID 10 o RAID 1+0) si ottengono selezionando quattro o più dischi.
- Se si seleziona RAID 5, è necessario aggiungere almeno tre dischi per creare il gruppo di volumi.
- Se si seleziona RAID 6, è necessario aggiungere almeno cinque dischi per creare il gruppo di volumi.

A proposito di questa attività

Durante la creazione del gruppo di volumi, è possibile determinare le caratteristiche del gruppo, ad esempio il numero di dischi, la funzionalità di sicurezza, la funzionalità di data assurance (da), la protezione contro la perdita di shelf e la protezione contro la perdita di cassetto.

Per gli array di storage EF600 e EF300, le impostazioni includono anche il provisioning delle risorse, le dimensioni dei blocchi dei dischi e le dimensioni dei blocchi dei volumi.

> Con dischi con capacità maggiore e la possibilità di distribuire volumi tra controller, la creazione di più di un volume per gruppo di volumi è un buon modo per sfruttare la capacità dello storage e proteggere i dati.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage per il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › Volume group** (Crea[gruppo di volumi]).

   Viene visualizzata la finestra di dialogo Create Volume Group (Crea gruppo di volumi).

4. Digitare un nome per il gruppo di volumi.
5. Seleziona il livello RAID che meglio soddisfa i tuoi requisiti di storage e protezione dei dati. Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il livello RAID selezionato.
6. (Facoltativo) se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il tipo di disco e il livello RAID selezionati.

7. (Facoltativo) è possibile selezionare il metodo automatico o manuale per definire le unità da utilizzare nel gruppo di volumi. Il metodo automatico è la selezione predefinita.

   > Non utilizzare il metodo manuale a meno che non si sia esperti in grado di comprendere la ridondanza dei dischi e le configurazioni ottimali dei dischi.

Per selezionare i dischi manualmente, fare clic sul collegamento **Manually Select drives (Advanced)** (Seleziona manualmente i dischi (avanzati)**). Quando si fa clic su di esso, viene visualizzato *Automatically Select drives (Advanced)**.

Il metodo Manuale consente di selezionare le unità specifiche che compongono il gruppo di volumi. È possibile selezionare dischi non assegnati specifici per ottenere la capacità richiesta. Se l'array di storage contiene dischi con tipi di supporti diversi o tipi di interfaccia diversi, è possibile scegliere solo la capacità non configurata per un singolo tipo di disco per creare il nuovo gruppo di volumi.

8. In base alle caratteristiche del disco visualizzate, selezionare le unità che si desidera utilizzare nel gruppo di volumi, quindi fare clic su **Create** (Crea).

Le caratteristiche del disco visualizzate dipendono dalla selezione del metodo automatico o manuale. Per ulteriori informazioni, consultare la documentazione di Gestione di sistema di SANtricity, "Creare un gruppo di volumi".

Aggiungere capacità a un pool o a un gruppo di volumi

È possibile aggiungere dischi per espandere la capacità libera in un pool o un gruppo di volumi esistente.

Prima di iniziare

- I dischi devono essere in uno stato ottimale.
- I dischi devono avere lo stesso tipo di disco (HDD o SSD).
- Il pool o il gruppo di volumi deve essere in uno stato ottimale.
- Se il pool o il gruppo di volumi contiene tutti i dischi con funzionalità di protezione, aggiungere solo i dischi in grado di protezione per continuare a utilizzare le funzionalità di crittografia dei dischi con funzionalità di protezione.

Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard).

A proposito di questa attività

In questa attività, è possibile aggiungere capacità libera da includere nel pool o nel gruppo di volumi. È possibile utilizzare questa capacità libera per creare volumi aggiuntivi. I dati nei volumi rimangono accessibili durante questa operazione.

Per i pool, è possibile aggiungere un massimo di 60 dischi alla volta. Per i gruppi di volumi, è possibile aggiungere un massimo di due dischi alla volta. Se è necessario aggiungere più dischi del numero massimo, ripetere la procedura. (Un pool non può contenere più dischi rispetto al limite massimo per un array di storage).

> Con l'aggiunta di dischi, potrebbe essere necessario aumentare la capacità di conservazione. Si consiglia di aumentare la capacità riservata dopo un'operazione di espansione.

> Evitare di utilizzare dischi che siano in grado di aggiungere capacità a un pool o a un gruppo di volumi che non sono in grado di supportare da. Il pool o il gruppo di volumi non può sfruttare le funzionalità del disco da-capable. Prendere in considerazione l'utilizzo di dischi che non sono in grado di supportare da in questa situazione.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.

2. Selezionare **Provisioning › Configura pool e gruppi di volumi**.
3. Selezionare il pool o il gruppo di volumi a cui si desidera aggiungere le unità, quindi fare clic su **Add Capacity** (Aggiungi capacità).

   Viene visualizzata la finestra di dialogo Add Capacity (Aggiungi capacità). Vengono visualizzate solo le unità non assegnate compatibili con il pool o il gruppo di volumi.

4. In **Select drives to add Capacity…** (Seleziona dischi per aggiungere capacità), selezionare una o più unità che si desidera aggiungere al pool o al gruppo di volumi esistente.

   Il firmware del controller dispone le unità non assegnate con le opzioni migliori elencate in alto. La capacità libera totale aggiunta al pool o al gruppo di volumi viene visualizzata sotto l'elenco in **capacità totale selezionata**.

Dettagli campo

Campo	Descrizione
Shelf	Indica la posizione dello shelf del disco.
Baia	Indica la posizione dell'alloggiamento del disco
Capacità (GiB)	Indica la capacità del disco. • Se possibile, selezionare dischi con capacità uguale a quella dei dischi correnti nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità inferiore, tenere presente che la capacità utilizzabile di ogni disco attualmente presente nel pool o nel gruppo di volumi è ridotta. Pertanto, la capacità del disco è la stessa nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità maggiore, tenere presente che la capacità utilizzabile dei dischi non assegnati aggiunti viene ridotta in modo che corrispondano alle capacità correnti dei dischi nel pool o nel gruppo di volumi.
Sicuro	Indica se il disco è sicuro. • È possibile proteggere il pool o il gruppo di volumi con la funzione Drive Security, ma per utilizzare questa funzione è necessario che tutti i dischi siano protetti. • È possibile creare un pool o un gruppo di volumi con una combinazione di dischi sicuri e non sicuri, ma non è possibile attivare la funzione Drive Security. • Un pool o un gruppo di volumi con tutti i dischi con funzionalità di protezione non può accettare un disco con funzionalità di protezione non sicura per lo sparing o l'espansione, anche se la funzionalità di crittografia non è in uso. • Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). Un disco FIPS può essere di livello 140-2 o 140-3, con il livello 140-3 come livello di sicurezza superiore. Se si seleziona una combinazione di dischi di livello 140-2 e 140-3, il pool o il gruppo di volumi opereranno al livello di sicurezza inferiore (140-2).

Campo	Descrizione
Compatibile CON DA	Indica se il disco è compatibile con Data Assurance (da). • Si sconsiglia l'utilizzo di dischi che non sono in grado di aggiungere capacità a un pool o a un gruppo di volumi con funzionalità da. Il pool o il gruppo di volumi non dispone più delle funzionalità da e non è più possibile attivare il da sui volumi appena creati all'interno del pool o del gruppo di volumi. • Si sconsiglia l'utilizzo di dischi in grado di aggiungere capacità a un pool o a un gruppo di volumi non compatibili con da, in quanto tale pool o gruppo di volumi non può sfruttare le funzionalità del disco compatibile con da (gli attributi del disco non corrispondono). Considerare l'utilizzo di dischi non compatibili con da in questa situazione.
Compatibile con DULBE	Indica se il disco dispone dell'opzione Deallocated (disallocato) o Unwritten Logical Block Error (DULBE). DULBE è un'opzione sui dischi NVMe che consente allo storage array EF300 o EF600 di supportare volumi con provisioning di risorse.

5. Fare clic su **Aggiungi**.

   Se si aggiungono unità a un pool o a un gruppo di volumi, viene visualizzata una finestra di dialogo di conferma se si seleziona un'unità che impedisce al pool o al gruppo di volumi di avere uno o più dei seguenti attributi:

   - Protezione contro la perdita di shelf
   - Protezione in caso di perdita del cassetto
   - Funzionalità di crittografia completa del disco
   - Funzionalità Data Assurance
   - Funzionalità DULBE
6. Per continuare, fare clic su **Sì**, altrimenti fare clic su **Annulla**.

Risultato

Dopo aver aggiunto le unità non assegnate a un pool o a un gruppo di volumi, i dati di ciascun volume del pool o del gruppo di volumi vengono ridistribuiti per includere le unità aggiuntive.

Creazione della cache SSD

Per accelerare dinamicamente le performance del sistema, puoi utilizzare la funzione SSD cache per memorizzare nella cache i dati più utilizzati (dati "hot") su unità a stato solido (SSD) a latenza inferiore. La cache SSD viene utilizzata esclusivamente per le letture host.

Prima di iniziare

L'array di storage deve contenere alcune unità SSD.

La cache SSD non è disponibile sul sistema storage EF600 o EF300.

A proposito di questa attività

Quando crei una cache SSD, puoi utilizzare una o più unità. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. Selezionare i volumi che si desidera memorizzare nella cache, quindi il caching viene automaticamente e dinamico.

Per creare la cache SSD, seguire queste linee guida.

- È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
- È supportata una sola cache SSD per array di storage.
- La capacità massima di cache SSD utilizzabile su un array di storage dipende dalla capacità della cache primaria del controller.
- La cache SSD non è supportata sulle immagini Snapshot.
- Se si importano o esportano volumi con cache SSD attivata o disattivata, i dati memorizzati nella cache non vengono importati o esportati.
- Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.
- Se i volumi associati sono abilitati per la sicurezza, creare una cache SSD abilitata per la sicurezza.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per la cache.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › SSD cache** (Crea[cache SSD]).

   Viene visualizzata la finestra di dialogo Create SSD cache (Crea cache SSD).

4. Digitare un nome per la cache SSD.
5. Selezionare l'SSD cache Candidate che si desidera utilizzare in base alle seguenti caratteristiche.

Dettagli campo

Caratteristica	Utilizzare
Capacità	Mostra la capacità disponibile in GiB. Selezionare la capacità per le esigenze di storage dell'applicazione. La capacità massima per la cache SSD dipende dalla capacità della cache primaria del controller. Se si assegna una quantità superiore a quella massima alla cache SSD, la capacità aggiuntiva non è utilizzabile. La capacità della cache SSD è importante per la capacità complessiva allocata.
Dischi totali	Mostra il numero di dischi disponibili per questa cache SSD. Selezionare l'SSD candidate con il numero di dischi desiderato
Sicuro	Indica se SSD cache Candidate è composto interamente da dischi sicuri, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). Se si desidera creare una cache SSD sicura, cercare "Yes - FDE" o "Yes - FIPS" nella colonna Secure-capable.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se si desidera creare una cache SSD abilitata per la protezione, selezionare la casella di controllo **Enable Security** (attiva sicurezza). NOTA: Una volta attivata, la protezione non può essere disattivata. È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo SSD cache Candidate. Data Assurance (da) verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Se si desidera utilizzare il da, selezionare un SSD cache Candidate che sia compatibile con il da. Questa opzione è disponibile solo se la funzione da è stata attivata. La cache SSD può contenere sia dischi da-capable che non da-capable, ma tutti i dischi devono essere da-capable per poter utilizzare da.

6. Associare la cache SSD ai volumi per i quali si desidera implementare il caching in lettura SSD. Per attivare immediatamente la cache SSD sui volumi compatibili, selezionare la casella di controllo **Enable SSD cache on existing compatible volumes that are mapped to hosts** (attiva cache SSD sui volumi compatibili esistenti mappati agli host).

   I volumi sono compatibili se condividono le stesse funzionalità di Drive Security e da.

7. Fare clic su **Create** (Crea).

Modificare le impostazioni di configurazione di un pool

È possibile modificare le impostazioni di un pool, inclusi nome, impostazioni degli avvisi di capacità, priorità di modifica e capacità di conservazione.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni di configurazione per un pool.

Non è possibile modificare il livello RAID di un pool utilizzando l'interfaccia del plug-in. Il plug-in configura automaticamente i pool come RAID 6.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il pool che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Pool Settings (Impostazioni pool).

4. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del pool in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome del pool fornito dall'utente. Specificare un nome per un pool è obbligatorio.
Avvisi di capacità	È possibile inviare notifiche di avviso quando la capacità libera di un pool raggiunge o supera una determinata soglia. Quando i dati memorizzati nel pool superano la soglia specificata, il plug-in invia un messaggio, consentendo di aggiungere più spazio di storage o di eliminare oggetti non necessari. Gli avvisi vengono visualizzati nell'area Notifiche della dashboard e possono essere inviati dal server agli amministratori tramite messaggi e-mail e messaggi trap SNMP. È possibile definire i seguenti avvisi di capacità: • **Critical alert** — questo avviso critico informa l'utente quando la capacità libera nel pool raggiunge o supera la soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica. • **Early alert** — questo avviso anticipato informa l'utente quando la capacità libera di un pool sta raggiungendo una soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica.
Priorità di modifica	È possibile specificare i livelli di priorità per le operazioni di modifica in un pool in relazione alle prestazioni del sistema. Una priorità più elevata per le operazioni di modifica in un pool consente di completare più rapidamente un'operazione, ma può rallentare le prestazioni di i/o dell'host. Una priorità più bassa fa sì che le operazioni richiedano più tempo, ma le prestazioni di i/o dell'host ne risentono meno. È possibile scegliere tra cinque livelli di priorità: Minimo, basso, medio, alto e massimo. Maggiore è il livello di priorità, maggiore è l'impatto sull'i/o host e sulle prestazioni del sistema. • **Priorità di ricostruzione critica** — questa barra di scorrimento determina la priorità di un'operazione di ricostruzione dei dati quando guasti multipli dei dischi causano una condizione in cui alcuni dati non hanno ridondanza e un guasto aggiuntivo dei dischi potrebbe causare la perdita di dati. • **Priorità di ricostruzione degradata** — questa barra di scorrimento determina la priorità dell'operazione di ricostruzione dei dati quando si verifica un guasto al disco, ma i dati continuano a essere ridondanti e un guasto aggiuntivo al disco non comporta la perdita di dati. • **Priorità delle operazioni in background** — questa barra di scorrimento determina la priorità delle operazioni in background del pool che si verificano mentre il pool si trova in uno stato ottimale. Queste operazioni includono Dynamic Volume Expansion (DVE), Instant Availability Format (IAF) e la migrazione dei dati su un disco sostituito o aggiunto.

Impostazione	Descrizione
Capacità di conservazione ("capacità di ottimizzazione" per EF600 o EF300)	**Capacità di conservazione** — è possibile definire il numero di dischi per determinare la capacità riservata al pool per supportare potenziali guasti del disco. Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti. I pool utilizzano la capacità di conservazione durante il processo di ricostruzione dei dati invece delle unità hot spare, utilizzate nei gruppi di volumi. Utilizzare i controlli di spinner per regolare il numero di dischi. In base al numero di dischi, la capacità di conservazione nel pool viene visualizzata accanto alla casella di selezione. Tenere presenti le seguenti informazioni sulla capacità di conservazione. • Poiché la capacità di conservazione viene sottratta dalla capacità libera totale di un pool, la quantità di capacità che si riserva influisce sulla quantità di capacità libera disponibile per la creazione dei volumi. Se si specifica 0 per la capacità di conservazione, tutta la capacità libera del pool viene utilizzata per la creazione del volume. • Se si riduce la capacità di conservazione, si aumenta la capacità che può essere utilizzata per i volumi del pool. **Capacità di ottimizzazione aggiuntiva (solo array EF600 e EF300)** — quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e performance e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

5. Fare clic su **Save** (Salva).

Modificare le impostazioni di configurazione di un gruppo di volumi

È possibile modificare le impostazioni di un gruppo di volumi, inclusi il nome e il livello RAID.

Prima di iniziare

Se si modifica il livello RAID per soddisfare le esigenze di performance delle applicazioni che accedono al gruppo di volumi, assicurarsi di soddisfare i seguenti prerequisiti:

- Il gruppo di volumi deve trovarsi in uno stato ottimale.

- È necessario disporre di capacità sufficiente nel gruppo di volumi per la conversione al nuovo livello RAID.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il gruppo di volumi che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Group Settings (Impostazioni gruppo di volumi).

4. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del gruppo di volumi in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome fornito dall'utente del gruppo di volumi. Specificare un nome per un gruppo di volumi.
Livello RAID	Selezionare il nuovo livello RAID dal menu a discesa. • **RAID 0 striping** — offre performance elevate ma non fornisce alcuna ridondanza dei dati. Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi. Un gruppo RAID di striping combina due o più dischi in un'unica grande unità logica. • **Mirroring RAID 1** — offre performance elevate e la migliore disponibilità dei dati ed è adatto per la memorizzazione di dati sensibili a livello aziendale o personale. Protegge i dati eseguendo automaticamente il mirroring del contenuto di un disco nel secondo disco della coppia mirrorata. Fornisce protezione in caso di guasto di un singolo disco. • **RAID 10 striping/mirroring** — fornisce una combinazione di RAID 0 (striping) e RAID 1 (mirroring) e si ottiene selezionando quattro o più dischi. RAID 10 è adatto per applicazioni di transazioni di volumi elevati, come un database, che richiedono performance elevate e tolleranza agli errori. • **RAID 5** — ottimale per ambienti multiutente (come storage di database o file system) in cui le dimensioni i/o tipiche sono ridotte e l'attività di lettura è molto elevata. • **RAID 6** — ottimale per ambienti che richiedono una protezione di ridondanza oltre RAID 5, ma che non richiedono elevate prestazioni di scrittura. RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando (CLI). Quando si modifica il livello RAID, non è possibile annullare questa operazione dopo l'inizio. Durante la modifica, i dati rimangono disponibili.
Capacità di ottimizzazione (solo array EF600)	Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e prestazioni e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

5. Fare clic su **Save** (Salva).

Viene visualizzata una finestra di dialogo di conferma se la capacità viene ridotta, la ridondanza del volume viene persa o la protezione dalla perdita di shelf/cassetto viene persa a seguito della modifica del livello RAID. Selezionare **Sì** per continuare, altrimenti fare clic su **No**.

Risultato

Se si modifica il livello RAID per un gruppo di volumi, il plug-in modifica i livelli RAID di ogni volume che comprende il gruppo di volumi. Le prestazioni potrebbero essere leggermente compromesse durante l'operazione.

Modificare le impostazioni della cache SSD

È possibile modificare il nome della cache SSD e visualizzarne lo stato, la capacità massima e corrente, lo stato di Drive Security e Data Assurance e i volumi e i dischi associati.

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con la cache SSD.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare la cache SSD che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo SSD cache Settings (Impostazioni cache SSD).

4. Rivedere o modificare le impostazioni della cache SSD in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	Visualizza il nome della cache SSD, che è possibile modificare. È necessario specificare un nome per la cache SSD.
Caratteristiche	Mostra lo stato della cache SSD. Gli stati possibili includono: • Ottimale • Sconosciuto • Degradato • Non riuscito (Uno stato di errore determina un evento MEL critico). • Sospeso
Capacità	Mostra la capacità corrente e la capacità massima consentita per la cache SSD. La capacità massima consentita per la cache SSD dipende dalle dimensioni della cache principale del controller: • Fino a 1 GiB • Da 1 GiB a 2 GiB • Da 2 GiB a 4 GiB • Più di 4 GiB
Sicurezza e da	Mostra lo stato di Drive Security e Data Assurance per la cache SSD. • **Secure-capable** - indica se la cache SSD è composta interamente da dischi sicuri. Un disco sicuro è un disco con crittografia automatica in grado di proteggere i propri dati da accessi non autorizzati. • **Secure-enabled** — indica se la sicurezza è attivata nella cache SSD. • **Da Capable** — indica se la cache SSD è composta interamente da dischi compatibili con da. Un disco con funzionalità da può controllare e correggere gli errori che potrebbero verificarsi quando i dati vengono comunicati tra l'host e lo storage array.
Oggetti associati	Mostra i volumi e i dischi associati alla cache SSD.

5. Fare clic su **Save** (Salva).

Visualizzare le statistiche della cache SSD

È possibile visualizzare le statistiche per la cache SSD, ad esempio letture, scritture, accessi alla cache, percentuale di allocazione della cache, e percentuale di utilizzo della cache.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

A proposito di questa attività

Le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate, sono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare statistiche dettagliate per la cache SSD solo quando si esportano tutte le statistiche SSD in un file .csv.

Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con la cache SSD.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare la cache SSD per la quale si desidera visualizzare le statistiche, quindi fare clic su **More › View SSD cache** statistics.

   Viene visualizzata la finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD) che visualizza le statistiche nominali per la cache SSD selezionata.

   Dettagli campo

Impostazione	Descrizione
Letture	Mostra il numero totale di letture host dai volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Scrive	Il numero totale di scritture dell'host nei volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Riscontri nella cache	Mostra il numero di accessi alla cache.
La cache colpisce %	Mostra la percentuale di accessi alla cache. Questo numero deriva da riscontri cache / (letture + scritture). La percentuale di hit della cache deve essere superiore al 50% per un funzionamento efficace della cache SSD.
Allocazione della cache %	Mostra la percentuale di storage cache SSD allocato, espressa come percentuale dello storage cache SSD disponibile per questo controller e derivata dai byte allocati/disponibili.
% Utilizzo cache	Mostra la percentuale di storage cache SSD che contiene i dati dei volumi abilitati, espressa come percentuale di storage cache SSD allocata. Questa quantità rappresenta l'utilizzo o la densità della cache SSD. Derivato da byte allocati/byte disponibili.
Esporta tutto	Esporta tutte le statistiche della cache SSD in formato CSV. Il file esportato contiene tutte le statistiche disponibili per la cache SSD (nominale e dettagliata).

4. Fare clic su **Annulla** per chiudere la finestra di dialogo.

Controllare la ridondanza del volume

Sotto la guida del supporto tecnico o secondo le istruzioni del Recovery Guru, è possibile controllare la ridondanza su un volume in un pool o un gruppo di volumi per determinare se i dati su quel volume sono coerenti.

I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

Prima di iniziare

- Lo stato del pool o del gruppo di volumi deve essere ottimale.
- Il pool o il gruppo di volumi non deve avere alcuna operazione di modifica del volume in corso.
- È possibile controllare la ridondanza su qualsiasi livello RAID tranne su RAID 0, perché RAID 0 non ha ridondanza dei dati. (I pool sono configurati solo come RAID 6).

> Controllare la ridondanza del volume solo quando richiesto dal Recovery Guru e sotto la guida del supporto tecnico.

A proposito di questa attività

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6 e verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se il firmware del controller determina che i dati sono incoerenti.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare **operazioni non comuni › controllare la ridondanza del volume**.

   Viene visualizzata la finestra di dialogo Check Redundancy (verifica ridondanza).

4. Selezionare i volumi che si desidera controllare, quindi digitare check per confermare che si desidera eseguire questa operazione.
5. Fare clic su **Controlla**.

   Viene avviata l'operazione di controllo della ridondanza del volume. I volumi nel pool o nel gruppo di volumi vengono sottoposti a scansione in sequenza, a partire dalla parte superiore della tabella nella finestra di dialogo. Queste azioni si verificano quando viene eseguita la scansione di ciascun volume:

   - Il volume viene selezionato nella tabella dei volumi.

- Lo stato del controllo di ridondanza viene visualizzato nella colonna Status (Stato).
- Il controllo si interrompe in caso di errore di parità o supporto, quindi riporta l'errore. La seguente tabella fornisce ulteriori informazioni sullo stato del controllo di ridondanza:

Dettagli campo

Stato	Descrizione
In sospeso	Si tratta del primo volume da sottoporre a scansione e non è stato fatto clic su Start (Avvia) per avviare il controllo di ridondanza. -Oppure- l'operazione di controllo della ridondanza viene eseguita su altri volumi nel pool o nel gruppo di volumi.
Verifica in corso	Il volume è sottoposto al controllo di ridondanza.
Superato	Il volume ha superato il controllo di ridondanza. Non sono state rilevate incongruenze nelle informazioni di ridondanza.
Non riuscito	Il volume non ha superato il controllo di ridondanza. Sono state rilevate incoerenze nelle informazioni di ridondanza.
Errore supporto	Il disco rigido è difettoso e illeggibile. Seguire le istruzioni visualizzate nel Recovery Guru.
Errore di parità	La parità non è quella che dovrebbe essere per una determinata parte dei dati. Un errore di parità è potenzialmente grave e potrebbe causare una perdita permanente di dati.

6. Fare clic su **Done** (fine) dopo aver controllato l'ultimo volume del pool o del gruppo di volumi.

Eliminare pool o gruppo di volumi

È possibile eliminare un pool o un gruppo di volumi per creare una maggiore capacità non assegnata, che è possibile riconfigurare per soddisfare le esigenze di storage dell'applicazione.

Prima di iniziare

- È necessario aver eseguito il backup dei dati su tutti i volumi del pool o del gruppo di volumi.
- È necessario aver interrotto tutti gli input/output (i/o).
- È necessario smontare tutti i file system sui volumi.
- È necessario eliminare tutte le relazioni mirror nel pool o nel gruppo di volumi.
- È necessario interrompere qualsiasi operazione di copia del volume in corso per il pool o il gruppo di volumi.
- Il pool o il gruppo di volumi non deve partecipare a un'operazione di mirroring asincrono.
- I dischi nel gruppo di volumi non devono avere una prenotazione persistente.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare un pool o un gruppo di volumi dall'elenco.

È possibile selezionare un solo pool o gruppo di volumi alla volta. Scorrere l'elenco per visualizzare altri pool o gruppi di volumi.

4. Selezionare **attività non comuni › Elimina** e confermare.

Risultati

Il sistema esegue le seguenti operazioni:

- Elimina tutti i dati del pool o del gruppo di volumi.
- Elimina tutte le unità associate al pool o al gruppo di volumi.
- Annulla l'assegnazione delle unità associate, che consente di riutilizzarle in pool o gruppi di volumi nuovi o esistenti.

Consolidare la capacità libera per un gruppo di volumi

Utilizzare l'opzione consolida capacità libera per consolidare le estensioni libere esistenti su un gruppo di volumi selezionato. Eseguendo questa azione, è possibile creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi.

Prima di iniziare

- Il gruppo di volumi deve contenere almeno un'area di capacità libera.
- Tutti i volumi nel gruppo di volumi devono essere online e in uno stato ottimale.
- Le operazioni di modifica del volume non devono essere in corso, ad esempio la modifica delle dimensioni del segmento di un volume.

A proposito di questa attività

Non è possibile annullare l'operazione dopo l'inizio. I dati rimangono accessibili durante l'operazione di consolidamento.

È possibile avviare la finestra di dialogo consolida capacità libera utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, la raccomandazione di consolidare la capacità libera viene visualizzata nella home page dell'area di notifica. Fare clic sul collegamento **consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Consolida capacità libera dalla pagina Pools & Volume Groups come descritto nella seguente attività.

Ulteriori informazioni sulle aree di capacità libera

Un'area di capacità libera è la capacità libera che può derivare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità disponibile durante la creazione del volume. Quando si crea un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume viene limitata alla maggiore area di capacità libera del gruppo di volumi. Ad esempio, se un gruppo di volumi ha una capacità libera totale di 15 GiB e l'area di capacità libera più grande è di 10 GiB, il volume più grande che è possibile creare è di 10 GiB.

È possibile consolidare la capacità libera su un gruppo di volumi per migliorare le prestazioni di scrittura. La capacità libera del gruppo di volumi si frammenterà nel tempo man mano che l'host scrive, modifica ed elimina i file. Infine, la capacità disponibile non verrà collocata in un singolo blocco contiguo, ma verrà distribuita in piccoli frammenti all'interno del gruppo di volumi. Ciò causa un'ulteriore frammentazione dei file, poiché l'host deve scrivere nuovi file come frammenti per inserirli negli intervalli disponibili dei cluster liberi.

Consolidando la capacità libera su un gruppo di volumi selezionato, si noteranno migliori performance del file system ogni volta che l'host scrive nuovi file. Il processo di consolidamento consentirà inoltre di evitare la frammentazione dei nuovi file in futuro.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il gruppo di volumi con capacità libera che si desidera consolidare, quindi selezionare **Uncommon Tasks › consolida capacità libera del gruppo di volumi**.

   Viene visualizzata la finestra di dialogo consolida capacità libera.
4. Tipo `consolidate` per confermare che si desidera eseguire questa operazione.
5. Fare clic su **consolida**.

Risultato

Il sistema inizia a consolidare (deframmentare) le aree di capacità libera del gruppo di volumi in una quantità contigua per le successive attività di configurazione dello storage.

Al termine

Dalla barra laterale di navigazione, selezionare **Operations** per visualizzare l'avanzamento dell'operazione di consolidamento della capacità libera. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Accendere le luci di individuazione

È possibile individuare le unità per identificare fisicamente tutte le unità che comprendono un pool, un gruppo di volumi o una cache SSD selezionata. Un indicatore LED si accende su ogni disco nel pool, gruppo di volumi o cache SSD selezionato.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).

3. Selezionare il pool, il gruppo di volumi o la cache SSD che si desidera individuare, quindi fare clic su **More › Turn on locator lights** (attiva indicatori di ricerca).

   Viene visualizzata una finestra di dialogo che indica che le spie dei dischi che compongono il pool, il gruppo di volumi o la cache SSD selezionati sono accese.

4. Una volta individuati correttamente i dischi, fare clic su **Spegni**.

Rimuovere la capacità

È possibile rimuovere i dischi per ridurre la capacità di un pool o di una cache SSD esistente.

Dopo aver rimosso i dischi, i dati in ciascun volume del pool o della cache SSD vengono ridistribuiti nei dischi rimanenti. I dischi rimossi non vengono assegnati e la loro capacità diventa parte della capacità libera totale dell'array di storage.

A proposito di questa attività

Quando si rimuove la capacità, attenersi alle seguenti linee guida:

- Non è possibile rimuovere l'ultimo disco in una cache SSD senza prima eliminare la cache SSD.
- Non è possibile ridurre il numero di dischi in un pool a meno di 11 dischi.
- È possibile rimuovere un massimo di 12 dischi alla volta. Se è necessario rimuovere più di 12 dischi, ripetere la procedura.
- Non è possibile rimuovere i dischi se la capacità libera nel pool o nella cache SSD non è sufficiente per contenere i dati, quando tali dati vengono ridistribuiti ai dischi rimanenti nel pool o nella cache SSD.

Di seguito sono riportati i potenziali impatti sulle performance:

- La rimozione dei dischi da un pool o da una cache SSD potrebbe ridurre le performance dei volumi.
- La capacità di conservazione non viene consumata quando si rimuove la capacità da un pool o da una cache SSD. Tuttavia, la capacità di conservazione potrebbe diminuire in base al numero di dischi rimasti nel pool o nella cache SSD.

Di seguito sono riportati gli impatti sui dischi sicuri:

- Se si rimuove l'ultimo disco che non supporta la protezione, il pool viene lasciato con tutti i dischi che supportano la protezione. In questa situazione, è possibile attivare la protezione per il pool.
- Se si rimuove l'ultimo disco non compatibile con Data Assurance (da), il pool viene lasciato con tutti i dischi compatibili con da.
- Tutti i nuovi volumi creati nel pool saranno compatibili con da. Se si desidera che i volumi esistenti siano compatibili con il da, è necessario eliminare e ricreare il volume.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.

   Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).

2. Selezionare il pool o la cache SSD, quindi fare clic su **More › Remove Capacity**.

   Viene visualizzata la finestra di dialogo Remove Capacity (capacità di rimozione).

3. Selezionare una o più unità nell'elenco.

   Quando si selezionano o deselezionano i dischi nell'elenco, il campo capacità totale selezionata viene aggiornato. Questo campo mostra la capacità totale del pool o della cache SSD risultante dopo la rimozione dei dischi selezionati.

4. Fare clic su **Rimuovi**, quindi confermare la rimozione delle unità.

Risultato

La nuova capacità ridotta del pool o della cache SSD viene riflessa nella vista Pools e Volume Groups.

Abilitare la protezione per un pool o un gruppo di volumi

È possibile attivare Drive Security per un pool o un gruppo di volumi per impedire l'accesso non autorizzato ai dati sulle unità contenute nel pool o nel gruppo di volumi.

L'accesso in lettura e scrittura per i dischi è disponibile solo attraverso un controller configurato con una chiave di sicurezza.

Prima di iniziare

- La funzione Drive Security deve essere attivata.
- È necessario creare una chiave di sicurezza.
- Il pool o il gruppo di volumi deve trovarsi in uno stato ottimale.
- Tutti i dischi del pool o del gruppo di volumi devono essere dischi sicuri.

A proposito di questa attività

Se si desidera utilizzare Drive Security, selezionare un pool o un gruppo di volumi che supporti la protezione. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.

Una volta attivato il sistema di protezione, è possibile rimuoverlo solo eliminando il pool o il gruppo di volumi, quindi cancellando i dischi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il pool o il gruppo di volumi in cui si desidera attivare la protezione, quindi fare clic su **More › Enable Security** (Altro[attiva protezione]).

   Viene visualizzata la finestra di dialogo Conferma abilitazione protezione.

4. Confermare che si desidera attivare la protezione per il pool o il gruppo di volumi selezionato, quindi fare clic su **Enable** (attiva).

Rimuovere il plug-in di storage per vCenter

È possibile rimuovere il plug-in da vCenter Server Appliance e disinstallare il webserver del plug-in dall'host dell'applicazione.

Si tratta di due passaggi distinti che è possibile eseguire in qualsiasi ordine. Tuttavia, se si sceglie di rimuovere

il webserver del plug-in dall'host dell'applicazione prima di annullare la registrazione del plug-in, lo script di registrazione viene rimosso durante tale processo e non è possibile utilizzare il metodo 1 per annullare la registrazione.

Annullare la registrazione del plug-in da un'appliance vCenter Server

Per annullare la registrazione del plug-in da un'appliance vCenter Server, selezionare uno dei seguenti metodi:

- Metodo 1: Eseguire lo script di registrazione
- Metodo 2: Utilizzare le pagine Mob di vCenter Server

Metodo 1: Eseguire lo script di registrazione

1. Aprire un prompt dalla riga di comando e accedere alla seguente directory:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Eseguire `vcenter-register.bat` file:

   ```
   vcenter-register.bat ^

   -action unregisterPlugin ^

   -vcenterHostname <vCenter FQDN> ^

   -username <Administrator Username> ^
   ```

3. Verificare che lo script sia stato eseguito correttamente.

   I registri vengono salvati in `%install_dir%/working/logs/vc-registration.log`.

Metodo 2: Utilizzare le pagine Mob di vCenter Server

1. Aprire un browser Web e immettere il seguente URL:

   https://<FQDN[] Di vCenter Server>/MOB

2. Accedere con le credenziali di amministratore.
3. Cercare il nome della proprietà di `extensionManager` e fare clic sul collegamento associato alla proprietà.
4. Espandere l'elenco delle proprietà facendo clic su **More**… in fondo all'elenco.
5. Verificare che l'interno `plugin.netapp.eseries` è nell'elenco.
6. Se presente, fare clic sul metodo `UnregisterExtension`.
7. Inserire il valore `plugin.netapp.eseries` Nella finestra di dialogo e fare clic su **Invoke method**.
8. Chiudere la finestra di dialogo e aggiornare il browser Web.
9. Verificare che il `plugin.netapp.eseries` interno non presente nell'elenco.

Questa procedura disregistra il plug-in da vCenter Server Appliance; tuttavia, non rimuove i file dei pacchetti di plug-in dal server. Per rimuovere i file dei pacchetti, utilizzare SSH per accedere a vCenter Server Appliance e accedere alla seguente directory: `etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`. Quindi rimuovere la directory associata al plug-in.

Rimuovere il webserver del plug-in dall'host dell'applicazione

Per rimuovere il software del plug-in dall'host dell'applicazione, attenersi alla seguente procedura:

1. Dal server applicazioni, accedere a **pannello di controllo**.
2. Accedere a **applicazioni e funzionalità**, quindi selezionare **Plugin storage SANtricity per vCenter**.
3. Fare clic su **Disinstalla/Cambia**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Fare clic su **Disinstalla**.

   Una volta completata la disinstallazione, viene visualizzato un messaggio di conferma.

5. Fare clic su **fine**.

FAQ

Quali impostazioni vengono importate?

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che carica le configurazioni da un array di storage a più array di storage.

Le impostazioni importate durante questa operazione dipendono dalla configurazione dell'array di storage di origine in System Manager. È possibile importare le seguenti impostazioni in più array di storage:

- **Avvisi via email** — le impostazioni includono un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — le impostazioni includono un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — le impostazioni includono un nome di comunità e un indirizzo IP per il server SNMP.
- **AutoSupport** — le impostazioni includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.
- **Directory Services** — la configurazione include il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.
- **Configurazione dello storage** — le configurazioni includono volumi (solo volumi thick e non repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.
- **Impostazioni di sistema** — le configurazioni includono le impostazioni di scansione dei supporti per un volume, la cache SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Perché non vengono visualizzati tutti gli array di storage?

Durante l'operazione Import Settings (Impostazioni di importazione), alcuni storage array potrebbero non essere disponibili nella finestra di dialogo di selezione della destinazione.

Gli array di storage potrebbero non essere visualizzati per i seguenti motivi:

- La versione del firmware è inferiore alla 8.50.
- Lo storage array non è in linea.
- Il sistema non è in grado di comunicare con tale array (ad esempio, l'array presenta problemi di certificato, password o rete).

Perché questi volumi non sono associati a un carico di lavoro?

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

In che modo il carico di lavoro selezionato influisce sulla creazione di volumi?

Durante la creazione del volume, vengono richieste informazioni sull'utilizzo di un carico di lavoro. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze. In alternativa, è possibile saltare questo passaggio nella sequenza di creazione del volume.

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

- **Specifico dell'applicazione** — quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.
  - Microsoft SQL Server
  - Server Microsoft Exchange
  - Applicazioni di videosorveglianza
  - VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

    È possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).
- **Altri (o applicazioni senza supporto specifico per la creazione di volumi)** — Altri carichi di lavoro utilizzano una configurazione del volume che è necessario specificare manualmente quando si desidera creare un carico di lavoro non associato a un'applicazione specifica o se non esiste un'ottimizzazione

integrata per l'applicazione che si intende utilizzare sull'array di storage. Specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Perché non vengono visualizzati tutti i volumi, gli host o i cluster di host?

I volumi Snapshot con un volume di base abilitato da non possono essere assegnati a un host che non supporta Data Assurance (da). È necessario disattivare il da sul volume di base prima di poter assegnare un volume snapshot a un host che non supporta il da.

Prendere in considerazione le seguenti linee guida per l'host a cui si sta assegnando il volume di snapshot:

- Un host non è in grado di supportare da se è collegato all'array di storage attraverso un'interfaccia i/o che non è in grado di supportare da.
- Un cluster host non è in grado di supportare da se ha almeno un membro host che non è in grado di supportare da.

> Non è possibile disattivare il da su un volume associato a snapshot (gruppi di coerenza, gruppi di snapshot, immagini snapshot e volumi di snapshot), copie di volumi, e specchi. Tutti gli oggetti snapshot e capacità riservata associati devono essere cancellati prima che il da possa essere disattivato sul volume di base.

Perché non è possibile eliminare il carico di lavoro selezionato?

Questo carico di lavoro è costituito da un gruppo di volumi creati utilizzando l'interfaccia della riga di comando (CLI) o migrati (importati/esportati) da un array di storage diverso. Di conseguenza, i volumi di questo carico di lavoro non sono associati a un carico di lavoro specifico dell'applicazione, pertanto non è possibile eliminare il carico di lavoro.

In che modo i carichi di lavoro specifici dell'applicazione mi aiutano a gestire lo storage array?

Le caratteristiche del volume del carico di lavoro specifico dell'applicazione determinano il modo in cui il carico di lavoro interagisce con i componenti dell'array di storage e aiutano a determinare le performance dell'ambiente in una determinata configurazione.

Un'applicazione è un software come SQL Server o Exchange. È possibile definire uno o più workload per supportare ciascuna applicazione. Per alcune applicazioni, il sistema consiglia automaticamente una configurazione del volume che ottimizzi lo storage. Caratteristiche come il tipo di i/o, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume.

Cosa devo fare per riconoscere la capacità espansa?

Se si aumenta la capacità di un volume, l'host potrebbe non riconoscere immediatamente l'aumento della capacità del volume.

La maggior parte dei sistemi operativi riconosce la capacità del volume espanso e si espande automaticamente dopo l'avvio dell'espansione del volume. Tuttavia, alcuni potrebbero non farlo. Se il sistema operativo non riconosce automaticamente la capacità del volume espanso, potrebbe essere necessario eseguire una nuova scansione o un riavvio del disco.

Una volta espansa la capacità del volume, è necessario aumentare manualmente le dimensioni del file system

per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso.

Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Quando si desidera utilizzare la selezione dell'host di assegnazione in un secondo momento?

Se si desidera accelerare il processo di creazione dei volumi, è possibile saltare la fase di assegnazione dell'host in modo che i volumi appena creati vengano inizializzati offline.

I volumi appena creati devono essere inizializzati. Il sistema può inizializzarli utilizzando una delle due modalità, ovvero un processo di inizializzazione in background di IAF (immediate Available Format) o un processo offline.

Quando si esegue il mapping di un volume a un host, tutti i volumi di inizializzazione del gruppo vengono forzati a passare all'inizializzazione in background. Questo processo di inizializzazione in background consente l'i/o host simultaneo, che a volte può richiedere molto tempo.

Quando nessuno dei volumi in un gruppo di volumi viene mappato, viene eseguita l'inizializzazione offline. Il processo offline è molto più veloce del processo in background.

Cosa occorre sapere sui requisiti relativi alle dimensioni dei blocchi host?

Per i sistemi EF300 e EF600, è possibile impostare un volume in modo che supporti una dimensione di blocco di 512 byte o 4 KiB (chiamata anche "dimensione del settore"). È necessario impostare il valore corretto durante la creazione del volume. Se possibile, il sistema suggerisce il valore predefinito appropriato.

Prima di impostare le dimensioni del blocco del volume, leggere le seguenti limitazioni e linee guida.

- Alcuni sistemi operativi e macchine virtuali (in particolare VMware, al momento) richiedono una dimensione di blocco di 512 byte e non supportano 4KiB, quindi assicurarsi di conoscere i requisiti dell'host prima di creare un volume. In genere, è possibile ottenere le migliori prestazioni impostando un volume in modo che presenti una dimensione di blocco di 4 KiB; tuttavia, assicurarsi che l'host supporti blocchi da 4 KiB (o "4 Kn").
- Il tipo di dischi selezionati per il pool o il gruppo di volumi determina anche le dimensioni dei blocchi di volume supportate, come indicato di seguito:
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 512 byte, è possibile creare solo volumi con blocchi da 512 byte.
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 4 KiB, è possibile creare volumi con blocchi da 512 byte o 4 KiB.
- Se l'array dispone di una scheda di interfaccia host iSCSI, tutti i volumi sono limitati a blocchi da 512 byte (indipendentemente dalla dimensione del blocco del gruppo di volumi). Ciò è dovuto a un'implementazione hardware specifica.
- Una volta impostata, non è possibile modificare le dimensioni di un blocco. Se è necessario modificare le dimensioni di un blocco, è necessario eliminare il volume e ricrearlo.

Perché dovrei creare un cluster host?

È necessario creare un cluster host se si desidera che due o più host condividano l'accesso allo stesso set di volumi. In genere, i singoli host dispongono di un software di

clustering installato su di essi per coordinare l'accesso ai volumi.

Come si fa a sapere quale tipo di sistema operativo host è corretto?

Il campo host Operating System Type (tipo di sistema operativo host) contiene il sistema operativo dell'host. È possibile selezionare il tipo di host consigliato dall'elenco a discesa o consentire all'HCA (host Context Agent) di configurare l'host e il tipo di sistema operativo appropriato.

I tipi di host visualizzati nell'elenco a discesa dipendono dal modello di array di storage e dalla versione del firmware. Le versioni più recenti visualizzano prima le opzioni più comuni, che sono le più probabili. L'aspetto in questo elenco non implica che l'opzione sia completamente supportata.

> Per ulteriori informazioni sul supporto degli host, fare riferimento a. "Tool di matrice di interoperabilità NetApp".

Alcuni dei seguenti tipi di host potrebbero essere visualizzati nell'elenco:

Tipo di sistema operativo host	Sistema operativo e driver multipath
Linux DM-MP (kernel 3.10 o successivo)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.10 o successivo.
VMware ESXi	Supporta i sistemi operativi VMware ESXi che eseguono l'architettura NMP (Native Multipathing Plug-in) utilizzando il modulo SATP_ALUA Storage Array Type Policy integrato da VMware.
Windows (in cluster o non in cluster)	Supporta configurazioni in cluster o non in cluster di Windows che non eseguono il driver di multipathing atto.
ATTO Cluster (tutti i sistemi operativi)	Supporta tutte le configurazioni del cluster utilizzando il driver multipathing della tecnologia atto, Inc.
Linux (Veritas DMP)	Supporta i sistemi operativi Linux che utilizzano una soluzione multipathing Veritas DMP.
Linux (atto)	Supporta i sistemi operativi Linux che utilizzano un driver multipathing per la tecnologia atto, Inc.
Sistema operativo Mac	Supporta le versioni di Mac OS che utilizzano un driver multipathing per la tecnologia atto, Inc.
Windows (atto)	Supporta i sistemi operativi Windows che utilizzano un driver multipathing per la tecnologia atto, Inc.
FlexArray (ALUA)	Supporta un sistema NetApp FlexArray che utilizza ALUA per il multipathing.
SVC IBM	Supporta una configurazione IBM SAN Volume Controller.

Tipo di sistema operativo host	Sistema operativo e driver multipath
Impostazione predefinita di fabbrica	Riservato all'avvio iniziale dello storage array. Se il tipo di sistema operativo host in uso è impostato su Factory Default, modificarlo in modo che corrisponda al sistema operativo host e al driver multipath in esecuzione sull'host connesso.
Linux DM-MP (Kernal 3.9 o precedente)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.9 o precedente.
Cluster di finestre (obsoleto)	Se il tipo di sistema operativo host è impostato su questo valore, utilizzare l'impostazione Windows (in cluster o non in cluster).

Una volta installato l'HCA e collegato lo storage all'host, l'HCA invia la topologia host ai controller di storage attraverso il percorso i/O. In base alla topologia dell'host, i controller di storage definiscono automaticamente l'host e le porte host associate, quindi impostano il tipo di host.

> Se l'HCA non seleziona il tipo di host consigliato, è necessario impostare manualmente il tipo di host.

Come faccio ad associare le porte host a un host?

Se si crea manualmente un host, è necessario utilizzare l'utility HBA (host bus adapter) appropriata disponibile sull'host per determinare gli identificatori di porta host associati a ciascun HBA installato nell'host.

Quando si dispone di queste informazioni, selezionare gli identificatori di porta host che hanno effettuato l'accesso allo storage array dall'elenco fornito nella finestra di dialogo Create host (Crea host).

> Assicurarsi di selezionare gli identificatori di porta host appropriati per l'host che si sta creando. Se si associano identificatori di porta host errati, potrebbe verificarsi un accesso non intenzionale da un altro host a questi dati.

Se si creano automaticamente host utilizzando l'HCA (host Context Agent) installato su ciascun host, l'HCA deve associare automaticamente gli identificatori di porta host a ciascun host e configurarli in modo appropriato.

Qual è il cluster predefinito?

Il cluster predefinito è un'entità definita dal sistema che consente a qualsiasi identificatore di porta host non associato che abbia eseguito l'accesso all'array di storage di accedere ai volumi assegnati al cluster predefinito.

Un identificatore di porta host non associato è una porta host che non è logicamente associata a un particolare host ma che è fisicamente installata in un host e collegata all'array di storage.

> Se si desidera che gli host abbiano accesso specifico a determinati volumi nell'array di storage, non è necessario utilizzare il cluster predefinito. È invece necessario associare gli identificatori delle porte host ai rispettivi host. Questa attività può essere eseguita manualmente durante l'operazione Create host (Crea host) o automaticamente utilizzando l'HCA (host Context Agent) installato su ciascun host. Quindi, assegnare i volumi a un singolo host o a un cluster host.

Utilizzare il cluster predefinito solo in situazioni speciali in cui l'ambiente di storage esterno favorisce l'accesso a tutti gli host e a tutti gli identificatori di porta host connessi allo storage array a tutti i volumi (modalità all-access) senza rendere specifici gli host noti allo storage array o all'interfaccia utente.

Inizialmente, è possibile assegnare i volumi solo al cluster predefinito tramite l'interfaccia della riga di comando (CLI). Tuttavia, dopo aver assegnato almeno un volume al cluster predefinito, questa entità (chiamata cluster predefinito) viene visualizzata nell'interfaccia utente, dove è possibile gestire questa entità.

Che cos'è il controllo di ridondanza?

Un controllo di ridondanza determina se i dati su un volume in un pool o un gruppo di volumi sono coerenti. I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6, quindi verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se i dati sono determinati come incoerenti dal firmware del controller.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Che cos'è la capacità di conservazione?

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata in un pool per supportare potenziali guasti del disco.

Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione in base al numero di dischi nel pool.

I pool utilizzano la capacità di conservazione durante la ricostruzione, mentre i gruppi di volumi utilizzano dischi hot spare per lo stesso scopo. Il metodo della capacità di conservazione è un miglioramento rispetto ai dischi hot spare perché consente una ricostruzione più rapida. La capacità di conservazione viene distribuita su un certo numero di dischi nel pool invece che su un disco nel caso di un disco hot spare, in modo da non essere limitati dalla velocità o dalla disponibilità di un disco.

Qual è il livello RAID migliore per la mia applicazione?

Per massimizzare le performance di un gruppo di volumi, è necessario selezionare il

livello RAID appropriato.

È possibile determinare il livello RAID appropriato conoscendo le percentuali di lettura e scrittura per le applicazioni che accedono al gruppo di volumi. Utilizzare la pagina Performance (prestazioni) per ottenere queste percentuali.

Livelli RAID e performance applicative

RAID si basa su una serie di configurazioni, chiamate livelli, per determinare il modo in cui i dati di ridondanza e utente vengono scritti e recuperati dai dischi. Ogni livello RAID offre diverse funzionalità di performance. Le applicazioni con un'elevata percentuale di lettura sono in grado di funzionare correttamente utilizzando volumi RAID 5 o RAID 6, a causa delle eccezionali prestazioni di lettura delle configurazioni RAID 5 e RAID 6.

Le applicazioni con una bassa percentuale di lettura (elevata intensità di scrittura) non funzionano altrettanto sui volumi RAID 5 o RAID 6. Le prestazioni degradate sono il risultato del modo in cui un controller scrive i dati e i dati di ridondanza sui dischi di un gruppo di volumi RAID 5 o RAID 6.

Selezionare un livello RAID in base alle seguenti informazioni.

RAID 0

Descrizione:

- Non ridondante, modalità striping.
- RAID 0 esegue lo striping dei dati su tutti i dischi del gruppo di volumi.

Caratteristiche di protezione dei dati:

- RAID 0 non è consigliato per esigenze di alta disponibilità. RAID 0 è migliore per i dati non critici.
- Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- Per RAID livello 0 è richiesto un minimo di un disco.
- I gruppi di volumi RAID 0 possono avere più di 30 dischi.
- È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 1 o RAID 10

Descrizione:

- Modalità striping/mirror.

Come funziona:

- RAID 1 utilizza il mirroring del disco per scrivere i dati su due dischi duplicati contemporaneamente.
- RAID 10 utilizza lo striping dei dischi per eseguire lo striping dei dati su un set di coppie di dischi mirrorati.

Caratteristiche di protezione dei dati:

- RAID 1 e RAID 10 offrono performance elevate e la migliore disponibilità dei dati.

- RAID 1 e RAID 10 utilizzano il mirroring del disco per eseguire una copia esatta da un disco a un altro.
- Se uno dei dischi di una coppia di dischi si guasta, lo storage array può passare istantaneamente all'altro disco senza alcuna perdita di dati o di servizio.
- Un guasto a un singolo disco causa il degrado dei volumi associati. L'unità mirror consente di accedere ai dati.
- Un errore di coppia di dischi in un gruppo di volumi causa il malfunzionamento di tutti i volumi associati e la perdita di dati.

Requisiti del numero di unità:

- Per RAID 1 sono necessari almeno due dischi: Un disco per i dati dell'utente e un disco per i dati mirrorati.
- Se si selezionano quattro o più dischi, RAID 10 viene configurato automaticamente nel gruppo di volumi: Due dischi per i dati dell'utente e due dischi per i dati mirrorati.
- È necessario disporre di un numero pari di dischi nel gruppo di volumi. Se non si dispone di un numero pari di dischi e si dispone di altri dischi non assegnati, passare a **Pools & Volume Groups** per aggiungere ulteriori dischi al gruppo di volumi e riprovare l'operazione.
- I gruppi di volumi RAID 1 e RAID 10 possono avere più di 30 dischi. È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 5

Descrizione:

- Modalità i/o elevata.

Come funziona:

- I dati dell'utente e le informazioni ridondanti (parità) vengono sottoposti a striping tra i dischi.
- La capacità equivalente di un disco viene utilizzata per le informazioni ridondanti.

Caratteristiche di protezione dei dati

- Se un singolo disco si guasta in un gruppo di volumi RAID 5, tutti i volumi associati diventano degradati. Le informazioni ridondanti consentono di accedere ai dati.
- Se due o più dischi si guastano in un gruppo di volumi RAID 5, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- È necessario disporre di un minimo di tre dischi nel gruppo di volumi.
- In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

RAID 6

Descrizione:

- Modalità i/o elevata.

Come funziona:

- I dati dell'utente e le informazioni ridondanti (doppia parità) vengono sottoposti a striping tra i dischi.

- La capacità equivalente di due dischi viene utilizzata per le informazioni ridondanti.

Caratteristiche di protezione dei dati:

- Se uno o due dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati diventano degradati, ma le informazioni ridondanti consentono di continuare ad accedere ai dati.
- Se tre o più dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- È necessario disporre di un minimo di cinque dischi nel gruppo di volumi.
- In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

> Non è possibile modificare il livello RAID di un pool. L'interfaccia utente configura automaticamente i pool come RAID 6.

Livelli RAID e protezione dei dati

RAID 1, RAID 5 e RAID 6 scrivono i dati di ridondanza sul disco per la tolleranza di errore. I dati di ridondanza possono essere una copia dei dati (mirrorati) o un codice di correzione degli errori derivato dai dati. È possibile utilizzare i dati di ridondanza per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto.

È possibile configurare un singolo livello RAID in un singolo gruppo di volumi. Tutti i dati di ridondanza per quel gruppo di volumi vengono memorizzati all'interno del gruppo di volumi. La capacità del gruppo di volumi è la capacità aggregata dei dischi membri meno la capacità riservata ai dati di ridondanza. La quantità di capacità necessaria per la ridondanza dipende dal livello RAID utilizzato.

Perché alcuni dischi non vengono visualizzati?

Nella finestra di dialogo Add Capacity (Aggiungi capacità), non tutti i dischi sono disponibili per l'aggiunta di capacità a un pool o a un gruppo di volumi esistente.

I dischi non sono idonei per uno dei seguenti motivi:

- Un disco deve essere non assegnato e non abilitato alla sicurezza. I dischi già parte di un altro pool, di un altro gruppo di volumi o configurati come hot spare non sono idonei. Se un disco non è assegnato ma è abilitato per la protezione, è necessario cancellarlo manualmente affinché sia idoneo.
- Un disco in uno stato non ottimale non è idoneo.
- Se la capacità di un disco è troppo piccola, non è idonea.
- Il tipo di disco deve corrispondere all'interno di un pool o di un gruppo di volumi. Non è possibile combinare i seguenti elementi:
  - Dischi rigidi (HDD) con dischi a stato solido (SSD)
  - NVMe con unità SAS
  - Dischi con blocchi di volumi da 512 byte e 4 KiB
- Se un pool o un gruppo di volumi contiene tutti i dischi con funzionalità di protezione, i dischi con funzionalità di protezione non sono elencati.
- Se un pool o un gruppo di volumi contiene tutti i dischi FIPS (Federal Information Processing Standard), i

dischi non FIPS non sono elencati.

- Se un pool o un gruppo di volumi contiene tutte le unità compatibili con Data Assurance (da) e nel pool o nel gruppo di volumi è presente almeno un volume abilitato da, un'unità che non supporta da non è idonea, quindi non può essere aggiunta a tale pool o gruppo di volumi. Tuttavia, se nel pool o nel gruppo di volumi non è presente alcun volume abilitato da, è possibile aggiungere un'unità che non supporta da a a tale pool o gruppo di volumi. Se si decide di combinare questi dischi, tenere presente che non è possibile creare volumi abilitati da.

> È possibile aumentare la capacità dell'array di storage aggiungendo nuove unità o eliminando pool o gruppi di volumi.

Perché non posso aumentare la mia capacità di conservazione?

Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, potrebbe non essere possibile aumentare la capacità di conservazione.

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata a un pool per supportare potenziali guasti del disco. Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione in base al numero di dischi nel pool. Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, non è possibile aumentare la capacità di conservazione senza aggiungere capacità al pool aggiungendo unità o eliminando volumi.

È possibile modificare la capacità di conservazione da Pools & Volume Groups. Selezionare il pool che si desidera modificare. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni), quindi selezionare la scheda **Settings** (Impostazioni).

> La capacità di conservazione viene specificata come un numero di dischi, anche se la capacità di conservazione effettiva viene distribuita tra i dischi del pool.

Cos'è Data Assurance?

Data Assurance (da) implementa lo standard T10 Protection Information (PI), che aumenta l'integrità dei dati verificando e correggendo gli errori che potrebbero verificarsi quando i dati vengono trasferiti lungo il percorso di i/O.

L'utilizzo tipico della funzione Data Assurance consente di controllare la parte del percorso i/o tra i controller e i dischi. Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi.

Quando questa funzione è attivata, l'array di storage aggiunge i codici di controllo degli errori (noti anche come CRC (Cyclic Redundancy Checks) a ciascun blocco di dati del volume. Dopo lo spostamento di un blocco di dati, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono scritti su disco né restituiti all'host. Se si desidera utilizzare la funzione da, selezionare un pool o un gruppo di volumi che supporti da quando si crea un nuovo volume (cercare **Sì** accanto a **da** nella tabella dei candidati del gruppo di volumi e pool).

Assicurarsi di assegnare questi volumi abilitati da a un host utilizzando un'interfaccia i/o in grado di supportare da. Le interfacce i/o in grado di da includono Fibre Channel, SAS, iSCSI su TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE e iSER su InfiniBand (estensioni iSCSI per RDMA/IB). DA non è supportato da SRP su InfiniBand.

Che cos'è la sicurezza FDE/FIPS?

La protezione FDE/FIPS si riferisce a dischi sicuri che crittografano i dati durante la scrittura e decrittare i dati durante la lettura utilizzando una chiave di crittografia univoca.

Queste unità sicure impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). I dischi FIPS sono stati sottoposti a test di certificazione.

> Per i volumi che richiedono il supporto FIPS, utilizzare solo dischi FIPS. La combinazione di dischi FIPS e FDE in un gruppo di volumi o in un pool comporterà il trattamento di tutti i dischi come dischi FDE. Inoltre, un disco FDE non può essere aggiunto o utilizzato come spare in un gruppo di volumi o pool all-FIPS.

Che cos'è il supporto sicuro (Drive Security)?

Drive Security è una funzione che impedisce l'accesso non autorizzato ai dati su dischi abilitati alla sicurezza quando vengono rimossi dallo storage array.

Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).

Come si visualizzano e interpretano tutte le statistiche della cache SSD?

È possibile visualizzare statistiche nominali e statistiche dettagliate per la cache SSD.

Le statistiche nominali sono un sottoinsieme delle statistiche dettagliate. Le statistiche dettagliate possono essere visualizzate solo quando si esportano tutte le statistiche SSD in un file .csv. Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Statistiche nominali

Per visualizzare le statistiche della cache SSD, accedere alla pagina **Manage** (Gestione). Selezionare **Provisioning › Configure Pools & Volume Groups** (Configura pool e gruppi di volumi). Selezionare la cache SSD per cui si desidera visualizzare le statistiche, quindi selezionare **More › View Statistics** (Visualizza statistiche). Le statistiche nominali vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD).

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

L'elenco include le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate.

Statistiche dettagliate

Le statistiche dettagliate sono costituite dalle statistiche nominali e da statistiche aggiuntive. Queste statistiche aggiuntive vengono salvate insieme alle statistiche nominali, ma a differenza delle statistiche nominali, non vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare le statistiche dettagliate solo dopo aver esportato le statistiche in un file .csv.

Le statistiche dettagliate sono elencate dopo le statistiche nominali.

Che cos'è la protezione contro la perdita di shelf e la perdita di cassetto?

La protezione contro le perdite di shelf e la protezione contro le perdite di cassetto sono attributi di pool e gruppi di volumi che consentono di mantenere l'accesso ai dati in caso di guasto di un singolo shelf o cassetto.

Protezione contro la perdita di shelf

Uno shelf è l'enclosure che contiene i dischi o i dischi e il controller. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo shelf di dischi. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione dello shelf di dischi o il guasto di entrambi i moduli i/o (IOM).

> La protezione contro la perdita di shelf non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

I criteri per la protezione dalla perdita di shelf dipendono dal metodo di protezione, come descritto nella tabella seguente.

Livello	Criteri per la protezione contro la perdita di shelf	Numero minimo di shelf richiesti
Piscina	Il pool deve includere dischi di almeno cinque shelf e deve essere presente un numero uguale di dischi in ogni shelf. La protezione contro la perdita di shelf non è applicabile agli shelf ad alta capacità; se il sistema contiene shelf ad alta capacità, fare riferimento alla protezione contro la perdita di cassetto.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo cassetto.	3
RAID 3 o RAID 5	Ogni disco del gruppo di volumi si trova in uno shelf separato.	3
RAID 1	Ogni disco di una coppia RAID 1 deve essere collocato in uno shelf separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di shelf.	Non applicabile

Protezione in caso di perdita del cassetto

Un cassetto è uno dei compartimenti di uno shelf che si tira per accedere ai dischi. Solo gli scaffali ad alta capacità dispongono di cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo cassetto. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione del cassetto o il guasto di un componente interno del cassetto.

> La protezione contro la perdita di cassetto non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a un cassetto (e di conseguenza a un altro disco nel pool o nel gruppo di volumi) causa la perdita di dati.

I criteri per la protezione dalle perdite di cassetto dipendono dal metodo di protezione, come descritto nella tabella seguente:

Livello	Criteri per la protezione contro le perdite di cassetto	Numero minimo di cassetti richiesti
Piscina	I candidati al pool devono includere unità di tutti i cassetti e deve essere presente un numero uguale di unità in ciascun cassetto. Il pool deve includere dischi di almeno cinque cassetti e deve essere presente un numero uguale di dischi in ciascun cassetto. Uno shelf da 60 dischi può ottenere la protezione contro la perdita di cassetto quando il pool contiene 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 dischi. È possibile aggiungere incrementi in multipli di 5 al pool dopo la creazione iniziale.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo cassetto.	3
RAID 3 o 5	Ciascuna unità del gruppo di volumi si trova in un cassetto separato	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione perdita cassetto.	Non applicabile

Come posso mantenere la protezione contro la perdita di scaffali e cassetti?

Per mantenere la protezione contro le perdite di shelf e cassetti per un pool o un gruppo di volumi, utilizzare i criteri specificati nella tabella seguente.

Livello	Criteri per la protezione contro le perdite di scaffali/cassetti	Numero minimo di shelf/cassetti richiesti
Piscina	Per gli shelf, il pool non deve contenere più di due dischi in un singolo shelf. Per i cassetti, il pool deve includere un numero uguale di unità da ciascun cassetto.	6 per i ripiani 5 per i cassetti
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo shelf o cassetto.	3

Livello	Criteri per la protezione contro le perdite di scaffali/cassetti	Numero minimo di shelf/cassetti richiesti
RAID 3 o RAID 5	Ciascuna unità del gruppo di volumi si trova in uno shelf o in un cassetto separato.	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in uno shelf o in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di scaffali/cassetti.	Non applicabile

> La protezione contro le perdite di shelf/cassetto non viene mantenuta se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf o a un cassetto di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

Che cos'è la capacità di ottimizzazione per i pool?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra performance, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Pool Settings (Impostazioni pool) consente di regolare la capacità di ottimizzazione del pool. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

> Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) è disponibile solo per i sistemi storage EF600 e EF300.

Qual è la capacità di ottimizzazione per i gruppi di volumi?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo di volumi (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra prestazioni, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Volume Group Settings

(Impostazioni gruppo di volumi) consente di regolare la capacità di ottimizzazione di un gruppo di volumi. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

> Additional Optimization Capacity Slider è disponibile solo per i sistemi storage EF600 e EF300.

Quali sono le funzionalità di provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Cosa occorre sapere sulla funzionalità dei volumi con provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

> La funzionalità di provisioning delle risorse non è al momento disponibile. In alcune viste, i componenti potrebbero essere segnalati come capaci di provisioning delle risorse, ma la capacità di creare volumi con provisioning delle risorse è stata disattivata fino a quando non sarà possibile riattivarli in un aggiornamento futuro.

Volumi con provisioning delle risorse

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di

dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Attivazione e disattivazione della funzione

Il provisioning delle risorse è attivato per impostazione predefinita nei sistemi in cui i dischi supportano DULBE. È possibile disattivare l'impostazione predefinita da Pools & Volume Groups. La disattivazione del provisioning delle risorse è un'azione permanente per i volumi esistenti e non può essere annullata (ad esempio, non è possibile riattivare il provisioning delle risorse per questi gruppi di volumi e pool).

Tuttavia, se si desidera riattivare il provisioning delle risorse per i nuovi volumi creati, è possibile farlo dal **Impostazioni › sistema**. Tenere presente che quando si riattiva il provisioning delle risorse, vengono influenzati solo i gruppi di volumi e i pool appena creati. Tutti i gruppi di volumi e i pool esistenti rimarranno invariati. Se lo si desidera, è anche possibile disattivare nuovamente il provisioning delle risorse dal **Impostazioni › sistema**.

Qual è la differenza tra la chiave di sicurezza interna e la gestione esterna delle chiavi di sicurezza?

Quando si implementa la funzione Drive Security, è possibile utilizzare una chiave di sicurezza interna o una chiave di sicurezza esterna per bloccare i dati quando un disco abilitato alla protezione viene rimosso dall'array di storage.

Una chiave di sicurezza è una stringa di caratteri che viene condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Le chiavi interne vengono conservate nella memoria persistente del controller. Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol).

Cosa occorre sapere prima di creare una chiave di sicurezza?

Una chiave di sicurezza viene condivisa da controller e dischi abilitati alla sicurezza all'interno di un array di storage. Se un disco abilitato alla protezione viene rimosso dall'array di storage, la chiave di sicurezza protegge i dati da accessi non autorizzati.

È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi:

- Gestione interna delle chiavi nella memoria persistente del controller.
- Gestione esterna delle chiavi su un server di gestione delle chiavi esterno.

Gestione interna delle chiavi

Le chiavi interne vengono mantenute e "nascoste" in una posizione non accessibile sulla memoria persistente del controller. Prima di creare una chiave di sicurezza interna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

È quindi possibile creare una chiave di sicurezza interna, che implica la definizione di un identificatore e di una passphrase. L'identificatore è una stringa associata alla chiave di sicurezza e memorizzata sul controller e su

tutti i dischi associati alla chiave. La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Al termine, la chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Gestione esterna delle chiavi

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol). Prima di creare una chiave di sicurezza esterna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security
3. Ottenere un file di certificato client firmato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste KMIP.
   a. Innanzitutto, completare e scaricare una richiesta di firma del certificato (CSR) del client. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
   b. Successivamente, viene richiesto un certificato client firmato da una CA attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
   c. Una volta ottenuto un file di certificato client, copiarlo sull'host in cui si accede a System Manager.
4. Recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

È quindi possibile creare una chiave esterna che preveda la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, vengono caricati anche i file dei certificati. Al termine, il sistema si connette al server di gestione delle chiavi con le credenziali immesse. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Perché è necessario definire una passphrase?

La password viene utilizzata per crittografare e decrittare il file della chiave di sicurezza memorizzato nel client di gestione locale. Senza la passphrase, la chiave di sicurezza non può essere decifrata e utilizzata per sbloccare i dati da un disco abilitato alla sicurezza se viene reinstallata in un altro array di storage.

Soluzioni legacy

Cloud Connector

Panoramica di SANtricity® Cloud Connector

Il connettore cloud di SANtricity è un'applicazione Linux basata su host che consente di eseguire backup e recovery completi basati su blocchi e file di volumi e-Series su

account S3 (ad esempio, Amazon Simple Storage Service e NetApp StorageGRID) e appliance NetApp AltaVault.

Disponibile per l'installazione su piattaforme Linux RedHat e SUSE, il connettore cloud SANtricity è una soluzione in pacchetto (file .bin). Dopo aver installato SANtricity Cloud Connector, è possibile configurare l'applicazione per eseguire processi di backup e ripristino dei volumi e-Series su un'appliance AltaVault o sugli account Amazon S3 o StorageGRID esistenti. Tutti i processi eseguiti tramite SANtricity Cloud Connector utilizzano API basate SU REST.

Lo strumento SANtricity Cloud Connector non è più disponibile per il download.

Considerazioni

Quando si utilizzano queste procedure, tenere presente che:

- I processi di configurazione e backup/ripristino descritti in queste procedure si applicano alla versione dell'interfaccia utente grafica di SANtricity Cloud Connector.
- I flussi di lavoro API REST per l'applicazione SANtricity Cloud Connector non sono descritti in queste procedure. Per gli sviluppatori esperti, gli endpoint sono disponibili per ogni operazione di SANtricity Cloud Connector nella documentazione API. È possibile accedere alla documentazione API accedendo a. `http://<hostname.domain>:<port>/docs` tramite un browser.

Tipi di backup

Il connettore cloud di SANtricity offre due tipi di backup: Backup basati su immagine e su file.

- **Backup basato su immagine**

  Un backup basato su immagine legge i blocchi di dati raw da un volume di snapshot ed esegue il backup su un file noto come immagine. Viene eseguito il backup di tutti i blocchi di dati del volume Snapshot, inclusi i blocchi vuoti, i blocchi occupati dai file cancellati, i blocchi associati alla partizione e i metadati del file system. I backup delle immagini hanno il vantaggio di memorizzare tutte le informazioni con il volume snapshot indipendentemente dallo schema di partizione o dai file system su di esso.

  L'immagine non viene memorizzata nella destinazione di backup come singolo file, ma viene suddivisa in una serie di blocchi di dati, che hanno una dimensione di 64 MB. I blocchi di dati consentono a SANtricity Cloud Connector di utilizzare più connessioni alla destinazione di backup, migliorando in tal modo le prestazioni del processo di backup.

  Per i backup su StorageGRID e Amazon Web Services (S3), ogni blocco di dati utilizza una chiave di crittografia separata per crittografare il blocco. La chiave è un hash SHA256 composto dalla combinazione di una passphrase fornita dall'utente e dell'hash SHA256 dei dati dell'utente. Per i backup su AltaVault, SANtricity Cloud Connector non crittografa i blocchi di dati mentre AltaVault esegue questa operazione.

- **Backup basato su file**

  Un backup basato su file legge i file contenuti in una partizione del file system e li esegue il backup in una serie di blocchi di dati di 64 MB. Un backup basato su file non esegue il backup di file cancellati o di partizioni e metadati del file system. Come per i backup basati su immagini, i blocchi di dati consentono a SANtricity Cloud Connector di utilizzare più connessioni alla destinazione di backup, migliorando in tal modo le performance del processo di backup.

  Per i backup su StorageGRID e Amazon Web Services, ogni blocco di dati utilizza una chiave di crittografia separata per crittografare il blocco. La chiave è un hash SHA256 costituito dalla combinazione di password

fornite dall'utente e hash SHA256 dei dati dell'utente. Per i backup su AltaVault, i blocchi di dati non vengono crittografati da SANtricity Cloud Connector perché AltaVault esegue questa operazione.

Requisiti di sistema per Cloud Connector

Il sistema deve soddisfare i requisiti di compatibilità per SANtricity Cloud Connector.

Requisiti hardware dell'host

L'hardware deve soddisfare i seguenti requisiti minimi:

- Almeno 5 GB di memoria; 4 GB per la dimensione massima configurata dell'heap
- L'installazione del software richiede almeno 5 GB di spazio libero su disco

È necessario installare il proxy dei servizi Web di SANtricity per utilizzare il connettore cloud di SANtricity. È possibile installare Web Services Proxy in locale oppure eseguire l'applicazione in remoto su un server diverso. Per informazioni sull'installazione del proxy dei servizi Web di SANtricity, consultare "Argomenti relativi ai proxy dei servizi Web".

Browser supportati

Con l'applicazione SANtricity Cloud Connector sono supportati i seguenti browser (sono indicate le versioni minime):

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

> La documentazione API per l'applicazione Cloud Connector di SANtricity non viene caricata quando si utilizza l'impostazione visualizzazione compatibilità nel browser Microsoft Internet Explorer v11. Per garantire che la documentazione API venga visualizzata correttamente nel browser Microsoft Internet Explorer v11, si consiglia di disattivare l'impostazione visualizzazione compatibilità.

Array di storage e firmware del controller compatibili

Prima di utilizzare l'applicazione SANtricity Cloud Connector, verificare la compatibilità degli array di storage e del firmware.

Per un elenco completo e aggiornato di tutti gli array di storage compatibili e del firmware per il connettore cloud SANtricity, consultare la "Tool di matrice di interoperabilità NetApp".

Sistemi operativi compatibili

L'applicazione SANtricity Cloud Connector 4.0 è compatibile e supportata sui seguenti sistemi operativi:

Sistema operativo	Versione	Architettura
Red Hat Enterprise Linux (RHEL)	7.x	64 bit

Sistema operativo	Versione	Architettura
SUSE Linux Enterprise Server (SLES)	12.x	64 bit

File system supportati

È necessario utilizzare i file system supportati per eseguire backup e ripristini tramite l'applicazione SANtricity Cloud Connector.

I seguenti file system sono supportati per le operazioni di backup e ripristino nell'applicazione SANtricity Cloud Connector:

- ext2
- ext3
- ext4

Installare SANtricity Cloud Connector

Il pacchetto di soluzioni di connettori cloud SANtricity (file .bin) è disponibile solo per le piattaforme Linux RedHat e SUSE.

È possibile installare l'applicazione SANtricity Cloud Connector in modalità grafica o console su un sistema operativo Linux compatibile. Durante il processo di installazione, è necessario specificare i numeri delle porte non SSL e SSL per SANtricity Cloud Connector. Una volta installato, SANtricity Cloud Connector viene eseguito come processo daemon.

Lo strumento SANtricity Cloud Connector non è più disponibile per il download.

Prima di iniziare

Leggere le seguenti note:

- Se il proxy dei servizi Web di SANtricity è già installato sullo stesso server di SANtricity, si verificheranno conflitti tra numeri di porta non SSL e numeri di porta SSL. In questo caso, scegliere i numeri appropriati per la porta non SSL e la porta SSL durante l'installazione di SANtricity Cloud Connector.
- Se vengono apportate modifiche hardware all'host, reinstallare l'applicazione SANtricity Cloud Connector per garantire la coerenza della crittografia.
- I backup creati fino alla versione 3.1 dell'applicazione SANtricity Cloud Connector non sono compatibili con la versione 4.0 dell'applicazione SANtricity Cloud Connector. Se si intende mantenere questi backup, è necessario continuare a utilizzare la versione precedente di SANtricity Cloud Connector. Per garantire la corretta installazione di release 3.1 e 4.0 separate di SANtricity Cloud Connector, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

Installazione di Device Mapper multipath (DM-MP)

Tutti gli host che eseguono il connettore cloud di SANtricity devono anche eseguire il multipath (DM-MP) di Linux Device Mapper e avere installato il pacchetto multipath-tools.

Il processo di rilevamento di SANtricity Cloud Connector si basa sul pacchetto di strumenti multipath per il rilevamento e il riconoscimento dei volumi e dei file da eseguire per il backup o il ripristino. Per ulteriori informazioni su come impostare e configurare la funzione di mappatura dei dispositivi, consultare la *Guida ai*

driver multipath di SANtricity Storage Manager per la release di SANtricity in uso nella sezione "E-Series e risorse di documentazione SANtricity".

Installare Cloud Connector

È possibile installare SANtricity Cloud Connector sui sistemi operativi Linux in modalità grafica o console.

Modalità grafica

È possibile utilizzare la modalità grafica per installare SANtricity Cloud Connector su un sistema operativo Linux.

Prima di iniziare

Indicare una posizione host per l'installazione di SANtricity Cloud Connector.

Fasi

1. Scaricare il file di installazione di SANtricity Cloud Connector nella posizione host desiderata.
2. Aprire una finestra terminale.
3. Accedere al file di directory contenente il file di installazione di SANtricity Cloud Connector.
4. Avviare il processo di installazione di SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin -i gui
   ```

   In questo comando, `xxxx` indica il numero di versione dell'applicazione.

   Viene visualizzata la finestra Installer.

5. Esaminare la dichiarazione Introduzione, quindi fare clic su **Avanti**.

   Il Contratto di licenza per NetApp, Inc Il software viene visualizzato nella finestra del programma di installazione.

6. Accettare i termini del Contratto di licenza, quindi fare clic su **Avanti**.

   Vengono visualizzati i backup creati con le release precedenti di SANtricity Cloud Connector.

7. Per riconoscere i backup creati con le release precedenti di SANtricity, fare clic su **Avanti**.

   > Per installare la versione 4.0 di SANtricity Cloud Connector mantenendo una versione precedente, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

   La pagina Choose Install (Scegli installazione) viene visualizzata all'interno della finestra Installer (programma di installazione). Il campo dove si desidera installare visualizza la seguente cartella di installazione predefinita: `opt/netapp/santricity_cloud_connector4/`

8. Scegliere una delle seguenti opzioni:
   - Per accettare la posizione predefinita, fare clic su **Avanti**.
   - Per modificare la posizione predefinita, immettere una nuova posizione per la cartella. Viene visualizzata la pagina Enter the non SSL Jetty Port Number (immettere il numero di porta Jetty non

SSL). Alla porta non SSL viene assegnato il valore predefinito 8080.

9. Scegliere una delle seguenti opzioni:
   - Per accettare il numero di porta SSL predefinito, fare clic su **Avanti**.
   - Per modificare il numero di porta SSL predefinito, immettere il nuovo valore del numero di porta desiderato.
10. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta non SSL predefinito, fare clic su **Avanti**.
    - Per modificare il numero di porta non SSL predefinito, immettere il nuovo valore del numero di porta desiderato. Viene visualizzata la pagina Pre-Installation Summary (Riepilogo preinstallazione).
11. Esaminare il Riepilogo pre-installazione visualizzato, quindi fare clic su **Installa**.

    Viene avviata l'installazione di SANtricity Cloud Connector e viene visualizzata una richiesta di installazione di Webserver Daemon.

12. Fare clic su **OK** per confermare la richiesta di installazione di Webserver Daemon.

    Viene visualizzato il messaggio Installation complete (Installazione completata).

13. Fare clic su **Done** (fine) per uscire dal programma di installazione di SANtricity Cloud Connecter.

Modalità console

È possibile utilizzare la modalità console per installare SANtricity Cloud Connector su un sistema operativo Linux.

Prima di iniziare

Indicare una posizione host per l'installazione di SANtricity Cloud Connector.

Fasi

1. Scaricare il file di installazione di SANtricity Cloud Connector nella posizione dell'host i/o desiderata.
2. Aprire una finestra terminale.
3. Accedere al file di directory contenente il file di installazione di SANtricity Cloud Connector.
4. Avviare il processo di installazione di SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin -i console
   ```

   In questo comando, `xxxx` indica il numero di versione dell'applicazione.

   Il processo di installazione di SANtricity Cloud Connector viene inizializzato.

5. Premere **Invio** per procedere con il processo di installazione.

   Il Contratto di licenza con l'utente finale per NetApp, Inc Il software viene visualizzato nella finestra del programma di installazione.

   > Per annullare il processo di installazione in qualsiasi momento, digitare `quit` nella finestra del programma di installazione.

6. Premere **Invio** per passare a ciascuna parte del Contratto di licenza con l'utente finale.

   La dichiarazione di accettazione del Contratto di licenza viene visualizzata sotto la finestra del programma di installazione.

7. Per accettare i termini del Contratto di licenza con l'utente finale e procedere con l'installazione di SANtricity Cloud Connector, immettere `Y` E premere **Invio** nella finestra del programma di installazione.

   Vengono visualizzati i backup creati con le release precedenti di SANtricity Cloud Connector.

   > Se non si accettano i termini del Contratto per l'utente finale, digitare `N` E premere **Invio** per terminare il processo di installazione di SANtricity Cloud Connector.

8. Per riconoscere i backup creati con le release precedenti di SANtricity, premere **Invio**.

   > Per installare la versione 4.0 di SANtricity Cloud Connector mantenendo una versione precedente, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

   Viene visualizzato il messaggio Scegli cartella di installazione con la seguente cartella di installazione predefinita per SANtricity Cloud Connector:`/opt/netapp/santricity_cloud_connector4/`.

9. Scegliere una delle seguenti opzioni:
   - Per accettare la posizione di installazione predefinita, premere **Invio**.
   - Per modificare la posizione di installazione predefinita, immettere la nuova posizione della cartella. Viene visualizzato il messaggio inserire il numero di porta Jetty non SSL. Alla porta non SSL viene assegnato il valore predefinito 8080.
10. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta SSL predefinito, premere **Avanti**.
    - Per modificare il numero di porta SSL predefinito, immettere il nuovo valore del numero di porta desiderato.
11. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta non SSL predefinito, premere **Invio**.
    - Per modificare il numero di porta non SSL predefinito, inserire il nuovo valore del numero di porta. Viene visualizzato il riepilogo pre-installazione di SANtricity Cloud Connector.
12. Esaminare il Riepilogo pre-installazione visualizzato e premere **Invio**.
13. Premere **Invio** per confermare la richiesta di configurazione di Webserver Daemon.

    Viene visualizzato il messaggio Installation complete (Installazione completata).

14. Premere **Invio** per uscire dal programma di installazione di SANtricity.

Aggiungere il certificato del server e il certificato CA in un archivio chiavi

Per utilizzare una connessione https sicura dal browser all'host di SANtricity Cloud Connector, è possibile accettare il certificato autofirmato dall'host di SANtricity Cloud Connector o aggiungere un certificato e una catena di attendibilità riconosciuti sia dal browser che dall'applicazione SANtricity Cloud Connector.

Prima di iniziare

L'applicazione SANtricity Cloud Connector deve essere installata su un host.

Fasi

1. Arrestare il servizio utilizzando `systemctl` comando.
2. Dalla posizione di installazione predefinita, accedere alla directory di lavoro.

   > Il percorso di installazione predefinito per SANtricity Cloud Connector è `/opt/netapp/santricity_cloud_connector4`.

3. Utilizzando il `keytool` Creare il certificato del server e la richiesta di firma del certificato (CSR).

   ESEMPIO

   ```
   keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
   L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
   -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
   keystore_cloudconnect.jks -storepass changeit
   keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
   -storepass changeit -file cloudconnect.csr
   ```

4. Inviare la CSR generata all'autorità di certificazione (CA) desiderata.

   L'autorità di certificazione firma la richiesta di certificato e restituisce un certificato firmato. Inoltre, si riceve un certificato dalla CA stessa. Questo certificato CA deve essere importato nel keystore.

5. Importare il certificato e la catena del certificato CA nell'archivio chiavi dell'applicazione: `/<install Path>/working/keystore`

   ESEMPIO

   ```
   keytool -import -alias ca-root -file root-ca.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
   -keystore keystore_cloudconnect.jks -storepass <password>
   ```

6. Riavviare il servizio.

Aggiungere il certificato StorageGRID in un keystore

Se si configura StorageGRID come tipo di destinazione per l'applicazione Cloud Connector di SANtricity, è necessario prima aggiungere un certificato StorageGRID nell'archivio chiavi di SANtricity Cloud Connector.

Prima di iniziare

- Si dispone di un certificato StorageGRID firmato.
- L'applicazione SANtricity Cloud Connector è installata su un host.

Fasi

1. Arrestare il servizio utilizzando `systemctl` comando.
2. Dalla posizione di installazione predefinita, accedere alla directory di lavoro.

   > Il percorso di installazione predefinito per SANtricity Cloud Connector è `/opt/netapp/santricity_cloud_connector4`.

3. Importare il certificato StorageGRID nell'archivio chiavi dell'applicazione: `/<install Path>/working/keystore`

   ESEMPIO

   ```
   opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
   -trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
   /home/ictlabsg01.cer -keystore
   /opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
   ```

4. Riavviare il servizio.

Configurare SANtricity Cloud Connector per la prima volta

Una volta completata l'installazione, è possibile configurare l'applicazione SANtricity Cloud Connector tramite la configurazione guidata. La configurazione guidata viene visualizzata dopo l'accesso iniziale a SANtricity Cloud Connector.

Accedere a SANtricity Cloud Connector per la prima volta

Quando si inizializza SANtricity Cloud Connector per la prima volta, è necessario immettere una password predefinita per accedere all'applicazione.

Prima di iniziare

Assicurarsi di avere accesso a un browser connesso a Internet.

Fasi

1. Aprire un browser supportato.
2. Connettersi al server SANtricity Connector configurato (ad es. `http://localhost:8080/`).

   Viene visualizzata la pagina di accesso iniziale per l'applicazione SANtricity Cloud Connector.

3. Nel campo Password amministratore, immettere la password predefinita di `password`.
4. Fare clic su **Log in** (Accedi).

   Viene visualizzata la Configurazione guidata di SANtricity Cloud Connector.

Utilizzando la Configurazione guidata

La configurazione guidata viene visualizzata dopo aver eseguito correttamente l'accesso iniziale a SANtricity Cloud Connector.

La configurazione guidata consente di impostare la password dell'amministratore, le credenziali di gestione dell'accesso proxy dei servizi Web, il tipo di destinazione di backup desiderato e la password di crittografia per SANtricity Cloud Connector.

Fase 1: Impostare la password dell'amministratore

È possibile personalizzare la password utilizzata per gli accessi successivi a SANtricity Cloud Connector attraverso la pagina Imposta password amministratore.

La creazione di una password tramite la pagina Imposta password amministratore sostituisce effettivamente la password predefinita utilizzata durante l'accesso iniziale per l'applicazione SANtricity Cloud Connector.

Fasi

1. Nella pagina Set Administrator Password (Imposta password amministratore), inserire la password di accesso desiderata per SANtricity Cloud Connector nel campo **Enter the new Administrator password** (immettere la nuova password amministratore).
2. Nel campo **immettere nuovamente la nuova password amministratore**, immettere nuovamente la password dal primo campo.
3. Fare clic su **Avanti**.

   La password impostata per SANtricity Cloud Connector viene accettata e la pagina Imposta password viene visualizzata nella Configurazione guidata.

   > La password dell'amministratore definita dall'utente non viene impostata fino al completamento della configurazione guidata.

Fase 2: Impostare la password

Nella pagina Enter the Encryption Pass phrase (immettere la password di crittografia), è possibile specificare una password alfanumerica compresa tra 8 e 32 caratteri.

Una password specificata dall'utente è richiesta come parte della chiave di crittografia dei dati utilizzata dall'applicazione Cloud Connector di SANtricity.

Fasi

1. Nel campo **definisci una password**, immettere la password desiderata.
2. Nel campo **Re-Enter your pass phrase** (immettere nuovamente la password), immettere nuovamente la password nel primo campo.
3. Fare clic su **Avanti**.

   La password immessa per l'applicazione SANtricity Cloud Connector viene accettata e viene visualizzata la pagina Seleziona tipo di destinazione per la configurazione guidata.

Fase 3: Selezionare il tipo di destinazione

Le funzionalità di backup e ripristino sono disponibili per i tipi di destinazione Amazon S3, AltaVault e StorageGRID tramite SANtricity Cloud Connector. È possibile specificare il tipo di destinazione dello storage desiderato per l'applicazione SANtricity Cloud Connector nella pagina selezionare il tipo di destinazione.

Prima di iniziare

Assicurarsi di disporre di uno dei seguenti elementi: Punto di montaggio AltaVault, account Amazon AWS o

account StorageGRID.

Fasi

1. Nel menu a discesa, selezionare una delle seguenti opzioni:
    - Amazon AWS
    - AltaVault
    - StorageGRID

    Nella Configurazione guidata viene visualizzata la pagina Target Type (tipo di destinazione) per l'opzione selezionata.

2. Fare riferimento alle istruzioni di configurazione appropriate per AltaVault, Amazon AWS o StorageGRID.

Configurare l'appliance AltaVault

Dopo aver selezionato l'opzione AltaVault appliance nella pagina selezionare il tipo di destinazione, vengono visualizzate le opzioni di configurazione per il tipo di destinazione AltaVault.

Prima di iniziare

- Si dispone del percorso di montaggio NFS per un'appliance AltaVault.
- Hai specificato l'appliance AltaVault come tipo di destinazione.

Fasi

1. Nel campo **percorso di montaggio NFS**, inserire il punto di montaggio per il tipo di destinazione AltaVault.

    I valori nel campo **NFS Mount Path** devono seguire il formato del percorso Linux.

2. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

    Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

3. Fare clic su **Test connessione** per verificare la connessione per le impostazioni AltaVault specificate.
4. Fare clic su **Avanti**.

    Il tipo di destinazione specificato per il connettore cloud di SANtricity viene accettato e la pagina Proxy dei servizi web viene visualizzata nella Configurazione guidata.

5. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Configurare l'account Amazon AWS

Dopo aver selezionato l'opzione Amazon AWS nella pagina Select the Target Type (Seleziona tipo di destinazione), vengono visualizzate le opzioni di configurazione per il tipo di destinazione Amazon AWS.

Prima di iniziare

- Hai un account Amazon AWS stabilito.

- Hai specificato Amazon AWS come tipo di destinazione.

Fasi

1. Nel campo **Access Key ID** (ID chiave di accesso), immettere l'ID di accesso per la destinazione Amazon AWS.
2. Nel campo **Secret Access Key** (chiave di accesso segreta), immettere la chiave di accesso segreta per la destinazione.
3. Nel campo **Nome bucket**, immettere il nome del bucket per la destinazione.
4. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

   Si consiglia di attivare questa impostazione per garantire che i dati della destinazione di backup possano essere ripristinati in caso di perdita del database.

   Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

5. Fare clic su **Test Connection** (verifica connessione) per verificare le credenziali Amazon AWS immesse.
6. Fare clic su **Avanti**.

   Il tipo di destinazione specificato per il connettore cloud SANtricity viene accettato e la pagina Proxy dei servizi Web viene visualizzata nella Configurazione guidata.

7. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Configurare l'account StorageGRID

Dopo aver selezionato l'opzione StorageGRID nella pagina selezionare il tipo di destinazione, vengono visualizzate le opzioni di configurazione per il tipo di destinazione StorageGRID.

Prima di iniziare

- Hai un account StorageGRID stabilito.
- Hai un certificato StorageGRID firmato nel keystore di SANtricity Cloud Connector.
- È stato specificato StorageGRID come tipo di destinazione.

Fasi

1. Nel campo **URL**, immettere l'URL del servizio cloud Amazon S3
2. Nel campo **Access Key ID** (ID chiave di accesso), inserire l'ID di accesso per la destinazione S3.
3. Nel campo **Secret Access Key** (chiave di accesso segreta), inserire la chiave di accesso segreta per la destinazione S3.
4. Nel campo **Nome bucket**, immettere il nome del bucket per la destinazione S3.
5. Per utilizzare l'accesso in stile tracciato, selezionare la casella di controllo **Usa accesso in stile tracciato**.

   Se deselezionata, viene utilizzato l'accesso in stile host virtuale.

6. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

> Si consiglia di attivare questa impostazione per garantire che i dati della destinazione di backup possano essere ripristinati in caso di perdita del database.

> Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

7. Fare clic su **Test Connection** (verifica connessione) per verificare le credenziali S3 immesse.

> Alcuni account compatibili con S3 potrebbero richiedere connessioni HTTP protette. Per informazioni sull'inserimento di un certificato StorageGRID nell'archivio chiavi, vedere "Aggiungere il certificato StorageGRID in un keystore".

8. Fare clic su **Avanti**.

   Il tipo di destinazione specificato per il connettore cloud SANtricity viene accettato e la pagina Proxy servizi web viene visualizzata nella Configurazione guidata.

9. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Fase 4: Connessione al proxy dei servizi Web

Le informazioni di accesso e di connessione per il proxy dei servizi Web utilizzato insieme a SANtricity Cloud Connector vengono inserite nella pagina Immetti credenziali e URL proxy dei servizi Web.

Prima di iniziare

Assicurarsi di disporre di una connessione stabilita con il proxy dei servizi Web di SANtricity.

Fasi

1. Nel campo **URL**, immettere l'URL del proxy dei servizi Web utilizzato per SANtricity Cloud Connector.
2. Nel campo **Nome utente**, immettere il nome utente per la connessione proxy dei servizi Web.
3. Nel campo **Password**, immettere la password per la connessione proxy dei servizi Web.
4. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali proxy dei servizi Web immesse.
5. Dopo aver verificato le credenziali di Web Services Proxy immesse tramite la connessione di prova.
6. Fare clic su **Avanti**

   Le credenziali del proxy dei servizi Web per il connettore cloud di SANtricity vengono accettate e la pagina Seleziona array di storage viene visualizzata nella Configurazione guidata.

Fase 5: Selezionare gli array di storage

In base alle credenziali del proxy dei servizi Web di SANtricity immesse tramite la Configurazione guidata, viene visualizzato un elenco degli array di storage disponibili nella pagina Seleziona array di storage. In questa pagina è possibile selezionare gli array di storage utilizzati da SANtricity Cloud Connector per i processi di backup e ripristino.

Prima di iniziare

Assicurarsi che gli array di storage siano configurati per l'applicazione proxy dei servizi Web di SANtricity.

> Gli array di storage non raggiungibili osservati dall'applicazione SANtricity Cloud Connector causeranno eccezioni API nel file di log. Questo è il comportamento previsto dell'applicazione SANtricity Cloud Connector ogni volta che un elenco di volumi viene estratto da un array irraggiungibile. Per evitare queste eccezioni API nel file di log, è possibile risolvere il problema principale direttamente con l'array di storage o rimuovere l'array di storage interessato dall'applicazione proxy dei servizi Web di SANtricity.

Fasi

1. Selezionare ciascuna casella di controllo accanto all'array di storage che si desidera assegnare all'applicazione SANtricity Cloud Connector per le operazioni di backup e ripristino.
2. Fare clic su **Avanti**.

   Gli array di storage selezionati vengono accettati e viene visualizzata la pagina Select hosts (Seleziona host) nella Configurazione guidata.

> È necessario configurare una password valida per qualsiasi array di storage selezionato nella pagina Select Storage Array (Seleziona array di storage). È possibile configurare le password degli array di storage attraverso la documentazione dell'API proxy dei servizi Web di SANtricity.

Fase 6: Selezionare gli host

In base agli array di storage ospitati dal proxy dei servizi Web selezionati tramite la Configurazione guidata, è possibile selezionare un host disponibile per mappare i volumi di backup e ripristinare i volumi candidati all'applicazione SANtricity Cloud Connector attraverso la pagina Seleziona host.

Prima di iniziare

Assicurarsi di disporre di un host tramite il proxy dei servizi Web di SANtricity.

Fasi

1. Nel menu a discesa dello storage array elencato, selezionare l'host desiderato.
2. Ripetere il passaggio 1 per tutti gli array di storage aggiuntivi elencati nella pagina Select host (Seleziona host).
3. Fare clic su **Avanti**.

   L'host selezionato per SANtricity Cloud Connector viene accettato e la pagina di revisione viene visualizzata nella Configurazione guidata.

Fase 7: Esaminare la configurazione iniziale

L'ultima pagina della configurazione guidata di SANtricity Cloud Connector fornisce un riepilogo dei risultati immessi per la revisione.

Esaminare i risultati dei dati di configurazione validati.

- Se tutti i dati di configurazione sono stati validati e stabiliti correttamente, fare clic su **fine** per completare il processo di configurazione.

- Se non è possibile validare una sezione dei dati di configurazione, fare clic su **Back** (Indietro) per accedere alla pagina appropriata della configurazione guidata e rivedere i dati inviati.

Accedere a SANtricity Cloud Connector

È possibile accedere all'interfaccia utente grafica per l'applicazione SANtricity Cloud Connector attraverso il server configurato in un browser supportato. Assicurati di disporre di un account SANtricity Cloud Connector stabilito.

Fasi

1. In un browser supportato, connettersi al server SANtricity Cloud Connector configurato (ad esempio, `http://localhost:8080/`).

   Viene visualizzata la pagina di accesso dell'applicazione SANtricity Cloud Connector.

2. Inserire la password di amministratore configurata.
3. Fare clic su **Login**.

   Viene visualizzata la landing page dell'applicazione SANtricity Cloud Connector.

Backup

Puoi accedere all'opzione Backup nel pannello di navigazione a sinistra dell'applicazione SANtricity Cloud Connector. L'opzione Backup visualizza la pagina Backup, che consente di creare nuovi processi di backup basati su immagine o file.

Utilizzare la pagina **backup** dell'applicazione SANtricity Cloud Connector per creare ed elaborare i backup dei volumi e-Series. È possibile creare backup basati su immagini o file ed eseguire tali operazioni immediatamente o in un secondo momento. Inoltre, è possibile scegliere di eseguire backup completi o incrementali in base all'ultimo backup completo eseguito. È possibile eseguire un massimo di sei backup incrementali in base all'ultimo backup completo eseguito tramite l'applicazione SANtricity Cloud Connector.

> Tutti i timestamp per i processi di backup e ripristino elencati nell'applicazione SANtricity Cloud Connector utilizzano l'ora locale.

Creare un nuovo backup basato su immagine

È possibile creare nuovi backup basati su immagini tramite la funzione Crea nella pagina dei backup dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurarsi di disporre di array di storage dal proxy dei servizi Web registrato al connettore cloud di SANtricity.

Fasi

1. Nella pagina Backup, fare clic su **Crea**.

   Viene visualizzata la finestra Create Backup (Crea backup).

2. Selezionare **Crea un backup basato su immagine**.
3. Fare clic su **Avanti**.

Nella finestra Create Backup (Crea backup) viene visualizzato un elenco dei volumi e-Series disponibili.

4. Selezionare il volume e-Series desiderato e fare clic su **Avanti**.

   Viene visualizzata la pagina **assegnare un nome al backup e fornire una descrizione** della finestra di conferma della creazione del backup.

5. Per modificare il nome del backup generato automaticamente, immettere il nome desiderato nel campo **Nome processo**.
6. Se necessario, aggiungere una descrizione per il backup nel campo **Descrizione lavoro**.

   Inserire una descrizione del lavoro che consenta di identificare facilmente il contenuto del backup.

7. Fare clic su **Avanti**.

   Un riepilogo del backup basato su immagine selezionato viene visualizzato nella pagina **Review backup information** della finestra Create Backup (Crea backup).

8. Esaminare il backup selezionato e fare clic su **fine**.

   Viene visualizzata la pagina di conferma della finestra Create Backup (Crea backup).

9. Selezionare una delle seguenti opzioni:
   - **Sì** — Avvia un backup completo per il backup selezionato.
   - **NO** — non viene eseguito Un backup completo per il backup basato sull'immagine selezionato.

   Un backup completo per il backup basato sull'immagine selezionato può essere eseguito in un secondo momento attraverso la funzione Esegui nella pagina Backup.

10. Fare clic su **OK**.

    Il backup per il volume e-Series selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Backup.

Creare una nuova cartella/backup basato su file

È possibile creare nuovi backup basati su file/cartelle tramite la funzione Crea nella pagina dei backup dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurarsi di disporre di array di storage dal proxy dei servizi Web registrato al connettore cloud di SANtricity.

Un backup basato su file esegue il backup incondizionato di tutti i file sul file system specificato. Tuttavia, è possibile eseguire un ripristino selettivo di file e cartelle.

Fasi

1. Nella pagina Backup, fare clic su **Crea**.

   Viene visualizzata la finestra Create Backup (Crea backup).

2. Selezionare **Crea un backup basato su file/cartella**.

3. Fare clic su **Avanti**.

   Nella finestra Create Backup (Crea backup) viene visualizzato un elenco di volumi contenenti file system disponibili per il backup.

4. Selezionare il volume desiderato e fare clic su **Avanti**.

   Nella finestra Create Backup (Crea backup) viene visualizzato un elenco dei filesystem disponibili sul volume selezionato.

   > Se il file system non viene visualizzato, verificare che il tipo di file sia supportato dall'applicazione SANtricity Cloud Connector. Per ulteriori informazioni, fare riferimento a. "File system supportati".

5. Selezionare il file system desiderato contenente la cartella o i file di cui eseguire il backup e fare clic su **Avanti**.

   Viene visualizzata la pagina **assegnare un nome al backup e fornire una descrizione** della finestra di conferma della creazione del backup.

6. Per modificare il nome del backup generato automaticamente, immettere il nome desiderato nel campo **Nome processo**.
7. Se necessario, aggiungere una descrizione per il backup nel campo **Descrizione lavoro**.

   > Inserire una descrizione del lavoro che consenta di identificare facilmente il contenuto del backup.

8. Fare clic su **Avanti**.

   Un riepilogo del backup basato su file o cartella selezionato viene visualizzato nella pagina **Review backup information** della finestra Create Backup (Crea backup).

9. Esaminare la cartella o il backup basato su file selezionato e fare clic su **fine**.

   Viene visualizzata la pagina di conferma della finestra Create Backup (Crea backup).

10. Selezionare una delle seguenti opzioni:
    - **Sì** — Avvia un backup completo per il backup selezionato.
    - **NO** — non viene eseguito Un backup completo per il backup selezionato.

    > Un backup completo per il backup basato su file selezionato può essere eseguito anche in un secondo momento attraverso la funzione Esegui nella pagina dei backup.

11. Fare clic su **Chiudi**.

    Il backup per il volume e-Series selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Backup.

Eseguire backup completi e incrementali

È possibile eseguire backup completi e incrementali tramite la funzione Esegui nella pagina dei backup. I backup incrementali sono disponibili solo per i backup basati su file.

Prima di iniziare

Assicurarsi di aver creato un processo di backup tramite SANtricity Cloud Connector.

Fasi

1. Nella scheda Backup, selezionare il processo di backup desiderato e fare clic su **Esegui**.

   > Il backup completo viene eseguito automaticamente ogni volta che viene selezionato un processo di backup basato su immagine o un processo di backup senza un backup iniziale eseguito in precedenza.

   Viene visualizzata la finestra Esegui backup.

2. Selezionare una delle seguenti opzioni:
   - **Completo** — esegue il backup di tutti i dati per il backup basato su file selezionato.
   - **Incrementale** — esegue il backup delle modifiche apportate solo dall'ultimo backup eseguito.

     > È possibile eseguire un numero massimo di sei backup incrementali in base all'ultimo backup completo eseguito tramite l'applicazione SANtricity Cloud Connector.

3. Fare clic su **Esegui**.

   Viene avviata la richiesta di backup.

Eliminare un processo di backup

La funzione Delete (Elimina) elimina i dati di backup nella posizione di destinazione specificata per il backup selezionato insieme al set di backup.

Prima di iniziare

Assicurarsi che sia presente un backup con lo stato completato, non riuscito o annullato.

Fasi

1. Nella pagina Backup, selezionare il backup desiderato e fare clic su **Delete** (Elimina).

   > Se si seleziona un backup di base completo per l'eliminazione, vengono eliminati anche tutti i backup incrementali associati.

   Viene visualizzata la finestra Confirm Delete (Conferma eliminazione).

2. Nel campo **Type delete**, digitare `DELETE` per confermare l'azione di eliminazione.
3. Fare clic su **Delete** (Elimina).

   Il backup selezionato viene eliminato.

Ripristini

È possibile accedere all'opzione Ripristina nel pannello di navigazione a sinistra dell'applicazione SANtricity Cloud Connector. L'opzione Restore (Ripristina) visualizza la pagina Restore (Ripristina), che consente di creare nuovi processi di ripristino basati su

immagine o file.

Il connettore cloud di SANtricity utilizza il concetto di job per eseguire il ripristino effettivo di un volume e-Series. Prima di eseguire un ripristino, è necessario identificare il volume e-Series da utilizzare per l'operazione. Dopo aver aggiunto un volume e-Series per il ripristino all'host di SANtricity Cloud Connector, è possibile utilizzare `Restore` Dell'applicazione SANtricity Cloud Connector per creare ed elaborare i ripristini.

> Tutti i timestamp per i processi di backup e ripristino elencati nell'applicazione SANtricity Cloud Connector utilizzano l'ora locale.

Creare un nuovo ripristino basato su immagine

È possibile creare nuovi ripristini basati su immagine tramite la funzione Crea nella pagina di ripristino dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurati di avere a disposizione un backup basato su immagine tramite SANtricity Cloud Connector.

Fasi

1. Nella pagina di ripristino dell'applicazione SANtricity Cloud Connector, fare clic su **Crea**.

   Viene visualizzata la finestra Restore (Ripristino).

2. Selezionare il backup desiderato.
3. Fare clic su **Avanti**.

   La pagina Select Backup Point (Seleziona punto di backup) viene visualizzata nella finestra Restore (Ripristino).

4. Selezionare il backup completo desiderato.
5. Fare clic su **Avanti**.

   La pagina Select Restore Target (Seleziona destinazione ripristino) viene visualizzata nella finestra Restore (Ripristino).

6. Selezionare il volume di ripristino e fare clic su **Avanti**.

   La pagina Review (Revisione) viene visualizzata nella finestra Restore (Ripristino).

7. Esaminare l'operazione di ripristino selezionata e fare clic su **fine**.

   Il ripristino per il volume host di destinazione selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Creare un nuovo ripristino basato su file

È possibile creare nuovi ripristini basati su file tramite la funzione Crea nella pagina Ripristino dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurati di avere a disposizione un backup basato su file tramite SANtricity Cloud Connector.

Fasi

1. Nella pagina di ripristino dell'applicazione SANtricity Cloud Connector, fare clic su **Crea**.

   Viene visualizzata la finestra Restore (Ripristino).

2. Nella finestra Restore (Ripristino), selezionare il backup basato su file desiderato.
3. Fare clic su **Avanti**.

   La pagina Select Backup Point (Seleziona punto di backup) viene visualizzata nella finestra Create Restore Job (Crea processo di ripristino).

4. Nella pagina Select Backup Point (Seleziona punto di backup), selezionare il backup completo desiderato.
5. Fare clic su **Avanti**.

   Nella finestra Restore (Ripristino) viene visualizzato un elenco dei file system o delle cartelle/file disponibili.

6. Selezionare le cartelle o i file da ripristinare e fare clic su **Avanti**.

   La pagina Select Restore Target (Seleziona destinazione ripristino) viene visualizzata nella finestra Restore (Ripristino).

7. Selezionare il volume di ripristino e fare clic su **Avanti**.

   La pagina Review (Revisione) viene visualizzata nella finestra Restore (Ripristino).

8. Esaminare l'operazione di ripristino selezionata e fare clic su **fine**.

   Il ripristino per il volume host di destinazione selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Eliminare un ripristino

È possibile utilizzare la funzione Delete (Elimina) per eliminare un elemento di ripristino selezionato dalla sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Prima di iniziare

Assicurarsi che sia presente un processo di ripristino con lo stato completato, non riuscito o annullato.

Fasi

1. Nella pagina Restore (Ripristino), fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra Confirm Delete (Conferma eliminazione).

2. Nel campo **Type delete**, digitare `delete` per confermare l'azione di eliminazione.
3. Fare clic su **Delete** (Elimina).

   > Non è possibile eliminare un ripristino sospeso.

   Il ripristino selezionato viene eliminato.

Modificare le impostazioni di SANtricity Cloud Connector

L'opzione Settings (Impostazioni) consente di modificare le configurazioni correnti

dell'applicazione per l'account S3, gli array e gli host di storage gestiti e le credenziali del proxy dei servizi Web. Puoi anche modificare la password per l'applicazione SANtricity Cloud Connector tramite l'opzione Impostazioni.

Modificare le impostazioni dell'account S3

È possibile modificare le impostazioni S3 esistenti per l'applicazione SANtricity Cloud Connector nella finestra S3 account Settings (Impostazioni account S3).

Prima di iniziare

Quando si modificano le impostazioni dell'URL o dell'etichetta del bucket S3, tenere presente che l'accesso a qualsiasi backup esistente configurato tramite SANtricity Cloud Connector verrà compromesso.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni > Configurazione**.

   Viene visualizzata la pagina Impostazioni - Configurazione.

2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni) per S3 account Settings (Impostazioni account S3).

   Viene visualizzata la pagina S3 account Settings (Impostazioni account S3).

3. Nel file URL, immettere l'URL per il servizio cloud S3.
4. Nel campo **Access Key ID** (ID chiave di accesso), inserire l'ID di accesso per la destinazione S3.
5. Nel campo **Secret Access Key** (chiave di accesso segreta), inserire la chiave di accesso per la destinazione S3.
6. Nel campo **S3 Bucket Name** (Nome bucket S3), immettere il nome del bucket per la destinazione S3.
7. Se necessario, selezionare la casella di controllo **Usa accesso stile percorso**.
8. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali S3 immesse.
9. Fare clic su **Save** (Salva) per applicare le modifiche.

   Vengono applicate le impostazioni modificate dell'account S3.

Gestire gli array di storage

È possibile aggiungere o rimuovere gli array di storage dal proxy dei servizi Web registrato sull'host di SANtricity Cloud Connector nella pagina Gestione array di storage.

La pagina Gestisci array di storage visualizza un elenco di array di storage dal proxy dei servizi Web disponibile per la registrazione con l'host di SANtricity Cloud Connector.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni > Storage Array**.

   Viene visualizzata la schermata Settings - Storage Arrays (Impostazioni - array di storage).

2. Per aggiungere array di storage a SANtricity Cloud Connector, fare clic su **Aggiungi**.
   a. Nella finestra Add Storage Arrays (Aggiungi array di storage), selezionare ciascuna casella di controllo

accanto agli array di storage desiderati dall'elenco dei risultati.

b. Fare clic su **Aggiungi**.

L'array di storage selezionato viene aggiunto al connettore cloud SANtricity e visualizzato nella sezione Result list (elenco risultati) della schermata Settings - Storage Arrays (Impostazioni - array di storage).

3. Per modificare l'host per un array di storage aggiunto, fare clic su **Edit** (Modifica) per la voce nella sezione Result list (elenco risultati) della schermata Settings - Storage Arrays (Impostazioni - array di storage).
   a. Nel menu a discesa Associated host (host associato), selezionare l'host desiderato per lo storage array.
   b. Fare clic su **Save** (Salva).

   L'host selezionato viene assegnato all'array di storage.

4. Per rimuovere un array di storage esistente dall'host di SANtricity Cloud Connector, selezionare gli array di storage desiderati dall'elenco dei risultati in basso e fare clic su **Rimuovi**.
   a. Nel campo Confirm Remove Storage Array (Conferma rimozione array di storage), digitare `REMOVE`.
   b. Fare clic su **Rimuovi**.

   L'array di storage selezionato viene rimosso dall'host del connettore cloud SANtricity.

Modificare le impostazioni del proxy dei servizi Web

È possibile modificare le impostazioni proxy dei servizi Web esistenti per l'applicazione SANtricity connettore nella finestra Impostazioni proxy dei servizi Web.

Prima di iniziare

Il proxy dei servizi Web utilizzato con il connettore cloud SANtricity deve avere aggiunto gli array appropriati e la password corrispondente impostata.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni › Configurazione**.

   Viene visualizzata la schermata Impostazioni - Configurazione.

2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni) per Web Services Proxy.

   Viene visualizzata la schermata delle impostazioni del proxy dei servizi Web.

3. Nel campo URL, immettere l'URL del proxy dei servizi Web utilizzato per SANtricity Cloud Connector.
4. Nel campo User Name (Nome utente), immettere il nome utente per la connessione proxy dei servizi Web.
5. Nel campo Password, immettere la password per la connessione proxy dei servizi Web.
6. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali proxy dei servizi Web immesse.
7. Fare clic su **Save** (Salva) per applicare le modifiche.

Modificare la password di SANtricity Cloud Connector

È possibile modificare la password per l'applicazione SANtricity Cloud Connector nella schermata Modifica password.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni › Configurazione**.

   Viene visualizzata la schermata Impostazioni - Configurazione.

2. Fare clic su **Modifica password** per SANtricity Cloud Connector.

   Viene visualizzata la schermata Change Password (Modifica password).

3. Nel campo Current password (Password corrente), immettere la password corrente per l'applicazione SANtricity Cloud Connector.
4. Nel campo Nuova password, immettere la nuova password per l'applicazione SANtricity Cloud Connector.
5. Nel campo Confirm new password (Conferma nuova password), immettere nuovamente la nuova password.
6. Fare clic su **Change** (Modifica) per applicare la nuova password.

   La password modificata viene applicata all'applicazione SANtricity Cloud Connector.

Disinstallare SANtricity Cloud Connector

È possibile disinstallare SANtricity Cloud Connector tramite il programma di disinstallazione grafico o la modalità console.

Disinstallare utilizzando la modalità grafica

È possibile utilizzare la modalità grafica per disinstallare SANtricity Cloud Connector su un sistema operativo Linux.

Fasi

1. Dalla finestra di un terminale, accedere alla directory contenente il file di disinstallazione di SANtricity Cloud Connector.

   Il file di disinstallazione per SANtricity Cloud Connector è disponibile nella seguente directory predefinita:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Dalla directory contenente il file di disinstallazione di SANtricity Cloud Connector, eseguire il seguente comando:

   ```
   ./uninstall_cloud_connector4 -i gui
   ```

   Il processo di disinstallazione di SANtricity Cloud Connector viene inizializzato.

3. Nella finestra di disinstallazione, fare clic su **Disinstalla** per procedere con la disinstallazione di SANtricity Cloud Connector.

   Il processo di disinstallazione viene completato e l'applicazione SANtricity Cloud Connector viene disinstallata nel sistema operativo Linux.

Disinstallare utilizzando la modalità console

È possibile utilizzare la modalità console per disinstallare SANtricity Cloud Connector su un sistema operativo Linux.

Fasi

1. Dalla finestra di un terminale, accedere alla directory contenente il file di disinstallazione di SANtricity Cloud Connector.

   Il file di disinstallazione per SANtricity Cloud Connector è disponibile nella seguente directory predefinita:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Dalla directory contenente il file di disinstallazione di SANtricity Cloud Connector, eseguire il seguente comando:

   ```
   ./uninstall_cloud_connector4 -i console
   ```

   Il processo di disinstallazione di SANtricity Cloud Connector viene inizializzato.

3. Nella finestra di disinstallazione, premere **Invio** per procedere con la disinstallazione di SANtricity Cloud Connector.

   Il processo di disinstallazione viene completato e l'applicazione SANtricity Cloud Connector viene disinstallata nel sistema operativo Linux.

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.