Sistema

SANtricity 11.5

NetApp
February 12, 2024

Sommario

Sistema

Impostazioni dello storage array

Concetti

Performance e impostazioni della cache

La memoria cache è un'area di storage volatile temporaneo sul controller che ha un tempo di accesso più rapido rispetto ai supporti del disco.

Con il caching, le performance di i/o complessive possono essere aumentate come segue:

- I dati richiesti dall'host per una lettura potrebbero essere già nella cache da un'operazione precedente, eliminando così la necessità di accesso al disco.
- I dati di scrittura vengono scritti inizialmente nella cache, consentendo all'applicazione di continuare invece di attendere la scrittura dei dati sul disco.

Le impostazioni predefinite della cache soddisfano i requisiti della maggior parte degli ambienti, ma è possibile modificarle se necessario.

Impostazioni della cache dell'array di storage

Per tutti i volumi nell'array di storage, è possibile specificare i seguenti valori dalla pagina System (sistema):

- **Valore iniziale per il flushing** — la percentuale di dati non scritti nella cache che attiva un flush della cache (scrittura su disco). Quando la cache contiene la percentuale iniziale specificata di dati non scritti, viene attivato un flusso. Per impostazione predefinita, il controller avvia lo svuotamento della cache quando la cache raggiunge il 80% di memoria piena.
- **Cache block size** — dimensione massima di ciascun blocco di cache, un'unità organizzativa per la gestione della cache. La dimensione predefinita del blocco della cache è 8 KiB, ma può essere impostata su 4, 8, 16 o 32 KiB. Idealmente, la dimensione del blocco della cache dovrebbe essere impostata sulla dimensione i/o predominante delle applicazioni. I file system o le applicazioni di database utilizzano generalmente dimensioni inferiori, mentre le dimensioni maggiori sono adatte per le applicazioni che richiedono un trasferimento di dati di grandi dimensioni o l'i/o sequenziale

Impostazioni della cache del volume

Per i singoli volumi in un array di storage, è possibile specificare i seguenti valori dalla pagina Volumes (**Storage › Volumes**):

- **Read caching** — 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.
  - **Dynamic Read cache prefetch** — 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.

- **Write caching** — 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.

> Possibile perdita di dati — se si attiva l'opzione* Write caching without batteries 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).

  - **Write caching senza batterie** — l'impostazione write caching 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.
  - **Cache in 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.

Panoramica del bilanciamento automatico del carico

Il bilanciamento automatico del carico offre una migliore gestione delle risorse di i/o reagendo in modo dinamico alle variazioni di carico nel tempo e regolando automaticamente la proprietà del controller del volume per correggere eventuali problemi di sbilanciamento del carico quando i carichi di lavoro si spostano tra i controller.

Il carico di lavoro di ciascun controller viene costantemente monitorato e, grazie alla collaborazione dei driver multipath installati sugli host, può essere automaticamente bilanciato quando necessario. Quando il carico di lavoro viene riregolato automaticamente tra i controller, l'amministratore dello storage viene alleggerito dall'onere di regolare manualmente la proprietà del controller di volume per adattarsi alle modifiche di carico sull'array di storage.

Quando il bilanciamento automatico del carico è attivato, esegue le seguenti funzioni:

- Monitora e bilancia automaticamente l'utilizzo delle risorse dei controller.
- Regola automaticamente la proprietà del controller del volume quando necessario, ottimizzando in tal modo la larghezza di banda i/o tra gli host e lo storage array.

Attivazione e disattivazione del bilanciamento automatico del carico

Il bilanciamento automatico del carico è attivato per impostazione predefinita su tutti gli array di storage.

È possibile disattivare il bilanciamento automatico del carico sull'array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un determinato volume per bilanciare il carico di lavoro.
- Si opera in un ambiente altamente ottimizzato in cui la distribuzione del carico è appositamente configurata per ottenere una distribuzione specifica tra i controller.

Tipi di host che supportano la funzione di bilanciamento automatico del carico

Anche se il bilanciamento automatico del carico è attivato a livello di array di storage, il tipo di host selezionato per un cluster di host o host ha un'influenza diretta sul funzionamento della funzione.

Durante il bilanciamento del carico di lavoro dell'array di storage tra controller, la funzione di bilanciamento automatico del carico tenta di spostare volumi accessibili da entrambi i controller e mappati solo a un host o a un cluster host in grado di supportare la funzione di bilanciamento automatico del carico.

Questo comportamento impedisce a un host di perdere l'accesso a un volume a causa del processo di bilanciamento del carico; tuttavia, la presenza di volumi mappati agli host che non supportano il bilanciamento automatico del carico influisce sulla capacità dell'array di storage di bilanciare il carico di lavoro. Per bilanciare il carico di lavoro, il driver multipath deve supportare TPGS e il tipo di host deve essere incluso nella tabella seguente.

> Affinché un cluster host possa essere considerato in grado di eseguire il bilanciamento automatico del carico, tutti gli host del gruppo devono essere in grado di supportare il bilanciamento automatico del carico.

Tipo di host che supporta il bilanciamento automatico del carico	Con questo driver multipath
Windows o Windows Clustered	MPIO con NetApp e-Series DSM
Linux DM-MP (kernel 3.10 o successivo)	DM-MP con `scsi_dh_alua` gestore di dispositivi
VMware	Plug-in multipathing nativo (NMP) con `VMW_SATP_ALUA Storage Array Type` plug-in

> Con eccezioni minori, i tipi di host che non supportano il bilanciamento automatico del carico continuano a funzionare normalmente, indipendentemente dal fatto che la funzione sia attivata o meno. Un'eccezione è rappresentata dal fatto che se un sistema presenta un failover, gli array di storage spostano di nuovo i volumi non mappati o non assegnati al controller proprietario quando il percorso dei dati ritorna. Tutti i volumi mappati o assegnati a host con bilanciamento del carico non automatico non vengono spostati.

Vedere "Tool di matrice di interoperabilità" Per informazioni sulla compatibilità di driver multipath specifici, livello di sistema operativo e supporto del vassoio del disco del controller.

Verifica della compatibilità del sistema operativo con la funzione di bilanciamento automatico del carico

Verificare la compatibilità del sistema operativo con la funzione di bilanciamento automatico del carico prima di configurare un nuovo sistema (o di migrare un sistema esistente).

1. Accedere alla "Tool di matrice di interoperabilità" per trovare la soluzione e verificare il supporto.

   Se il sistema esegue Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, contattare il supporto tecnico.

2. Aggiornare e configurare `/etc/multipath.conf file`.
3. Assicurarsi che entrambi `retain_attached_device_handler` e. `detect_prio` sono impostati su `yes` per il vendor e il prodotto applicabili, oppure utilizzare le impostazioni predefinite.

Tipo di sistema operativo host predefinito

Il tipo di host predefinito viene utilizzato dall'array di storage quando gli host sono inizialmente connessi. Definisce il modo in cui i controller dell'array di storage funzionano con il sistema operativo dell'host quando si accede ai volumi. È possibile modificare il tipo di host in caso di necessità di modificare il funzionamento dello storage array rispetto agli host ad esso collegati.

In genere, è necessario modificare il tipo di host predefinito prima di connettere gli host all'array di storage o quando si collegano altri host.

Tenere presenti le seguenti linee guida:

- Se tutti gli host che si desidera connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo.
- Se si prevede di collegare host con sistemi operativi diversi allo storage array (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda alla maggior parte dei sistemi operativi degli host.

  Ad esempio, se si connettono otto host diversi all'array di storage e sei di questi host eseguono un sistema operativo Windows, è necessario selezionare Windows come tipo di sistema operativo host predefinito.

- Se la maggior parte degli host connessi dispone di diversi sistemi operativi, impostare il tipo di host su Factory Default (impostazione predefinita).

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo HP-UX, Altri tre sistemi operativi Linux sono in esecuzione, è necessario selezionare Factory Default (predefinito) come tipo di sistema operativo host predefinito.

Come fare

Modificare il nome dell'array di storage

È possibile modificare il nome dell'array di storage visualizzato nella barra del titolo di Gestore di sistema di SANtricity.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Generale**, cercare il campo **Nome:**.

   Se non è stato definito un nome di array di storage, in questo campo viene visualizzato "Sconosciuto".

3. Fare clic sull'icona **Edit** (matita) accanto al nome dell'array di storage.

   Il campo diventa modificabile.

4. Immettere un nuovo nome.

   Un nome può contenere lettere, numeri e caratteri speciali sottolineatura (_), trattino (-) e cancelletto (n.). Un nome non può contenere spazi. Un nome può avere una lunghezza massima di 30 caratteri. Il nome deve essere univoco.

5. Fare clic sull'icona **Salva** (segno di spunta).

> Se si desidera chiudere il campo modificabile senza apportare modifiche, fare clic sull'icona Annulla (X).

Risultato

Il nuovo nome viene visualizzato nella barra del titolo di Gestore di sistema di SANtricity.

Accendere le spie di localizzazione degli array di storage

Per individuare la posizione fisica di un array di storage in un cabinet, è possibile accendere i relativi indicatori LED.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **General**, fare clic su **Turn on Storage Array Locator Lights**.

   Viene visualizzata la finestra di dialogo **Turn on Storage Array Locator Lights** (attiva indicatori array di storage) e si accendono le spie di localizzazione degli array di storage corrispondenti.
3. Una volta individuato fisicamente lo storage array, tornare alla finestra di dialogo e selezionare **Spegni**.

Risultati

Le luci di individuazione si spengono e la finestra di dialogo si chiude.

Sincronizzare gli orologi degli array di storage

Se il protocollo NTP (Network Time Protocol) non è attivato, è possibile impostare manualmente gli orologi sui controller in modo che siano sincronizzati con il client di gestione (il sistema utilizzato per eseguire il browser che accede a Gestore di sistema di SANtricity).

A proposito di questa attività

La sincronizzazione garantisce che i timbri dell'ora dell'evento nel registro eventi corrispondano ai timestamp scritti nei file di registro dell'host. Durante il processo di sincronizzazione, i controller rimangono disponibili e operativi.

> Se NTP è attivato in System Manager, non utilizzare questa opzione per sincronizzare gli orologi. Al contrario, NTP sincronizza automaticamente i clock con un host esterno utilizzando SNTP (Simple Network Time Protocol).

> Dopo la sincronizzazione, si potrebbe notare che le statistiche delle performance vengono perse o inclinate, che le pianificazioni vengono influenzate (ASUP, snapshot, ecc.) e che i timestamp nei dati del registro risultano inclinati. L'utilizzo di NTP evita questo problema.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **General**, fare clic su **Synchronize Storage Array Clocks** (Sincronizza blocchi array di storage).

Viene visualizzata la finestra di dialogo **Synchronize Storage Array Blocks** (Sincronizza blocchi array di storage). Mostra la data e l'ora correnti dei controller e del computer utilizzato come client di gestione.

Per gli array di storage simplex, viene visualizzato un solo controller.

3. Se gli orari visualizzati nella finestra di dialogo non corrispondono, fare clic su **Synchronize** (Sincronizza).

Risultati

Una volta completata la sincronizzazione, i timestamp degli eventi sono gli stessi per il registro eventi e per i registri host.

Salvare la configurazione dello storage array

È possibile salvare le informazioni di configurazione di uno storage array in un file di script per risparmiare tempo durante la configurazione di storage array aggiuntivi con la stessa configurazione.

Prima di iniziare

Lo storage array non deve essere sottoposto a operazioni che modificano le impostazioni di configurazione logica. Esempi di queste operazioni includono la creazione o l'eliminazione di volumi, il download del firmware del controller, l'assegnazione o la modifica di dischi hot spare o l'aggiunta di capacità (dischi) a un gruppo di volumi.

A proposito di questa attività

Il salvataggio della configurazione dello storage array genera uno script CLI (Command Line Interface) che contiene le impostazioni dello storage array, la configurazione del volume, la configurazione dell'host o le assegnazioni host-to-volume per uno storage array. È possibile utilizzare questo script CLI generato per replicare una configurazione in un altro array di storage con la stessa configurazione hardware.

Tuttavia, non si consiglia di utilizzare questo script CLI generato per il disaster recovery. Invece, per eseguire un ripristino del sistema, utilizzare il file di backup del database di configurazione creato manualmente o contattare il supporto tecnico per ottenere questi dati dai dati di supporto automatico più recenti.

Questa operazione *non* salva queste impostazioni:

- La durata della batteria
- L'ora del giorno del controller
- Le impostazioni della memoria ad accesso casuale statica non volatile (NVSRAM)
- Qualsiasi funzionalità premium
- La password dello storage array
- Lo stato operativo e gli stati dei componenti hardware
- Lo stato operativo (eccetto ottimale) e gli stati dei gruppi di volumi
- Servizi di copia, come il mirroring e la copia del volume

Rischio di errori dell'applicazione — non utilizzare questa opzione se lo storage array sta eseguendo un'operazione che modificherà qualsiasi impostazione di configurazione logica. Esempi di queste operazioni includono la creazione o l'eliminazione di volumi, il download del firmware del controller, l'assegnazione o la modifica di dischi hot spare o l'aggiunta di capacità (dischi) a un gruppo di volumi.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Save Storage Array Configuration** (Salva configurazione array di storage).
3. Selezionare gli elementi della configurazione che si desidera salvare:
   - **Impostazioni array di storage**
   - **Configurazione del volume**
   - **Configurazione host**
   - **Assegnazioni host-to-volume**

   > Se si seleziona la voce **host-to-volume assignments**, per impostazione predefinita vengono selezionate anche la voce **Volume Configuration** (Configurazione volume) e la voce **host Configuration** (Configurazione host). Non è possibile salvare **assegnazioni host-to-volume** senza salvare anche **Configurazione volume** e **Configurazione host**.

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

   Il file viene salvato nella cartella Download del browser con il nome `storage-array-configuration.cfg`.

Al termine

Per caricare una configurazione di array di storage in un altro array di storage, utilizzare Gestione unificata di SANtricity.

Configurazione chiara degli array di storage

Utilizzare l'operazione Clear Configuration (Cancella configurazione) per eliminare tutti i pool, i gruppi di volumi, i volumi, le definizioni degli host e le assegnazioni degli host dall'array di storage.

Prima di iniziare

- Prima di cancellare la configurazione dello storage array, eseguire il backup dei dati.

A proposito di questa attività

Sono disponibili due opzioni di configurazione Clear Storage Array:

- **Volume** — in genere, è possibile utilizzare l'opzione Volume per riconfigurare un array di storage di test come array di storage di produzione. Ad esempio, è possibile configurare un array di storage per il test e, al termine del test, rimuovere la configurazione di test e configurare l'array di storage per un ambiente di produzione.
- **Storage Array** - in genere, è possibile utilizzare l'opzione Storage Array per spostare uno storage array in un altro reparto o gruppo. Ad esempio, è possibile utilizzare uno storage array in Engineering e ora Engineering sta ottenendo un nuovo storage array, quindi si desidera spostare lo storage array corrente in Administration, dove verrà riconfigurato.

  L'opzione Storage Array elimina alcune impostazioni aggiuntive.

	Volume	Array di storage
Elimina pool e gruppi di volumi	X	X
Elimina i volumi	X	X
Elimina host e cluster di host	X	X
Elimina le assegnazioni degli host	X	X
Elimina il nome dell'array di storage		X
Ripristina le impostazioni predefinite della cache dell'array di storage		X

Rischio di perdita di dati — questa operazione elimina tutti i dati dall'array di storage. (Non esegue una cancellazione sicura). Non è possibile annullare questa operazione dopo l'avvio. Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Clear Storage Array Configuration** (Cancella configurazione array di storage).
3. Nell'elenco a discesa, selezionare **Volume** o **Storage Array**.
4. **Opzionale**: Se si desidera salvare la configurazione (non i dati), utilizzare i collegamenti nella finestra di dialogo.
5. Confermare che si desidera eseguire l'operazione.

Risultati

- La configurazione corrente viene eliminata, distruggendo tutti i dati esistenti sull'array di storage.
- Tutti i dischi non sono assegnati.

Configurare il banner di accesso

È possibile creare un banner di accesso che viene presentato agli utenti prima di stabilire le sessioni in Gestore di sistema di SANtricity. Il banner può includere un avviso e un messaggio di consenso.

A proposito di questa attività

Quando si crea un banner, questo viene visualizzato prima della schermata di accesso in una finestra di dialogo.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Nella sezione **Generale**, selezionare **Configura banner di accesso**.

Viene visualizzata la finestra di dialogo **Configura banner di accesso**.

3. Inserire il testo che si desidera visualizzare nel banner di accesso.

   Non utilizzare tag HTML o altri tag di markup per la formattazione.

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

Risultato

La volta successiva che gli utenti accedono a System Manager, il testo viene visualizzato in una finestra di dialogo. Gli utenti devono fare clic su **OK** per passare alla schermata di accesso.

Gestire i timeout delle sessioni

È possibile configurare i timeout in Gestore di sistema di SANtricity, in modo che le sessioni inattive degli utenti vengano disconnesse dopo un determinato periodo di tempo.

A proposito di questa attività

Per impostazione predefinita, il timeout della sessione per System Manager è di 30 minuti. È possibile regolare l'orario oppure disattivare completamente i timeout della sessione.

Se Access Management viene configurato utilizzando le funzionalità SAML (Security Assertion Markup Language) incorporate nell'array, potrebbe verificarsi un timeout di sessione quando la sessione SSO dell'utente raggiunge il limite massimo. Questo potrebbe verificarsi prima del timeout della sessione di System Manager.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Nella sezione **Generale**, selezionare **attiva/Disattiva timeout sessione**.

   Viene visualizzata la finestra di dialogo **Enable/Disable Session Timeout** (attiva/Disattiva timeout sessione).

3. Utilizzare i comandi per aumentare o diminuire il tempo in minuti.

   Il timeout minimo che è possibile impostare per System Manager è di 15 minuti.

   Per disattivare i timeout della sessione, deselezionare la casella di controllo **Imposta la durata…**.

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

Modificare le impostazioni della cache per lo storage array

Per tutti i volumi nell'array di storage, è possibile regolare le impostazioni della memoria cache per lo spurgo e le dimensioni dei blocchi.

A proposito di questa attività

La memoria cache è un'area di storage volatile temporaneo sul controller, che ha un tempo di accesso più rapido rispetto ai supporti del disco. Per ottimizzare le prestazioni della cache, è possibile regolare le seguenti impostazioni:

Impostazione della cache	Descrizione
Avvia il vampate di cache a richiesta	Start demand cache wlushing specifica la percentuale di dati non scritti nella cache che attiva un write-on della cache (scrittura su disco). Per impostazione predefinita, il vampate della cache viene avviato quando i dati non scritti raggiungono il 80% della capacità. Una percentuale più elevata è una buona scelta per gli ambienti con operazioni principalmente di scrittura, in modo che le nuove richieste di scrittura possano essere elaborate dalla cache senza dover accedere al disco. Le impostazioni più basse sono migliori in ambienti in cui l'i/o è irregolare (con burst di dati), in modo che il sistema scarichi frequentemente la cache tra burst di dati. Tuttavia, una percentuale iniziale inferiore al 80% può causare una riduzione delle performance.
Dimensione del blocco della cache	La dimensione del blocco della cache determina la dimensione massima di ciascun blocco della cache, che è un'unità organizzativa per la gestione della cache. Per impostazione predefinita, la dimensione del blocco è 8 KiB. System Manager consente di impostare la dimensione del blocco della cache su 4, 8, 16 o 32 KiB. Le applicazioni utilizzano blocchi di dimensioni diverse, che hanno un impatto sulle performance dello storage. Una dimensione inferiore è una buona scelta per file system o applicazioni di database. Una dimensione maggiore è ideale per le applicazioni che generano i/o sequenziale, come ad esempio i contenuti multimediali.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change cache Settings** (Modifica impostazioni cache).

   Viene visualizzata la finestra di dialogo Change cache Settings (Modifica impostazioni cache).

3. Regolare i seguenti valori:
   - Avvia il vampare della cache a richiesta — Scegli una percentuale appropriata per l'i/o utilizzato nel tuo ambiente. Se si sceglie un valore inferiore al 80%, si potrebbe notare una riduzione delle performance.
   - Cache block size (dimensione blocco cache) — scegliere una dimensione appropriata per le applicazioni.
4. Fare clic su **Save** (Salva).

Impostare il reporting sulla connettività host

È possibile attivare il reporting della connettività host in modo che lo storage array monitoraggi continuamente la connessione tra i controller e gli host configurati, quindi

avvisa l'utente in caso di interruzione della connessione. Questa funzione è attivata per impostazione predefinita.

A proposito di questa attività

Se si disattiva il reporting sulla connettività host, il sistema non monitora più i problemi di connettività o di driver multipath con un host collegato allo storage array.

> La disattivazione del reporting sulla connettività host disattiva anche il bilanciamento automatico del carico, che monitora e bilancia l'utilizzo delle risorse del controller.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Enable/Disable host Connectivity Reporting** (attiva/Disattiva report connettività host).

   Il testo sotto questa opzione indica se è attivata o disattivata.

   Viene visualizzata una finestra di dialogo di conferma.
3. Fare clic su **Sì** per continuare.

   Selezionando questa opzione, è possibile attivare o disattivare la funzione.

Impostare il bilanciamento automatico del carico

La funzione **Automatic Load Balancing** garantisce che il traffico i/o in entrata dagli host sia gestito e bilanciato dinamicamente tra entrambi i controller. Questa funzione è attivata per impostazione predefinita, ma è possibile disattivarla da System Manager.

A proposito di questa attività

Quando il bilanciamento automatico del carico è attivato, esegue le seguenti funzioni:

- Monitora e bilancia automaticamente l'utilizzo delle risorse dei controller.
- Regola automaticamente la proprietà del controller del volume quando necessario, ottimizzando in tal modo la larghezza di banda i/o tra gli host e lo storage array.

È possibile disattivare il bilanciamento automatico del carico sull'array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un determinato volume per bilanciare il carico di lavoro.
- Si opera in un ambiente altamente ottimizzato in cui la distribuzione del carico è appositamente configurata per ottenere una distribuzione specifica tra i controller.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Enable/Disable Automatic Load Balancing** (attiva/Disattiva bilanciamento automatico del carico).

   Il testo sotto questa opzione indica se la funzione è attualmente attivata o disattivata.

Viene visualizzata una finestra di dialogo di conferma.

3. Confermare facendo clic su **Sì** per continuare.

   Selezionando questa opzione, è possibile attivare o disattivare la funzione.

   > Se questa funzione viene spostata da Disabled (disattivata) a Enabled (attivata), viene attivata automaticamente anche la funzione di reporting della connettività host.

Modificare il tipo di host predefinito

Utilizzare l'impostazione Change Default host Operating System (Modifica sistema operativo host predefinito) per modificare il tipo di host predefinito a livello di array di storage. In genere, è necessario modificare il tipo di host predefinito prima di connettere gli host all'array di storage o quando si collegano altri host.

A proposito di questa attività

Tenere presenti le seguenti linee guida:

- Se tutti gli host che si desidera connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo.
- Se si prevede di collegare host con sistemi operativi diversi allo storage array (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda alla maggior parte dei sistemi operativi degli host.

  Ad esempio, se si connettono otto host diversi all'array di storage e sei di questi host eseguono un sistema operativo Windows, è necessario selezionare Windows come tipo di sistema operativo host predefinito.

- Se la maggior parte degli host connessi dispone di diversi sistemi operativi, impostare il tipo di host su Factory Default (impostazione predefinita).

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo HP-UX, Altri tre sistemi operativi Linux sono in esecuzione, è necessario selezionare Factory Default (predefinito) come tipo di sistema operativo host predefinito.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change Default host Operating System Type** (Modifica tipo di sistema operativo host predefinito).
3. Selezionare il tipo di sistema operativo host che si desidera utilizzare come predefinito.
4. Fare clic su **Cambia**.

Attivare o disattivare l'interfaccia di gestione legacy

È possibile attivare o disattivare l'interfaccia di gestione legacy (Symbol), un metodo di comunicazione tra lo storage array e il client di gestione. Per impostazione predefinita, l'interfaccia di gestione legacy è attiva. Se la si disattiva, l'array di storage e il client di gestione utilizzeranno un metodo di comunicazione più sicuro (API REST su https); tuttavia, alcuni strumenti e attività potrebbero risentirne se la funzione è disattivata.

A proposito di questa attività

L'impostazione influisce sulle operazioni come segue:

- **On** (impostazione predefinita) — impostazione richiesta per il mirroring, per i comandi CLI che funzionano solo sugli storage array E5700 e E5600 e alcuni altri strumenti come l'utility QuickConnect e l'adattatore OCI.
- **Off** — impostazione richiesta per applicare la riservatezza nelle comunicazioni tra lo storage array e il client di gestione e per accedere a strumenti esterni. Impostazione consigliata per la configurazione di un server di directory (LDAP).

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Change Management Interface** (interfaccia di gestione delle modifiche).
3. Nella finestra di dialogo, fare clic su **Sì** per continuare.

FAQ

Che cos'è la cache del controller?

La cache del controller è uno spazio di memoria fisica che ottimizza due tipi di operazioni di i/o (input/output): Tra controller e host e tra controller e dischi.

Per i trasferimenti di dati in lettura e scrittura, gli host e i controller comunicano tramite connessioni ad alta velocità. Tuttavia, le comunicazioni dal back-end del controller ai dischi sono più lente, perché i dischi sono dispositivi relativamente lenti.

Quando la cache del controller riceve i dati, il controller riconosce alle applicazioni host che i dati sono ora memorizzati. In questo modo, le applicazioni host non devono attendere che l'i/o venga scritto su disco. Le applicazioni possono invece continuare a lavorare. I dati memorizzati nella cache sono facilmente accessibili anche dalle applicazioni server, eliminando la necessità di letture aggiuntive del disco per accedere ai dati.

La cache del controller influisce sulle prestazioni complessive dello storage array in diversi modi:

- La cache funge da buffer, in modo che i trasferimenti di dati su host e disco non debbano essere sincronizzati.
- I dati per un'operazione di lettura o scrittura dall'host potrebbero trovarsi nella cache di un'operazione precedente, eliminando così la necessità di accedere al disco.
- Se viene utilizzato il caching in scrittura, l'host può inviare comandi di scrittura successivi prima che i dati di un'operazione di scrittura precedente vengano scritti su disco.
- Se il prefetch della cache è attivato, l'accesso in lettura sequenziale è ottimizzato. Il prefetch della cache rende più probabile che un'operazione di lettura trovi i propri dati nella cache, invece di leggere i dati dal disco.

Possibile perdita di dati — se si attiva l'opzione **Write caching without batteries** 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**.

Cos'è il vampate di cache?

Quando la quantità di dati non scritti nella cache raggiunge un determinato livello, il controller scrive periodicamente i dati memorizzati nella cache su un disco. Questo processo di scrittura è chiamato "vampate".

Il controller utilizza due algoritmi per il flushing della cache: Basato sulla domanda e basato sull'età. Il controller utilizza un algoritmo basato sulla domanda fino a quando la quantità di dati memorizzati nella cache non scende al di sotto della soglia di scaricamento della cache. Per impostazione predefinita, un'operazione di svuotamento inizia quando il 80% della cache è in uso.

In System Manager, è possibile impostare la soglia "Start demand cache flushing" per supportare al meglio il tipo di i/o utilizzato nell'ambiente. In un ambiente che è principalmente operazioni di scrittura, è necessario impostare la percentuale "Start demand cache wlushing" alta per aumentare la probabilità che qualsiasi nuova richiesta di scrittura possa essere elaborata dalla cache senza dover passare al disco. Un'impostazione di percentuale elevata limita il numero di lavaggi della cache in modo che nella cache rimanga più dati, aumentando così la possibilità di più accessi alla cache.

In un ambiente in cui l'i/o è irregolare (con burst di dati), è possibile utilizzare un basso flushing della cache in modo che il sistema scarichi frequentemente la cache tra burst di dati. In un ambiente i/o diverso che elabora una varietà di carichi, o quando il tipo di carichi non è noto, impostare la soglia al 50% come una buona base intermedia. Tenere presente che se si sceglie una percentuale iniziale inferiore al 80%, le prestazioni potrebbero essere ridotte perché i dati necessari per una lettura host potrebbero non essere disponibili. La scelta di una percentuale inferiore aumenta anche il numero di scritture su disco necessarie per mantenere il livello di cache, aumentando così l'overhead del sistema.

L'algoritmo basato sull'età specifica il periodo di tempo durante il quale i dati di scrittura possono rimanere nella cache prima che possano essere trasferiti sui dischi. I controller utilizzano l'algoritmo basato sull'età fino al raggiungimento della soglia di scaricamento della cache. L'impostazione predefinita è 10 secondi, ma questo periodo di tempo viene conteggiato solo durante i periodi di inattività. Non è possibile modificare i tempi di scaricamento in System Manager; è invece necessario utilizzare il comando Set Storage Array nell'interfaccia della riga di comando (CLI).

Possibile perdita di dati — se si attiva l'opzione **Write caching without batteries** 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**.

Che cos'è la dimensione del blocco della cache?

Il controller dell'array di storage organizza la cache in "blocchi", ovvero blocchi di memoria che possono essere di 4, 8, 16 o 32 KiB. Tutti i volumi sul sistema storage condividono lo stesso spazio cache; pertanto, i volumi possono avere una sola dimensione del blocco cache.

I blocchi della cache non corrispondono ai blocchi da 512 byte utilizzati dal sistema a blocchi logici dei dischi.

Le applicazioni utilizzano blocchi di dimensioni diverse, che possono avere un impatto sulle performance dello storage. Per impostazione predefinita, la dimensione del blocco in System Manager è 8 KiB, ma è possibile impostare il valore su 4, 8, 16 o 32 KiB. Una dimensione inferiore è una buona scelta per file system o applicazioni di database. Una dimensione maggiore è una buona scelta per le applicazioni che richiedono un

grande trasferimento di dati, l'i/o sequenziale o un'elevata larghezza di banda, come ad esempio le applicazioni multimediali.

Quando è necessario sincronizzare gli orologi degli array di storage?

È necessario sincronizzare manualmente gli orologi del controller nell'array di storage se si nota che gli indicatori di data e ora visualizzati in System Manager non sono allineati con quelli visualizzati nel client di gestione (il computer che accede a System Manager tramite il browser). Questa attività è necessaria solo se NTP (Network Time Protocol) non è attivato in System Manager.

> Si consiglia vivamente di utilizzare un server NTP invece di sincronizzare manualmente gli orologi. NTP sincronizza automaticamente gli orologi con un server esterno utilizzando SNTP (Simple Network Time Protocol).

È possibile controllare lo stato della sincronizzazione dalla finestra di dialogo **Synchronize Storage Array Blocks**, disponibile nella pagina System (sistema). Se gli orari visualizzati nella finestra di dialogo non corrispondono, eseguire una sincronizzazione. È possibile visualizzare periodicamente questa finestra di dialogo, che indica se le visualizzazioni dell'ora dei clock del controller sono state separate e non sono più sincronizzate.

Che cos'è il reporting sulla connettività host?

Quando il reporting sulla connettività host è attivato, lo storage array monitora continuamente la connessione tra i controller e gli host configurati, quindi avvisa l'utente in caso di interruzione della connessione.

In caso di cavi allentati, danneggiati o mancanti o di altri problemi con l'host, potrebbero verificarsi interruzioni della connessione. In queste situazioni, il sistema potrebbe aprire un messaggio Recovery Guru:

- **Host Redundancy Lost** — si apre se uno dei controller non riesce a comunicare con l'host.
- **Host Type Incorrect (tipo host errato)** — si apre se il tipo di host non è specificato correttamente nell'array di storage, con conseguenti problemi di failover.

È possibile disattivare la funzione di reporting della connettività host in situazioni in cui il riavvio di un controller potrebbe richiedere più tempo del timeout di connessione. La disattivazione di questa funzione elimina i messaggi Recovery Gurus.

> La disattivazione del reporting sulla connettività host disattiva anche il bilanciamento automatico del carico, che monitora e bilancia l'utilizzo delle risorse del controller. Tuttavia, se si riattiva il reporting sulla connettività host, la funzione di bilanciamento automatico del carico non viene riattivata automaticamente.

Impostazioni iSCSI

Concetti

Terminologia iSCSI

Scopri in che modo i termini iSCSI si applicano al tuo storage array.

Termine	Descrizione
CAP	Il metodo CHAP (Challenge Handshake Authentication Protocol) convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa denominata CHAP*secret*.
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di System Manager.
DHCP	Il protocollo DHCP (Dynamic host Configuration Protocol) è un protocollo utilizzato sulle reti IP (Internet Protocol) per la distribuzione dinamica dei parametri di configurazione della rete, ad esempio gli indirizzi IP.
IB	InfiniBand (IB) è uno standard di comunicazione per la trasmissione dei dati tra server e sistemi storage dalle performance elevate.
Risposta PING ICMP	ICMP (Internet Control message Protocol) è un protocollo utilizzato dai sistemi operativi dei computer collegati in rete per inviare messaggi. I messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.
IQN	Un identificatore IQN (iSCSI Qualified Name) è un nome univoco per un iSCSI Initiator o una destinazione iSCSI.
Er	ISER (iSCSI Extensions for RDMA) è un protocollo che estende il protocollo iSCSI per il funzionamento sui trasporti RDMA, come InfiniBand o Ethernet.
ISNS	Internet Storage Name Service (iSNS) è un protocollo che consente il rilevamento, la gestione e la configurazione automatici dei dispositivi iSCSI e Fibre Channel sulle reti TCP/IP.
Indirizzo MAC	Gli identificatori di controllo dell'accesso ai supporti (indirizzi MAC) vengono utilizzati da Ethernet per distinguere tra canali logici separati che collegano due porte sulla stessa interfaccia di rete di trasporto fisica.
Client di gestione	Un client di gestione è il computer in cui è installato un browser per accedere a System Manager.
MTU	Una MTU (Maximum Transmission Unit) è il pacchetto o frame di dimensioni maggiori che può essere inviato in una rete.
RDMA	RDMA (Remote Direct Memory Access) è una tecnologia che consente ai computer di rete di scambiare dati nella memoria principale senza coinvolgere il sistema operativo di entrambi i computer.
Sessione di rilevamento senza nome	Quando l'opzione per le sessioni di rilevamento senza nome è attivata, gli iniziatori iSCSI non devono specificare l'IQN di destinazione per recuperare le informazioni del controller.

Come fare

Configurare le porte iSCSI

Se il controller include una connessione host iSCSI, è possibile configurare le impostazioni della porta iSCSI dalla pagina hardware o dalla pagina sistema.

Prima di iniziare

- Il controller deve includere porte iSCSI; in caso contrario, le impostazioni iSCSI non sono disponibili.
- È necessario conoscere la velocità di rete (la velocità di trasferimento dei dati tra le porte e l'host).

A proposito di questa attività

Questa attività descrive come accedere alla configurazione della porta iSCSI dalla pagina hardware. È inoltre possibile accedere alla configurazione dalla pagina System (sistema) (**Impostazioni › sistema**).

> Le impostazioni e le funzioni iSCSI vengono visualizzate solo se lo storage array supporta iSCSI.

Fasi

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

   Il grafico cambia per mostrare i controller invece dei dischi.
3. Fare clic sul controller con le porte iSCSI che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.
4. Selezionare **Configure iSCSI ports** (Configura porte iSCSI).

   > L'opzione **Configure iSCSI ports** (Configura porte iSCSI) viene visualizzata solo se System Manager rileva le porte iSCSI sul controller.

   Viene visualizzata la finestra di dialogo Configure iSCSI Ports (Configura porte iSCSI).
5. Nell'elenco a discesa, selezionare la porta che si desidera configurare, quindi fare clic su **Avanti**.
6. Selezionare le impostazioni della porta di configurazione, quindi fare clic su **Avanti**.

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

Dettagli campo

Impostazione della porta	Descrizione
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. NOTA: Se si desidera disattivare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
TCP listening port (porta di ascolto TCP) (disponibile facendo clic su Show More port settings (Mostra altre impostazioni porta).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile facendo clic su Mostra altre impostazioni della porta).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

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

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

Dettagli campo

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router.
Abilitare il supporto VLAN (disponibile facendo clic su Mostra altre impostazioni).	Selezionare questa opzione per attivare una VLAN e inserire il relativo ID. Una VLAN è una rete logica che si comporta come se fosse fisicamente separata da altre LAN (Local Area Network) fisiche e virtuali supportate dagli stessi switch, dagli stessi router o da entrambi.
Abilitare la priorità ethernet (disponibile facendo clic su Mostra altre impostazioni).	Selezionare questa opzione per attivare il parametro che determina la priorità di accesso alla rete. Utilizzare il dispositivo di scorrimento per selezionare una priorità compresa tra 1 (più bassa) e 7 (più alta). In un ambiente LAN (Local Area Network) condiviso, ad esempio Ethernet, molte stazioni potrebbero entrare in contatto per l'accesso alla rete. L'accesso avviene in base all'ordine di arrivo e all'ordine di arrivo. Due stazioni potrebbero tentare di accedere alla rete contemporaneamente, causando la disattivazione di entrambe le stazioni e l'attesa prima di riprovare. Questo processo è ridotto al minimo per Ethernet commutata, in cui una sola stazione è collegata a una porta dello switch.

8. Fare clic su **fine**.

Configurare l'autenticazione iSCSI

Per una maggiore sicurezza in una rete iSCSI, è possibile impostare l'autenticazione tra controller (destinazioni) e host (iniziatori). System Manager utilizza il metodo Challenge Handshake Authentication Protocol (CHAP), che convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa denominata CHAP*secret*.

Prima di iniziare

È possibile impostare il segreto CHAP per gli iniziatori (host iSCSI) prima o dopo aver impostato il segreto CHAP per le destinazioni (controller). Prima di seguire le istruzioni di questa attività, è necessario attendere che gli host abbiano stabilito prima una connessione iSCSI, quindi impostare il segreto CHAP sui singoli host. Una volta effettuate le connessioni, i nomi IQN degli host e i relativi segreti CHAP vengono elencati nella finestra di dialogo per l'autenticazione iSCSI (descritta in questa attività) e non è necessario immetterli manualmente.

A proposito di questa attività

È possibile selezionare uno dei seguenti metodi di autenticazione:

- **Autenticazione unidirezionale** — utilizzare questa impostazione per consentire al controller di autenticare l'identità degli host iSCSI (autenticazione unidirezionale).
- **Autenticazione bidirezionale** — utilizzare questa impostazione per consentire al controller e agli host iSCSI di eseguire l'autenticazione (autenticazione bidirezionale). Questa impostazione fornisce un secondo livello di sicurezza consentendo al controller di autenticare l'identità degli host iSCSI e, a sua volta, agli host iSCSI di autenticare l'identità del controller.

Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Settings (Impostazioni) solo se lo storage array supporta iSCSI.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **iSCSI settings**, fare clic su **Configure Authentication** (Configura autenticazione).

   Viene visualizzata la finestra di dialogo Configure Authentication (Configura autenticazione), che mostra il metodo attualmente impostato. Inoltre, indica se alcuni host hanno configurato segreti CHAP.

3. Selezionare una delle seguenti opzioni:
   - **Nessuna autenticazione** — se non si desidera che il controller autentichi l'identità degli host iSCSI, selezionare questa opzione e fare clic su **fine**. La finestra di dialogo si chiude e la configurazione è terminata.
   - **Autenticazione unidirezionale** — per consentire al controller di autenticare l'identità degli host iSCSI, selezionare questa opzione e fare clic su **Avanti** per visualizzare la finestra di dialogo Configura CHAP di destinazione.
   - **Autenticazione bidirezionale** — per consentire sia al controller che agli host iSCSI di eseguire l'autenticazione, selezionare questa opzione e fare clic su **Avanti** per visualizzare la finestra di dialogo Configura CHAP di destinazione.
4. Per l'autenticazione unidirezionale o bidirezionale, immettere o confermare il segreto CHAP per il controller (la destinazione). Il segreto CHAP deve essere compreso tra 12 e 57 caratteri ASCII stampabili.

   Se il segreto CHAP per il controller è stato configurato in precedenza, i caratteri nel campo vengono mascherati. Se necessario, è possibile sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

5. Effettuare una delle seguenti operazioni:
   - Se si sta configurando l'autenticazione *unidirezionale*, fare clic su **fine**. La finestra di dialogo si chiude e la configurazione è terminata.
   - Se si sta configurando l'autenticazione *bidirezionale*, fare clic su **Avanti** per visualizzare la finestra di dialogo Configure Initiator CHAP.

6. Per l'autenticazione bidirezionale, immettere o confermare un segreto CHAP per uno qualsiasi degli host iSCSI (gli iniziatori), che può essere compreso tra 12 e 57 caratteri ASCII stampabili. Se non si desidera configurare l'autenticazione bidirezionale per un determinato host, lasciare vuoto il campo **Initiator CHAP Secret**.

> Se il segreto CHAP per un host è stato configurato in precedenza, i caratteri nel campo vengono mascherati. Se necessario, è possibile sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

7. Fare clic su **fine**.

Risultato

L'autenticazione avviene durante la sequenza di login iSCSI tra i controller e gli host iSCSI, a meno che non sia stata specificata alcuna autenticazione.

Abilitare le impostazioni di rilevamento iSCSI

È possibile attivare le impostazioni relative al rilevamento dei dispositivi di storage in una rete iSCSI. Le impostazioni di rilevamento di destinazione consentono di registrare le informazioni iSCSI dell'array di storage utilizzando il protocollo iSNS (Internet Storage Name Service) e di determinare se consentire sessioni di rilevamento senza nome

Prima di iniziare

Se il server iSNS utilizza un indirizzo IP statico, tale indirizzo deve essere disponibile per la registrazione iSNS. Sono supportati sia IPv4 che IPv6.

A proposito di questa attività

È possibile attivare le seguenti impostazioni relative al rilevamento iSCSI:

- **Abilitare il server iSNS per registrare una destinazione** — quando abilitato, lo storage array registra il proprio iSCSI Qualified Name (IQN) e le informazioni sulle porte dal server iSNS. Questa impostazione consente il rilevamento iSNS, in modo che un iniziatore possa recuperare le informazioni IQN e sulla porta dal server iSNS.
- **Enable unnamed Discovery sessions** (attiva sessioni di rilevamento senza nome) — quando sono attivate sessioni di rilevamento senza nome, l'iniziatore (host iSCSI) non deve fornire l'IQN del controller di destinazione durante la sequenza di accesso per una connessione di tipo Discovery. Se disattivati, gli host devono fornire l'IQN per stabilire una sessione di rilevamento per il controller. Tuttavia, l'IQN di destinazione è sempre richiesto per una sessione normale (i/o Bearing). La disattivazione di questa impostazione può impedire agli host iSCSI non autorizzati di connettersi al controller utilizzando solo il relativo indirizzo IP.

> Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Settings (Impostazioni) solo se lo storage array supporta iSCSI.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **iSCSI settings** (Impostazioni iSCSI), fare clic su **View/Edit Target Discovery Settings** (Visualizza/Modifica impostazioni rilevamento destinazione).

   Viene visualizzata la finestra di dialogo **Target Discovery Settings** (Impostazioni rilevamento destinazione). Sotto il campo Enable iSNS server… (attiva server iSNS) la finestra di dialogo indica se il

controller è già registrato.

3. Per registrare il controller, selezionare **Enable iSNS server to register my target**, quindi selezionare una delle seguenti opzioni:
   - **Ottieni automaticamente la configurazione dal server DHCP** — selezionare questa opzione se si desidera configurare il server iSNS utilizzando un server DHCP (Dynamic host Configuration Protocol). Tenere presente che se si utilizza questa opzione, tutte le porte iSCSI del controller devono essere configurate per utilizzare anche DHCP. Se necessario, aggiornare le impostazioni della porta iSCSI del controller per attivare questa opzione.

     Affinché il server DHCP fornisca l'indirizzo del server iSNS, è necessario configurare il server DHCP in modo che utilizzi l'opzione 43 — "informazioni specifiche del fornitore". Questa opzione deve contenere l'indirizzo IPv4 del server iSNS nei byte di dati 0xa-0xd (10-13).

   - **Specificare manualmente la configurazione statica** — selezionare questa opzione se si desidera inserire un indirizzo IP statico per il server iSNS. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Nel campo, immettere un indirizzo IPv4 o IPv6. Se sono stati configurati entrambi, IPv4 è l'impostazione predefinita. Immettere anche una porta TCP in attesa (utilizzare il valore predefinito 3205 o immettere un valore compreso tra 49152 e 65535).
4. Per consentire allo storage array di partecipare a sessioni di rilevamento senza nome, selezionare **Enable unnamed Discovery sessions** (attiva sessioni di rilevamento senza nome).
   - Se attivato, gli iniziatori iSCSI non devono specificare l'IQN di destinazione per recuperare le informazioni del controller.
   - Se disattivata, le sessioni di rilevamento vengono impedite a meno che l'iniziatore non fornisca l'IQN di destinazione. La disattivazione delle sessioni di rilevamento senza nome offre una maggiore sicurezza.
5. Fare clic su **Save** (Salva).

Risultato

Quando System Manager tenta di registrare il controller con il server iSNS, viene visualizzata una barra di avanzamento. Questo processo potrebbe richiedere fino a cinque minuti.

Visualizzare i pacchetti di statistiche iSCSI

È possibile visualizzare i dati relativi alle connessioni iSCSI allo storage array.

A proposito di questa attività

System Manager mostra questi tipi di statistiche iSCSI. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Ethernet MAC statistics** — fornisce statistiche per il controllo dell'accesso ai supporti (MAC). MAC fornisce anche un meccanismo di indirizzamento chiamato indirizzo fisico o indirizzo MAC. L'indirizzo MAC è un indirizzo univoco assegnato a ciascun adattatore di rete. L'indirizzo MAC consente di inviare pacchetti di dati a una destinazione all'interno della sottorete.
- **Ethernet TCP/IP statistics** — fornisce le statistiche per TCP/IP, ovvero il protocollo TCP (Transmission Control Protocol) e il protocollo Internet (IP) per il dispositivo iSCSI. Con TCP, le applicazioni sugli host collegati in rete possono creare connessioni tra loro, attraverso le quali possono scambiare dati in pacchetti. L'IP è un protocollo orientato ai dati che comunica i dati attraverso una rete interconnessa a commutazione di pacchetto. Le statistiche IPv4 e IPv6 vengono visualizzate separatamente.
- **Statistiche Local Target/Initiator (protocollo)** — Mostra le statistiche per la destinazione iSCSI, che

fornisce l'accesso a livello di blocco ai relativi supporti di storage, e mostra le statistiche iSCSI per lo storage array quando viene utilizzato come iniziatore nelle operazioni di mirroring asincrono.

- **DCBX Statistiche degli stati operativi** — Visualizza gli stati operativi delle varie funzioni Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistics** — Visualizza le statistiche LLDP (link Layer Discovery Protocol) Type Length Value (TLV).
- **DCBX TLV statistics** — Visualizza le informazioni che identificano le porte host degli array di storage in un ambiente Data Center Bridging (DCB). Queste informazioni vengono condivise con i peer di rete per scopi di identificazione e funzionalità.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **View iSCSI Statistics Packages** (Visualizza pacchetti di statistiche iSCSI).
3. Fare clic su una scheda per visualizzare i diversi set di statistiche.
4. Per impostare la linea di base, fare clic su **Set new baseline** (Imposta nuova linea di base).

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. Per tutte le statistiche iSCSI viene utilizzata la stessa linea di base.

Terminare la sessione iSCSI

È possibile terminare una sessione iSCSI che non è più necessaria. Le sessioni iSCSI possono essere eseguite con host o array di storage remoti in una relazione di mirroring asincrona.

A proposito di questa attività

È possibile terminare una sessione iSCSI per i seguenti motivi:

- **Accesso non autorizzato** — se un iSCSI Initiator è connesso e non deve avere accesso, è possibile terminare la sessione iSCSI per forzare iSCSI Initiator a disconnettersi dallo storage array. L'iSCSI Initiator potrebbe aver eseguito l'accesso perché era disponibile il metodo di autenticazione None.
- **Downtime del sistema** — se è necessario rimuovere un array di storage e si nota che gli iniziatori iSCSI sono ancora connessi, è possibile terminare le sessioni iSCSI per estrarre gli iniziatori iSCSI dall'array di storage.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).

   Viene visualizzato un elenco delle sessioni iSCSI correnti.

3. Selezionare la sessione che si desidera terminare
4. Fare clic su **End Session** (fine sessione) e confermare che si desidera eseguire l'operazione.

Visualizzare le sessioni iSCSI

È possibile visualizzare informazioni dettagliate sulle connessioni iSCSI allo storage array. Le sessioni iSCSI possono essere eseguite con host o array di storage remoti in una relazione di mirroring asincrona.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).

   Viene visualizzato un elenco delle sessioni iSCSI correnti.

3. Per visualizzare ulteriori informazioni su una sessione iSCSI specifica, selezionare una sessione, quindi fare clic su **View Details** (Visualizza dettagli).

Dettagli campo

Elemento	Descrizione
SSID (Session Identifier)	Stringa esadecimale che identifica una sessione tra un iSCSI Initiator e una destinazione iSCSI. L'SSID è composto dall'ISID e dal TPGT.
ID sessione iniziatore (ISID)	Parte iniziatore dell'identificatore di sessione. L'iniziatore specifica l'ISID durante l'accesso.
Gruppo di portali di destinazione	La destinazione iSCSI.
Tag del gruppo di portali di destinazione (TPGT)	La parte di destinazione dell'identificatore di sessione. Identificatore numerico a 16 bit per un gruppo di portali di destinazione iSCSI.
Nome iSCSI iniziatore	Il nome univoco mondiale dell'iniziatore.
Etichetta iSCSI iniziatore	L'etichetta utente impostata in System Manager.
Alias iSCSI iniziatore	Un nome che può essere associato anche a un nodo iSCSI. L'alias consente a un'organizzazione di associare una stringa intuitiva al nome iSCSI. Tuttavia, l'alias non sostituisce il nome iSCSI. L'alias iSCSI iniziatore può essere impostato solo sull'host, non in System Manager
Host	Server che invia input e output allo storage array.
ID connessione (CID)	Un nome univoco per una connessione all'interno della sessione tra l'iniziatore e la destinazione. L'iniziatore genera questo ID e lo presenta alla destinazione durante le richieste di accesso. L'ID di connessione viene visualizzato anche durante le disconnessioni che chiudono le connessioni.
Identificatore della porta Ethernet	La porta del controller associata alla connessione.
Indirizzo IP iniziatore	L'indirizzo IP dell'iniziatore.
Parametri di accesso negoziati	I parametri che vengono transatti durante l'accesso alla sessione iSCSI.
Metodo di autenticazione	La tecnica per autenticare gli utenti che desiderano accedere alla rete iSCSI. I valori validi sono **CHAP** e **None**.
Metodo di digest dell'intestazione	La tecnica per mostrare i possibili valori di intestazione per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.

Elemento	Descrizione
Metodo di data digest	La tecnica per mostrare i possibili valori dei dati per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.
Numero massimo di connessioni	Il maggior numero di connessioni consentite per la sessione iSCSI. Il numero massimo di connessioni può essere compreso tra 1 e 4. Il valore predefinito è **1**.
Alias di destinazione	L'etichetta associata alla destinazione.
Alias iniziatore	Etichetta associata all'iniziatore.
Indirizzo IP di destinazione	L'indirizzo IP della destinazione per la sessione iSCSI. I nomi DNS non sono supportati.
R2T iniziale	Lo stato iniziale pronto per il trasferimento. Lo stato può essere **Sì** o **No**.
Lunghezza massima del burst	Il payload SCSI massimo in byte per questa sessione iSCSI. La lunghezza massima del burst può essere compresa tra 512 e 262,144 (256 KB). Il valore predefinito è **262,144 (256 KB)**.
Lunghezza del primo burst	Il payload SCSI in byte per i dati non richiesti per questa sessione iSCSI. La lunghezza del primo burst può essere compresa tra 512 e 131,072 (128 KB). Il valore predefinito è **65,536 (64 KB)**.
Tempo di attesa predefinito	Il numero minimo di secondi di attesa prima di tentare di stabilire una connessione dopo la chiusura o la reimpostazione della connessione. Il valore predefinito del tempo di attesa può essere compreso tra 0 e 3600. Il valore predefinito è **2**.
Tempo di conservazione predefinito	Il numero massimo di secondi in cui la connessione è ancora possibile in seguito a una interruzione della connessione o a un ripristino della connessione. Il tempo di conservazione predefinito può essere compreso tra 0 e 3600. Il valore predefinito è **20**.
R2T massimo in sospeso	Il numero massimo di "pronti per i trasferimenti" in sospeso per questa sessione iSCSI. Il valore massimo di ready to transfer può essere compreso tra 1 e 16. Il valore predefinito è **1**.
Livello di ripristino degli errori	Il livello di ripristino degli errori per questa sessione iSCSI. Il valore del livello di ripristino degli errori è sempre impostato su **0**.
Lunghezza massima del segmento di dati di ricezione	La quantità massima di dati che l'iniziatore o la destinazione possono ricevere in qualsiasi PDU (Payload Data Unit) iSCSI.

Elemento	Descrizione
Nome di destinazione	Il nome ufficiale della destinazione (non l'alias). Il nome di destinazione con il formato *iqn*.
Nome dell'iniziatore	Il nome ufficiale dell'iniziatore (non l'alias). Il nome dell'iniziatore che utilizza il formato *iqn* o *eui*.

4. Per salvare il report in un file, fare clic su **Save** (Salva).

   Il file viene salvato nella cartella Download del browser con il nome file `iscsi-session-connections.txt`.

Configurare iSER su porte InfiniBand

Se il controller include una porta iSER su InfiniBand, è possibile configurare la connessione di rete all'host. Le impostazioni di configurazione sono disponibili nella pagina hardware o nella pagina sistema.

Prima di iniziare

- Il controller deve includere una porta iSER su InfiniBand; in caso contrario, le impostazioni iSER su InfiniBand non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

A proposito di questa attività

È possibile accedere alla configurazione di iSER su InfiniBand dalla pagina **hardware** o dal **Impostazioni › sistema**. Questa attività descrive come configurare le porte dalla pagina **hardware**.

> Le impostazioni e le funzioni di iSER su InfiniBand vengono visualizzate solo se il controller dello storage array include una porta iSER su InfiniBand.

Fasi

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

   Il grafico cambia per mostrare i controller invece dei dischi.

3. Fare clic sul controller con la porta iSER su InfiniBand che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configura iSER su porte InfiniBand**.

   Viene visualizzata la finestra di dialogo Configura porte iSER su InfiniBand.

5. Nell'elenco a discesa, selezionare la porta HIC che si desidera configurare, quindi immettere l'indirizzo IP dell'host.
6. Fare clic su **Configura**.

7. Completare la configurazione, quindi reimpostare iSER sulla porta InfiniBand facendo clic su **Sì**.

Visualizza le statistiche di iSER su InfiniBand

Se il controller dello storage array include una porta iSER su InfiniBand, è possibile visualizzare i dati relativi alle connessioni host.

A proposito di questa attività

System Manager mostra i seguenti tipi di statistiche iSER su InfiniBand. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche di destinazione locale (protocollo)** — fornisce statistiche per la destinazione iSER su InfiniBand, che mostra l'accesso a livello di blocco ai propri supporti di storage.
- **Statistiche dell'interfaccia iSER su InfiniBand** — fornisce statistiche per tutte le porte iSER sull'interfaccia InfiniBand, che includono statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

È possibile accedere alle statistiche di iSER su InfiniBand dalla pagina System (sistema) (**Impostazioni › sistema**) o dalla pagina Support (supporto). Queste istruzioni descrivono come accedere alle statistiche dalla pagina di supporto.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Visualizza statistiche iSER su InfiniBand**.
3. Fare clic su una scheda per visualizzare i diversi set di statistiche.
4. Per impostare la linea di base, fare clic su **Set new baseline** (Imposta nuova linea di base).

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. La stessa linea di base viene utilizzata per tutte le statistiche iSER su InfiniBand.

FAQ

Cosa accade quando si utilizza un server iSNS per la registrazione?

Quando si utilizzano le informazioni del server iSNS (Internet Storage Name Service), è possibile configurare gli host (iniziatori) in modo che interrogino il server iSNS per recuperare le informazioni dal server di destinazione (controller).

Questa registrazione fornisce al server iSNS le informazioni relative al nome qualificato iSCSI (IQN) e alla porta del controller e consente di eseguire query tra gli iniziatori (host iSCSI) e le destinazioni (controller).

Quali metodi di registrazione sono supportati automaticamente per iSCSI?

L'implementazione iSCSI supporta il metodo di ricerca iSNS (Internet Storage Name Service) o l'utilizzo del comando Invia destinazioni.

Il metodo iSNS consente il rilevamento iSNS tra gli iniziatori (host iSCSI) e le destinazioni (controller). Il controller di destinazione viene registrato per fornire al server iSNS le informazioni relative a iSCSI Qualified Name (IQN) e porta del controller.

Se non si configura iSNS, l'host iSCSI può inviare il comando Invia destinazioni durante una sessione di rilevamento iSCSI. In risposta, il controller restituisce le informazioni sulla porta (ad esempio, il valore IQN di destinazione, l'indirizzo IP della porta, la porta di ascolto e il gruppo di porte di destinazione). Questo metodo di ricerca non è necessario se si utilizza iSNS, perché l'iniziatore host può recuperare gli IP di destinazione dal server iSNS.

Come si interpretano le statistiche di iSER su InfiniBand?

La finestra di dialogo **View iSER over InfiniBand Statistics** (Visualizza statistiche iSER su InfiniBand) visualizza le statistiche di destinazione locale (protocollo) e le statistiche dell'interfaccia iSER over InfiniBand (IB). Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche di destinazione locale (protocollo)** — fornisce statistiche per la destinazione iSER su InfiniBand, che mostra l'accesso a livello di blocco ai propri supporti di storage.
- **Statistiche dell'interfaccia iSER su InfiniBand** — fornisce statistiche per tutte le porte iSER su InfiniBand sull'interfaccia InfiniBand, che includono statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Cosa devo fare per configurare o diagnosticare iSER su InfiniBand?

La seguente tabella elenca le funzioni di System Manager che è possibile utilizzare per configurare e gestire le sessioni iSER su InfiniBand.

> Le impostazioni di iSER su InfiniBand sono disponibili solo se il controller dello storage array include una porta di gestione host iSER su InfiniBand.

Configurare e diagnosticare iSER su InfiniBand

Azione	Posizione
Configurare iSER su porte InfiniBand	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configura iSER su porte InfiniBand**. oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere fino a **iSER over InfiniBand settings**, quindi selezionare **Configure iSER over InfiniBand Ports** (Configura iSER su porte InfiniBand).

Azione	Posizione
Visualizza le statistiche di iSER su InfiniBand	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **iSER over InfiniBand settings**, quindi selezionare **View iSER over InfiniBand Statistics** (Visualizza statistiche iSER su InfiniBand).

System (sistema): Impostazioni NVMe

Concetti

Panoramica di NVMe

Alcuni controller includono una porta per l'implementazione di NVMe (non-volatile Memory Express) su un fabric InfiniBand o su un fabric RoCE (RDMA over Converged Ethernet). NVMe consente comunicazioni dalle performance elevate tra gli host e lo storage array.

Che cos'è NVMe?

NVM sta per "memoria non volatile" ed è la memoria persistente utilizzata in molti tipi di dispositivi di storage. *NVMe* (NVM Express) è un'interfaccia o protocollo standardizzato progettato specificamente per le comunicazioni multi-coda ad alte prestazioni con i dispositivi NVM.

Che cos'è NVMe sui fabric?

NVMe over Fabrics (NVMe-of) è una specifica tecnologica che consente il trasferimento di dati e comandi basati su messaggi NVMe tra un computer host e lo storage in rete. Per SANtricity OS 11.40 e versioni successive, un host può accedere a un array di storage NVMe (chiamato *sottosistema*) utilizzando un fabric InfiniBand o RDMA. I comandi NVMe sono abilitati e incapsulati nei layer di astrazione di trasporto sia sul lato host che sul lato del sottosistema. Questo estende l'interfaccia NVMe dalle performance elevate end-to-end dall'host allo storage e standardizza e semplifica il set di comandi.

Lo storage NVMe-of viene presentato a un host come dispositivo di storage a blocchi locale. Il volume (denominato *namespace*) può essere montato su un file system come con qualsiasi altro dispositivo di storage a blocchi. È possibile utilizzare l'API REST, SMcli o Gestore di sistema di SANtricity per eseguire il provisioning dello storage in base alle esigenze.

Che cos'è un NQN (NVMe Qualified Name)?

NQN (NVMe Qualified Name) viene utilizzato per identificare la destinazione dello storage remoto. Il nome qualificato NVMe per l'array di storage viene sempre assegnato dal sottosistema e non può essere modificato. Esiste un solo NVMe Qualified Name per l'intero array. La lunghezza massima del nome qualificato NVMe è di 223 caratteri. È possibile confrontarlo con un nome qualificato iSCSI.

Che cos'è un namespace e un ID namespace?

Uno spazio dei nomi è l'equivalente di un'unità logica in SCSI, che si riferisce a un volume nell'array. L'ID dello spazio dei nomi (NSID) equivale a un numero di unità logica (LUN) in SCSI. L'NSID viene creato al momento della creazione dello spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255.

Che cos'è un controller NVMe?

Analogamente a un Nexus SCSI i_T, che rappresenta il percorso dall'iniziatore dell'host alla destinazione del sistema di storage, un controller NVMe creato durante il processo di connessione dell'host fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. Un NQN per l'host più un identificatore di porta host identificano in modo univoco un controller NVMe. Sebbene un controller NVMe possa essere associato solo a un singolo host, può accedere a più spazi dei nomi.

È possibile configurare gli host a cui accedere e impostare l'ID dello spazio dei nomi per l'host utilizzando Gestione di sistema di SANtricity. Quindi, quando viene creato il controller NVMe, viene creato e utilizzato l'elenco degli ID dello spazio dei nomi accessibili dal controller NVMe per configurare le connessioni consentite.

Terminologia NVMe

Scopri in che modo i termini NVMe si applicano al tuo storage array.

Termine	Descrizione
InfiniBand	InfiniBand (IB) è uno standard di comunicazione per la trasmissione dei dati tra server e sistemi storage dalle performance elevate.
Namespace	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.
ID spazio dei nomi	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.
NQN	NVMe Qualified Name (NQN) viene utilizzato per identificare la destinazione dello storage remoto (lo storage array).
NVM	La memoria non volatile (NVM) è una memoria persistente utilizzata in molti tipi di dispositivi di storage.
NVMe	NVMe (non-volatile Memory Express) è un'interfaccia progettata per i dispositivi di storage basati su flash, come ad esempio i dischi SSD. NVMe riduce l'overhead di i/o e include miglioramenti delle performance rispetto alle interfacce dei dispositivi logici precedenti.
NVMe-of	NVMe-of (non-volatile Memory Express over Fabrics) è una specifica che consente ai comandi e ai dati NVMe di trasferire in rete tra un host e lo storage.
Controller NVMe	Durante il processo di connessione all'host viene creato un controller NVMe. Fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage.
Coda NVMe	Una coda viene utilizzata per il passaggio di comandi e messaggi sull'interfaccia NVMe.

Termine	Descrizione
Sottosistema NVMe	Lo storage array con una connessione host NVMe.
RDMA	L'accesso remoto diretto alla memoria (RDMA) consente uno spostamento dei dati più diretto all'interno e all'esterno di un server implementando un protocollo di trasporto nell'hardware della scheda di interfaccia di rete (NIC).
ROCE	RDMA over Converged Ethernet (RoCE) è un protocollo di rete che consente l'accesso remoto diretto alla memoria (RDMA) su una rete Ethernet.
SSD	I dischi a stato solido (SSD) sono dispositivi di storage che utilizzano la memoria a stato solido (flash) per memorizzare i dati in modo persistente. Gli SSD emulano i dischi rigidi convenzionali e sono disponibili con le stesse interfacce utilizzate dai dischi rigidi.

Come fare

Configurare NVMe sulle porte InfiniBand

Se il controller include una connessione NVMe su InfiniBand, è possibile configurare le impostazioni della porta NVMe dalla pagina hardware o dalla pagina sistema.

Prima di iniziare

- Il controller deve includere una porta host NVMe over InfiniBand; in caso contrario, le impostazioni NVMe over InfiniBand non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

A proposito di questa attività

È possibile accedere alla configurazione NVMe su InfiniBand dalla pagina **hardware** o dal **Impostazioni › sistema**. Questa attività descrive come configurare le porte dalla pagina **hardware**.

> Le impostazioni e le funzioni NVMe over InfiniBand vengono visualizzate solo se il controller dello storage array include una porta NVMe over InfiniBand.

Fasi

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

   Il grafico cambia per mostrare i controller invece dei dischi.
3. Fare clic sul controller con la porta NVMe over InfiniBand che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.
4. Selezionare **Configura NVMe su porte InfiniBand**.

   Viene visualizzata la finestra di dialogo **Configure NVMe over InfiniBand Ports** (Configura porte NVMe su InfiniBand).

5. Nell'elenco a discesa, selezionare la porta HIC che si desidera configurare, quindi immettere l'indirizzo IP dell'host.
6. Fare clic su **Configura**.
7. Completare la configurazione, quindi reimpostare NVMe sulla porta InfiniBand facendo clic su **Sì**.

Configurare NVMe sulle porte RoCE

Se il controller include una connessione per NVMe su RoCE (RDMA over Converged Ethernet), è possibile configurare le impostazioni della porta NVMe dalla pagina hardware o dalla pagina sistema.

Prima di iniziare

- Il controller deve includere un NVMe su una porta host RoCE; in caso contrario, le impostazioni NVMe su RoCE non sono disponibili in System Manager.
- È necessario conoscere l'indirizzo IP della connessione host.

A proposito di questa attività

È possibile accedere alla configurazione NVMe over RoCE dalla pagina **hardware** o dal **Impostazioni › sistema**. Questa attività descrive come configurare le porte dalla pagina hardware.

> Le impostazioni e le funzioni NVMe over RoCE vengono visualizzate solo se il controller dello storage array include una porta NVMe over RoCE.

Fasi

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

   Il grafico cambia per mostrare i controller invece dei dischi.

3. Fare clic sul controller con la porta NVMe over RoCE che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configure NVMe over RoCE ports** (Configura NVMe su porte RoCE).

   Viene visualizzata la finestra di dialogo Configure NVMe over RoCE Ports (Configura porte NVMe su RoCE).

5. Nell'elenco a discesa, selezionare la porta HIC che si desidera configurare.
6. Fare clic su **Avanti**.

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

Dettagli campo

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità che corrisponde alla velocità del modulo SFP sulla porta.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. Se si desidera disattivare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
Dimensione MTU (disponibile facendo clic su Mostra altre impostazioni della porta).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.

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

7. Configurare le impostazioni IPv4 e/o IPv6, automaticamente o manualmente.

Dettagli campo

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. (Se lo si desidera, è possibile tagliare e incollare gli indirizzi nei campi). Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router.

8. Fare clic su **fine**.

Visualizza le statistiche NVMe over Fabrics

È possibile visualizzare i dati relativi alle connessioni NVMe over Fabrics allo storage array.

A proposito di questa attività

System Manager mostra questi tipi di statistiche NVMe over Fabrics. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **NVMe Subsystem statistics** — fornisce statistiche per il controller NVMe, inclusi timeout e errori di connessione.
- **RDMA Interface statistics** — fornisce statistiche per l'interfaccia RDMA, incluse informazioni sui pacchetti ricevuti e trasmessi.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

È possibile accedere alle statistiche NVMe over Fabrics dalla pagina System (sistema) (**Impostazioni › sistema**) o dalla pagina Support (supporto). Queste istruzioni descrivono come accedere alle statistiche dalla pagina di supporto.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).
3. Per impostare la linea di base, fare clic su **Set new baseline** (Imposta nuova linea di base).

   L'impostazione della linea di base consente di impostare un nuovo punto di partenza per la raccolta delle statistiche. La stessa linea di base viene utilizzata per tutte le statistiche NVMe.

FAQ

Come si interpretano le statistiche NVMe su InfiniBand?

La finestra di dialogo **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe su fabric) visualizza le statistiche per il sottosistema NVMe e l'interfaccia NVMe over InfiniBand (NVMe su InfiniBand). Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **NVMe Subsystem statistics** — Mostra le statistiche del controller NVMe e della relativa coda. Il controller NVMe fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti. Per ulteriori informazioni su queste statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.
- **RDMA Interface statistics** — fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, che includono statistiche sulle performance e informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Per ulteriori informazioni sulle statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le

statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Come si interpretano le statistiche NVMe sulle fabric?

La finestra di dialogo **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe su fabric) visualizza le statistiche per il sottosistema NVMe e l'interfaccia NVMe over RoCE. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **NVMe Subsystem statistics** — Mostra le statistiche del controller NVMe e della relativa coda. Il controller NVMe fornisce un percorso di accesso tra un host e gli spazi dei nomi nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti. Per ulteriori informazioni su queste statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.
- **RDMA Interface statistics** — fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, che includono statistiche sulle performance e informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Per ulteriori informazioni sulle statistiche, fare clic su **Visualizza legenda per le intestazioni delle tabelle**.

È possibile visualizzare ciascuna di queste statistiche come statistiche raw o come statistiche baseline. Le statistiche raw sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche di riferimento sono statistiche point-in-time raccolte dall'ora di riferimento impostata.

Quali altre operazioni è necessario eseguire per configurare o diagnosticare NVMe su InfiniBand?

La seguente tabella elenca le funzioni di System Manager che è possibile utilizzare per configurare e gestire le sessioni NVMe su InfiniBand.

> Le impostazioni NVMe over InfiniBand sono disponibili solo se il controller dello storage array include una porta NVMe over InfiniBand.

Configurare e diagnosticare NVMe su InfiniBand

Azione	Posizione
Configurare NVMe sulle porte InfiniBand	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configura NVMe su porte InfiniBand**. oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over InfiniBand settings**, quindi selezionare **Configure NVMe over InfiniBand Ports** (Configura NVMe su porte InfiniBand).

Azione	Posizione
Visualizza le statistiche NVMe su InfiniBand	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over InfiniBand Settings**, quindi selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).

Quali altre operazioni è necessario eseguire per configurare o diagnosticare NVMe su RoCE?

È possibile configurare e gestire NVMe su RoCE dalle pagine hardware e impostazioni.

> Le impostazioni NVMe over RoCE sono disponibili solo se il controller dello storage array include una porta NVMe over RoCE.

Configurare e diagnosticare NVMe su RoCE

Azione	Posizione
Configurare NVMe sulle porte RoCE	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configure NVMe over RoCE ports** (Configura NVMe su porte RoCE). oppure 1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over RoCE settings**, quindi selezionare **Configure NVMe over RoCE Ports** (Configura NVMe su porte RoCE).
Visualizza le statistiche NVMe over Fabrics	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **NVMe over RoCE settings**, quindi selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).

Funzionalità add-on

Concetti

Come funzionano le funzionalità aggiuntive

I componenti aggiuntivi sono funzionalità non incluse nella configurazione standard di System Manager e richiedono una chiave per l'attivazione. Una funzione aggiuntiva può essere una singola funzionalità premium o un pacchetto di funzionalità.

I seguenti passaggi forniscono una panoramica sull'attivazione di una funzionalità Premium o Feature Pack:

1. Ottenere le seguenti informazioni:
   - Numero di serie dello chassis e Feature Enable Identifier, che identificano l'array di storage per la funzione da installare. Questi elementi sono disponibili in System Manager.
   - Codice di attivazione della funzione, disponibile sul sito del supporto al momento dell'acquisto della funzione.
2. Per ottenere la chiave funzione, contattare il proprio provider di storage o accedere al sito di attivazione delle funzionalità Premium. Fornire il numero di serie dello chassis, l'identificatore di abilitazione della funzione e il codice di attivazione della funzione.
3. Utilizzando System Manager, attivare la funzionalità Premium o il Feature Pack utilizzando il file delle chiavi funzione.

Terminologia delle funzionalità aggiuntive

Scopri in che modo i termini delle funzionalità aggiuntive si applicano al tuo storage array.

Termine	Descrizione
Identificatore di abilitazione della funzione	Feature Enable Identifier è una stringa univoca che identifica lo storage array specifico. Questo identificatore garantisce che, quando si ottiene la funzionalità premium, venga associata solo a quel particolare array di storage. Questa stringa viene visualizzata sotto Add-Ons nella pagina System (sistema).
File delle chiavi di funzione	Un file Feature Key è un file ricevuto per lo sblocco e l'attivazione di una funzionalità Premium o Feature Pack.
Feature Pack	Un Feature Pack è un bundle che modifica gli attributi degli array di storage (ad esempio, la modifica del protocollo da Fibre Channel a iSCSI). I Feature Pack richiedono una chiave speciale per attivarli.
Funzionalità Premium	Una funzione premium è un'opzione aggiuntiva che richiede una chiave per attivarla. Non è incluso nella configurazione standard di System Manager.

Come fare

Ottenere un file delle chiavi di funzione

Per attivare una funzionalità o un Feature Pack premium sull'array di storage, è necessario prima ottenere un file delle chiavi delle funzioni. Una chiave è associata a un solo array di storage.

A proposito di questa attività

Questa attività descrive come raccogliere le informazioni necessarie per la funzione e inviare una richiesta per un file delle chiavi di funzione. Le informazioni richieste includono:

- Numero di serie dello chassis
- Identificatore di abilitazione della funzione
- Codice di attivazione della funzione

Fasi

1. In System Manager, individuare e registrare il numero di serie dello chassis. Per visualizzare questo numero di serie, passare il mouse sul riquadro Support Center.
2. In System Manager, individuare Feature Enable Identifier. Accedere a **Impostazioni › sistema**, quindi scorrere verso il basso fino a **componenti aggiuntivi**. Cercare **Feature Enable Identifier**. Annotare il numero per l'identificatore di abilitazione della funzione.
3. Individuare e registrare il codice di attivazione della funzione. Per i features pack, questo codice di attivazione viene fornito nelle istruzioni appropriate per l'esecuzione della conversione.

   Le istruzioni NetApp sono disponibili all'interno del sito "Centro di documentazione dei sistemi NetApp e-Series".

   Per le funzioni Premium, è possibile accedere al codice di attivazione dal sito del supporto, come indicato di seguito:

   a. Accedere a. "Supporto NetApp".
   b. Accedere al **Products › Manage Products › Software Licenses** (prodotti[Gestisci prodotti > licenze software]).
   c. Inserire il numero di serie dello chassis dello storage array, quindi fare clic su **Go**.
   d. Cercare i codici di attivazione delle funzioni nella colonna **chiave di licenza**.
   e. Annotare il codice di attivazione della funzione desiderata.
4. Richiedere un file delle chiavi di funzione inviando un'e-mail o un documento di testo al proprio fornitore di storage con le seguenti informazioni: Numero di serie dello chassis, codice di attivazione delle funzioni e identificatore di abilitazione delle funzioni.

   È inoltre possibile visitare il sito Web all'indirizzo "Attivazione della licenza NetApp: Attivazione della funzionalità Premium dello storage Array" e inserire le informazioni richieste per ottenere la funzionalità o il feature pack. (Le istruzioni su questo sito sono relative alle funzioni premium, non ai pacchetti di funzionalità).

Al termine

Se si dispone di un file delle chiavi delle funzioni, è possibile attivare la funzionalità Premium o il Feature Pack.

Abilitare una funzione premium

Una funzione premium è un'opzione aggiuntiva che richiede una chiave per l'attivazione.

Prima di iniziare

- È stata ottenuta una chiave funzione. Se necessario, contattare il supporto tecnico per ottenere una chiave.
- Il file delle chiavi è stato caricato sul client di gestione (il sistema con un browser per l'accesso a System Manager).

A proposito di questa attività

Questa attività descrive come utilizzare System Manager per attivare una funzione Premium.

> Se si desidera disattivare una funzione Premium, è necessario utilizzare il comando Disable Storage Array Feature (Disattiva funzionalità array di storage) `(disable storageArray (featurePack | feature=featureAttributeList)` Nell'interfaccia della riga di comando (CLI).

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **attiva funzionalità Premium**.

   Viene visualizzata la finestra di dialogo Enable a Premium Feature (attiva una funzione Premium).
3. Fare clic su **Browse**, quindi selezionare il file delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.
4. Fare clic su **Enable** (attiva).

Abilitare il Feature Pack

Un Feature Pack è un bundle che modifica gli attributi degli array di storage (ad esempio, la modifica del protocollo da Fibre Channel a iSCSI). I Feature Pack richiedono una chiave speciale per l'abilitazione.

Prima di iniziare

- Sono state seguite le istruzioni appropriate per l'esecuzione della conversione e la preparazione del sistema per i nuovi attributi dell'array di storage.

  > Le istruzioni di conversione sono disponibili all'interno del sito "Centro di documentazione dei sistemi NetApp e-Series".

- Lo storage array non è in linea, quindi non vi accedono host o applicazioni.
- Viene eseguito il backup di tutti i dati.
- È stato ottenuto un file Feature Pack.

  Il file del Feature Pack viene caricato sul client di gestione (il sistema con un browser per l'accesso a System Manager).

> È necessario pianificare una finestra di manutenzione del downtime e interrompere tutte le operazioni di i/o tra l'host e i controller. Inoltre, tenere presente che non è possibile accedere ai dati sull'array di storage fino a quando la conversione non è stata completata correttamente.

A proposito di questa attività

Questa attività descrive come utilizzare System Manager per attivare un Feature Pack. Al termine, riavviare lo storage array.

Fasi

1. Selezionare **Impostazioni › sistema**.

2. In **componenti aggiuntivi**, selezionare **Cambia Feature Pack**.
3. Fare clic su **Browse**, quindi selezionare il file delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Digitare **CHANGE** nel campo.
5. Fare clic su **Cambia**.

   Viene avviata la migrazione dei Feature Pack e i controller vengono riavviati. I dati della cache non scritti vengono cancellati, il che garantisce l'assenza di attività i/O. Entrambi i controller si riavviano automaticamente per rendere effettivo il nuovo Feature Pack. Una volta completato il riavvio, lo storage array torna allo stato di risposta.

Gestione delle chiavi di sicurezza

Concetti

Funzionamento della funzione Drive Security

Drive Security è una funzionalità di storage array che offre un ulteriore livello di sicurezza con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Quando questi dischi vengono utilizzati con la funzione Drive Security, richiedono una chiave di sicurezza per l'accesso ai dati. Quando i dischi vengono fisicamente rimossi dall'array, non possono funzionare fino a quando non vengono installati in un altro array, a questo punto, saranno in uno stato di sicurezza bloccato fino a quando non viene fornita la chiave di sicurezza corretta.

Come implementare Drive Security

Per implementare Drive Security, attenersi alla seguente procedura.

1. Dotare lo storage array di dischi sicuri, sia FDE che FIPS. (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.
2. Creare una chiave di sicurezza, ovvero una stringa di caratteri condivisa dal controller e dalle unità per l'accesso in lettura/scrittura. È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Per la gestione esterna delle chiavi, è necessario stabilire l'autenticazione con il server di gestione delle chiavi.
3. Abilitare Drive Security per pool e gruppi di volumi:
   - Creare un pool o un gruppo di volumi (cercare **Sì** nella colonna **Secure-capable** della tabella dei candidati).
   - Selezionare un pool o un gruppo di volumi quando si crea un nuovo volume (cercare **Sì** accanto a **Secure-capable** nella tabella dei candidati del pool e del gruppo di volumi).

Funzionamento di Drive Security a livello di unità

Un disco sicuro, FDE o FIPS, crittografa i dati durante la scrittura e decrta i dati durante la lettura. La crittografia e la decrittografia non influiscono sulle prestazioni o sul flusso di lavoro dell'utente. Ogni disco

dispone di una propria chiave di crittografia univoca, che non può mai essere trasferita dal disco.

La funzione Drive Security offre un ulteriore livello di protezione con dischi sicuri. Quando si selezionano gruppi di volumi o pool su questi dischi per Drive Security, i dischi cercano una chiave di sicurezza prima di consentire l'accesso ai dati. È possibile attivare Drive Security per pool e gruppi di volumi in qualsiasi momento, senza influire sui dati esistenti sul disco. Tuttavia, non è possibile disattivare Drive Security senza cancellare tutti i dati presenti sul disco.

Funzionamento di Drive Security a livello di storage array

Con la funzione Drive Security, è possibile creare una chiave di sicurezza condivisa tra i dischi e i controller abilitati alla protezione in un array di storage. Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller non applica la chiave di sicurezza.

Se un disco abilitato alla protezione viene rimosso dall'array di storage e reinstallato in un array di storage diverso, il disco si trova in uno stato di sicurezza bloccata. L'unità riposizionata cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, applicare la chiave di sicurezza dall'array di storage di origine. Una volta completato correttamente il processo di sblocco, l'unità riallocata utilizzerà la chiave di sicurezza già memorizzata nell'array di storage di destinazione e il file della chiave di sicurezza importato non sarà più necessario.

> Per la gestione interna delle chiavi, la chiave di sicurezza effettiva viene memorizzata nel controller in una posizione non accessibile. Non è in formato leggibile né accessibile all'utente.

Funzionamento di Drive Security a livello di volume

Quando si crea un pool o un gruppo di volumi da dischi con funzionalità di protezione, è anche possibile attivare Drive Security per tali pool o gruppi di volumi. L'opzione Drive Security (protezione disco) rende sicuri i dischi e i gruppi di volumi e i pool associati-*enabled*.

Prima di creare pool e gruppi di volumi abilitati alla protezione, tenere presenti le seguenti linee guida:

- I gruppi di volumi e i pool devono essere costituiti interamente da dischi sicuri. (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.
- I gruppi di volumi e i pool devono trovarsi in uno stato ottimale.

Come funziona la gestione delle chiavi di sicurezza

Quando si implementa la funzione Drive Security, i dischi abilitati alla protezione (FIPS o FDE) richiedono una chiave di sicurezza per l'accesso ai dati. Una chiave di sicurezza è una stringa di caratteri condivisa tra questi tipi di dischi e i controller di un array di storage.

Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller non applica la chiave di sicurezza. Se un disco abilitato alla protezione viene rimosso dall'array di storage, i dati dell'unità vengono bloccati. Quando il disco viene reinstallato in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale.

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 conservate nella memoria persistente del controller. Per implementare la gestione interna delle chiavi, attenersi alla seguente procedura:

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. 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. Per creare una chiave interna, accedere al **Impostazioni › sistema › Gestione chiave di sicurezza › Crea chiave interna**.

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). Per implementare la gestione esterna delle chiavi, attenersi alla seguente procedura:

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. Completare e scaricare una CSR (Certificate Signing Request) client per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
4. Creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
5. Assicurarsi che il certificato client e una copia del certificato per il server di gestione delle chiavi siano disponibili sull'host locale.
6. 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. Per creare una chiave esterna, accedere al **Impostazioni › sistema › Gestione chiave di sicurezza › Crea chiave esterna**.

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.

Promuovere la terminologia in materia di sicurezza

Scopri come si applicano i termini di Drive Security al tuo storage array.

Termine	Descrizione
Funzione di protezione del disco	Drive Security è una funzionalità di storage array che offre un ulteriore livello di sicurezza con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Quando questi dischi vengono utilizzati con la funzione Drive Security, richiedono una chiave di sicurezza per l'accesso ai dati. Quando i dischi vengono fisicamente rimossi dall'array, non possono funzionare fino a quando non vengono installati in un altro array, a questo punto, saranno in uno stato di sicurezza bloccato fino a quando non viene fornita la chiave di sicurezza corretta.
Dischi FDE	I dischi con crittografia completa del disco (FDE) eseguono la crittografia sul disco a livello hardware. Il disco rigido contiene un chip ASIC che crittografa i dati durante le operazioni di scrittura, quindi decrta i dati durante le operazioni di lettura.
Dischi FIPS	I dischi FIPS utilizzano gli standard FIPS (Federal Information Processing Standards) 140-2 livello 2. Si tratta essenzialmente di dischi FDE conformi agli standard governativi degli Stati Uniti per garantire metodi e algoritmi di crittografia efficaci. I dischi FIPS hanno standard di sicurezza più elevati rispetto ai dischi FDE.
Client di gestione	Un sistema locale (computer, tablet, ecc.) che include un browser per l'accesso a System Manager.
Password	La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. La stessa passphrase utilizzata per crittografare la chiave di sicurezza deve essere fornita quando la chiave di sicurezza di cui è stato eseguito il backup viene importata come risultato di una migrazione del disco o di uno scambio head. Una password può contenere da 8 a 32 caratteri. La password per Drive Security è indipendente dalla password Administrator dell'array di storage.

Termine	Descrizione
Dischi sicuri	I dischi che supportano la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard), che crittografano i dati durante la scrittura e decrittare i dati durante la lettura. Questi dischi sono considerati sicuri-*capaci* perché possono essere utilizzati per una maggiore sicurezza utilizzando la funzione Drive Security. Se la funzione Drive Security è attivata per i gruppi di volumi e i pool utilizzati con questi dischi, i dischi diventano sicuri-*abilitati*.
Dischi sicuri	Le unità abilitate alla protezione vengono utilizzate con la funzione Drive Security. Quando si attiva la funzione Drive Security e si applica Drive Security a un pool o a un gruppo di volumi su dischi sicuri-*capaci*, i dischi diventano sicuri-*abilitati*. L'accesso in lettura e scrittura è disponibile solo attraverso un controller configurato con la chiave di sicurezza corretta. Questa sicurezza aggiuntiva impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array.
Chiave di sicurezza	Una chiave di sicurezza è una stringa di caratteri condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, i dischi abilitati alla protezione cambiano in uno stato di sicurezza bloccato fino a quando il controller non applica la chiave di sicurezza. Se un disco abilitato alla protezione viene rimosso dall'array di storage, i dati dell'unità vengono bloccati. Quando il disco viene reinstallato in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale. È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi: • Gestione interna delle chiavi — Crea e mantieni le chiavi di sicurezza nella memoria persistente del controller. • Gestione esterna delle chiavi — Crea e gestisci le chiavi di sicurezza su un server di gestione delle chiavi esterno.
Identificatore della chiave di sicurezza	L'identificatore della chiave di sicurezza è una stringa associata alla chiave di sicurezza durante la creazione della chiave. L'identificatore viene memorizzato sul controller e su tutti i dischi associati alla chiave di sicurezza.

Come fare

Creare una chiave di sicurezza interna

Per utilizzare la funzione Drive Security, è possibile creare una chiave di sicurezza interna condivisa dai controller e dalle unità sicure nell'array di storage. Le chiavi interne vengono conservate nella memoria persistente del controller.

Prima di iniziare

- Nello storage array devono essere installate unità sicure. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo **Impossibile creare la chiave di sicurezza** durante questa attività. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

> Se nell'array di storage sono installati sia dischi FDE che FIPS, tutti condividono la stessa chiave di sicurezza.

A proposito di questa attività

In questa attività, si definiscono un identificatore e una passphrase da associare alla chiave di sicurezza interna.

> La password per Drive Security è indipendente dalla password Administrator dell'array di storage.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Create Internal Key** (Crea chiave interna).

   Se non è stata ancora generata una chiave di sicurezza, viene visualizzata la finestra di dialogo **Crea chiave di sicurezza**.

3. Inserire le informazioni nei seguenti campi:

   - Definire un identificatore della chiave di sicurezza — è possibile accettare il valore predefinito (nome dello storage array e data/ora, generato dal firmware del controller) o inserire un valore personalizzato. È possibile inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

     > I caratteri aggiuntivi vengono generati automaticamente, aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

   - Definire una passphrase/immettere nuovamente una passphrase — inserire e confermare una passphrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
     - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
     - Un numero (uno o più).
     - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

Assicurarsi di registrare le voci per un utilizzo successivo. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati dell'unità.

4. Fare clic su **Create** (Crea).

   La chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. Insieme alla chiave effettiva, è disponibile un file di chiavi crittografate che viene scaricato dal browser.

   Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Risultato

È ora possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, tutti i dischi abilitati per la sicurezza vengono attivati in uno stato di sicurezza bloccata. In questo stato, i dati non sono accessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione del disco. Se qualcuno rimuove fisicamente un disco bloccato e lo installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai dati.

Al termine

È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Creare una chiave di sicurezza esterna

Per utilizzare la funzione Drive Security con un server di gestione delle chiavi, è necessario creare una chiave esterna condivisa dal server di gestione delle chiavi e dalle unità sicure nell'array di storage.

Prima di iniziare

- Nell'array devono essere installate unità sicure. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).

  Se nell'array di storage sono installati sia dischi FDE che FIPS, tutti condividono la stessa chiave di sicurezza.

- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo **Impossibile creare la chiave di sicurezza** durante questa attività. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- I certificati client e server sono disponibili sull'host locale in modo che l'array di storage e il server di gestione delle chiavi possano autenticarsi l'uno con l'altro. Il certificato del client convalida i controller, mentre il certificato del server convalida il server di gestione delle chiavi.

A proposito di questa attività

In questa attività, definire l'indirizzo IP del server di gestione delle chiavi e il numero di porta utilizzato, quindi

caricare i certificati per la gestione delle chiavi esterne.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Create External Key** (Crea chiave esterna).

   Se la gestione interna delle chiavi è attualmente configurata, viene visualizzata una finestra di dialogo che richiede di confermare che si desidera passare alla gestione esterna delle chiavi.

   Viene visualizzata la finestra di dialogo **Crea chiave di sicurezza esterna**.

3. In **Connect to Key Server** (connessione al server chiavi), immettere le informazioni nei seguenti campi:
   - Key management server address (Indirizzo server di gestione delle chiavi) — inserire il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - Key management port number (numero porta di gestione delle chiavi) — inserire il numero di porta utilizzato per le comunicazioni KMIP (Key Management Interoperability Protocol). Il numero di porta più comune utilizzato per le comunicazioni del server di gestione delle chiavi è 5696.
   - Select client certificate (Seleziona certificato client) — fare clic sul primo pulsante Browse (Sfoglia) per selezionare il file di certificato per i controller dell'array di storage.
   - Selezionare il certificato del server del server di gestione delle chiavi — fare clic sul secondo pulsante Sfoglia per selezionare il file di certificato per il server di gestione delle chiavi.
4. Fare clic su **Avanti**.
5. In **Create/Backup Key** (chiave di creazione/backup), immettere le informazioni nel campo seguente:
   - Definire una passphrase/immettere nuovamente una passphrase — inserire e confermare una passphrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
     - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
     - Un numero (uno o più).
     - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

   Assicurarsi di registrare le voci per un utilizzo successivo. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere la password per sbloccare i dati dell'unità.

6. Fare clic su **fine**.

   Il sistema si connette al server di gestione delle chiavi con le credenziali immesse. Una copia della chiave di sicurezza viene quindi memorizzata nel sistema locale.

   Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

7. Registrare la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

   La pagina visualizza il seguente messaggio con collegamenti aggiuntivi per la gestione esterna delle chiavi:

```
Current key management method: External
```

8. Verificare la connessione tra lo storage array e il server di gestione delle chiavi selezionando **Test Communication**.

   I risultati del test vengono visualizzati nella finestra di dialogo.

Risultati

Quando è attivata la gestione delle chiavi esterne, è possibile creare gruppi di volumi o pool abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

> Ogni volta che si spegne e si riaccende l'alimentazione dei dischi, tutti i dischi abilitati per la sicurezza vengono attivati in uno stato di sicurezza bloccata. In questo stato, i dati non sono accessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione del disco. Se qualcuno rimuove fisicamente un disco bloccato e lo installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai dati.

Al termine

- È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Modificare la chiave di sicurezza

In qualsiasi momento, è possibile sostituire una chiave di sicurezza con una nuova. Potrebbe essere necessario modificare una chiave di sicurezza nei casi in cui si verifica una potenziale violazione della sicurezza presso l'azienda e si desidera assicurarsi che il personale non autorizzato non possa accedere ai dati dei dischi.

Prima di iniziare

Una chiave di sicurezza esiste già.

A proposito di questa attività

Questa attività descrive come modificare una chiave di sicurezza e sostituirla con una nuova. Dopo questo processo, la vecchia chiave viene invalidata.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Change Key** (Cambia chiave).

   Viene visualizzata la finestra di dialogo **Change Security Key** (Modifica chiave di sicurezza).

3. Immettere le informazioni nei seguenti campi.

   - Definire un identificatore della chiave di sicurezza — (solo per le chiavi di sicurezza interne). Accettare il valore predefinito (nome dell'array di storage e data/ora, generato dal firmware del controller) o inserire un valore personalizzato. È possibile inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

     > I caratteri aggiuntivi vengono generati automaticamente e aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

- Definire una passphrase/immettere nuovamente una passphrase — in ciascuno di questi campi, inserire la password. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:
  - Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
  - Un numero (uno o più).
  - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

Assicurarsi di registrare le voci per un utilizzo successivo — se è necessario spostare un disco abilitato alla sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati del disco.

4. Fare clic su **Cambia**.

   La nuova chiave di sicurezza sovrascrive la chiave precedente, che non è più valida.

Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Al termine

È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Passare dalla gestione delle chiavi esterna a quella interna

È possibile modificare il metodo di gestione di Drive Security da un server di chiavi esterno al metodo interno utilizzato dall'array di storage. La chiave di sicurezza precedentemente definita per la gestione esterna delle chiavi viene quindi utilizzata per la gestione interna delle chiavi.

Prima di iniziare

È stata creata una chiave esterna.

A proposito di questa attività

In questa attività, si disattiva la gestione delle chiavi esterne e si scarica una nuova copia di backup sull'host locale. La chiave esistente viene ancora utilizzata per Drive Security, ma verrà gestita internamente nell'array di storage.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Disable External Key Management** (Disattiva gestione chiavi esterne).

   Viene visualizzata la finestra di dialogo **Disable External Key Management** (Disattiva gestione chiavi esterne).

3. In **definire una passphrase/immettere nuovamente la passphrase**, inserire e confermare una passphrase per il backup della chiave. Il valore può contenere da 8 a 32 caratteri e deve includere

ciascuno dei seguenti elementi:

- Una lettera maiuscola (una o più lettere). Tenere presente che la password distingue tra maiuscole e minuscole.
- Un numero (uno o più).
- Un carattere non alfanumerico, ad esempio !, *, @ (uno o più).

Assicurarsi di registrare le voci per un utilizzo successivo. Se è necessario spostare un'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere l'identificatore e la password per sbloccare i dati dell'unità.

4. Fare clic su **Disable** (Disattiva).

   La chiave di backup viene scaricata sull'host locale.

5. Registrare l'identificativo della chiave, la password e la posizione del file delle chiavi scaricato, quindi fare clic su **Chiudi**.

Risultati

Drive Security è ora gestito internamente attraverso lo storage array.

Al termine

- È necessario convalidare la chiave di sicurezza per assicurarsi che il file delle chiavi non sia corrotto.

Modificare le impostazioni del server di gestione delle chiavi

Se è stata configurata la gestione esterna delle chiavi, è possibile visualizzare e modificare le impostazioni del server di gestione delle chiavi in qualsiasi momento.

Prima di iniziare

È necessario configurare la gestione esterna delle chiavi.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **View/Edit Key Management Server Settings** (Visualizza/Modifica impostazioni del server di gestione delle chiavi).
3. Modificare le informazioni nei seguenti campi:
   - Key management server address (Indirizzo server di gestione delle chiavi) — inserire il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - KMIP port number (numero porta KMIP) — inserire il numero di porta utilizzato per le comunicazioni KMIP (Key Management Interoperability Protocol).
4. Fare clic su **Save** (Salva).

Eseguire il backup della chiave di sicurezza

Dopo aver creato o modificato una chiave di sicurezza, è possibile creare una copia di backup del file delle chiavi nel caso in cui l'originale venga danneggiato.

Prima di iniziare

- Una chiave di sicurezza esiste già.

A proposito di questa attività

Questa attività descrive come eseguire il backup di una chiave di sicurezza creata in precedenza. Durante questa procedura, viene creata una nuova passphrase per il backup. Questa password non deve corrispondere alla password utilizzata al momento della creazione o dell'ultima modifica della chiave originale. La password viene applicata solo al backup che si sta creando.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Backup key**.

   Viene visualizzata la finestra di dialogo **Backup Security Key** (chiave di sicurezza di backup).

3. Nei campi **Definisci password/Inserisci nuova password**, immettere e confermare una password per il backup.

   Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti elementi:

   - Una lettera maiuscola (una o più lettere)
   - Un numero (uno o più)
   - Un carattere non alfanumerico, ad esempio !, *, @ (uno o più)

   Assicurarsi di registrare i dati immessi per un utilizzo successivo. Per accedere al backup di questa chiave di sicurezza, è necessaria la password.

4. Fare clic su **Backup**.

   Viene scaricato un backup della chiave di sicurezza sull'host locale, quindi viene visualizzata la finestra di dialogo **Conferma/Registra backup chiave di sicurezza**.

   Il percorso del file della chiave di sicurezza scaricato potrebbe dipendere dalla posizione di download predefinita del browser.

5. Registrare la password in una posizione sicura, quindi fare clic su **Chiudi**.

Al termine

È necessario convalidare la chiave di sicurezza per il backup.

Convalidare la chiave di sicurezza

È possibile convalidare la chiave di sicurezza per assicurarsi che non sia stata danneggiata e per verificare di disporre di una password corretta.

Prima di iniziare

È stata creata una chiave di sicurezza.

A proposito di questa attività

Questa attività descrive come convalidare la chiave di sicurezza creata in precedenza. Si tratta di un passaggio importante per assicurarsi che il file delle chiavi non sia corrotto e che la password sia corretta, in modo da poter accedere in seguito ai dati delle unità se si sposta un disco abilitato alla sicurezza da un array

di storage a un altro.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **Security key management**, selezionare **Validate Key** (convalida chiave).

   Viene visualizzata la finestra di dialogo **Validate Security Key** (convalida chiave di sicurezza).

3. Fare clic su **Browse**, quindi selezionare il file delle chiavi (ad esempio, `drivesecurity.slk`).
4. Inserire la password associata alla chiave selezionata.

   Quando si seleziona un file di chiavi e una password validi, il pulsante **convalida** diventa disponibile.

5. Fare clic su **Validate** (convalida).

   I risultati della convalida vengono visualizzati nella finestra di dialogo.

6. Se il risultato è "la chiave di sicurezza è stata convalidata correttamente", fare clic su **Chiudi**. Se viene visualizzato un messaggio di errore, seguire le istruzioni suggerite visualizzate nella finestra di dialogo.

Sbloccare i dischi utilizzando una chiave di sicurezza

Se si spostano dischi abilitati alla protezione da un array di storage a un altro, è necessario importare la chiave di sicurezza appropriata nel nuovo array di storage. L'importazione della chiave consente di sbloccare i dati presenti sui dischi.

Prima di iniziare

- L'array di storage di destinazione (in cui si spostano i dischi) deve già disporre di una chiave di sicurezza configurata. I dischi migrati verranno ridimitati nell'array di storage di destinazione.
- È necessario conoscere la chiave di sicurezza associata ai dischi che si desidera sbloccare.
- Il file della chiave di sicurezza è disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Se si spostano i dischi in un array di storage gestito da un sistema diverso, è necessario spostare il file della chiave di sicurezza in quel client di gestione.

A proposito di questa attività

Questa attività descrive come sbloccare i dati in dischi abilitati alla sicurezza che sono stati rimossi da un array di storage e reinstallati in un altro. Una volta che l'array rileva i dischi, viene visualizzata una condizione di "attenzione necessaria" insieme allo stato "chiave di sicurezza necessaria" per questi dischi riposizionati. È possibile sbloccare i dati delle unità importando la chiave di sicurezza nell'array di storage. Durante questo processo, selezionare il file della chiave di sicurezza e immettere la password per la chiave.

La password non corrisponde alla password Administrator dell'array di storage.

Se nel nuovo array di storage sono installate altre unità abilitate alla protezione, potrebbero utilizzare una chiave di sicurezza diversa da quella che si sta importando. Durante il processo di importazione, la vecchia chiave di sicurezza viene utilizzata solo per sbloccare i dati dei dischi che si stanno installando. Quando il processo di sblocco ha esito positivo, i dischi appena installati vengono reinseriti nella chiave di sicurezza dell'array di storage di destinazione.

Fasi

1. Selezionare **Impostazioni › sistema**.

2. In **Security key management**, selezionare **Unlock Secure Drives**.

   Viene visualizzata la finestra di dialogo **Unlock Secure Drives**. Tutti i dischi che richiedono una chiave di sicurezza sono mostrati nella tabella.

3. In alternativa, passare il mouse su un numero di disco per visualizzare la posizione dell'unità (numero di shelf e numero di alloggiamento).
4. Fare clic su **Browse**, quindi selezionare il file della chiave di sicurezza corrispondente al disco che si desidera sbloccare.

   Il file delle chiavi selezionato viene visualizzato nella finestra di dialogo.

5. Inserire la password associata al file delle chiavi.

   I caratteri immessi vengono mascherati.

6. Fare clic su **Sblocca**.

   Se l'operazione di sblocco ha esito positivo, viene visualizzata la finestra di dialogo "i dischi protetti associati sono stati sbloccati".

Risultati

Quando tutti i dischi sono bloccati e quindi sbloccati, ogni controller nell'array di storage viene riavviato. Tuttavia, se nell'array di storage di destinazione sono già presenti alcuni dischi sbloccati, i controller non verranno riavviati.

FAQ

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.

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.

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. Completare e scaricare una CSR (Certificate Signing Request) client per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
4. Creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
5. Assicurarsi che il certificato client e una copia del certificato per il server di gestione delle chiavi siano disponibili sull'host locale.

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.

Perché è importante registrare le informazioni sulle chiavi di sicurezza?

Se si perdono le informazioni della chiave di sicurezza e non si dispone di un backup, si potrebbero perdere i dati durante la riassegnazione di dischi abilitati alla protezione o l'aggiornamento di un controller. È necessaria la chiave di sicurezza per sbloccare i dati sui dischi.

Assicurarsi di registrare l'identificatore della chiave di sicurezza, la password associata e la posizione sull'host locale in cui è stato salvato il file della chiave di sicurezza.

Cosa occorre sapere prima di eseguire il backup di una chiave di sicurezza?

Se la chiave di sicurezza originale viene danneggiata e non si dispone di un backup, l'accesso ai dati sui dischi viene perso se vengono migrati da uno storage array a un altro.

Prima di eseguire il backup di una chiave di sicurezza, tenere presenti le seguenti linee guida:

- Assicurarsi di conoscere l'identificatore della chiave di sicurezza e la password del file della chiave originale.

Solo le chiavi interne utilizzano identificatori. Quando è stato creato l'identificatore, sono stati generati automaticamente caratteri aggiuntivi e aggiunti ad entrambe le estremità della stringa di identificazione. I caratteri generati garantiscono che l'identificatore sia univoco.

- Viene creata una nuova password per il backup. Questa password non deve corrispondere alla password utilizzata al momento della creazione o dell'ultima modifica della chiave originale. La password viene applicata solo al backup che si sta creando.

La password per Drive Security non deve essere confusa con la password Administrator dell'array di storage. La password per Drive Security protegge i backup di una chiave di sicurezza. La password Administrator protegge l'intero array di storage da accessi non autorizzati.

- Il file della chiave di sicurezza di backup viene scaricato nel client di gestione. Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser. Assicurarsi di registrare la posizione in cui sono memorizzate le informazioni della chiave di sicurezza.

Cosa devo sapere prima di sbloccare dischi sicuri?

Per sbloccare i dati da un disco abilitato alla protezione che viene migrato a un nuovo array di storage, è necessario importare la chiave di sicurezza.

Prima di sbloccare dischi sicuri, tenere presenti le seguenti linee guida:

- L'array di storage di destinazione (in cui si spostano i dischi) deve disporre già di una chiave di sicurezza. I dischi migrati verranno ridimitati nell'array di storage di destinazione.
- Per i dischi che si stanno migrando, si conoscono l'identificatore della chiave di sicurezza e la password che corrisponde al file della chiave di sicurezza.
- Il file della chiave di sicurezza è disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager).

Che cos'è l'accessibilità in lettura/scrittura?

La finestra **Drive Settings** contiene informazioni sugli attributi **Drive Security**. "Read/Write Accessible" (lettura/scrittura accessibile) è uno degli attributi che viene visualizzato se i dati di un disco sono stati bloccati.

Per visualizzare gli attributi **Drive Security**, accedere alla pagina hardware. Selezionare un'unità, fare clic su **Visualizza impostazioni**, quindi fare clic su **Mostra altre impostazioni**. Nella parte inferiore della pagina, il valore dell'attributo Read/Write Accessible (lettura/scrittura accessibile) è **Yes** (Sì) quando il disco è sbloccato. Il valore dell'attributo lettura/scrittura accessibile è **No, chiave di sicurezza non valida** quando l'unità è bloccata. È possibile sbloccare un'unità sicura importando una chiave di sicurezza (accedere a **Impostazioni › sistema › Sblocca unità protette**).

Cosa occorre sapere sulla convalida della chiave di sicurezza?

Dopo aver creato una chiave di sicurezza, è necessario convalidare il file della chiave per assicurarsi che non sia corrotto.

Se la convalida non riesce, procedere come segue:

- Se l’identificatore della chiave di sicurezza non corrisponde all’identificatore sul controller, individuare il file della chiave di sicurezza corretto e riprovare la convalida.
- Se il controller non riesce a decrittare la chiave di sicurezza per la convalida, è possibile che la password sia stata inserita in modo errato. Controllare due volte la password, immetterla di nuovo se necessario, quindi riprovare a eseguire la convalida. Se il messaggio di errore viene visualizzato di nuovo, selezionare un backup del file delle chiavi (se disponibile) e riprovare la convalida.
- Se non si riesce ancora a convalidare la chiave di sicurezza, il file originale potrebbe essere danneggiato. Creare un nuovo backup della chiave e convalidare tale copia.

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).