Documentazione del software SANtricity 11.80

SANtricity 11.8

NetApp
April 05, 2024

Sommario

Documentazione del software SANtricity 11.80

Note di rilascio

Novità di SANtricity OS 11.80

La seguente tabella descrive le nuove funzionalità di Gestione di sistema di SANtricity 11.8.

Nuove funzionalità della versione 11.80

Nuova funzionalità	Descrizione
Enhanced Volume Parity Scan (scansione parity volume avanzata)	La scansione della parità del volume può ora essere avviata come processo in background tramite l'API REST o tramite CLI. La scansione di parità risultante viene eseguita in background per tutto il tempo necessario per completare l'operazione di scansione. Le operazioni di scansione sopravvivono ai riavvii del controller e alle operazioni di failover.
Supporto SAML per Unified Manager	Unified Manager ora supporta SAML (Security Assertion Markup Language). Una volta abilitato SAML per Unified Manager, gli utenti devono utilizzare l'autenticazione a più fattori rispetto al provider di identità per interagire con l'interfaccia utente. Una volta abilitato SAML su Unified Manager, l'API REST non può essere utilizzata senza passare attraverso IdP per autenticare le richieste.
Funzione di configurazione automatica	Ora supporta la possibilità di impostare il parametro delle dimensioni del blocco del volume da utilizzare con la funzione di configurazione automatica per la configurazione iniziale dell'array. Questa funzione è disponibile nella CLI solo come parametro "blocksize".
Firma crittografica del firmware del controller	Il firmware del controller è firmato crittograficamente. Le firme vengono controllate durante il download iniziale e ad ogni avvio del controller. Nessun impatto previsto per l'utente finale. Le firme sono supportate da un certificato Extended Validation emesso dalla CA.
Firma crittografica del firmware del disco	Il firmware del disco è firmato crittograficamente. Le firme vengono controllate durante il download iniziale e supportate da un certificato Extended Validation emesso dalla CA. Il contenuto del firmware del disco viene ora fornito come file ZIP, che contiene il firmware precedente non firmato e il nuovo firmware firmato. L'utente deve scegliere il file appropriato in base alla versione di rilascio del codice in esecuzione sul sistema di destinazione.

Nuova funzionalità	Descrizione

Gestione server chiavi esterne - dimensione chiave certificato	La nuova chiave di certificato predefinita è di 3072 bit (da 2048). Sono supportate dimensioni delle chiavi fino a 4096 bit. Un bit NVSRAM deve essere modificato per supportare le dimensioni delle chiavi non predefinite.
	
	I valori di selezione delle dimensioni chiave sono i seguenti:
	
	• VALORE PREDEFINITO = 0
	• LUNGHEZZA 2048 = 1
	• LUNGHEZZA 3072 = 2
	• LUNGHEZZA 4096 = 3
	
	Per modificare la dimensione della chiave in 4096 tramite SMcli:
	
	`set controller[b] globalnvsrambyte[0xc0]=3;`
	`set controller[a] globalnvsrambyte[0xc0]=3;`
	
	Interrogare le dimensioni della chiave:
	
	`show allcontrollers globalnvsrambyte[0xc0];`

Miglioramenti dei pool di dischi	I pool di dischi creati con i controller che eseguono la versione 11,80 o superiore saranno *pool versione 1* anziché *pool versione 0*. Un'operazione di downgrade è limitata quando esiste un pool di dischi *versione 1*. La versione di un pool di dischi può essere identificata nel profilo dell'array di storage.
System Manager e Unified Manager non verranno lanciati a meno che non vengano soddisfatti i requisiti minimi del browser	È necessaria una versione minima del browser prima dell'avvio di System Manager o di Unified Manager. Di seguito sono riportate le versioni minime supportate: • Firefox versione minima 80 • Chrome versione minima 89 • Edge versione minima 90 • Safari versione minima 14
Supporto per unità SSD FIPS 140-3 NVMe	Sono ora supportati i dischi SSD NVMe FIPS 140-3 certificati NetApp. Verranno identificati correttamente come tali nel profilo dello storage array e in System Manager.
Supporto della cache di lettura SSD su EF300 e EF600	La cache di lettura SSD è ora supportata sui controller EF300 e EF600 che utilizzano HDD con un'espansione SAS.

Nuova funzionalità	Descrizione
Supporto del mirroring remoto asincrono iSCSI e Fibre Channel su EF300 e EF600	Il mirroring remoto asincrono (ARVM) è ora supportato sui controller EF300 e EF600 con volumi basati su NVMe e SAS.
Supporto di EF300 e EF600 senza unità sul vassoio di base	Sono ora supportate le configurazioni dei controller EF300 e EF600 senza unità NVMe sul vassoio di base.
Porte USB disattivate per tutte le piattaforme	Le porte USB sono ora disabilitate su tutte le piattaforme.

Note di rilascio

Le Note sulla versione sono disponibili al di fuori di questo sito. Ti verrà richiesto di effettuare l'accesso utilizzando le credenziali del sito di supporto NetApp.

- "11.80 Note di rilascio"
- "11.70 Note di rilascio"
- "11.60 Note di rilascio"
- "11.50 Note di rilascio"

Inizia subito

Panoramica del software SANtricity

I sistemi e-Series includono il software SANtricity per il provisioning dello storage e altre attività.

Questo sito descrive come utilizzare le seguenti interfacce di gestione SANtricity:

- System Manager - interfaccia basata su Web utilizzata per gestire un singolo array di storage nella rete.
- Unified Manager: Interfaccia basata su web utilizzata per visualizzare e gestire tutti gli array di storage della rete.

Gli storage array EF600 e EF300 non supportano il mirroring sincrono o i thin volumi.

Gestore di sistema di SANtricity

System Manager è un software di gestione basato su web integrato in ciascun controller. Per accedere all'interfaccia utente, puntare un browser verso l'indirizzo IP del controller. L'installazione guidata consente di iniziare a configurare il sistema.

System Manager offre una vasta gamma di funzionalità di gestione, tra cui:

Prestazioni
Visualizza fino a 30 giorni di dati sulle performance, tra cui latenza di i/o, IOPS, utilizzo della CPU e throughput.
Storage
Eseguire il provisioning dello storage utilizzando pool o gruppi di volumi e creare carichi di lavoro delle applicazioni.
Protezione dei dati
Eseguire backup e disaster recovery utilizzando snapshot, copia del volume e mirroring remoto.

Hardware
Controllare lo stato dei componenti ed eseguire alcune funzioni correlate a tali componenti, ad esempio l'assegnazione di dischi hot spare.
Avvisi
Avvisare gli amministratori degli eventi importanti che si verificano sullo storage array. Gli avvisi possono essere inviati tramite e-mail, trap SNMP e syslog.
Gestione degli accessi
Configurare l'autenticazione dell'utente che richiede agli utenti di accedere al sistema con le credenziali assegnate.
Impostazioni di sistema
Configurare altre funzionalità delle performance di sistema, come la cache SSD e il bilanciamento del carico automatico.
Supporto
Visualizza i dati diagnostici, gestisci gli aggiornamenti e configura AutoSupport, che monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.

Gestore unificato SANtricity

Unified Manager è un software basato sul web utilizzato per gestire l'intero dominio. Da una vista centrale, è possibile visualizzare lo stato di tutti gli array e-Series ed EF-Series più recenti, come E2800, EF280, EF300, E5700, EF570, E EF600. È inoltre possibile eseguire operazioni batch su array di storage selezionati.

Unified Manager viene installato su un server di gestione insieme al proxy dei servizi Web. Per accedere a Unified Manager, aprire un browser e immettere l'URL che punta al server in cui è installato il proxy dei servizi

Web.

Unified Manager offre una vasta gamma di funzionalità di gestione, tra cui:

Rilevare gli array di storage
Trova e Aggiungi gli array di storage che desideri gestire nella rete aziendale. È quindi possibile visualizzare lo stato di tutti gli array di storage da una singola pagina.
Lancio
Aprire un'istanza di System Manager per eseguire singole operazioni di gestione su un determinato array di storage.
Impostazioni di importazione
Eseguire un'importazione in batch da uno storage array a più array, incluse le impostazioni per gli avvisi, AutoSupport e i servizi di directory.
Mirroring
Configurare coppie di mirroring asincrone o sincrono tra due array di storage.
Gestisci gruppi
Organizza gli array di storage in gruppi per una gestione più semplice.

Upgrade Center
Aggiornare il software del sistema operativo SANtricity su più array di storage.
Certificati
Creare richieste di firma del certificato (CSR), importare certificati e gestire i certificati esistenti per più array di storage.
Gestione degli accessi
Configurare l'autenticazione dell'utente che richiede agli utenti di accedere a Unified Manager con le credenziali assegnate.

Browser e sistemi operativi supportati

Il software SANtricity supporta diversi tipi di browser e sistemi operativi.

Browser

Sono supportati i seguenti browser e versioni.

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

Per Unified Manager, il proxy dei servizi Web deve essere installato e disponibile nel browser. Per ulteriori informazioni, vedere "Panoramica dei proxy dei servizi web SANtricity"

Sistemi operativi

Sono supportati i seguenti sistemi operativi e versioni.

Sistema operativo	Versione/architettura minima
Red Hat Enterprise Linux (RHEL)	7.x, 8.x / 64 bit
SUSE Linux Enterprise Server (SLES)	12.x, 15.x / 64 bit
Oracle Linux (OL)	7.x, 8.x / 64 bit
Server Windows	2016, 2019, 2022 / 64 bit
Ubuntu	18.04, 20.04 / 64 bit

Configurazione di System Manager

Accedere a System Manager

Per accedere all'interfaccia utente di System Manager, puntare un browser verso l'indirizzo IP del controller. L'installazione guidata consente di iniziare a configurare il sistema.

Prima di iniziare

- Installare e configurare l'hardware, come descritto in una delle guide di configurazione rapide:
  - "Configurazione di Linux Express"
  - "Configurazione di VMware Express"
  - "Configurazione di Windows Express"
- Configurare una stazione di gestione che soddisfi i seguenti requisiti:
  - Connesso a una rete a 1 Gbps o più veloce.
  - Collegato alla stessa subnet delle porte di gestione dello storage.
  - Utilizzato come stazione separata, anziché come host (i/o collegato) utilizzato per la gestione dei dati.
  - Configurazione per la gestione out-of-band, in cui una stazione di gestione dello storage invia comandi al sistema di storage attraverso le connessioni Ethernet al controller.
  - Configurazione con un browser supportato. Vedere "Browser e sistemi operativi supportati".

Fasi

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

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

   La prima volta che System Manager viene aperto su un array non configurato, viene visualizzato il prompt Set Administrator Password (Imposta password amministratore).

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

   L'installazione guidata viene avviata al primo accesso.

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

Per ulteriori informazioni sull'installazione guidata, vedere "Panoramica dell'installazione guidata".

Panoramica dell'installazione guidata

Utilizzare la procedura guidata di installazione per configurare lo storage array, inclusi hardware, host, applicazioni, carichi di lavoro, Pool, avvisi e AutoSupport.

Configurazione iniziale

Quando si apre System Manager per la prima volta, viene avviata l'installazione guidata. L'installazione guidata richiede di eseguire le attività di configurazione di base, ad esempio assegnare un nome allo storage array, configurare gli host, selezionare le applicazioni e creare pool di storage.

> Prima di continuare con la configurazione iniziale, accedere al Centro aggiornamenti (**supporto › Centro aggiornamenti**) e assicurarsi che il software del sistema operativo SANtricity sia aggiornato. Se necessario, eseguire l'aggiornamento alla versione più recente e aggiornare il browser per continuare la configurazione. Per ulteriori informazioni, vedere "Panoramica di Upgrade Center".

Se si annulla la procedura guidata, non è possibile avviarla di nuovo manualmente. La procedura guidata viene riavviata automaticamente quando si apre System Manager o si aggiorna il browser e viene soddisfatta almeno una delle seguenti condizioni:

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

Terminologia

L'installazione guidata utilizza i seguenti termini.

Termine	Descrizione
Applicazione	Un'applicazione è un programma software, ad esempio Microsoft SQL Server o Microsoft Exchange.

Termine	Descrizione
Avviso	Gli avvisi informano gli amministratori degli eventi importanti che si verificano sugli array di storage. Gli avvisi possono essere inviati tramite e-mail, trap SNMP o syslog.
AutoSupport	La funzione AutoSupport monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.
Hardware	L'hardware del sistema storage include array di storage, controller e dischi.
Host	Un host è un server che invia i/o a un volume su un array di storage.
Oggetto	Un oggetto è qualsiasi componente di storage logico o fisico. Gli oggetti logici includono gruppi di volumi, pool e volumi. Gli oggetti fisici includono lo storage array, gli array controller, gli host e i dischi.
Piscina	Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all'host di accedere allo storage sull'array di storage. Un volume viene creato dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Anche se un volume può essere costituito da più di un disco, un volume viene visualizzato come un componente logico per l'host.
Gruppo di volumi	Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.
Carico di lavoro	Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

FAQ

Cosa succede se non vengono visualizzati tutti i componenti hardware?

Se non vengono visualizzati tutti i componenti hardware nella finestra di dialogo Verify

hardware (verifica hardware), potrebbe indicare che uno shelf di dischi non è collegato correttamente o che uno shelf incompatibile è installato nell'array di storage.

Verificare che tutti gli shelf di dischi siano collegati correttamente. In caso di dubbi sulla compatibilità degli shelf di dischi, contattare il supporto tecnico.

Cosa succede se non vengono visualizzati tutti gli host?

Se gli host connessi non vengono visualizzati, il rilevamento automatico non è riuscito, gli host non sono collegati correttamente o non sono connessi host.

Una volta completata la configurazione, è possibile configurare gli host in un secondo momento. È possibile creare gli host automaticamente o manualmente come segue:

- Se è stato installato l'HCA (host Context Agent) sugli host, l'HCA invia le informazioni di configurazione dell'host all'array di storage. System Manager configura automaticamente questi host e li visualizza nell'installazione guidata iniziale. (HCA non si applica agli host NVMe over Fabrics).
- È possibile creare manualmente gli host e associare gli identificatori di porta host appropriati accedendo al **Storage › hosts**. Gli host creati manualmente vengono visualizzati anche nella procedura guidata **Initial Setup**.
- La destinazione e l'host devono essere configurati per il tipo di porta host (ad esempio, iSCSI o NVMe su RoCE) e una sessione per lo storage stabilita prima che il rilevamento automatico funzioni.

In che modo l'identificazione delle applicazioni mi aiuta a gestire lo storage array?

Quando si identificano le applicazioni, System Manager consiglia automaticamente una configurazione del volume che ottimizza lo storage in base al tipo di applicazione.

L'ottimizzazione dei volumi per applicazione può rendere più efficienti le operazioni di storage dei dati. Caratteristiche come il tipo di i/o, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume. Inoltre, è possibile visualizzare i dati delle performance per applicazione e per carico di lavoro per valutare la latenza, gli IOPS e i MiB/s delle applicazioni e i carichi di lavoro associati.

Che cos'è un carico di lavoro?

Per alcune applicazioni della rete, ad esempio SQL Server o Exchange, è possibile definire un carico di lavoro che ottimizzi lo storage per tale applicazione.

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

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

Come si configura il metodo di consegna per AutoSupport?

Per accedere alle attività di configurazione per i metodi di erogazione AutoSupport, accedere al **supporto › Centro di assistenza**, quindi fare clic sulla scheda **AutoSupport**.

Sono supportati i seguenti protocolli: HTTPS, HTTP e SMTP.

Come posso sapere se devo accettare la configurazione del pool consigliata?

L'accettazione della configurazione del pool consigliata dipende da alcuni fattori.

Determinare il tipo di storage più adatto alle proprie esigenze rispondendo alle seguenti domande:

- Preferisci più pool di capacità inferiori, invece dei pool più grandi possibili?
- Preferisci i gruppi di volumi RAID rispetto ai pool?
- Preferisci eseguire il provisioning manuale dei dischi, invece di avere una configurazione consigliata per te?

Se hai risposto Sì a una di queste domande, puoi rifiutare la configurazione del pool consigliata.

System Manager non ha rilevato alcun host. Cosa devo fare?

Se gli host connessi non vengono visualizzati, il rilevamento automatico non è riuscito, gli host non sono collegati correttamente o non sono connessi host.

Una volta completata la configurazione, è possibile configurare gli host in un secondo momento. È possibile creare gli host automaticamente o manualmente come segue:

- Se è stato installato l'HCA (host Context Agent) sugli host, l'HCA invia le informazioni di configurazione dell'host all'array di storage. System Manager configura automaticamente questi host e li visualizza nella procedura guidata **Initial Setup**. (HCA non si applica agli host NVMe over Fabrics).
- È possibile creare manualmente gli host e associare gli identificatori di porta host appropriati accedendo al **Storage › hosts**. Gli host creati manualmente vengono visualizzati anche nella procedura guidata **Initial Setup**.
- La destinazione e l'host devono essere configurati per il tipo di porta host (ad esempio, iSCSI o NVMe su RoCE) e una sessione per lo storage stabilita prima che il rilevamento automatico funzioni.

Configurazione di Unified Manager

Installare Unified Manager

Unified Manager è incluso nel proxy dei servizi Web, un server API RESTful installato separatamente su un sistema host per gestire i sistemi storage NetApp e-Series.

Per installare il proxy dei servizi Web e Unified Manager, consultare le seguenti istruzioni nel centro di documentazione di e-Series e SANtricity:

1. "Verifica dei requisiti di installazione e aggiornamento"

2. "Scaricare e installare il file proxy dei servizi Web"

Accedi a Unified Manager

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

> Per i browser supportati, vedere "Browser e sistemi operativi supportati".

Fasi

1. Aprire un browser e immettere il seguente URL:

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

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

   Viene visualizzata la pagina di accesso a Unified Manager.

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

   La password può contenere fino a 30 caratteri.

Per ulteriori informazioni su utenti e password, vedere "Come funziona Access Management".

Gestione di un singolo array con System Manager 11.8

Interfaccia principale

Panoramica dell'interfaccia di System Manager

System Manager è un'interfaccia basata su Web che consente di gestire un array di storage in una singola vista.

Pagina iniziale

La home page fornisce una vista dashboard per la gestione quotidiana dello storage array. Quando si accede a System Manager, viene visualizzata la prima pagina iniziale.

La vista dashboard comprende quattro aree di riepilogo che contengono informazioni chiave sullo stato e lo stato dello storage array. Ulteriori informazioni sono disponibili nell'area di riepilogo.

Area	Descrizione
Notifiche	L'area Notifiche visualizza le notifiche dei problemi che indicano lo stato dello storage array e dei relativi componenti. Inoltre, questo portlet visualizza avvisi automatici che consentono di risolvere i problemi prima che influiscano su altre aree dell'ambiente di storage.
Performance	L'area Performance (prestazioni) consente di confrontare e confrontare l'utilizzo delle risorse nel tempo. È possibile visualizzare le metriche delle performance di uno storage array per i tempi di risposta (IOPS), le velocità di trasferimento (MiB/s) e la quantità di capacità di elaborazione utilizzata (CPU).
Capacità	L'area Capacity (capacità) visualizza una vista a grafico della capacità allocata, della capacità di storage libera e della capacità di storage non assegnata nell'array di storage.
Gerarchia dello storage	L'area Storage Hierarchy (gerarchia di storage) offre una vista organizzata dei vari componenti hardware e oggetti storage gestiti dallo storage array. Fare clic sulla freccia a discesa per eseguire una determinata azione sul componente hardware o sull'oggetto di storage.

Impostazioni dell'interfaccia

È possibile modificare le preferenze di visualizzazione e altre impostazioni dall'interfaccia principale.

Impostazione	Descrizione
Visualizzare le preferenze	Modificare i valori di capacità e i tempi dal menu a discesa Preferences (Preferenze) nell'angolo superiore destro dell'interfaccia.

Impostazione	Descrizione
Timeout della sessione	Configurare i timeout in modo che le sessioni inattive degli utenti vengano disconnesse dopo un determinato periodo di tempo.
Aiuto	Accedere alla documentazione della Guida e ad altre risorse dal menu a discesa nell'angolo superiore destro dell'interfaccia.

Login e password degli utenti

L'utente corrente che ha effettuato l'accesso al sistema viene visualizzato nella parte superiore destra dell'interfaccia.

Per ulteriori informazioni su utenti e password, consulta:

- "Impostare la protezione della password amministratore"
- "Modificare le password"

Visualizzare i dati sulle performance

Panoramica delle performance

La pagina Performance (prestazioni) offre semplici metodi per monitorare le performance dello storage array.

Cosa si può imparare dai dati sulle performance?

I grafici e le tabelle delle performance mostrano i dati delle performance quasi in tempo reale, consentendo di determinare se un array di storage sta riscontrando problemi. È inoltre possibile salvare i dati sulle performance per creare una vista storica di un array di storage e identificare quando si è verificato un problema o cosa ne ha causato uno.

Scopri di più:

- "Grafici delle performance e linee guida"
- "Termini di performance"

Come posso visualizzare i dati sulle performance?

I dati relativi alle performance sono disponibili nella home page e nella pagina Storage.

Scopri di più:

- "Visualizzare i dati delle performance grafiche"
- "Visualizzare e salvare i dati delle performance in formato tabulare"
- "Interpretare i dati delle performance"

Grafici delle performance e linee guida

La pagina Performance fornisce grafici e tabelle di dati che consentono di valutare le

performance dello storage array in diverse aree chiave.

Le funzioni delle performance consentono di eseguire queste attività:

- Visualizzare i dati delle performance quasi in tempo reale per determinare se si verificano problemi in un array di storage.
- Esportare i dati delle performance per creare una vista storica di un array di storage e identificare quando si è verificato un problema o cosa ne ha causato.
- Seleziona gli oggetti, le metriche delle performance e il periodo di tempo che desideri visualizzare.
- Confronta le metriche.

È possibile visualizzare i dati delle performance in tre formati:

- **Grafico in tempo reale** — traccia i dati delle performance su un grafico quasi in tempo reale.
- **Near real-time tabular** — Elenca i dati delle performance in una tabella in quasi real-time.
- **File CSV esportato** — consente di salvare i dati delle performance tabulari in un file di valori separati da virgole per ulteriori visualizzazioni e analisi.

Caratteristiche dei formati di dati delle performance

Tipo di monitoraggio delle performance	Intervallo di campionamento	Durata visualizzata	Numero massimo di oggetti visualizzati	Possibilità di salvare i dati
Grafico in tempo reale, live Grafico in tempo reale, storico	10 sec (live) 5 min (storico) I punti dati visualizzati dipendono dall'intervallo di tempo selezionato	L'intervallo di tempo predefinito è di 1 ora. Scelte: • 5 minuti • 1 ora • 8 ore • 1 giorno • 7 giorni • 30 giorni	5	No
Tabulare quasi in tempo reale (vista tabella)	10 sec - 1 ora	Valore più recente	Senza limiti	Sì
File CSV (comma-Separated Values)	Dipende dall'intervallo di tempo selezionato	Dipende dall'intervallo di tempo selezionato	Senza limiti	Sì

Linee guida per la visualizzazione dei dati sulle performance

- La raccolta dei dati sulle performance è sempre attiva. Non esiste alcuna opzione per disattivarla.

- Ogni volta che trascorre l’intervallo di campionamento, viene eseguita una query sull’array di storage e i dati vengono aggiornati.
- Per i dati grafici, l’intervallo di tempo di 5 minuti supporta un aggiornamento di 10 secondi in media in 5 minuti. Tutti gli altri frame temporali vengono aggiornati ogni 5 minuti, mediati nel periodo di tempo selezionato.
- I dati delle performance nelle viste grafiche vengono aggiornati in tempo reale. I dati delle performance nella vista tabella vengono aggiornati quasi in tempo reale.
- Se un oggetto monitorato cambia durante il tempo in cui vengono raccolti i dati, l’oggetto potrebbe non avere un set completo di punti di dati che coprono l’intervallo di tempo selezionato. Ad esempio, i set di volumi possono cambiare man mano che i volumi vengono creati, cancellati, assegnati o non assegnati, oppure è possibile aggiungere, rimuovere o non eseguire l’operazione.

Terminologia relativa alle performance

Scopri in che modo i termini relativi alle performance si applicano al tuo storage array.

Termine	Descrizione
Applicazione	Un’applicazione è un programma software, ad esempio SQL o Exchange.
CPU	CPU è l’abbreviazione di "Central Processing Unit" (unità di elaborazione centrale). CPU indica la percentuale della capacità di elaborazione dello storage array utilizzata.
Host	Un host è un server che invia i/o a un volume su un array di storage.
IOPS	IOPS è l’acronimo di Input/Output Operations per Second (operazioni di input/output al secondo).
Latenza	La latenza è l’intervallo di tempo che intercorre tra una richiesta, ad esempio per un comando di lettura o scrittura, e la risposta dall’host o dall’array di storage.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all’host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi.
MIB	MIB è l’abbreviazione di mebibyte (mega byte binari). Un MiB è di 220 o 1,048,576 byte. Confrontare con MB, che indica un valore di base 10. Un MB equivale a 1,024 byte.
Oggetto	Un oggetto è qualsiasi componente di storage logico o fisico. Gli oggetti logici includono gruppi di volumi, pool e volumi. Gli oggetti fisici includono lo storage array, gli array controller, gli host e i dischi.

Termine	Descrizione
Piscina	Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.
Leggi	Read è l'abbreviazione di "Read Operation" (operazione di lettura), che si verifica quando l'host richiede dati dall'array di storage.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all'host di accedere allo storage sull'array di storage. Un volume viene creato dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Anche se un volume può essere costituito da più di un disco, un volume viene visualizzato come un componente logico per l'host.
Nome del volume	Il nome di un volume è una stringa di caratteri assegnata al volume al momento della creazione. È possibile accettare il nome predefinito o fornire un nome più descrittivo che indichi il tipo di dati memorizzati nel volume.
Gruppo di volumi	Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.
Carico di lavoro	Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.
Di scrittura	Write è l'abbreviazione di "write operation" (operazione di scrittura) quando i dati vengono inviati dall'host all'array per lo storage.

Visualizzare i dati delle performance grafiche

È possibile visualizzare i dati delle performance grafiche per oggetti logici, oggetti fisici, applicazioni e carichi di lavoro.

A proposito di questa attività

I grafici delle performance mostrano i dati storici e i dati in tempo reale attualmente acquisiti. Una linea verticale sul grafico, denominata Live Updating, distingue i dati storici dai dati in tempo reale.

Vista home page

La home page contiene un grafico che mostra le performance a livello di array di storage. Da questa vista è possibile selezionare metriche limitate oppure fare clic su **View Performance Details** (Visualizza dettagli performance) per selezionare tutte le metriche disponibili.

Vista dettagliata

I grafici disponibili nella vista delle performance dettagliate sono disposti in tre schede:

- **Vista logica** — Visualizza i dati delle performance per gli oggetti logici raggruppati per gruppi di volumi e pool. Gli oggetti logici includono gruppi di volumi, pool e volumi.
- **Physical View** — Visualizza i dati relativi alle performance per controller, canali host, canali di dischi e dischi.
- **Visualizzazione applicazioni e carichi di lavoro** — Visualizza un elenco di oggetti logici (volumi) raggruppati in base ai tipi di applicazioni e ai carichi di lavoro definiti.

Fasi

1. Selezionare **Home**.
2. Per selezionare una vista a livello di array, fare clic sul pulsante IOPS, MiB/s o CPU.
3. Per ulteriori informazioni, fare clic su **Visualizza dettagli sulle prestazioni**.
4. Selezionare la scheda **Vista logica**, la scheda **Vista fisica** o la scheda **Vista applicazioni e carichi di lavoro**.

   A seconda del tipo di oggetto, in ciascuna scheda vengono visualizzati diversi grafici.

Visualizza schede	Dati relativi alle performance visualizzati per ciascun tipo di oggetto
Vista logica	• **Storage array**: IOPS, MiB/s. • **Pools**: Latenza, IOPS, MiB/s. • **Gruppi di volumi**: Latenza, IOPS, MiB/s. • **Volumi**: Latenza, IOPS, MiB/s.
Vista fisica	• **Controller**: IOPS, MiB/s, CPU, spazio di crescita • **Canali host**: Latenza, IOPS, MiB/s, spazio di crescita • **Drive channels**: Latenza, IOPS, MiB/s. • **Dischi**: Latenza, IOPS, MiB/s.
Applicazioni e carichi di lavoro Visualizza	• **Storage array**: IOPS, MiB/s. • **Applicazioni**: Latenza, IOPS, MiB/s. • **Carichi di lavoro**: Latenza, IOPS, MiB/s. • **Volumi**: Latenza, IOPS, MiB/s.

5. Utilizzare le opzioni per visualizzare gli oggetti e le informazioni necessarie.

Opzioni

Opzioni per la visualizzazione degli oggetti	Descrizione
Espandere un cassetto per visualizzare l'elenco degli oggetti.	I *cassetti di navigazione* contengono oggetti di storage, come pool, gruppi di volumi e unità. Fare clic sul cassetto per visualizzare l'elenco degli oggetti nel cassetto.
Selezionare gli oggetti da visualizzare.	Selezionare la casella di controllo a sinistra di ciascun oggetto per scegliere i dati delle prestazioni da visualizzare.
Utilizzare Filter per trovare nomi di oggetti o nomi parziali.	Nella casella Filter (filtro), immettere il nome o un nome parziale degli oggetti per elencare solo gli oggetti presenti nel cassetto.
Fare clic su **Aggiorna grafici** dopo aver selezionato gli oggetti.	Dopo aver selezionato gli oggetti dai cassetti, selezionare **Aggiorna grafici** per visualizzare i dati grafici degli elementi selezionati.
Nascondere o mostrare il grafico	Selezionare il titolo del grafico per nasconderlo o visualizzarlo.

6. Se necessario, utilizzare le opzioni aggiuntive per visualizzare i dati delle performance.

Opzioni aggiuntive

Opzione	Descrizione
Intervallo di tempo	Selezionare il periodo di tempo che si desidera visualizzare (5 minuti, 1 ora, 8 ore, 1 giorno, 7 giorni, o 30 giorni). L'impostazione predefinita è 1 ora. Il caricamento dei dati delle performance per un periodo di 30 giorni può richiedere diversi minuti. Non allontanarsi dalla pagina Web, aggiornare la pagina Web o chiudere il browser durante il caricamento dei dati.
Dettagli dei data point	Posizionare il cursore del mouse sul grafico per visualizzare le metriche relative a un particolare punto dati.
Barra di scorrimento	Utilizzare la barra di scorrimento sotto il grafico per visualizzare un intervallo di tempo precedente o successivo.
Barra di zoom	Sotto il grafico, trascinare le maniglie della barra di zoom per ridurre l'intervallo di tempo. Più ampia è la barra di zoom, meno granulari sono i dettagli del grafico. Per ripristinare il grafico, selezionare una delle opzioni relative all'intervallo di tempo.
Trascinare e rilasciare	Sul grafico, trascinare il cursore da un punto temporale all'altro per ingrandire un intervallo di tempo. Per ripristinare il grafico, selezionare una delle opzioni relative all'intervallo di tempo.

Visualizzare e salvare i dati delle performance in formato tabulare

È possibile visualizzare e salvare i dati dei grafici delle prestazioni in formato tabulare. In questo modo è possibile filtrare i dati che si desidera visualizzare.

Fasi

1. Da qualsiasi grafico dei dati delle performance, fare clic su **Avvia vista tabella**.

   Viene visualizzata una tabella che elenca tutti i dati relativi alle prestazioni per gli oggetti selezionati.

2. Utilizzare il menu a discesa Object selection (selezione oggetto) e il filtro secondo necessità.
3. Fare clic sul pulsante **Mostra/Nascondi colonne** per selezionare le colonne da includere nella tabella.

   È possibile fare clic su ciascuna casella di controllo per selezionare o deselezionare un elemento.

4. Selezionare **Export** (Esporta) nella parte inferiore della schermata per salvare la vista tabulare in un file di valori separati da virgola (CSV).

Viene visualizzata la finestra di dialogo Export Table (Esporta tavola), che indica il numero di righe da esportare e il formato del file da esportare (valori separati da virgole o formato CSV).

5. Fare clic su **Export** (Esporta) per procedere con il download oppure fare clic su **Cancel** (Annulla).

   A seconda delle impostazioni del browser, il file viene salvato oppure viene richiesto di scegliere un nome e una posizione per il file.

   Il formato predefinito del nome file è `performanceStatistics-yyyy-mm-dd_hh-mm-ss.csv`, che include la data e l'ora in cui il file è stato esportato.

Interpretare i dati delle performance

I dati sulle performance possono aiutarti a ottimizzare le performance del tuo storage array.

Quando si interpretano i dati sulle performance, tenere presente che diversi fattori influiscono sulle performance dello storage array. La seguente tabella descrive le aree principali da considerare.

Dati sulle performance	Implicazioni per l'ottimizzazione delle performance
Latenza (millisecondi o ms)	Monitorare l'attività di i/o di un oggetto specifico. Identificare potenzialmente gli oggetti che sono colli di bottiglia: • Se un gruppo di volumi viene condiviso tra diversi volumi, i singoli volumi potrebbero aver bisogno di gruppi di volumi propri per migliorare le performance sequenziali dei dischi e ridurre la latenza. • Con i pool, vengono introdotte latenze maggiori e potrebbero esistere carichi di lavoro irregolari tra i dischi, rendendo i valori di latenza meno significativi e, in generale, più elevati. • Il tipo di disco e la velocità influenzano la latenza. Con l'i/o casuale, i dischi a rotazione più rapida trascorrono meno tempo a spostarsi da e verso diverse posizioni del disco. • Un numero eccessivo di dischi determina un maggior numero di comandi in coda e un periodo di tempo maggiore per l'elaborazione del comando da parte del disco, aumentando la latenza generale del sistema. • I/o più grandi hanno una maggiore latenza grazie al tempo aggiuntivo richiesto per il trasferimento dei dati. • Una latenza maggiore potrebbe indicare che il modello di i/o è casuale. I dischi con i/o random avranno una latenza maggiore rispetto a quelli con flussi sequenziali. • Una disparità di latenza tra dischi o volumi di un gruppo di volumi comune potrebbe indicare un disco lento.

Dati sulle performance	Implicazioni per l'ottimizzazione delle performance
IOPS	I fattori che influiscono sulle operazioni di input/output al secondo (IOPS o iOS/sec) includono i seguenti elementi: • Schema di accesso (casuale o sequenziale) • Dimensione i/O. • Livello RAID • Dimensione del blocco della cache • Se il caching in lettura è attivato • Se il caching in scrittura è attivato • Prefetch di lettura della cache dinamica • Dimensione del segmento • Il numero di dischi nei gruppi di volumi o nell'array di storage Maggiore è il tasso di hit della cache, maggiori saranno i tassi di i/O. Con il caching in scrittura attivato si riscontrano velocità di i/o in scrittura più elevate rispetto a quelle disattivate. Per decidere se attivare il caching in scrittura per un singolo volume, esaminare gli IOPS correnti e il numero massimo di IOPS. Per i modelli di i/o sequenziali dovrebbero essere visualizzate velocità più elevate rispetto ai modelli di i/o random. Indipendentemente dal modello di i/o, abilitare il caching in scrittura per massimizzare la velocità di i/o e ridurre i tempi di risposta dell'applicazione. È possibile vedere i miglioramenti delle performance causati dalla modifica delle dimensioni dei segmenti nelle statistiche IOPS di un volume. Provare a determinare la dimensione ottimale del segmento oppure utilizzare la dimensione del file system o del blocco del database.
MIB/s	Le velocità di trasferimento o di throughput sono determinate dalla dimensione i/o dell'applicazione e dalla velocità di i/O. In genere, le richieste di i/o delle applicazioni di piccole dimensioni comportano una velocità di trasferimento inferiore, ma forniscono una velocità di i/o più rapida e tempi di risposta più brevi. Con richieste di i/o applicative più ampie, è possibile ottenere velocità di throughput più elevate. La comprensione dei modelli di i/o tipici delle applicazioni consente di determinare le velocità massime di trasferimento i/o per uno specifico array di storage.

Dati sulle performance	Implicazioni per l'ottimizzazione delle performance
CPU	Questo valore è una percentuale della capacità di elaborazione utilizzata. Si potrebbe notare una disparità nell'utilizzo della CPU degli stessi tipi di oggetti. Ad esempio, l'utilizzo della CPU di un controller è pesante o aumenta nel tempo, mentre quello dell'altro controller è più leggero o più stabile. In questo caso, è possibile modificare la proprietà del controller di uno o più volumi nel controller con la percentuale di CPU inferiore. Si consiglia di monitorare la CPU nell'array di storage. Se la CPU continua ad aumentare nel tempo mentre le performance delle applicazioni diminuiscono, potrebbe essere necessario aggiungere array di storage. Aggiungendo array di storage alla tua azienda, puoi continuare a soddisfare le esigenze applicative a un livello di performance accettabile.
Spazio di crescita	Per spazio di crescita si intende la capacità di performance residua dei controller, dei canali host del controller e dei canali del disco del controller. Questo valore viene espresso in percentuale e rappresenta il divario tra le massime performance possibili che questi oggetti sono in grado di offrire e i livelli di performance correnti. • Per i controller, lo spazio di crescita è una percentuale degli IOPS massimi possibili. • Per i canali, lo spazio di crescita è una percentuale del throughput massimo, o MiB/s. Il throughput in lettura, il throughput in scrittura e il throughput bidirezionale sono inclusi nel calcolo.

Visualizza la gerarchia dello storage

La gerarchia di storage sull'interfaccia principale fornisce una vista organizzata dei vari componenti hardware e oggetti storage gestiti dall'array di storage.

Per visualizzare la gerarchia dello storage, accedere alla home page e fare clic sulla freccia a discesa di un componente o di un oggetto storage dell'array di storage. Un array di storage è costituito da un insieme di componenti fisici e logici.

Componenti fisici

I componenti fisici di un array di storage sono descritti in questa tabella.

Componente	Descrizione
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di System Manager.

Componente	Descrizione
Shelf	Uno shelf è un enclosure installato in un cabinet o in un rack. Contiene i componenti hardware per lo storage array. Esistono due tipi di shelf: Uno shelf di controller e uno shelf di dischi. Uno shelf di controller include controller e dischi. Uno shelf di dischi include i moduli di input/output (IOM) e i dischi. Se lo storage array contiene tipi di supporti diversi o tipi di interfaccia diversi, viene visualizzato uno shelf di dischi per ciascun tipo di disco.
Disco	Un disco è un dispositivo elettromeccanico o un dispositivo di memoria a stato solido che fornisce il supporto di storage fisico per i dati.
Host	Un host è un server che invia i/o a un volume su un array di storage.
HBA (host bus adapter)	Un HBA (host bus adapter) è una scheda che risiede in un host e contiene una o più porte host.
Porta host	Una porta host è una porta di un HBA (host Bus Adapter) che fornisce la connessione fisica a un controller e viene utilizzata per le operazioni di i/O.
Client di gestione	Un client di gestione è il computer in cui è installato un browser per accedere a System Manager.

Componenti logici

I dischi dell'array di storage forniscono la capacità fisica dello storage per i dati. Utilizzare System Manager per configurare la capacità fisica in componenti logici, come pool, gruppi di volumi e volumi. Questi componenti sono gli strumenti utilizzati per configurare, memorizzare, gestire e conservare i dati sull'array di storage. I componenti logici di un array di storage sono descritti in questa tabella.

Componente	Descrizione
Piscina	Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.
Gruppo di volumi	Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all'host di accedere allo storage sull'array di storage.

Componente	Descrizione
LUN (Logical Unit Number)	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi.

Gestire le impostazioni dell'interfaccia

Gestire la protezione tramite password

È necessario configurare lo storage array con password per proteggerlo da accessi non autorizzati.

Impostare e modificare le password

Quando si avvia System Manager per la prima volta, viene richiesto di impostare una password di amministratore. Qualsiasi utente in possesso della password admin può apportare modifiche alla configurazione dello storage array, ad esempio l'aggiunta, la modifica o la rimozione di oggetti o impostazioni. Per impostare la password admin durante l'avvio iniziale, vedere "Accedere a System Manager".

Per motivi di sicurezza, è possibile tentare di inserire una password solo cinque volte prima che lo storage array entri in uno stato di "blocco". In questo stato, lo storage array rifiuterà i successivi tentativi di password. Prima di inserire nuovamente una password, attendere 10 minuti per ripristinare lo stato "normale" dello storage array.

Oltre alla password di amministratore, lo storage array include profili utente predefiniti con uno o più ruoli mappati. Per ulteriori informazioni, vedere "Autorizzazioni per i ruoli mappati". I profili utente e le mappature non possono essere modificati. È possibile modificare solo le password. Se si desidera modificare la password admin o altre password utente, vedere "Modificare le password".

Immettere nuovamente le password dopo il timeout della sessione

Il sistema richiede la password una sola volta durante una singola sessione di gestione. Tuttavia, una sessione scade dopo 30 minuti di inattività, dopodiché è necessario immettere nuovamente la password. Se un altro utente che gestisce lo stesso array di storage da un altro client di gestione modifica la password durante la sessione, viene richiesta una password la volta successiva che si tenta di eseguire un'operazione di configurazione o un'operazione di visualizzazione.

È possibile regolare il timeout della sessione o disattivarlo del tutto. Vedere "Gestire i timeout delle sessioni".

Rimuovere i dischi o la protezione tramite password

Se si rimuovono unità protette da password o si desidera disattivare la protezione tramite password, tenere presente quanto segue:

- **Se si rimuovono dischi con password di protezione**, la password viene memorizzata in un'area riservata di ciascun disco dell'array di storage. Se si rimuovono tutte le unità da un array di storage, la password non funzionerà più. Per correggere questa condizione, reinstallare uno dei dischi originali nell'array di storage.
- **Se si desidera rimuovere la protezione tramite password** — se non si desidera più avere comandi

protetti da password, inserire la password corrente dell'amministratore e lasciare vuote le caselle di testo della nuova password.

> L'esecuzione di comandi di configurazione su un array di storage può causare gravi danni, inclusa la perdita di dati. Per questo motivo, è necessario impostare sempre una password di amministratore per lo storage array. Utilizzare una password di amministratore lunga con almeno 15 caratteri alfanumerici per aumentare la protezione.

Impostare le unità predefinite per i valori di capacità

System Manager può visualizzare i valori di capacità in gibibyte (GiB) o tebibyte (TIB).

Le preferenze vengono memorizzate nella memoria locale del browser, in modo che tutti gli utenti possano disporre delle proprie impostazioni.

Fasi

1. Selezionare **Preferenze › Imposta preferenze**.
2. Fare clic sul pulsante di opzione **Gibytes** o **Tebytes** e confermare che si desidera eseguire l'operazione.

   Per le abbreviazioni e i valori, consultare la tabella seguente.

Abbreviazione	Valore
Gib	$1{,}024^3$ byte
TIB	$1{,}024^4$ byte

Impostare l'intervallo di tempo predefinito per i grafici delle prestazioni

È possibile modificare l'intervallo di tempo predefinito mostrato dai grafici delle prestazioni.

A proposito di questa attività

I grafici delle performance mostrati nella pagina iniziale e nella pagina delle performance mostrano inizialmente un intervallo di tempo di 1 ora. Le preferenze vengono memorizzate nella memoria locale del browser, in modo che tutti gli utenti possano disporre delle proprie impostazioni.

Fasi

1. Selezionare **Preferenze › Imposta preferenze**.
2. Nell'elenco a discesa, selezionare **5 minuti**, **1 ora**, **8 ore**, **1 giorno** o **7 giorni**, e confermare che si desidera eseguire l'operazione.

Configurare il banner di accesso

È possibile creare un banner di accesso che viene presentato agli utenti prima di stabilire le sessioni in System Manager. 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).

Risultati

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 System Manager, 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 General (Generale), selezionare **Enable/Disable Session Timeout** (attiva/Disattiva timeout sessione).

   Viene visualizzata la finestra di dialogo 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).

Gestire le notifiche

Panoramica delle notifiche dei problemi

System Manager utilizza icone e diversi altri metodi per notificare l'esistenza di problemi con lo storage array.

Icone

System Manager utilizza queste icone per indicare lo stato dello storage array e dei relativi componenti.

Icona	Descrizione
	Ottimale
	Non ottimale o non riuscito
	Richiede attenzione o riparazione
	Attenzione

System Manager visualizza queste icone in diverse posizioni.

- L'area Notifiche della pagina iniziale visualizza l'icona di errore e un messaggio.
- L'icona della pagina iniziale nell'area di navigazione visualizza l'icona di errore.
- Nella pagina dei componenti, i grafici per i dischi e i controller visualizzano l'icona del guasto.

Avvisi e LED

Inoltre, System Manager notifica i problemi in altri modi.

- System Manager invia notifiche SNMP o messaggi di errore via email.
- I LED Service Action Required (azione di servizio richiesta) sull'hardware si accendono.

Quando si riceve la notifica di un problema, utilizzare Recovery Guru per risolvere il problema. Se necessario, utilizzare la documentazione sull'hardware con le fasi di ripristino per sostituire i componenti guasti.

Visualizzare e agire sulle operazioni in corso

Per visualizzare e intraprendere azioni sulle operazioni a esecuzione prolungata, utilizzare la pagina Operations in Progress (operazioni in corso).

A proposito di questa attività

Per ciascuna operazione elencata nella pagina Operations in Progress (operazioni in corso), vengono visualizzate una percentuale di completamento e il tempo stimato rimanente per completare l'operazione. In alcuni casi, è possibile interrompere un'operazione o posizionarla con priorità più alta o più bassa. È inoltre possibile cancellare un'operazione di copia del volume completata dall'elenco.

Fasi

1. Nella pagina iniziale, selezionare **Mostra operazioni in corso**.

Viene visualizzata la pagina Operations in Progress (operazioni in corso).

2. Se lo si desidera, utilizzare i collegamenti nella colonna Actions (azioni) per interrompere o modificare la priorità di un'operazione.

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

   È possibile interrompere un'operazione di copia di un volume o modificarne la priorità.

3. Una volta completata l'operazione di copia di un volume, selezionare **Clear** per rimuoverlo dall'elenco.

   Al termine di un'operazione, nella parte superiore della pagina iniziale vengono visualizzati un messaggio informativo e l'icona della chiave gialla. Questo messaggio include un collegamento che consente di annullare l'operazione dalla pagina Operations in Progress (operazioni in corso).

Le operazioni visualizzate nella pagina operazioni in corso includono quanto segue:

Operazione	Stato possibile dell'operazione	Azioni da intraprendere
Copia del volume	Completato	Chiaro
Copia del volume	In corso	• Modificare la priorità • Arrestare
Copia del volume	In sospeso	Chiaro
Copia del volume	Non riuscito	• Chiaro • Copia di nuovo
Copia del volume	Interrotto	• Chiaro • Copia di nuovo
Creazione di volumi (solo volumi thick pool superiori a 64 TiB)	In corso	*nessuno*
Eliminazione del volume (solo volumi thick pool superiori a 64 TiB)	In corso	*nessuno*
Sincronizzazione iniziale del gruppo di mirror asincrono	In corso	Sospendere
Sincronizzazione iniziale del gruppo di mirror asincrono	Sospeso	Riprendi
Mirroring sincrono	In corso	Sospendere

Operazione	Stato possibile dell'operazione	Azioni da intraprendere
Mirroring sincrono	Sospeso	Riprendi
Rollback dell'immagine Snapshot	In corso	Annulla
Rollback dell'immagine Snapshot	In sospeso	Annulla
Rollback dell'immagine Snapshot	In pausa	• Annulla • Riprendi
Evacuazione del disco	In corso	Annulla (a seconda del tipo di evacuazione del disco)
Aggiungere capacità al pool o al gruppo di volumi	In corso	*nessuno*
Modificare un livello RAID per un volume	In corso	*nessuno*
Ridurre la capacità di un pool	In corso	*nessuno*
Recupero di volumi sottili	In corso	*nessuno*
Verificare il tempo rimanente per un'operazione con formato di disponibilità istantanea (IAF) per i volumi del pool	In corso	*nessuno*
Controllare la ridondanza dei dati di un gruppo di volumi	In corso	*nessuno*
Deframmentare un gruppo di volumi	In corso	*nessuno*
Inizializzare un volume	In corso	*nessuno*
Aumentare la capacità di un volume	In corso	*nessuno*
Modificare le dimensioni dei segmenti di un volume	In corso	*nessuno*
Copia del disco	In corso	*nessuno*
Ricostruzione dei dati	In corso	*nessuno*

Operazione	Stato possibile dell'operazione	Azioni da intraprendere
CopyBack	In corso	*nessuno*
Cancellazione del disco	In corso	*nessuno*
Importazione dello storage remoto	In corso	• Modificare la priorità • Arrestare
Importazione dello storage remoto	Interrotto	• Riprendi • Scollegare
Importazione dello storage remoto	Non riuscito	• Riprendi • Scollegare
Importazione dello storage remoto	Completato	Scollegare

Risolvere i problemi utilizzando Recovery Guru

Recovery Guru è un componente di System Manager che diagnostica i problemi degli array di storage e consiglia le procedure di ripristino per risolvere i problemi.

Fasi

1. Selezionare **Home**.
2. Fare clic sul collegamento **Recover from *n* Problems** (Ripristina da *n* problemi*) nella parte superiore centrale della finestra.

   Viene visualizzata la finestra di dialogo Recovery Guru.

3. Selezionare il primo problema visualizzato nell'elenco riepilogativo, quindi seguire le istruzioni della procedura di ripristino per risolvere il problema. Se necessario, seguire le istruzioni di sostituzione per sostituire i componenti guasti. Ripetere questo passaggio per ciascun problema elencato.

   Possono essere correlati diversi problemi all'interno di un array di storage. In questo caso, l'ordine in cui i problemi vengono corretti può influire sul risultato. Selezionare e correggere i problemi nell'ordine in cui sono elencati nell'elenco riepilogativo.

   I guasti multipli di un contenitore dell'alimentatore sono raggruppati ed elencati come un unico problema nell'elenco riepilogativo. Anche i guasti multipli di un filtro a carboni attivi della ventola sono elencati come un unico problema.

4. Per assicurarsi che la procedura di ripristino sia stata eseguita correttamente, fare clic su **Rinnova**.

   Se è stato selezionato un problema per un gruppo di mirror asincrono o un membro di un gruppo di mirror asincrono, fare clic su **Clear** prima per eliminare l'errore dal controller, quindi fare clic su **Remember** per rimuovere l'evento dal Recovery Guru.

   Se tutti i problemi sono stati corretti, l'icona dell'array di storage passa da richiede attenzione a ottimale. In caso di problemi, viene visualizzata un'icona di correzione mentre è in corso un'operazione, ad esempio la

ricostruzione.

5. **Opzionale:** per salvare le informazioni del Recovery Guru in un file, fare clic sull'icona **Salva**.

   Il file viene salvato nella cartella Download del browser con il nome `recovery-guru-failure-yyyy-mm-dd-hh-mm-ss-mmm.html`.

6. Per stampare le informazioni del Recovery Guru, fare clic sull'icona **Stampa**.

FAQ

Quali sono i browser supportati?

System Manager supporta queste versioni del browser.

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

Quali sono i tasti di scelta rapida?

È possibile navigare in System Manager utilizzando la sola tastiera.

Navigazione generale

Azione	Scelta rapida da tastiera
Passare all'elemento successivo.	Scheda
Consente di passare all'elemento precedente.	Maiusc + Tab
Selezionare un elemento.	Invio
Elenco a discesa - consente di passare all'elemento successivo o precedente.	Freccia verso il basso o verso l'alto
Casella di controllo—selezionare un elemento.	Barra spaziatrice
Pulsanti di opzione - consente di passare da un elemento all'altro.	Freccia verso il basso o verso l'alto

Azione	Scelta rapida da tastiera
Testo espandibile: Consente di espandere o contrarre l'elemento.	Invio

Navigazione nella tabella

Azione	Scelta rapida da tastiera
Selezionare una riga.	Per selezionare una riga, quindi premere Invio
Scorrere verso l'alto o verso il basso.	Freccia verso il basso/freccia verso l'alto o pagina verso il basso/pagina verso l'alto
Modificare l'ordinamento di una colonna.	Per selezionare un'intestazione di colonna, quindi premere Invio

Navigazione nel calendario

Azione	Scelta rapida da tastiera
Passare al mese precedente.	Pagina su
Passare al mese successivo.	Pagina giù
Passare all'anno precedente.	Ctrl + PagSu
Passare all'anno successivo.	Ctrl + pagina giù
Aprire il selettore data, se chiuso.	Control + Home
Passare al mese corrente.	Control / comando + Home
Passare al giorno precedente.	Control / comando + sinistra
Passare al giorno successivo.	Control / comando + destra
Passare alla settimana precedente.	Ctrl / comando + su
Passare alla settimana successiva.	Ctrl / comando + Giù
Selezionare la data di riferimento.	Invio
Chiudere il selettore di data e cancellare la data.	Control / comando + fine
Chiudere il selettore di data senza selezionare.	Fuga

In che modo le statistiche delle performance per i singoli volumi si riferiscono al totale?

Le statistiche per pool e gruppi di volumi vengono calcolate aggregando tutti i volumi, inclusi i volumi di capacità riservati.

La capacità riservata viene utilizzata internamente dal sistema di storage per supportare thin volumi, snapshot e mirroring asincrono e non è visibile agli host i/O. Di conseguenza, le statistiche del pool, del controller e dell'array di storage potrebbero non essere sommative per essere la somma dei volumi visualizzabili.

Tuttavia, per le statistiche delle applicazioni e dei carichi di lavoro, vengono aggregati solo i volumi visibili.

Perché i dati vengono visualizzati come zero nei grafici e nella tabella?

Quando viene visualizzato uno zero per un punto dati nei grafici e nella tabella, significa che non esiste alcuna attività i/o per l'oggetto per quel punto nel tempo. Questa situazione potrebbe verificarsi perché l'host non sta avviando l'i/o per quell'oggetto o potrebbe essere un problema con l'oggetto stesso.

I dati storici dell'oggetto sono ancora disponibili per la visualizzazione. I grafici e la tabella mostrano dati diversi da zero una volta che inizia l'attività di i/o per l'oggetto.

La tabella seguente elenca i motivi più comuni per cui un valore di punto dati potrebbe essere zero per un determinato oggetto.

Tipo di oggetto a livello di array	I dati del motivo vengono visualizzati come zero
Volume	• Il volume non ha assegnato host.
Gruppo di volumi	• Importazione del gruppo di volumi in corso. • Il gruppo di volumi non contiene un volume assegnato a un host, il gruppo di volumi ***and*** non contiene alcuna capacità riservata.
Disco	• Il disco è guasto. • Il disco è stato rimosso. • Il disco si trova in uno stato sconosciuto.
Controller	• Controller offline. • Controller guasto. • Il controller è stato rimosso. • Il controller si trova in uno stato sconosciuto.
Array di storage	• Lo storage array non contiene volumi.

Cosa mostra il grafico della latenza?

Il grafico della latenza fornisce statistiche di latenza, in millisecondi (ms), per volumi, gruppi di volumi, pool, applicazioni e carichi di lavoro. Questo grafico viene visualizzato

nelle schede Logical View (Vista logica), Physical View (Vista fisica) e Applications & workload View (Vista applicazioni e carichi di lavoro).

La latenza si riferisce a qualsiasi ritardo che si verifica durante la lettura o la scrittura dei dati. Spostare il cursore su un punto del grafico per visualizzare i seguenti valori, in millisecondi (ms), per quel momento:

- Tempo di lettura.
- Tempo di scrittura.
- Dimensione i/o media.

Cosa mostra il grafico IOPS?

Il grafico IOPS visualizza le statistiche per le operazioni di input/output al secondo. Nella pagina iniziale, questo grafico visualizza le statistiche per l'array di storage. Nelle schede Logical View (Vista logica), Physical View (Vista fisica) e Applications & workload View (Vista applicazioni e carichi di lavoro) del riquadro Performance (prestazioni), questo grafico visualizza le statistiche per array di storage, volumi, gruppi di volumi, pool, applicazioni, e carichi di lavoro.

IOPS è l'abbreviazione di *operazioni di input/output (i/o) al secondo*. Spostare il cursore su un punto del grafico per visualizzare i seguenti valori per quel punto temporale:

- Numero di operazioni di lettura.
- Numero di operazioni di scrittura.
- Operazioni totali di lettura e scrittura combinate.

Cosa mostra il grafico MiB/s?

Il grafico MiB/s visualizza le statistiche della velocità di trasferimento in megibyte al secondo. Nella pagina iniziale, questo grafico visualizza le statistiche per l'array di storage. Nelle schede Logical View (Vista logica), Physical View (Vista fisica) e Applications & workload View (Vista applicazioni e carichi di lavoro) del riquadro Performance (prestazioni), questo grafico visualizza le statistiche per array di storage, volumi, gruppi di volumi, pool, applicazioni, e carichi di lavoro.

MIB/s è l'abbreviazione di *mebibytes per second* o 1,048,576 byte per secondo. Spostare il cursore su un punto del grafico per visualizzare i seguenti valori per quel punto temporale:

- La quantità di dati letti.
- La quantità di dati scritti.
- La quantità totale combinata di dati letti e scritti.

Cosa mostra il grafico della CPU?

Il grafico della CPU visualizza le statistiche della capacità di elaborazione per ciascun controller (controller A e controller B). CPU è l'abbreviazione di *Central Processing Unit*. Nella pagina iniziale, questo grafico visualizza le statistiche per l'array di storage. Nella scheda Physical View (Vista fisica) del riquadro Performance (prestazioni), questo grafico

visualizza le statistiche per l'array di storage e i dischi.

Il grafico della CPU mostra la percentuale di capacità di elaborazione della CPU utilizzata rispetto alle operazioni sull'array. Anche quando non si verifica alcun i/o esterno, la percentuale di utilizzo della CPU può essere diversa da zero perché il sistema operativo dello storage potrebbe eseguire operazioni e monitoring in background. Spostare il cursore su un punto del grafico per visualizzare una percentuale di capacità di elaborazione utilizzata in quel momento.

Cosa mostra il grafico headroom?

Il grafico dello spazio di crescita è relativo alle restanti funzionalità delle performance per i controller degli array di storage. Questo grafico è visibile nella pagina iniziale e nella scheda Vista fisica del riquadro prestazioni.

Il grafico dello spazio di crescita mostra le restanti capacità di performance degli oggetti fisici nel sistema di storage. Spostare il cursore su un punto del grafico per visualizzare le percentuali di capacità IOPS e MIB/s rimanenti per il controller A e per il controller B.

Dove si possono trovare ulteriori informazioni sulle preferenze di visualizzazione?

Per trovare informazioni sulle opzioni di visualizzazione disponibili:

- Per ulteriori informazioni sulle unità predefinite per la visualizzazione dei valori di capacità, vedere "Impostare le unità predefinite per i valori di capacità".
- Per ulteriori informazioni sul periodo di tempo predefinito per la visualizzazione dei grafici delle prestazioni, vedere "Impostare l'intervallo di tempo predefinito per i grafici delle prestazioni".

Pool e gruppi di volumi

Panoramica su pool e gruppi di volumi

È possibile creare capacità di storage logico da un sottoinsieme di unità non assegnate nell'array di storage. Questa capacità logica può assumere la forma di un pool o di un gruppo di volumi, a seconda delle esigenze dell'ambiente.

Cosa sono pool e gruppi di volumi?

Un *pool* è un insieme di dischi raggruppati in modo logico. Un *gruppo di volumi* è un container per volumi con caratteristiche condivise. È possibile utilizzare un pool o un gruppo di volumi per creare volumi accessibili a un host.

Scopri di più:

- "Funzionamento di pool e gruppi di volumi"
- "Terminologia relativa alla capacità"
- "Decidere se utilizzare un pool o un gruppo di volumi"

Come si creano i pool?

È possibile consentire a System Manager di creare pool automaticamente quando rileva una capacità non assegnata in un array di storage. In alternativa, quando la creazione automatica non è in grado di determinare

la configurazione migliore, è possibile creare manualmente i pool dal **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups]).

Scopri di più:

- "Creazione automatica e manuale del pool"
- "Crea pool automaticamente"
- "Creare il pool manualmente"
- "Aggiungere capacità a un pool o a un gruppo di volumi"

Come si creano gruppi di volumi?

È possibile creare gruppi di volumi dal **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups]).

Scopri di più:

- "Creare un gruppo di volumi"
- "Aggiungere capacità a un pool o a un gruppo di volumi"

Informazioni correlate

Scopri di più sui concetti relativi a pool e gruppi di volumi:

- "Come funziona la capacità riservata"
- "Come funziona SSD cache"

Concetti

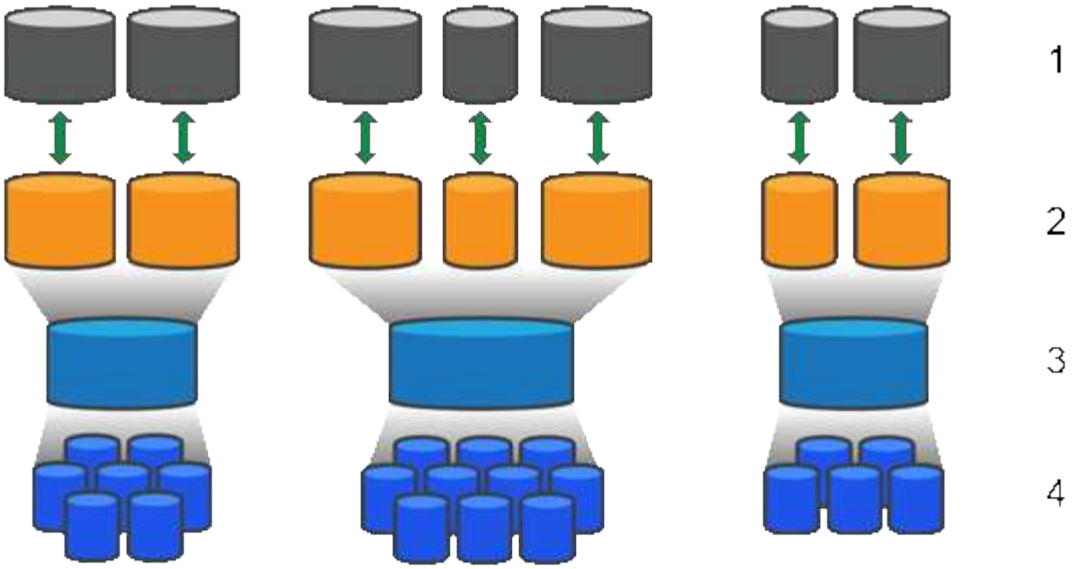
Funzionamento di pool e gruppi di volumi

Per eseguire il provisioning dello storage, creare un pool o un gruppo di volumi che conterrà i dischi rigidi (HDD) o SSD (Solid state Disk) che si desidera utilizzare nell'array di storage.

L'hardware fisico viene fornito in componenti logici in modo che i dati possano essere organizzati e recuperati facilmente. Sono supportati due tipi di raggruppamenti:

- Piscine
- Gruppi di volumi RAID

I pool e i gruppi di volumi sono le unità di storage di livello superiore in un array di storage: Suddividono la capacità dei dischi in divisioni gestibili. All'interno di queste divisioni logiche si trovano i singoli volumi o LUN in cui sono memorizzati i dati. La figura seguente illustra questo concetto.



[1] LUN host; [2] volumi; [3] gruppi di volumi o pool; [4] dischi HDD o SSD

Quando viene implementato un sistema storage, il primo passo consiste nel presentare la capacità disponibile dei dischi ai vari host:

- Creazione di pool o gruppi di volumi con capacità sufficiente
- Aggiunta del numero di dischi necessari per soddisfare i requisiti di performance al pool o al gruppo di volumi
- Selezione del livello di protezione RAID desiderato (se si utilizzano gruppi di volumi) per soddisfare specifici requisiti di business

È possibile avere pool o gruppi di volumi sullo stesso sistema di storage, ma un'unità non può far parte di più di un pool o gruppo di volumi. I volumi presentati agli host per i/o vengono quindi creati utilizzando lo spazio nel pool o nel gruppo di volumi.

Piscine

I pool sono progettati per aggregare i dischi rigidi fisici in un ampio spazio di storage e fornire una protezione RAID avanzata per l'IT. Un pool crea molti set RAID virtuali dal numero totale di dischi assegnati al pool e distribuisce i dati in modo uniforme tra tutti i dischi partecipanti. In caso di perdita o aggiunta di un disco, System Manager ribilancia dinamicamente i dati su tutti i dischi attivi.

I pool funzionano come un altro livello RAID, virtualizzando l'architettura RAID sottostante per ottimizzare le performance e la flessibilità durante l'esecuzione di attività come la ricostruzione, l'espansione del disco e la gestione della perdita del disco. System Manager imposta automaticamente il livello RAID a 6 in una configurazione 8+2 (otto dischi dati più due dischi di parità).

Corrispondenza dei dischi

È possibile scegliere tra HDD o SSD da utilizzare nei pool; tuttavia, come per i gruppi di volumi, tutti i dischi nel pool devono utilizzare la stessa tecnologia. I controller selezionano automaticamente i dischi da includere, quindi è necessario assicurarsi di disporre di un numero sufficiente di dischi per la tecnologia scelta.

Gestione dei dischi guasti

I pool hanno una capacità minima di 11 dischi; tuttavia, la capacità di un disco è riservata alla capacità di

riserva in caso di guasto di un disco. Questa capacità di riserva è denominata “capacità di conservazione”.

Quando vengono creati i pool, viene preservata una certa quantità di capacità per l’utilizzo in caso di emergenza. Questa capacità è espressa in termini di un numero di dischi in System Manager, ma l’implementazione effettiva è distribuita nell’intero pool di dischi. La quantità predefinita di capacità conservata si basa sul numero di dischi nel pool.

Una volta creato il pool, è possibile modificare il valore della capacità di conservazione su una capacità maggiore o minore oppure impostarlo su una capacità di conservazione non pari a 0 unità. La capacità massima che è possibile conservare (espressa come numero di dischi) è 10, ma la capacità disponibile potrebbe essere inferiore, in base al numero totale di dischi nel pool.

Gruppi di volumi

I gruppi di volumi definiscono il modo in cui la capacità viene assegnata ai volumi nel sistema di storage. I dischi sono organizzati in gruppi RAID e i volumi risiedono tra i dischi di un gruppo RAID. Pertanto, le impostazioni di configurazione dei gruppi di volumi identificano i dischi che fanno parte del gruppo e il livello RAID utilizzato.

Quando si crea un gruppo di volumi, i controller selezionano automaticamente le unità da includere nel gruppo. È necessario scegliere manualmente il livello RAID per il gruppo. La capacità del gruppo di volumi corrisponde al numero totale di dischi selezionati, moltiplicato per la capacità.

Corrispondenza dei dischi

Per le dimensioni e le prestazioni, è necessario associare le unità del gruppo di volumi. Se nel gruppo di volumi sono presenti dischi più piccoli e più grandi, tutti i dischi vengono riconosciuti come la capacità più piccola. Se nel gruppo di volumi sono presenti dischi più lenti e veloci, tutti i dischi vengono riconosciuti alla velocità più bassa. Questi fattori influiscono sulle performance e sulla capacità complessiva del sistema storage.

Non è possibile combinare diverse tecnologie di dischi (dischi HDD e SSD). RAID 3, 5 e 6 sono limitati a un massimo di 30 dischi. RAID 1 e RAID 10 utilizzano il mirroring, pertanto questi gruppi di volumi devono avere un numero pari di dischi.

Gestione dei dischi guasti

I gruppi di volumi utilizzano i dischi hot spare come standby nel caso in cui un disco si guasti in volumi RAID 1/10, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. Un’unità hot spare non contiene dati e aggiunge un altro livello di ridondanza all’array di storage.

Se un disco si guasta nell’array di storage, il disco hot spare viene sostituito automaticamente per il disco guasto senza richiedere uno swap fisico. Se il disco hot spare è disponibile quando si verifica un guasto, il controller utilizza i dati di ridondanza per ricostruire i dati dal disco guasto al disco hot spare.

Terminologia relativa alla capacità

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

Oggetti di storage

La seguente terminologia descrive i diversi tipi di oggetti storage che possono interagire con lo storage array.

Oggetto di storage	Descrizione
Host	Un host è un server che invia i/o a un volume su un array di storage.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi.
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un contenitore per una o più coppie mirrorate. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror.
Coppia di volumi mirrorati	Una coppia mirrorata è composta da due volumi, un volume primario e un volume secondario.
Piscina	Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.
Gruppo di coerenza Snapshot	Un gruppo di coerenza snapshot è un insieme di volumi che vengono trattati come una singola entità quando viene creata un'immagine snapshot. Ciascuno di questi volumi dispone di una propria immagine snapshot, ma tutte le immagini vengono create nello stesso momento.
Gruppo di snapshot	Un gruppo di snapshot è una raccolta di immagini snapshot da un singolo volume di base.
Volume Snapshot	Un volume di snapshot consente all'host di accedere ai dati nell'immagine di snapshot. Il volume Snapshot contiene la propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine snapshot originale.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all'host di accedere allo storage sull'array di storage.
Gruppo di volumi	Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.

Capacità dello storage

La seguente terminologia descrive i diversi tipi di capacità utilizzati nell'array di storage.

Tipo di capacità	Descrizione
Capacità allocata	La capacità allocata è la capacità fisica allocata dai dischi di un pool o di un gruppo di volumi. Si utilizza la capacità allocata per creare volumi e per le operazioni dei servizi di copia.
Capacità libera	La capacità libera è la capacità disponibile in un pool o gruppo di volumi che non è ancora stata allocata alle operazioni di creazione di volumi o di copia dei servizi e agli oggetti di storage.
Capacità del pool o del gruppo di volumi	La capacità di pool, volume o gruppo di volumi è la capacità di un array di storage assegnato a un pool o a un gruppo di volumi. Questa capacità viene utilizzata per creare volumi e soddisfare le diverse esigenze di capacità delle operazioni dei servizi di copia e degli oggetti di storage.
Capacità di pool inutilizzabile	La capacità inutilizzabile del pool è lo spazio in un pool che non può essere utilizzato a causa di dimensioni di unità non corrispondenti.
Capacità di conservazione	La capacità di conservazione è la quantità di capacità (numero di dischi) riservata in un pool per supportare potenziali guasti del disco.
Capacità riportata	La capacità riportata è la capacità che viene riportata all'host e a cui l'host può accedere.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.
Cache SSD	SSD cache è un insieme di dischi a stato solido (SSD) che vengono raggruppati logicamente nel vostro array di storage. La funzione SSD cache memorizza nella cache i dati più utilizzati (dati "hot") su unità SSD a latenza inferiore per accelerare dinamicamente i carichi di lavoro delle applicazioni.
Capacità non assegnata	La capacità non assegnata è lo spazio in un array di storage che è stato **non** assegnato a un pool o a un gruppo di volumi.
Capacità scritta	La capacità scritta è la quantità di capacità che è stata scritta dalla capacità riservata allocata per i thin volumi.

Decidere se utilizzare un pool o un gruppo di volumi

È possibile creare volumi utilizzando un pool o un gruppo di volumi. La scelta migliore dipende principalmente dai principali requisiti di storage, come il carico di lavoro i/o previsto, i requisiti di performance e i requisiti di protezione dei dati.

Motivi per scegliere un pool o un gruppo di volumi

Scegliere un pool

- Se hai bisogno di una ricostruzione più rapida dei dischi e di un'amministrazione dello storage semplificata, richiedono volumi thin e/o un carico di lavoro altamente casuale.
- Se si desidera distribuire i dati per ciascun volume in modo casuale su un set di dischi che compongono il pool.

  Non è possibile impostare o modificare il livello RAID dei pool o dei volumi nei pool. I pool utilizzano il livello RAID 6.

Scegliere un gruppo di volumi

- Se hai bisogno della massima larghezza di banda del sistema, della possibilità di ottimizzare le impostazioni dello storage e di un carico di lavoro altamente sequenziale.
- Se si desidera distribuire i dati tra i dischi in base a un livello RAID. È possibile specificare il livello RAID quando si crea il gruppo di volumi.
- Se si desidera scrivere i dati per ciascun volume in sequenza nel set di dischi che compongono il gruppo di volumi.

> Poiché i pool possono coesistere con i gruppi di volumi, un array di storage può contenere sia pool che gruppi di volumi.

Differenze di funzionalità tra pool e gruppi di volumi

Nella tabella seguente viene fornito un confronto delle funzionalità tra gruppi di volumi e pool.

Utilizzare	Piscina	Gruppo di volumi
Carico di lavoro casuale	Meglio	Bene
Carico di lavoro sequenziale	Bene	Meglio
Tempo di ricostruzione del disco	Più veloce	Più lento
Performance (modalità ottimale)	Buona: Ideale per piccoli blocchi, carichi di lavoro casuali.	Buona: Ideale per carichi di lavoro sequenziali a blocchi di grandi dimensioni
Performance (modalità di ricostruzione del disco)	Migliore: Di solito migliore di RAID 6	Degradato: Calo delle performance fino al 40%
Guasti a più dischi	Maggiore protezione dei dati: Ricostruzioni più rapide e prioritarie	Minore protezione dei dati: Ricostruzioni lente, maggiore rischio di perdita dei dati

Utilizzare	Piscina	Gruppo di volumi
Aggiunta di unità	Più veloce: Aggiungi al pool in tempo reale	Più lento: Richiede un'operazione di espansione dinamica della capacità
Supporto di thin volumi	Sì	No
Supporto di Solid state Disk (SSD)	Sì	Sì
Amministrazione semplificata	Sì: Nessuna hot spare o impostazioni RAID da configurare	No: È necessario allocare hot spare, configurare RAID
Performance sintonizzabili	No	Sì

Confronto funzionale di pool e gruppi di volumi

La funzione e lo scopo di un pool e di un gruppo di volumi sono identici. Entrambi gli oggetti sono un insieme di dischi raggruppati logicamente in un array di storage e vengono utilizzati per creare volumi ai quali un host può accedere.

La seguente tabella consente di decidere se un pool o un gruppo di volumi si adatta meglio alle proprie esigenze di storage.

Funzione	Piscina	Gruppo di volumi
Supporto di diversi livelli RAID	No Sempre RAID 6 in System Manager.	Sì. RAID 0, 1, 10, 5 e 6 disponibili.
Supporto di thin volumi	Sì	No
Crittografia completa del disco (FDE) supportata	Sì	Sì
Data Assurance (da) supportato	Sì	Sì
Protezione contro la perdita di shelf supportata	Sì	Sì
Protezione contro le perdite di cassetto supportata	Sì	Sì
Supporto di velocità di dischi miste	Consigliato per essere lo stesso, ma non richiesto. Il disco più lento determina la velocità di tutti i dischi.	Consigliato per essere lo stesso, ma non richiesto. Il disco più lento determina la velocità di tutti i dischi.

Funzione	Piscina	Gruppo di volumi
Capacità di dischi misti supportata	Consigliato per essere lo stesso, ma non richiesto. Il disco più piccolo determina la capacità di tutti i dischi.	Consigliato per essere lo stesso, ma non richiesto. Il disco più piccolo determina la capacità di tutti i dischi.
Numero minimo di dischi	11	Dipende dal livello RAID. RAID 0 richiede 1. RAID 1 o 10 richiede 2 (richiede un numero pari). RAID 5 è minimo 3. RAID 6 è minimo 5.
Numero massimo di dischi	Fino al limite massimo per lo storage array	RAID 1 e 10 - fino al limite massimo di dischi RAID 5, 6-30 dello storage array
Possibilità di scegliere singoli dischi durante la creazione di un volume	No	Sì
Può specificare le dimensioni del segmento durante la creazione di un volume	Sì. 128K supportato.	Sì
Consente di specificare le caratteristiche di i/o durante la creazione di un volume	No	Sì. Supporto di file system, database, contenuti multimediali e personalizzati.
Protezione dai guasti del disco	Utilizza la capacità di conservazione su ogni disco del pool, rendendo più rapida la ricostruzione.	Utilizza un disco hot spare. La ricostruzione è limitata dagli IOPS del disco.
Avviso quando si raggiunge il limite di capacità	Sì. Può impostare un avviso quando la capacità utilizzata raggiunge una percentuale della capacità massima.	No
Migrazione a un array storage diverso supportata	No Richiede prima la migrazione a un gruppo di volumi.	Sì
Dimensione dinamica dei segmenti (DSS)	No	Sì
Può modificare il livello RAID	No	Sì
Espansione dei volumi (aumento della capacità)	Sì	Sì

Funzione	Piscina	Gruppo di volumi
Espansione della capacità (aggiunta di capacità)	Sì	Sì
Riduzione della capacità	Sì	No

I tipi di dischi misti (HDD, SSD) non sono supportati per pool o gruppi di volumi.

Creazione automatica e manuale del pool

I pool vengono creati automaticamente o manualmente per consentire il raggruppamento dello storage fisico e l'allocazione dinamica in base alle esigenze. Quando viene creato un pool, è possibile aggiungere dischi fisici.

Creazione automatica

La creazione automatica del pool viene avviata quando System Manager rileva una capacità non assegnata in un array di storage. Quando viene rilevata una capacità non assegnata, System Manager richiede automaticamente di creare uno o più pool o di aggiungere la capacità non assegnata a un pool esistente o a entrambi.

La creazione automatica del pool si verifica quando si verifica una di queste condizioni:

- I pool non esistono nell'array di storage e sono presenti dischi simili a sufficienza per creare un nuovo pool.
- Vengono aggiunte nuove unità a un array di storage che dispone di almeno un pool.

Ogni disco in un pool deve essere dello stesso tipo di disco (HDD o SSD) e avere capacità simile. System Manager richiede di completare le seguenti attività:

- Creare un singolo pool se il numero di dischi di questi tipi è sufficiente.
- Creare più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
- Aggiungere le unità al pool esistente se un pool è già definito nell'array di storage e aggiungere nuove unità dello stesso tipo di disco al pool.
- Aggiungere i dischi dello stesso tipo al pool esistente e utilizzare gli altri tipi di dischi per creare pool diversi se i nuovi dischi sono di tipi diversi.

Creazione manuale

Se la creazione automatica non riesce a determinare la configurazione migliore, potrebbe essere necessario creare un pool manualmente. Questa situazione può verificarsi per uno dei seguenti motivi:

- I nuovi dischi potrebbero essere aggiunti a più di un pool.
- Uno o più dei nuovi candidati al pool possono utilizzare la protezione contro la perdita di shelf o la protezione contro la perdita di cassetto.
- Uno o più dei candidati attuali del pool non possono mantenere la protezione contro la perdita di shelf o lo stato di protezione contro la perdita di cassetto.

È inoltre possibile creare un pool manualmente se si dispone di più applicazioni sull'array di storage e non si desidera che queste competano per le stesse risorse del disco. In questo caso, è possibile creare

manualmente un pool più piccolo per una o più applicazioni. È possibile assegnare solo uno o due volumi invece di assegnare il carico di lavoro a un pool di grandi dimensioni con molti volumi attraverso i quali distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di un'applicazione specifica può consentire alle operazioni degli array di storage di funzionare più rapidamente, con meno conflitti.

Configurare lo storage

Crea pool automaticamente

La creazione del pool viene avviata automaticamente quando System Manager rileva dischi non assegnati nell'array di storage. È possibile utilizzare la creazione automatica del pool per configurare facilmente tutte le unità non assegnate nell'array di storage in un unico pool e per aggiungere unità nei pool esistenti.

Prima di iniziare

È possibile avviare la finestra di dialogo Configurazione automatica pool quando si verifica una delle seguenti condizioni:

- È stato rilevato almeno un disco non assegnato che può essere aggiunto a un pool esistente con tipi di disco simili.
- Sono stati rilevati undici (11) o più dischi non assegnati che possono essere utilizzati per creare un nuovo pool (se non possono essere aggiunti a un pool esistente a causa di tipi di dischi diversi).

A proposito di questa attività

Tenere presente quanto segue:

- Quando si aggiungono dischi a un array di storage, System Manager rileva automaticamente i dischi e richiede di creare un singolo pool o più pool in base al tipo di disco e alla configurazione corrente.
- Se i pool sono stati precedentemente definiti, System Manager richiede automaticamente di aggiungere le unità compatibili a un pool esistente. Quando vengono aggiunte nuove unità a un pool esistente, System Manager ridistribuisce automaticamente i dati nella nuova capacità, che ora include le nuove unità aggiunte.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace.

È possibile avviare la finestra di dialogo Configurazione automatica pool utilizzando uno dei seguenti metodi:

- Quando viene rilevata una capacità non assegnata, la raccomandazione di configurazione automatica del pool viene visualizzata nella pagina iniziale dell'area di notifica. Fare clic su **View Pool Auto-Configuration** (Visualizza configurazione automatica pool) per avviare la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Configurazione automatica pool dalla pagina Pools and Volume Groups come descritto nella seguente attività.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare **More › Avvia configurazione automatica del pool**.

   La tabella dei risultati elenca i nuovi pool, i pool esistenti con le unità aggiunte o entrambi. Per impostazione predefinita, un nuovo pool viene denominato con un numero sequenziale.

System Manager esegue le seguenti operazioni:

- Crea un singolo pool se il numero di dischi con lo stesso tipo di disco (HDD o SSD) è sufficiente e la capacità è simile.
- Crea più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
- Aggiunge le unità a un pool esistente se un pool è già definito nell'array di storage e si aggiungono nuove unità dello stesso tipo di disco al pool.
- Aggiunge le unità dello stesso tipo di unità al pool esistente e utilizza gli altri tipi di unità per creare pool diversi se le nuove unità sono di tipi diversi di unità.

3. Per modificare il nome di un nuovo pool, fare clic sull'icona **Modifica** (la matita).
4. Per visualizzare ulteriori caratteristiche del pool, posizionare il cursore o toccare l'icona **Dettagli** (la pagina).

   Vengono visualizzate informazioni relative al tipo di disco, alla funzionalità di sicurezza, alla funzione di data assurance (da), alla protezione contro la perdita di shelf e alla protezione contro la perdita di cassetto.

   Per gli array di storage EF600 e EF300, vengono visualizzate anche le impostazioni relative al provisioning delle risorse e alle dimensioni dei blocchi di volume.

5. Fare clic su **Accept** (Accetta).

Creare il pool manualmente

È possibile creare un pool manualmente (da un set di candidati) se la funzione di configurazione automatica del pool non fornisce un pool che soddisfa le proprie esigenze.

Un pool fornisce la capacità di storage logico necessaria per creare singoli volumi che possono essere utilizzati per ospitare le applicazioni.

Prima di iniziare

- È necessario disporre di un minimo di 11 dischi con lo stesso tipo di disco (HDD o SSD).
- La protezione contro la perdita di shelf richiede che i dischi che compongono il pool si trovino in almeno sei diversi shelf di dischi e che non vi siano più di due dischi in un singolo shelf di dischi.
- La protezione contro la perdita di cassetto richiede che le unità che compongono il pool siano collocate in almeno cinque cassetti diversi e che il pool includa un numero uguale di shelf di dischi da ciascun cassetto.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Attualmente, System Manager consente la selezione del disco nella funzione Advanced (Avanzate) quando si crea un gruppo di volumi. Per la creazione del pool, si consiglia di utilizzare tutti i dischi dell'array di storage.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sul **Create › Pool** (Crea[Pool])

   Viene visualizzata la finestra di dialogo Create Pool (Crea pool).

3. Digitare un nome per il pool.
4. **Opzionale:** se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   La tabella dei risultati elenca tutti i pool possibili che è possibile creare.

5. Selezionare il pool candidato che si desidera utilizzare in base alle seguenti caratteristiche, quindi fare clic su **Create** (Crea).

Caratteristica	Utilizzare
Capacità libera	Mostra la capacità libera del pool Candidate in GiB. Selezionare un pool candidato con la capacità adatta alle esigenze di storage dell'applicazione. Anche la capacità di conservazione (spare) viene distribuita in tutto il pool e non fa parte della capacità libera.
Totale dischi	Mostra il numero di dischi disponibili nel pool Candidate. System Manager riserva automaticamente il maggior numero possibile di dischi per la capacità di conservazione (per ogni sei dischi in un pool, System Manager riserva un disco per la capacità di conservazione). Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti.
Dimensioni blocco unità (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che i dischi del pool possono scrivere. I valori possono includere: • 512 — dimensione del settore di 512 byte. • 4K — dimensione del settore di 4,096 byte.
Sicuro	Indica se il pool candidato è costituito interamente da dischi con funzionalità di protezione, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). • È possibile proteggere il pool con Drive Security, ma tutti i dischi devono essere in grado di utilizzare questa funzione in modo sicuro. • Se si desidera creare un pool solo FDE, cercare **Yes - FDE** nella colonna Secure-capable. Se si desidera creare un pool solo FIPS, cercare **Sì - FIPS** o **Sì - FIPS (misto)**. "Misto" indica una combinazione di dischi di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il pool funzionerà al livello di sicurezza inferiore (140-2). • È possibile creare un pool composto da dischi che possono o non possono essere sicuri o che sono una combinazione di livelli di sicurezza. Se i dischi del pool includono dischi che non sono sicuri, non è possibile rendere il pool sicuro.

Caratteristica	Utilizzare
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se il pool è protetto ed è stata creata una chiave di sicurezza, è possibile attivare la protezione selezionando la casella di controllo. L'unico modo per rimuovere Drive Security dopo averlo attivato è eliminare il pool e cancellare i dischi.
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo candidato del pool. DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. SE tutti i dischi sono compatibili con da, IL VALORE DA è attivato. LA FUNZIONE DA può essere disattivata dopo la creazione del volume selezionando menu:Storage [Volumes > View/Edit Settings > Advanced > permanentemente disable data assurance] (volumi > Visualizza/Modifica impostazioni > Avanzate > Disattiva data assurance in modo permanente). Se il da è disattivato su un volume, non è possibile riattivarlo.
Funzionalità di provisioning delle risorse (solo EF300 e EF600)	Mostra se il provisioning delle risorse è disponibile per questo candidato del pool. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.
Protezione contro la perdita di shelf	Mostra se è disponibile la protezione contro la perdita di shelf. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool se si verifica una perdita totale di comunicazione con un singolo shelf di dischi.
Protezione in caso di perdita del cassetto	Mostra se è disponibile la protezione contro le perdite dei cassetti, fornita solo se si utilizza uno shelf di dischi che contiene cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi in un pool se si verifica una perdita totale di comunicazione con un singolo cassetto in uno shelf di dischi.
Dimensioni dei blocchi di volume supportate (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per i volumi nel pool: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Creare un gruppo di volumi

Si utilizza un gruppo di volumi per creare uno o più volumi accessibili all'host. Un gruppo di volumi è un container per volumi con caratteristiche condivise, come il livello RAID e la capacità.

Con dischi con capacità maggiore e la possibilità di distribuire volumi tra controller, la creazione di più di un volume per gruppo di volumi è un buon modo per sfruttare la capacità dello storage e proteggere i dati.

Prima di iniziare

Prima di creare un gruppo di volumi, consultare le seguenti linee guida:

- È necessario almeno un disco non assegnato.
- Esistono limiti per il numero di dischi che è possibile utilizzare in un singolo gruppo di volumi. Questi limiti variano in base al livello RAID.
- Per attivare la protezione contro la perdita di scaffali/cassetti, è necessario creare un gruppo di volumi che utilizzi dischi posizionati in almeno tre shelf o cassetti, a meno che non si utilizzi RAID 1, dove due shelf/cassetti sono il minimo.
- Se si dispone di uno storage array EF600 o EF300 e si prevede di creare manualmente un gruppo di volumi, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Attualmente, System Manager consente la selezione del disco nella funzione Advanced (Avanzate) quando si crea un gruppo di volumi.
- Esaminare in che modo la scelta del livello RAID influisce sulla capacità risultante del gruppo di volumi:
  - Se si seleziona RAID 1, è necessario aggiungere due dischi alla volta per assicurarsi che sia selezionata una coppia mirrorata. Il mirroring e lo striping (noto come RAID 10 o RAID 1+0) si ottengono selezionando quattro o più dischi.
  - Se si seleziona RAID 5, è necessario aggiungere almeno tre dischi per creare il gruppo di volumi.
  - Se si seleziona RAID 6, è necessario aggiungere almeno cinque dischi per creare il gruppo di volumi.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sul **Create › Volume group** (Crea[gruppo di volumi]).

   Viene visualizzata la finestra di dialogo Create Volume Group (Crea gruppo di volumi).

3. Digitare un nome per il gruppo di volumi.
4. Seleziona il livello RAID che meglio soddisfa i tuoi requisiti di storage e protezione dei dati.

   Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il livello RAID selezionato.

5. **Opzionale:** se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il tipo di disco e il livello RAID selezionati.

6. **Opzionale:** è possibile selezionare il metodo automatico o manuale per definire le unità da utilizzare nel gruppo di volumi. Il metodo automatico è la selezione predefinita.

   Per selezionare i dischi manualmente, fare clic sul collegamento **Manually Select drives (Advanced)** (Seleziona manualmente i dischi (avanzati)**). Quando si fa clic su di esso, viene visualizzato *Automatically Select drives (Advanced)**.

   Il metodo Manuale consente di selezionare le unità specifiche che compongono il gruppo di volumi. È

possibile selezionare dischi non assegnati specifici per ottenere la capacità richiesta. Se l'array di storage contiene dischi con tipi di supporti diversi o tipi di interfaccia diversi, è possibile scegliere solo la capacità non configurata per un singolo tipo di disco per creare il nuovo gruppo di volumi.

> Solo gli esperti che conoscono la ridondanza dei dischi e le configurazioni ottimali dei dischi devono utilizzare il metodo manuale.

7. In base alle caratteristiche del disco visualizzate, selezionare le unità che si desidera utilizzare nel gruppo di volumi, quindi fare clic su **Create** (Crea).

   Le caratteristiche del disco visualizzate dipendono dalla selezione del metodo automatico o manuale.

Caratteristiche del drive di metodo automatico

Caratteristica	Utilizzare
Capacità libera	Mostra la capacità disponibile in GiB. Selezionare un gruppo di volumi candidato con la capacità adatta alle esigenze di storage dell'applicazione.
Totale dischi	Mostra il numero di dischi disponibili per questo gruppo di volumi. Selezionare un gruppo di volumi candidato con il numero di dischi desiderato.
Dimensioni blocco unità (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che i dischi del gruppo possono scrivere. I valori possono includere: • 512 — dimensione del settore di 512 byte. • 4K — dimensione del settore di 4,096 byte.
Sicuro	Indica se questo gruppo di volumi candidato è composto interamente da dischi con funzionalità di protezione, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). • È possibile proteggere il gruppo di volumi con Drive Security, ma per utilizzare questa funzione è necessario che tutti i dischi siano protetti. • Se si desidera creare un gruppo di volumi solo FDE, cercare **Yes - FDE** nella colonna Secure-capable. Se si desidera creare un gruppo di volumi solo FIPS, cercare **Sì - FIPS** o **Sì - FIPS (misto)**. "Misto" indica una combinazione di dischi di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il gruppo di volumi funzionerà con il livello di protezione inferiore (140-2). • È possibile creare un gruppo di volumi composto da dischi che potrebbero o non essere sicuri o che siano una combinazione di livelli di sicurezza. Se i dischi del gruppo di volumi includono dischi che non supportano la protezione, non è possibile rendere sicuro il gruppo di volumi.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se il gruppo di volumi supporta la protezione ed è stata impostata una chiave di sicurezza, è possibile attivare Drive Security selezionando la casella di controllo. L'unico modo per rimuovere Drive Security dopo l'attivazione è eliminare il gruppo di volumi e cancellare i dischi.

Caratteristica	Utilizzare
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo gruppo. Data Assurance (da) verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Se si desidera utilizzare da, selezionare un gruppo di volumi che supporti da. (Per i dischi compatibili con da, il da viene attivato automaticamente sui volumi creati nel pool). Un gruppo di volumi può contenere dischi che supportano da o non da, ma tutti i dischi devono essere in grado di utilizzare questa funzione.
Funzionalità di provisioning delle risorse (solo EF300 e EF600)	Mostra se il provisioning delle risorse è disponibile per questo gruppo. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.
Protezione contro la perdita di shelf	Mostra se è disponibile la protezione contro la perdita di shelf. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un gruppo di volumi in caso di perdita totale di comunicazione con uno shelf.
Protezione in caso di perdita del cassetto	Mostra se è disponibile la protezione contro le perdite dei cassetti, fornita solo se si utilizza uno shelf di dischi che contiene cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo cassetto in uno shelf di dischi.
Dimensioni dei blocchi di volume supportate (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per i volumi nel gruppo: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Caratteristiche del drive con metodo manuale

Caratteristica	Utilizzare
Tipo di supporto	Indica il tipo di supporto. Sono supportati i seguenti tipi di supporto: • Disco rigido • Solid state Disk (SSD) Tutti i dischi di un gruppo di volumi devono essere dello stesso tipo di supporto (tutti gli SSD o tutti i dischi rigidi). I gruppi di volumi non possono avere una combinazione di tipi di supporti o di tipi di interfaccia.
Dimensioni blocco unità (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che i dischi del gruppo possono scrivere. I valori possono includere: • 512 — dimensione del settore di 512 byte. • 4K — dimensione del settore di 4,096 byte.
Capacità del disco	Indica la capacità del disco. • Se possibile, selezionare dischi con capacità uguale a quella dei dischi correnti del gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità inferiore, tenere presente che la capacità utilizzabile di ciascun disco attualmente presente nel gruppo di volumi è ridotta. Pertanto, la capacità del disco è la stessa per il gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità maggiore, tenere presente che la capacità utilizzabile dei dischi non assegnati aggiunti viene ridotta in modo che corrispondano alle capacità correnti dei dischi nel gruppo di volumi.
Vassoio	Indica la posizione del vassoio del disco.
Slot	Indica la posizione dello slot del disco.
Velocità (giri/min)	Indica la velocità del disco.
Dimensione del settore logico	Indica la dimensione e il formato del settore.

Caratteristica	Utilizzare
Sicuro	Indica se questo gruppo di volumi candidato è composto interamente da dischi con funzionalità di protezione, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). • È possibile proteggere il gruppo di volumi con Drive Security, ma per utilizzare questa funzione è necessario che tutti i dischi siano protetti. • Se si desidera creare un gruppo di volumi solo FDE, cercare **Yes - FDE** nella colonna Secure-capable. Se si desidera creare un gruppo di volumi solo FIPS, cercare **Sì - FIPS** o **Sì - FIPS (misto)**. "Misto" indica una combinazione di dischi di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il gruppo di volumi funzionerà con il livello di protezione inferiore (140-2). • È possibile creare un gruppo di volumi composto da dischi che potrebbero o non essere sicuri o che siano una combinazione di livelli di sicurezza. Se i dischi del gruppo di volumi includono dischi che non supportano la protezione, non è possibile rendere sicuro il gruppo di volumi.
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo gruppo. Data Assurance (da) verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono comunicati ai dischi attraverso i controller. Se si desidera utilizzare da, selezionare un gruppo di volumi che supporti da. (Per i dischi compatibili con da, il da viene attivato automaticamente sui volumi creati nel pool). Un gruppo di volumi può contenere dischi che supportano da o non da, ma tutti i dischi devono essere in grado di utilizzare questa funzione.
Dimensioni dei blocchi di volume supportate (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per i volumi nel gruppo: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.
Funzionalità di provisioning delle risorse (solo EF300 e EF600)	Mostra se il provisioning delle risorse è disponibile per questo gruppo. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Aggiungere capacità a un pool o a un gruppo di volumi

È possibile aggiungere dischi per espandere la capacità libera in un pool o un gruppo di volumi esistente.

L'espansione consente di includere ulteriore capacità libera nel pool o nel gruppo di volumi. È possibile utilizzare questa capacità libera per creare volumi aggiuntivi. I dati nei volumi rimangono accessibili durante questa operazione.

Prima di iniziare

- I dischi devono essere in uno stato ottimale.
- I dischi devono avere lo stesso tipo di disco (HDD o SSD).
- Il pool o il gruppo di volumi deve essere in uno stato ottimale.
- Il numero massimo di volumi consentito in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello di sistema di storage:
  - 2,048 volumi (serie EF600 ed E5700)
  - 1,024 volumi (EF300)
  - 512 volumi (serie E2800)
- Se il pool o il gruppo di volumi contiene tutti i dischi con funzionalità di protezione, aggiungere solo i dischi in grado di protezione per continuare a utilizzare le funzionalità di crittografia dei dischi con funzionalità di protezione.

  Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard).

A proposito di questa attività

Per i pool, è possibile aggiungere un massimo di 60 dischi alla volta. Per i gruppi di volumi, è possibile aggiungere un massimo di due dischi alla volta. Se è necessario aggiungere più dischi del numero massimo, ripetere la procedura. (Un pool non può contenere più dischi rispetto al limite massimo per un sistema storage).

> Con l'aggiunta di dischi, potrebbe essere necessario aumentare la capacità di conservazione. Si consiglia di aumentare la capacità riservata dopo un'operazione di espansione.

> Evitare di utilizzare dischi che siano in grado di aggiungere capacità a un pool o a un gruppo di volumi che non sono in grado di supportare da. Il pool o il gruppo di volumi non può sfruttare le funzionalità del disco da-capable. Prendere in considerazione l'utilizzo di dischi che non sono in grado di supportare da in questa situazione.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il pool o il gruppo di volumi a cui si desidera aggiungere le unità, quindi fare clic su **Add Capacity** (Aggiungi capacità).

   Viene visualizzata la finestra di dialogo Add Capacity (Aggiungi capacità). Vengono visualizzate solo le unità non assegnate compatibili con il pool o il gruppo di volumi.

3. In **Select drives to add Capacity…** (Seleziona dischi per aggiungere capacità), selezionare una o più unità che si desidera aggiungere al pool o al gruppo di volumi esistente.

   Il firmware del controller dispone le unità non assegnate con le opzioni migliori elencate in alto. La capacità libera totale aggiunta al pool o al gruppo di volumi viene visualizzata sotto l'elenco in **capacità totale selezionata**.

Dettagli del campo

Campo	Descrizione
Shelf	Indica la posizione dello shelf del disco.
Baia	Indica la posizione dell'alloggiamento del disco.
Capacità (GiB)	Indica la capacità del disco. • Se possibile, selezionare dischi con capacità uguale a quella dei dischi correnti nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità inferiore, tenere presente che la capacità utilizzabile di ogni disco attualmente presente nel pool o nel gruppo di volumi è ridotta. Pertanto, la capacità del disco è la stessa nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità maggiore, tenere presente che la capacità utilizzabile dei dischi non assegnati aggiunti viene ridotta in modo che corrispondano alle capacità correnti dei dischi nel pool o nel gruppo di volumi.
Sicuro	Indica se il disco è sicuro. • Per proteggere il pool o il gruppo di volumi con la funzione Drive Security, tutti i dischi devono essere protetti. • È possibile creare un pool o un gruppo di volumi con una combinazione di dischi sicuri e non sicuri, ma non è possibile attivare la funzione Drive Security. • Un pool o un gruppo di volumi con tutti i dischi con funzionalità di protezione non può accettare un disco con funzionalità di protezione non sicura per lo sparing o l'espansione, anche se la funzionalità di crittografia non è in uso. • I dischi che vengono segnalati come sicuri possono essere dischi con crittografia completa del disco (FDE) o dischi con tecnologia FIPS (Federal Information Processing Standard). • Un disco FIPS può essere di livello 140-2 o 140-3, con il livello 140-3 come livello di sicurezza superiore. Se si seleziona una combinazione di dischi di livello 140-2 e 140-3, il pool o il gruppo di volumi opereranno al livello di sicurezza inferiore (140-2).

Campo	Descrizione
Compatibile CON DA	Indica se il disco è compatibile con Data Assurance (da). • Si sconsiglia l'utilizzo di dischi che non sono in grado di aggiungere capacità a un pool o a un gruppo di volumi con funzionalità da. Il pool o il gruppo di volumi non dispone più delle funzionalità da e non è più possibile attivare il da sui volumi appena creati all'interno del pool o del gruppo di volumi. • Si sconsiglia l'utilizzo di dischi in grado di aggiungere capacità a un pool o a un gruppo di volumi non compatibili con da, in quanto tale pool o gruppo di volumi non può sfruttare le funzionalità del disco compatibile con da (gli attributi del disco non corrispondono). Considerare l'utilizzo di dischi non compatibili con da in questa situazione.
Compatibile con DULBE	Indica se il disco dispone dell'opzione Deallocated (disallocato) o Unwritten Logical Block Error (DULBE). DULBE è un'opzione sui dischi NVMe che consente allo storage array EF300 o EF600 di supportare volumi con provisioning di risorse.

4. Fare clic su **Aggiungi**.

   Se si aggiungono unità a un pool o a un gruppo di volumi, viene visualizzata una finestra di dialogo di conferma se si seleziona un'unità che impedisce al pool o al gruppo di volumi di avere uno o più dei seguenti attributi:

   - Protezione contro la perdita di shelf
   - Protezione in caso di perdita del cassetto
   - Funzionalità di crittografia completa del disco
   - Funzionalità Data Assurance
   - Funzionalità DULBE
5. Per continuare, fare clic su **Sì**; in caso contrario, fare clic su **Annulla**.

Risultati

Dopo aver aggiunto le unità non assegnate a un pool o a un gruppo di volumi, i dati di ciascun volume del pool o del gruppo di volumi vengono ridistribuiti per includere le unità aggiuntive.

Gestire lo storage

Controllare la ridondanza del volume

Sotto la guida del supporto tecnico o secondo le istruzioni del Recovery Guru, è possibile controllare la ridondanza su un volume in un pool o un gruppo di volumi per determinare se i dati su quel volume sono coerenti.

I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

Prima di iniziare

- Lo stato del pool o del gruppo di volumi deve essere ottimale.
- Il pool o il gruppo di volumi non deve avere alcuna operazione di modifica del volume in corso.
- È possibile controllare la ridondanza su qualsiasi livello RAID tranne su RAID 0, perché RAID 0 non ha ridondanza dei dati.

> Controllare la ridondanza del volume solo quando richiesto dal Recovery Guru e sotto la guida del supporto tecnico.

A proposito di questa attività

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6 e verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se il firmware del controller determina che i dati sono incoerenti.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare **operazioni non comuni › controllare la ridondanza del volume**.

   Viene visualizzata la finestra di dialogo Check Redundancy (verifica ridondanza).

3. Selezionare i volumi da controllare, quindi digitare `check` per confermare che si desidera eseguire questa operazione.
4. Fare clic su **Controlla**.

   Viene avviata l'operazione di controllo della ridondanza del volume. I volumi nel pool o nel gruppo di volumi vengono sottoposti a scansione in sequenza, a partire dalla parte superiore della tabella nella finestra di dialogo. Queste azioni si verificano quando viene eseguita la scansione di ciascun volume:

   - Il volume viene selezionato nella tabella dei volumi.
   - Lo stato del controllo di ridondanza viene visualizzato nella colonna **Status**.
   - Il controllo si interrompe in caso di errore di parità o supporto, quindi riporta l'errore.

Ulteriori informazioni sullo stato del controllo di ridondanza

Stato	Descrizione
In sospeso	Si tratta del primo volume da sottoporre a scansione e non è stato fatto clic su Start (Avvia) per avviare il controllo di ridondanza. oppure L'operazione di controllo della ridondanza viene eseguita su altri volumi nel pool o nel gruppo di volumi.
Verifica in corso	Il volume è sottoposto al controllo di ridondanza.
Superato	Il volume ha superato il controllo di ridondanza. Non sono state rilevate incongruenze nelle informazioni di ridondanza.
Non riuscito	Il volume non ha superato il controllo di ridondanza. Sono state rilevate incoerenze nelle informazioni di ridondanza.
Errore supporto	Il disco rigido è difettoso e illeggibile. Seguire le istruzioni visualizzate nel Recovery Guru.
Errore di parità	La parità non è quella che dovrebbe essere per una determinata parte dei dati. Un errore di parità è potenzialmente grave e potrebbe causare una perdita permanente di dati.

5. Fare clic su **Done** (fine) dopo aver controllato l'ultimo volume del pool o del gruppo di volumi.

Eliminare pool o gruppo di volumi

È possibile eliminare un pool o un gruppo di volumi per creare una maggiore capacità non assegnata, che è possibile riconfigurare per soddisfare le esigenze di storage dell'applicazione.

Prima di iniziare

- È necessario aver eseguito il backup dei dati su tutti i volumi del pool o del gruppo di volumi.
- È necessario aver interrotto tutti gli input/output (i/o).
- È necessario smontare tutti i file system sui volumi.
- È necessario eliminare tutte le relazioni mirror nel pool o nel gruppo di volumi.
- È necessario interrompere qualsiasi operazione di copia del volume in corso per il pool o il gruppo di volumi.
- Il pool o il gruppo di volumi non deve partecipare a un'operazione di mirroring asincrono.
- I dischi nel gruppo di volumi non devono avere una prenotazione persistente.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare un pool o un gruppo di volumi dall'elenco.

   È possibile selezionare un solo pool o gruppo di volumi alla volta. Scorrere l'elenco per visualizzare altri pool o gruppi di volumi.

3. Selezionare **attività non comuni › Elimina** e confermare.

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutti i dati del pool o del gruppo di volumi.
- Elimina tutte le unità associate al pool o al gruppo di volumi.
- Annulla l'assegnazione delle unità associate, che consente di riutilizzarle in pool o gruppi di volumi nuovi o esistenti.

Consolidare la capacità libera per un gruppo di volumi

Utilizzare l'opzione consolida capacità libera per consolidare le estensioni libere esistenti su un gruppo di volumi selezionato. Eseguendo questa azione, è possibile creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi.

Prima di iniziare

- Il gruppo di volumi deve contenere almeno un'area di capacità libera.
- Tutti i volumi nel gruppo di volumi devono essere online e in uno stato ottimale.
- Le operazioni di modifica del volume non devono essere in corso, ad esempio la modifica delle dimensioni del segmento di un volume.

A proposito di questa attività

Non è possibile annullare l'operazione dopo l'inizio. I dati rimangono accessibili durante l'operazione di consolidamento.

È possibile avviare la finestra di dialogo consolida capacità libera utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, il suggerimento "consolidare la capacità libera" viene visualizzato nella home page dell'area di notifica. Fare clic sul collegamento **consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Consolida capacità libera dalla pagina Pools & Volume Groups come descritto nella seguente attività.

Ulteriori informazioni sulle aree di capacità libera

Un'area di capacità libera è la capacità libera che può derivare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità disponibile durante la creazione del volume. Quando si crea un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume viene limitata alla maggiore area di capacità libera del gruppo di volumi. Ad esempio, se un gruppo di volumi ha una capacità libera totale di 15 GiB e l'area di capacità libera più grande è di 10 GiB, il volume più grande che è possibile creare è di 10 GiB.

È possibile consolidare la capacità libera su un gruppo di volumi per migliorare le prestazioni di scrittura. La capacità libera del gruppo di volumi si frammenterà nel tempo man mano che l'host scrive, modifica ed elimina i file. Infine, la capacità disponibile non verrà collocata in un singolo blocco contiguo, ma verrà distribuita in piccoli frammenti all'interno del gruppo di volumi. Ciò causa un'ulteriore frammentazione dei file, poiché l'host deve scrivere nuovi file come frammenti per inserirli negli intervalli disponibili dei cluster liberi.

Consolidando la capacità libera su un gruppo di volumi selezionato, si noteranno migliori performance del file system ogni volta che l'host scrive nuovi file. Il processo di consolidamento consentirà inoltre di evitare la frammentazione dei nuovi file in futuro.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il gruppo di volumi con capacità libera che si desidera consolidare, quindi selezionare **Uncommon Tasks › consolida capacità libera del gruppo di volumi**.

   Viene visualizzata la finestra di dialogo consolida capacità libera.

3. Tipo `consolidate` per confermare che si desidera eseguire questa operazione.
4. Fare clic su **consolida**.

   System Manager inizia a consolidare (deframmentare) le aree di capacità libera del gruppo di volumi in una quantità contigua per le successive attività di configurazione dello storage.

Al termine

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di consolidamento della capacità libera. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Esportare/importare gruppi di volumi

La migrazione dei gruppi di volumi consente di esportare un gruppo di volumi in modo da poter importare il gruppo di volumi in un array di storage diverso.

La funzione di esportazione/importazione non è supportata nell'interfaccia utente di Gestore di sistema di SANtricity. È necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Attivare le luci di individuazione in un pool, un gruppo di volumi o una cache SSD

È possibile individuare le unità per identificare fisicamente tutte le unità che comprendono

un pool, un gruppo di volumi o una cache SSD selezionata. Un indicatore LED si accende su ogni disco nel pool, gruppo di volumi o cache SSD selezionato.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il pool, il gruppo di volumi o la cache SSD che si desidera individuare, quindi fare clic su **More › Turn on locator lights** (attiva indicatori di ricerca).

   Viene visualizzata una finestra di dialogo che indica che le spie dei dischi che compongono il pool, il gruppo di volumi o la cache SSD selezionati sono accese.

3. Una volta individuati correttamente i dischi, fare clic su **Spegni**.

Rimuovere la capacità da un pool o da una cache SSD

È possibile rimuovere i dischi per ridurre la capacità di un pool o di una cache SSD esistente.

Dopo aver rimosso i dischi, i dati in ciascun volume del pool o della cache SSD vengono ridistribuiti nei dischi rimanenti. I dischi rimossi non vengono assegnati e la loro capacità diventa parte della capacità libera totale dell'array di storage.

A proposito di questa attività

Quando si rimuove la capacità, attenersi alle seguenti linee guida:

- Non è possibile rimuovere l'ultimo disco in una cache SSD senza prima eliminare la cache SSD.
- Non è possibile ridurre il numero di dischi in un pool a meno di 11 dischi.
- È possibile rimuovere un massimo di 12 dischi alla volta. Se è necessario rimuovere più di 12 dischi, ripetere la procedura.
- Non è possibile rimuovere i dischi se la capacità libera nel pool o nella cache SSD non è sufficiente per contenere i dati, quando tali dati vengono ridistribuiti ai dischi rimanenti nel pool o nella cache SSD.

Scopri i potenziali impatti sulle performance

- La rimozione dei dischi da un pool o da una cache SSD potrebbe ridurre le performance dei volumi.
- La capacità di conservazione non viene consumata quando si rimuove la capacità da un pool o da una cache SSD. Tuttavia, la capacità di conservazione potrebbe diminuire in base al numero di dischi rimasti nel pool o nella cache SSD.

Scopri gli impatti sui dischi sicuri

- Se si rimuove l'ultimo disco che non supporta la protezione, il pool viene lasciato con tutti i dischi che supportano la protezione. In questa situazione, è possibile attivare la protezione per il pool.
- Se si rimuove l'ultimo disco non compatibile con Data Assurance (da), il pool viene lasciato con tutti i dischi compatibili con da.

Tutti i nuovi volumi creati nel pool saranno compatibili con da. Se si desidera che i volumi esistenti siano compatibili con il da, è necessario eliminare e ricreare il volume.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il pool o la cache SSD, quindi fare clic su **More › Remove Capacity**.

   Viene visualizzata la finestra di dialogo Remove Capacity (capacità di rimozione).

3. Selezionare una o più unità nell'elenco.

   Quando si selezionano o deselezionano i dischi nell'elenco, il campo **capacità totale selezionata** si aggiorna. Questo campo mostra la capacità totale del pool o della cache SSD risultante dopo la rimozione dei dischi selezionati.

4. Fare clic su **Rimuovi**, quindi confermare la rimozione delle unità.

   La nuova capacità ridotta del pool o della cache SSD viene riflessa nella vista Pools e Volume Groups.

Modificare le impostazioni del pool e del gruppo

Modificare le impostazioni di configurazione di un pool

È possibile modificare le impostazioni di un pool, inclusi nome, impostazioni degli avvisi di capacità, priorità di modifica e capacità di conservazione.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni di configurazione per un pool.

> Non è possibile modificare il livello RAID di un pool utilizzando l'interfaccia di System Manager. System Manager configura automaticamente i pool come RAID 6.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il pool che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Pool Setting (impostazione pool).

3. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del pool in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome del pool fornito dall'utente. Specificare un nome per un pool è obbligatorio.
Avvisi di capacità	È possibile inviare notifiche di avviso quando la capacità libera di un pool raggiunge o supera una determinata soglia. Quando i dati memorizzati nel pool superano la soglia specificata, System Manager invia un messaggio, consentendo di aggiungere più spazio di storage o di eliminare oggetti non necessari. Gli avvisi vengono visualizzati nell'area Notifiche della dashboard e possono essere inviati dal server agli amministratori tramite messaggi e-mail e messaggi trap SNMP. È possibile definire i seguenti avvisi di capacità: • **Critical alert** — questo avviso critico informa l'utente quando la capacità libera nel pool raggiunge o supera la soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica. • **Early alert** — questo avviso anticipato informa l'utente quando la capacità libera di un pool sta raggiungendo una soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica.

Impostazione	Descrizione
Priorità di modifica	È possibile specificare i livelli di priorità per le operazioni di modifica in un pool in relazione alle prestazioni del sistema. Una priorità più elevata per le operazioni di modifica in un pool consente di completare più rapidamente un'operazione, ma può rallentare le prestazioni di i/o dell'host. Una priorità più bassa fa sì che le operazioni richiedano più tempo, ma le prestazioni di i/o dell'host ne risentono meno. È possibile scegliere tra cinque livelli di priorità: Minimo, basso, medio, alto e massimo. Maggiore è il livello di priorità, maggiore è l'impatto sull'i/o host e sulle prestazioni del sistema. • **Priorità di ricostruzione critica** — questa barra di scorrimento determina la priorità di un'operazione di ricostruzione dei dati quando guasti multipli dei dischi causano una condizione in cui alcuni dati non hanno ridondanza e un guasto aggiuntivo dei dischi potrebbe causare la perdita di dati. • **Priorità di ricostruzione degradata** — questa barra di scorrimento determina la priorità dell'operazione di ricostruzione dei dati quando si verifica un guasto al disco, ma i dati continuano a essere ridondanti e un guasto aggiuntivo al disco non comporta la perdita di dati. • **Priorità delle operazioni in background** — questa barra di scorrimento determina la priorità delle operazioni in background del pool che si verificano mentre il pool si trova in uno stato ottimale. Queste operazioni includono Dynamic Volume Expansion (DVE), Instant Availability Format (IAF) e la migrazione dei dati su un disco sostituito o aggiunto.

Impostazione	Descrizione
Capacità di conservazione ("capacità di ottimizzazione" per EF600 o EF300)	**Capacità di conservazione** — è possibile definire il numero di dischi per determinare la capacità riservata al pool per supportare potenziali guasti del disco. Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti. I pool utilizzano la capacità di conservazione durante il processo di ricostruzione dei dati invece delle unità hot spare, utilizzate nei gruppi di volumi. Utilizzare i controlli di spinner per regolare il numero di dischi. In base al numero di dischi, la capacità di conservazione nel pool viene visualizzata accanto alla casella di selezione. Tenere presenti le seguenti informazioni sulla capacità di conservazione. • Poiché la capacità di conservazione viene sottratta dalla capacità libera totale di un pool, la quantità di capacità che si riserva influisce sulla quantità di capacità libera disponibile per la creazione dei volumi. Se si specifica 0 per la capacità di conservazione, tutta la capacità libera del pool viene utilizzata per la creazione del volume. • Se si riduce la capacità di conservazione, si aumenta la capacità che può essere utilizzata per i volumi del pool. **Capacità di ottimizzazione aggiuntiva** (solo array EF600 e EF300) — quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e performance e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

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

Modificare le impostazioni di configurazione di un gruppo di volumi

È possibile modificare le impostazioni di un gruppo di volumi, inclusi il nome e il livello RAID.

Prima di iniziare

Se si modifica il livello RAID per soddisfare le esigenze di performance delle applicazioni che accedono al gruppo di volumi, assicurarsi di soddisfare i seguenti prerequisiti:

- Il gruppo di volumi deve trovarsi in uno stato ottimale.
- È necessario disporre di capacità sufficiente nel gruppo di volumi per la conversione al nuovo livello RAID.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il gruppo di volumi che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Group Settings (Impostazioni gruppo di volumi).

3. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del gruppo di volumi in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome fornito dall'utente del gruppo di volumi. Specificare un nome per un gruppo di volumi.
Livello RAID	Selezionare il nuovo livello RAID dal menu a discesa. • **RAID 0 striping** — offre performance elevate, ma non fornisce alcuna ridondanza dei dati. Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi. Un gruppo RAID di striping combina due o più dischi in un'unica grande unità logica. • **Mirroring RAID 1** — offre performance elevate e la migliore disponibilità dei dati, ed è adatto per la memorizzazione di dati sensibili a livello aziendale o personale. Protegge i dati eseguendo automaticamente il mirroring del contenuto di un disco nel secondo disco della coppia mirrorata. Fornisce protezione in caso di guasto di un singolo disco. • **RAID 10 striping/mirroring** — fornisce una combinazione di RAID 0 (striping) e RAID 1 (mirroring) e si ottiene selezionando quattro o più dischi. RAID 10 è adatto per applicazioni di transazioni di volumi elevati, come un database, che richiedono performance elevate e tolleranza agli errori. • **RAID 5** — ottimale per ambienti multiutente (come storage di database o file system) in cui le dimensioni i/o tipiche sono ridotte e l'attività di lettura è molto elevata. • **RAID 6** — ottimale per ambienti che richiedono una protezione di ridondanza oltre RAID 5, ma che non richiedono elevate prestazioni di scrittura. RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando (CLI). Quando si modifica il livello RAID, non è possibile annullare questa operazione dopo l'inizio. Durante la modifica, i dati rimangono disponibili.

Impostazione	Descrizione
Capacità di ottimizzazione (solo array EF600)	Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e prestazioni e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

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

   Viene visualizzata una finestra di dialogo di conferma in caso di riduzione della capacità, perdita della ridondanza del volume o perdita della protezione di shelf/cassetto a seguito della modifica del livello RAID. Selezionare **Sì** per continuare, altrimenti fare clic su **No**.

Risultati

Se si modifica il livello RAID per un gruppo di volumi, System Manager modifica i livelli RAID di ogni volume che comprende il gruppo di volumi. Le prestazioni potrebbero essere leggermente compromesse durante l'operazione.

Attivare o disattivare il provisioning delle risorse nei gruppi di volumi e nei pool esistenti

Per qualsiasi disco compatibile con DULBE, è possibile attivare o disattivare il provisioning delle risorse sui volumi esistenti in un pool o un gruppo di volumi.

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background. Tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati), in modo da migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura.

Per impostazione predefinita, il provisioning delle risorse è attivato nei sistemi in cui i dischi supportano DULBE. Non è necessario attivare il provisioning delle risorse a meno che non sia stato precedentemente disattivato.

Prima di iniziare

- È necessario disporre di uno storage array EF300 o EF600.
- È necessario disporre di gruppi di volumi o pool SSD, in cui tutti i dischi supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). In caso contrario, l'opzione di provisioning delle risorse non è disponibile.

A proposito di questa attività

Quando si attiva il provisioning delle risorse per gruppi di volumi e pool esistenti, tutti i volumi nel gruppo di volumi o pool selezionato vengono modificati per consentire la deallocazione dei blocchi. Questo processo potrebbe comportare un'operazione in background per garantire un'allocazione coerente con la granularità non mappata. Questa operazione non annulla la mappatura dello spazio. Una volta completata l'operazione in background, il sistema operativo deve annullare la mappatura dei blocchi inutilizzati per creare spazio libero.

Quando si disattiva il provisioning delle risorse per gruppi di volumi o pool esistenti, un'operazione in background riscrive tutti i blocchi logici in ogni volume. I dati esistenti rimangono intatti. Le scritture mappano o forniscono i blocchi sui dischi associati al gruppo di volumi o al pool.

> Per i nuovi gruppi di volumi e pool, è possibile attivare o disattivare il provisioning delle risorse dal **Impostazioni › sistema › Impostazioni aggiuntive › attiva/Disattiva volumi con provisioning delle risorse**.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare un pool o un gruppo di volumi dall'elenco.

   È possibile selezionare un solo pool o gruppo di volumi alla volta. Scorrere l'elenco per visualizzare altri pool o gruppi di volumi.

3. Selezionare **Uncommon Tasks**, quindi **Enable resource provisioning** o **Disable resource provisioning**.
4. Nella finestra di dialogo, confermare l'operazione.

> **Se si riattiva DULBE** — al termine dell'operazione in background, potrebbe essere necessario riavviare l'host in modo che rilevi le modifiche di configurazione di DULBE e quindi rimontare tutti i filesystem.

Attivare o disattivare il provisioning delle risorse per nuovi gruppi di volumi o pool

Se in precedenza è stata disattivata la funzionalità predefinita per il provisioning delle risorse, è possibile riattivarla per tutti i nuovi gruppi di volumi SSD o pool creati. È anche possibile disattivare nuovamente l'impostazione.

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background. Tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati), in modo da migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura.

> Per impostazione predefinita, il provisioning delle risorse è attivato nei sistemi in cui i dischi supportano DULBE.

Prima di iniziare

- È necessario disporre di uno storage array EF300 o EF600.
- È necessario disporre di gruppi di volumi o pool SSD, in cui tutti i dischi supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE).

A proposito di questa attività

Quando si riattiva il provisioning delle risorse per nuovi gruppi di volumi o pool, vengono influenzati solo i gruppi di volumi e i pool appena creati. Tutti i gruppi di volumi e i pool esistenti con provisioning delle risorse

abilitato rimarranno invariati.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Scorrere verso il basso fino a **Additional Settings** (Impostazioni aggiuntive), quindi fare clic su **Enable/Disable Resource-Provised Volumes** (attiva/Disattiva volumi con provisioning delle risorse

   La descrizione dell'impostazione indica se il provisioning delle risorse è attualmente attivato o disattivato.

3. Nella finestra di dialogo, confermare l'operazione.

Risultati

L'attivazione o la disattivazione del provisioning delle risorse influisce solo sui nuovi pool di SSD o gruppi di volumi creati dall'utente. I pool o i gruppi di volumi esistenti rimangono invariati.

Abilitare la protezione per un pool o un gruppo di volumi

È possibile attivare Drive Security per un pool o un gruppo di volumi per impedire l'accesso non autorizzato ai dati sulle unità contenute nel pool o nel gruppo di volumi. L'accesso in lettura e scrittura per i dischi è disponibile solo attraverso un controller configurato con una chiave di sicurezza.

Prima di iniziare

- La funzione Drive Security deve essere attivata.
- È necessario creare una chiave di sicurezza.
- Il pool o il gruppo di volumi deve trovarsi in uno stato ottimale.
- Tutti i dischi del pool o del gruppo di volumi devono essere dischi sicuri.

A proposito di questa attività

Se si desidera utilizzare Drive Security, selezionare un pool o un gruppo di volumi che supporti la protezione. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.

Una volta attivato il sistema di protezione, è possibile rimuoverlo solo eliminando il pool o il gruppo di volumi, quindi cancellando i dischi.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare il pool o il gruppo di volumi in cui si desidera attivare la protezione, quindi fare clic su **More › Enable Security** (Altro[attiva protezione]).

   Viene visualizzata la finestra di dialogo Conferma abilitazione protezione.

3. Confermare che si desidera attivare la protezione per il pool o il gruppo di volumi selezionato, quindi fare clic su **Enable** (attiva).

Gestire la cache SSD

Come funziona SSD cache

La funzionalità SSD cache è una soluzione basata su controller che memorizza nella cache i dati più utilizzati (dati "hot") su unità a stato solido (SSD) a bassa latenza per accelerare dinamicamente le prestazioni del sistema. La cache SSD viene utilizzata esclusivamente per le letture host.

Cache SSD rispetto alla cache primaria

La cache SSD è una cache secondaria da utilizzare con la cache primaria nella DRAM (Dynamic Random-Access Memory) del controller.

La cache SSD funziona in modo diverso dalla cache primaria:

- Per la cache primaria, ogni operazione di i/o deve eseguire lo stage dei dati nella cache per eseguire l'operazione.

  Nella cache primaria, i dati vengono memorizzati nella DRAM dopo la lettura da parte di un host.

- La cache SSD viene utilizzata solo se è utile inserire i dati nella cache per migliorare le prestazioni generali del sistema.

  Nella cache SSD, i dati vengono copiati dai volumi e memorizzati su due volumi RAID interni (uno per controller) che vengono creati automaticamente quando si crea una cache SSD.

I volumi RAID interni vengono utilizzati per l'elaborazione della cache interna. Questi volumi non sono accessibili o visualizzati nell'interfaccia utente. Tuttavia, questi due volumi vengono conteggiati rispetto al numero totale di volumi consentiti nell'array di storage.

Come viene utilizzata la cache SSD

Il caching intelligente inserisce i dati in un'unità a latenza inferiore, in modo che le risposte alle richieste future di tali dati possano avvenire molto più velocemente. Se un programma richiede dati che si trovano nella cache (chiamata "cache Hit"), l'unità a latenza inferiore può servire quella transazione. In caso contrario, si verifica un "cache miss" (errore cache) e l'accesso ai dati deve essere effettuato dal disco originale più lento. Man mano che si verificano più accessi alla cache, le performance complessive migliorano.

Quando un programma host accede ai dischi dell'array di storage, i dati vengono memorizzati nella cache SSD. Quando il programma host accede nuovamente agli stessi dati, questi vengono letti dalla cache SSD invece che dai dischi rigidi. I dati ad accesso comune vengono memorizzati nella cache SSD. L'accesso ai dischi rigidi avviene solo quando i dati non possono essere letti dalla cache SSD.

La cache SSD viene utilizzata solo quando è utile inserire i dati nella cache per migliorare le prestazioni generali del sistema.

Quando la CPU deve elaborare i dati di lettura, segue la procedura riportata di seguito:

1. Controllare la cache DRAM.
2. Se non viene trovato nella cache DRAM, controllare la cache SSD.
3. Se non viene trovato nella cache SSD, eseguire la configurazione dal disco rigido. Se i dati sono ritenuti utili per la cache, copiarli nella cache SSD.

Performance migliorate

La copia dei dati più accessibili (hot spot) nella cache SSD consente un funzionamento più efficiente del disco rigido, una latenza ridotta e velocità di lettura e scrittura accelerate. L'utilizzo di SSD dalle performance elevate per la cache dei dati dai volumi HDD migliora le performance di i/o e i tempi di risposta.

Semplici meccanismi di i/o dei volumi vengono utilizzati per spostare i dati da e verso la cache SSD. Dopo che i dati sono stati memorizzati nella cache e memorizzati negli SSD, le successive letture di tali dati vengono eseguite sulla cache SSD, eliminando così la necessità di accedere al volume HDD.

SSD cache e la funzione Drive Security

Per utilizzare la cache SSD su un volume che utilizza anche Drive Security (è abilitato per la protezione), le funzionalità di protezione del disco del volume e della cache SSD devono corrispondere. Se non corrispondono, il volume non sarà abilitato alla protezione.

Implementare la cache SSD

Per implementare la cache SSD, procedere come segue:

1. Creare la cache SSD.
2. Associare la cache SSD ai volumi per i quali si desidera implementare il caching in lettura SSD.

> Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.

Limitazioni della cache SSD

Scopri le restrizioni relative all'utilizzo della cache SSD sull'array di storage.

Restrizioni

- Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.
- Attualmente, è supportata una sola cache SSD per array di storage.
- La capacità massima di cache SSD utilizzabile su un array di storage è di 8 TB.
- La cache SSD non è supportata sulle immagini Snapshot.
- Se si importano o esportano volumi con cache SSD attivata o disattivata, i dati memorizzati nella cache non vengono importati o esportati.
- Non è possibile rimuovere l'ultimo disco in una cache SSD senza prima eliminare la cache SSD.

Restrizioni con Drive Security

- È possibile attivare la sicurezza su SSD cache solo quando si crea la cache SSD. Non è possibile attivare la protezione in un secondo momento, come su un volume.
- Se si utilizzano dischi che supportano la sicurezza con dischi che non sono sicuri in SSD cache, non è possibile attivare Drive Security per questi dischi.
- I volumi abilitati per la sicurezza devono disporre di una cache SSD abilitata per la sicurezza.

Creazione della cache SSD

Per accelerare dinamicamente le performance del sistema, puoi utilizzare la funzione SSD cache per memorizzare nella cache i dati più utilizzati (dati "hot") su unità a stato solido (SSD) a latenza inferiore. La cache SSD viene utilizzata esclusivamente per le letture host.

Prima di iniziare

L'array di storage deve contenere alcune unità SSD.

A proposito di questa attività

Quando si crea una nuova cache SSD, è possibile utilizzare un disco singolo o più dischi. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. Selezionare i volumi che si desidera memorizzare nella cache, quindi il caching viene automaticamente e dinamico.

Per creare una nuova cache SSD, seguire queste linee guida.

- È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
- È supportata una sola cache SSD per array di storage.
- Se solo un volume ha la cache SSD attivata, l'intera cache SSD verrà assegnata al controller proprietario di quel volume.
- La capacità massima di cache SSD utilizzabile su un array di storage dipende dalla capacità della cache primaria del controller.
- La cache SSD non è supportata sulle immagini Snapshot.
- Se si importano o esportano volumi con cache SSD attivata o disattivata, i dati memorizzati nella cache non vengono importati o esportati.
- Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.
- Se i volumi associati sono abilitati per la sicurezza, creare una cache SSD abilitata per la sicurezza.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sul **Create › SSD cache** (Crea[cache SSD]).

   Viene visualizzata la finestra di dialogo Create SSD cache (Crea cache SSD).

3. Digitare un nome per la cache SSD.
4. Selezionare l'SSD cache Candidate che si desidera utilizzare in base alle seguenti caratteristiche.

Caratteristica	Utilizzare
Capacità	Mostra la capacità disponibile in GiB. Seleziona la capacità per le esigenze di storage della tua applicazione. La capacità massima per la cache SSD dipende dalla capacità della cache primaria del controller. Se si assegna una quantità superiore a quella massima alla cache SSD, la capacità aggiuntiva non è utilizzabile. La capacità della cache SSD è importante per la capacità complessiva allocata.
Dischi totali	Mostra il numero di dischi disponibili per questa cache SSD. Selezionare l'SSD candidate con il numero di dischi desiderato.
Sicuro	Indica se SSD cache Candidate è composto interamente da dischi sicuri, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). Se si desidera creare una cache SSD abilitata per la sicurezza, cercare **Sì - FDE** o **Sì - FIPS** nella colonna abilitato per la sicurezza.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se si desidera creare una cache SSD abilitata per la protezione, selezionare la casella di controllo Enable Security (attiva protezione). Una volta attivata, la sicurezza non può essere disattivata. È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo SSD cache Candidate. Data Assurance (da) verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Se si desidera utilizzare il da, selezionare un SSD cache Candidate che sia compatibile con il da. Questa opzione è disponibile solo se la funzione da è stata attivata. La cache SSD può contenere sia dischi da-capable che non da-capable, ma tutti i dischi devono essere da-capable per poter utilizzare da.

5. Associare la cache SSD ai volumi per i quali si desidera implementare il caching in lettura SSD. Per attivare immediatamente la cache SSD sui volumi compatibili, selezionare la casella di controllo **Enable SSD cache on existing compatible volumes that are mapped to hosts** (attiva cache SSD sui volumi compatibili esistenti mappati agli host).

   I volumi sono compatibili se condividono le stesse funzionalità di Drive Security e da.

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

Modificare le impostazioni della cache SSD

È possibile modificare il nome della cache SSD e visualizzarne lo stato, la capacità massima e corrente, lo stato di Drive Security e Data Assurance e i volumi e i dischi associati.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la cache SSD che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo SSD cache Settings (Impostazioni cache SSD).

3. Rivedere o modificare le impostazioni della cache SSD in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Nome	Visualizza il nome della cache SSD, che è possibile modificare. È necessario specificare un nome per la cache SSD.
Caratteristiche	Mostra lo stato della cache SSD. Gli stati possibili includono: • Ottimale • Sconosciuto • Degradato • Non riuscito (Uno stato di errore determina un evento MEL critico). • Sospeso
Capacità	Mostra la capacità corrente e la capacità massima consentita per la cache SSD. La capacità massima consentita per la cache SSD dipende dalle dimensioni della cache principale del controller: • Fino a 1 GiB • Da 1 GiB a 2 GiB • Da 2 GiB a 4 GiB • Più di 4 GiB
Sicurezza e da	Mostra lo stato di Drive Security e Data Assurance per la cache SSD. • **Secure-capable** — indica se la cache SSD è composta interamente da dischi sicuri. Un disco sicuro è un disco con crittografia automatica in grado di proteggere i propri dati da accessi non autorizzati. • **Secure-enabled** — indica se la sicurezza è attivata nella cache SSD. • **Da Capable** — indica se la cache SSD è composta interamente da dischi compatibili con da. Un disco con funzionalità da può controllare e correggere gli errori che potrebbero verificarsi quando i dati vengono comunicati tra l'host e lo storage array.
Oggetti associati	Mostra i volumi e i dischi associati alla cache SSD.

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

Visualizzare le statistiche della cache SSD

È possibile visualizzare le statistiche per la cache SSD, ad esempio letture, scritture, accessi alla cache, percentuale di allocazione della cache, e percentuale di utilizzo della cache.

Le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate, sono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare statistiche dettagliate per la cache SSD solo quando si esportano tutte le statistiche SSD in a. `.csv` file.

Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la cache SSD per la quale si desidera visualizzare le statistiche, quindi fare clic su **More › View SSD cache statistics** (Visualizza statistiche cache SSD).

   Viene visualizzata la finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD) che visualizza le statistiche nominali per la cache SSD selezionata.

   Dettagli del campo

Impostazioni	Descrizione
Letture	Mostra il numero totale di letture host dai volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Scrive	Il numero totale di scritture dell'host nei volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Riscontri nella cache	Mostra il numero di accessi alla cache.
La cache colpisce %	Mostra la percentuale di accessi alla cache. Questo numero deriva da riscontri cache / (letture + scritture). La percentuale di hit della cache deve essere superiore al 50% per un funzionamento efficace della cache SSD.
Allocazione della cache %	Mostra la percentuale di storage cache SSD allocato, espressa come percentuale dello storage cache SSD disponibile per questo controller e derivata dai byte allocati/disponibili.
% Utilizzo cache	Mostra la percentuale di storage cache SSD che contiene i dati dei volumi abilitati, espressa come percentuale di storage cache SSD allocata. Questa quantità rappresenta l'utilizzo o la densità della cache SSD. Derivato da byte allocati/byte disponibili.
Esporta tutto	Esporta tutte le statistiche della cache SSD in formato CSV. Il file esportato contiene tutte le statistiche disponibili per la cache SSD (nominale e dettagliata).

3. Fare clic su **Annulla** per chiudere la finestra di dialogo.

Gestire la capacità riservata

Come funziona la capacità riservata

La capacità riservata viene creata automaticamente quando vengono fornite le operazioni del servizio di copia, ad esempio snapshot o operazioni di mirroring asincrono, per i volumi.

Lo scopo della capacità riservata è memorizzare le modifiche dei dati su questi volumi, in caso di problemi. Analogamente ai volumi, la capacità riservata viene creata da pool o gruppi di volumi.

Copiare gli oggetti del servizio che utilizzano la capacità riservata

La capacità riservata è il meccanismo di storage sottostante utilizzato dai seguenti oggetti del servizio di copia:

- Gruppi di snapshot
- Volumi snapshot di lettura/scrittura
- Volumi membri del gruppo di coerenza
- Volumi di coppia mirrorati

Quando si creano o si espandono questi oggetti del servizio di copia, è necessario creare una nuova capacità riservata da un pool o da un gruppo di volumi. La capacità riservata corrisponde in genere al 40% del volume di base per le operazioni di snapshot e al 20% del volume di base per le operazioni di mirroring asincrono. Tuttavia, la capacità riservata varia in base al numero di modifiche apportate ai dati originali.

Thin volumi e capacità riservata

Per un volume sottile, se è stata raggiunta la capacità massima di 256 TIB, non è possibile aumentarla. Assicurarsi che la capacità riservata del volume thin sia impostata su una dimensione superiore alla capacità massima indicata. (Un thin volume viene sempre sottoposto a thin provisioning, il che significa che la capacità viene allocata durante la scrittura dei dati nel volume).

Se si crea capacità riservata utilizzando un volume thin in un pool, esaminare le seguenti azioni e i risultati sulla capacità riservata:

- Se la capacità riservata di un volume thin non funziona, il volume thin stesso non passa automaticamente allo stato Failed (non riuscito). Tuttavia, poiché tutte le operazioni di i/o su un volume thin richiedono l'accesso al volume di capacità riservato, le operazioni di i/o restituiranno sempre una condizione di controllo all'host richiedente. Se il problema sottostante con il volume di capacità riservata può essere risolto, il volume di capacità riservato viene riportato a uno stato ottimale e il volume sottile diventa nuovamente funzionale.
- Se si utilizza un thin volume esistente per completare una coppia di mirroring asincrono, tale thin volume viene reinizializzato con un nuovo volume a capacità riservata. Durante il processo di sincronizzazione iniziale vengono trasferiti solo i blocchi con provisioning sul lato primario.

Avvisi di capacità

L'oggetto del servizio di copia dispone di un avviso di capacità configurabile e di una soglia di avviso, nonché di una risposta configurabile quando la capacità riservata è piena.

Quando la capacità riservata di un volume di oggetto del servizio di copia si avvicina al punto di riempimento, viene emesso un avviso all'utente. Per impostazione predefinita, questo avviso viene visualizzato quando il volume di capacità riservato è pieno al 75%; tuttavia, è possibile regolare questo punto di avviso verso l'alto o

verso il basso in base alle necessità. Se si riceve questo avviso, è possibile aumentare la capacità del volume di capacità riservato in quel momento. A questo proposito, ciascun oggetto del servizio di copia può essere configurato in modo indipendente.

Volumi di capacità riservati orfani

Un volume di capacità riservata orfano è un volume che non memorizza più i dati per le operazioni del servizio di copia in quanto l'oggetto del servizio di copia associato è stato eliminato. Quando l'oggetto del servizio di copia è stato eliminato, anche il volume di capacità riservata doveva essere eliminato. Tuttavia, non è stato possibile eliminare il volume con capacità riservata.

Poiché i volumi di capacità riservati orfani non sono accessibili da alcun host, sono candidati per la richiesta di recupero. Eliminare manualmente il volume di capacità riservata orfano in modo da poterne utilizzare la capacità per altre operazioni.

System Manager avvisa l'utente dei volumi di capacità riservati orfani con un messaggio "recuperare capacità inutilizzata" nell'area Notifiche della home page. È possibile fare clic su **recuperare capacità inutilizzata** per visualizzare la finestra di dialogo recuperare capacità inutilizzata, in cui è possibile eliminare il volume di capacità riservata orfano.

Caratteristiche della capacità riservata

- La capacità allocata alla capacità riservata deve essere presa in considerazione durante la creazione del volume per mantenere una capacità libera sufficiente.
- La capacità riservata può essere inferiore al volume di base (la dimensione minima è 8 MiB).
- Una parte dello spazio viene consumata dai metadati, ma è molto piccola (192 KiB), quindi non è necessario che venga presa in considerazione quando si determina la dimensione del volume di capacità riservata.
- La capacità riservata non è direttamente leggibile o scrivibile da un host.
- Esiste una capacità riservata per ogni volume snapshot di lettura/scrittura, gruppo di snapshot, volume membro del gruppo di coerenza e volume coppia mirrorata.

Aumentare la capacità riservata

È possibile aumentare la capacità riservata, ovvero la capacità fisicamente allocata utilizzata per qualsiasi operazione di servizio di copia su un oggetto di storage.

Per le operazioni di snapshot, si tratta in genere del 40% del volume di base; per le operazioni di mirroring asincrono si tratta in genere del 20% del volume di base. In genere, si aumenta la capacità riservata quando si riceve un avviso che indica che la capacità riservata dell'oggetto di storage sta diventando piena.

Prima di iniziare

- Il volume nel pool o nel gruppo di volumi deve avere uno stato ottimale e non deve essere in alcun stato di modifica.
- La capacità libera deve essere presente nel pool o nel gruppo di volumi che si desidera utilizzare per aumentare la capacità.

  Se non esiste capacità libera in alcun pool o gruppo di volumi, è possibile aggiungere capacità non assegnata sotto forma di unità inutilizzate a un pool o a un gruppo di volumi.

A proposito di questa attività

È possibile aumentare la capacità riservata solo con incrementi di 8 GiB per i seguenti oggetti di storage:

- Gruppo di snapshot
- Volume Snapshot
- Volume membro del gruppo di coerenza
- Volume di coppia mirrorato

Utilizzare una percentuale elevata se si ritiene che il volume primario subirà molte modifiche o se la durata di una determinata operazione di servizio di copia sarà molto lunga.

> Non è possibile aumentare la capacità riservata per un volume di snapshot di sola lettura. Solo i volumi Snapshot in lettura/scrittura richiedono una capacità riservata.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la scheda **capacità riservata**.
3. Selezionare l'oggetto di storage per il quale si desidera aumentare la capacità riservata, quindi fare clic su **aumenta capacità**.

   Viene visualizzata la finestra di dialogo aumenta capacità riservata.

4. Utilizzare la casella di selezione per regolare la percentuale di capacità.

   Se la capacità libera non esiste nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage dispone di capacità non assegnata, è possibile creare un nuovo pool o gruppo di volumi. È quindi possibile riprovare a eseguire questa operazione utilizzando la nuova capacità libera del pool o del gruppo di volumi.

5. Fare clic su **aumenta**.

Risultati

System Manager esegue le seguenti operazioni:

- Aumenta la capacità riservata per l'oggetto di storage.
- Visualizza la capacità riservata aggiunta di recente.

Ridurre la capacità riservata

L'opzione Riduci capacità consente di ridurre la capacità riservata per i seguenti oggetti di storage: Gruppo di snapshot, volume di snapshot e volume membro del gruppo di coerenza. È possibile ridurre la capacità riservata solo della quantità utilizzata per aumentarla.

Prima di iniziare

- L'oggetto di storage deve contenere più di un volume di capacità riservato.
- L'oggetto di storage non deve essere un volume di coppia mirrorato.
- Se l'oggetto di storage è un volume di snapshot, deve essere un volume di snapshot disattivato.
- Se l'oggetto di storage è un gruppo di snapshot, non deve contenere alcuna immagine snapshot associata.

A proposito di questa attività

Consultare le seguenti linee guida:

- È possibile rimuovere i volumi a capacità riservata solo nell'ordine inverso rispetto a quello in cui sono stati aggiunti.
- Non è possibile ridurre la capacità riservata per un volume snapshot di sola lettura perché non dispone di capacità riservata associata. Solo i volumi Snapshot in lettura/scrittura richiedono una capacità riservata.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare l'oggetto di storage per il quale si desidera ridurre la capacità riservata, quindi fare clic su **Riduci capacità**.

   Viene visualizzata la finestra di dialogo Riduci capacità riservata.

4. Selezionare la capacità di cui si desidera ridurre la capacità riservata, quindi fare clic su **Riduci**.

Risultati

System Manager esegue le seguenti operazioni:

- Aggiorna la capacità dell'oggetto storage.
- Visualizza la capacità riservata aggiornata per l'oggetto di storage.
- Quando si riduce la capacità di un volume di snapshot, System Manager passa automaticamente il volume di snapshot a uno stato Disabled (Disattivato). Disattivato indica che il volume snapshot non è attualmente associato a un'immagine snapshot e, di conseguenza, non può essere assegnato a un host per i/O.

Modificare le impostazioni di capacità riservata per un gruppo di snapshot

È possibile modificare le impostazioni di un gruppo di snapshot per modificarne il nome, le impostazioni di eliminazione automatica, il numero massimo di immagini snapshot consentite, il punto percentuale in cui System Manager invia una notifica di avviso di capacità riservata o il criterio da utilizzare quando la capacità riservata raggiunge la percentuale massima definita.

Durante la creazione di un gruppo di snapshot, viene creata una capacità riservata per memorizzare i dati di tutte le immagini di snapshot contenute nel gruppo.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare il gruppo di snapshot che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo Snapshot Group Settings (Impostazioni gruppo snapshot).

4. Modificare le impostazioni del gruppo di snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Impostazioni gruppo Snapshot	Nome
Il nome del gruppo di snapshot. Specificare un nome per il gruppo di snapshot è obbligatorio.	Eliminazione automatica
Un'impostazione che mantiene il numero totale di immagini snapshot nel gruppo pari o inferiore a un massimo definito dall'utente. Quando questa opzione è attivata, System Manager elimina automaticamente l'immagine snapshot meno recente nel gruppo ogni volta che viene creata una nuova istantanea, in modo da rispettare il numero massimo di immagini snapshot consentito per il gruppo.	Limite dell'immagine Snapshot
Un valore configurabile che specifica il numero massimo di immagini snapshot consentite per un gruppo di snapshot.	Calendario di Snapshot
Se sì, viene impostata una pianificazione per la creazione automatica di snapshot.	**Impostazioni di capacità riservate**

Impostazione	Descrizione
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per un gruppo di snapshot è quasi piena. Quando la capacità riservata per il gruppo di snapshot supera la soglia specificata, System Manager invia un avviso, consentendo di aumentare la capacità riservata o di eliminare oggetti non necessari.
Policy per la capacità massima riservata	È possibile scegliere una delle seguenti policy: • **Rimuovi l'immagine snapshot meno recente** — System Manager rimuove automaticamente l'immagine snapshot meno recente nel gruppo di snapshot, che rilascia la capacità riservata dell'immagine snapshot per il riutilizzo all'interno del gruppo. • **Rifiuta scritture nel volume di base** — quando la capacità riservata raggiunge la massima percentuale definita, System Manager rifiuta qualsiasi richiesta di scrittura i/o nel volume di base che ha attivato l'accesso alla capacità riservata.
Oggetti associati	Volume di base
Il nome del volume di base utilizzato per il gruppo. Un volume di base è l'origine da cui viene creata un'immagine snapshot. Può essere un volume spesso o sottile e viene in genere assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un pool di dischi.	Immagini Snapshot

5. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni del gruppo di snapshot.

Modificare le impostazioni di capacità riservata per un volume di snapshot

È possibile modificare le impostazioni di un volume di snapshot per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata di un volume di snapshot è quasi piena.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare il volume di snapshot che si desidera modificare, quindi fare clic su **View/Edit Settings**

(Visualizza/Modifica impostazioni).

Viene visualizzata la finestra di dialogo Snapshot Volume Reserved Capacity Settings (Impostazioni capacità riservata volume snapshot).

4. Modificare le impostazioni di capacità riservata per il volume di snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per un volume membro è quasi piena. Quando la capacità riservata per il volume di snapshot supera la soglia specificata, il sistema invia un avviso, consentendo di aumentare la capacità riservata o di eliminare oggetti non necessari.

5. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni della capacità riservata del volume di snapshot.

Modificare le impostazioni di capacità riservata per un volume membro del gruppo di coerenza

È possibile modificare le impostazioni di un volume membro del gruppo di coerenza per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata di un volume membro è quasi piena e per modificare il criterio da utilizzare quando la capacità riservata raggiunge il valore massimo definito percentuale.

A proposito di questa attività

La modifica delle impostazioni di capacità riservata per un singolo volume membro modifica anche le impostazioni di capacità riservata per tutti i volumi membri associati a un gruppo di coerenza.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare il volume membro del gruppo di coerenza che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Member Volume Reserved Capacity Settings (Impostazioni capacità riservata volume membro).

4. Modificare le impostazioni di capacità riservata per il volume membro in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per un volume membro è quasi piena. Quando la capacità riservata per il volume membro supera la soglia specificata, System Manager invia un avviso, consentendo di aumentare la capacità riservata o di eliminare oggetti non necessari. La modifica dell'impostazione Avviso per un volume membro lo modifica per *tutti* volumi membri appartenenti allo stesso gruppo di coerenza.
Policy per la capacità massima riservata	È possibile scegliere una delle seguenti policy: • **Rimuovi l'immagine snapshot meno recente** — System Manager rimuove automaticamente l'immagine snapshot meno recente nel gruppo di coerenza, che rilascia la capacità riservata del membro per il riutilizzo all'interno del gruppo. • **Rifiuta scritture nel volume di base** — quando la capacità riservata raggiunge la massima percentuale definita, System Manager rifiuta qualsiasi richiesta di scrittura i/o nel volume di base che ha attivato l'accesso alla capacità riservata.

5. Fare clic su **Save** (Salva) per applicare le modifiche.

Risultati

System Manager modifica le impostazioni di capacità riservata per il volume membro, nonché le impostazioni di capacità riservata per tutti i volumi membro del gruppo di coerenza.

Modificare le impostazioni di capacità riservata per un volume di coppia mirrorata

È possibile modificare le impostazioni di un volume di coppia mirrorata per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per un volume di coppia mirrorata è quasi piena.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la scheda **capacità riservata**.
3. Selezionare il volume della coppia mirrorata che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni capacità riservata volume coppia mirrorata.

4. Modificare le impostazioni di capacità riservata per il volume di coppia mirrorata in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per una coppia mirrorata è quasi piena. Quando la capacità riservata per la coppia mirrorata supera la soglia specificata, System Manager invia un avviso, consentendo di aumentare la capacità riservata. La modifica dell'impostazione Avviso per una coppia mirrorata modifica l'impostazione Avviso per tutte le coppie mirrorate che appartengono allo stesso gruppo di coerenza mirror.

5. Fare clic su **Save** (Salva) per applicare le modifiche.

Annulla l'immagine snapshot in sospeso

È possibile annullare un'immagine snapshot in sospeso prima del completamento. Gli snapshot vengono eseguiti in modo asincrono e lo stato dello snapshot rimane in sospeso fino al completamento dello snapshot. L'immagine snapshot viene completata al termine dell'operazione di sincronizzazione.

A proposito di questa attività

Un'immagine snapshot si trova in uno stato in sospeso a causa delle seguenti condizioni simultanee:

- Il volume di base per un gruppo di snapshot o uno o più volumi membri di un gruppo di coerenza che contiene questa immagine snapshot è membro di un gruppo di mirror asincrono.
- Il volume o i volumi sono attualmente in un'operazione di sincronizzazione del mirroring asincrono.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare il gruppo di snapshot per il quale si desidera annullare un'immagine snapshot in sospeso, quindi fare clic su **attività non comuni › Annulla immagine snapshot in sospeso**.
4. Fare clic su **Sì** per confermare che si desidera annullare l'immagine istantanea in sospeso.

Elimina gruppo di snapshot

Si elimina un gruppo di snapshot quando si desidera eliminarne definitivamente i dati e rimuoverlo dal sistema. L'eliminazione di un gruppo di snapshot consente di recuperare la capacità riservata per il riutilizzo nel pool o nel gruppo di volumi.

A proposito di questa attività

Quando si elimina un gruppo di snapshot, vengono eliminate anche tutte le immagini snapshot del gruppo.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Fare clic sulla scheda **Reserved Capacity** (capacità riservata).
3. Selezionare il gruppo di snapshot che si desidera eliminare, quindi fare clic su **attività non comuni › Elimina gruppo di snapshot**.

   Viene visualizzata la finestra di dialogo Confirm Delete Snapshot Group.

4. Tipo `delete` per confermare.

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutte le immagini snapshot associate al gruppo di snapshot.
- Disattiva tutti i volumi di snapshot associati alle immagini del gruppo di snapshot.
- Elimina la capacità riservata esistente per il gruppo di snapshot.

FAQ

Che cos'è un gruppo di volumi?

Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.

Che cos'è un pool?

Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.

I pool possono eliminare la necessità per gli amministratori di monitorare l'utilizzo su ciascun host per determinare quando è probabile che esauriscano lo spazio di storage ed evitare le interruzioni di ridimensionamento dei dischi convenzionali. Quando un pool si sta esaurendo, è possibile aggiungere dischi aggiuntivi al pool senza interruzioni e la crescita della capacità è trasparente per l'host.

Con i pool, i dati vengono ridistribuiti automaticamente per mantenere l'equilibrio. Distribuendo le informazioni di parità e la capacità di riserva in tutto il pool, ogni disco del pool può essere utilizzato per ricostruire un disco guasto. Questo approccio non utilizza dischi hot spare dedicati, ma la capacità di conservazione (spare) viene riservata in tutto il pool. In caso di guasto al disco, i segmenti su altri dischi vengono letti per ricreare i dati. Viene quindi scelto un nuovo disco per scrivere ciascun segmento che si trovava su un disco guasto in modo da mantenere la distribuzione dei dati tra i dischi.

Che cos'è la capacità riservata?

La capacità riservata è la capacità allocata fisicamente che memorizza i dati per gli oggetti del servizio di copia come immagini snapshot, volumi membri del gruppo di coerenza e volumi di coppia mirrorati.

Il volume di capacità riservata associato a un'operazione di servizio di copia risiede in un pool o in un gruppo di volumi. La capacità riservata viene creata da un pool o da un gruppo di volumi.

Che cos'è la sicurezza FDE/FIPS?

La protezione FDE/FIPS si riferisce a dischi sicuri che crittografano i dati durante la scrittura e decrittare i dati durante la lettura utilizzando una chiave di crittografia univoca. Queste unità sicure impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage.

Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). I dischi FIPS sono stati sottoposti a test di certificazione.

> Per i volumi che richiedono il supporto FIPS, utilizzare solo dischi FIPS. La combinazione di dischi FIPS e FDE in un gruppo di volumi o in un pool comporterà il trattamento di tutti i dischi come dischi FDE. Inoltre, un disco FDE non può essere aggiunto o utilizzato come spare in un gruppo di volumi o pool all-FIPS.

Che cos'è il controllo di ridondanza?

Un controllo di ridondanza determina se i dati su un volume in un pool o un gruppo di volumi sono coerenti. I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6, quindi verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se i dati sono determinati come incoerenti dal firmware del controller.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Quali sono le differenze tra pool e gruppi di volumi?

Un pool è simile a un gruppo di volumi, con le seguenti differenze.

- I dati di un pool vengono memorizzati in modo casuale su tutti i dischi del pool, a differenza dei dati di un gruppo di volumi, che vengono memorizzati sullo stesso set di dischi.
- Un pool presenta un minor degrado delle performance in caso di guasto di un disco e richiede meno tempo per la ricostruzione.
- Un pool dispone di capacità di conservazione integrata, pertanto non richiede dischi hot spare dedicati.
- Un pool consente di raggruppare un gran numero di dischi.

- Un pool non richiede un livello RAID specificato.

Perché dovrei configurare manualmente un pool?

I seguenti esempi descrivono il motivo per cui si desidera configurare manualmente un pool.

- Se si dispone di più applicazioni sull'array di storage e non si desidera che queste possano competere con le stesse risorse del disco, si potrebbe prendere in considerazione la possibilità di creare manualmente un pool più piccolo per una o più applicazioni.

  È possibile assegnare solo uno o due volumi invece di assegnare il carico di lavoro a un pool di grandi dimensioni con molti volumi attraverso i quali distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di un'applicazione specifica può consentire alle operazioni degli array di storage di funzionare più rapidamente, con meno conflitti.

  Per creare manualmente un pool: Selezionare **Storage**, quindi selezionare **Pools & Volume Groups**. Dalla scheda All Capacity (tutte le capacità), fare clic su **Create › Pool** (Crea[Pool]).

- Se sono presenti più pool dello stesso tipo di disco, viene visualizzato un messaggio che indica che System Manager non può consigliare automaticamente i dischi per un pool. Tuttavia, è possibile aggiungere manualmente le unità a un pool esistente.

  Per aggiungere manualmente le unità a un pool esistente: Dalla pagina Pools & Volume Groups, selezionare il pool, quindi fare clic su **Add Capacity** (Aggiungi capacità).

Perché gli avvisi di capacità sono importanti?

Gli avvisi relativi alla capacità indicano quando aggiungere dischi a un pool. Un pool ha bisogno di capacità libera sufficiente per eseguire correttamente le operazioni degli array di storage. È possibile evitare interruzioni di queste operazioni configurando System Manager in modo che invii avvisi quando la capacità libera di un pool raggiunge o supera una determinata percentuale.

Questa percentuale viene impostata quando si crea un pool utilizzando l'opzione **Pool auto-Configuration** o l'opzione **Create pool**. Se si sceglie l'opzione automatica, le impostazioni predefinite determinano automaticamente quando si ricevono notifiche di avviso. Se si sceglie di creare manualmente il pool, è possibile determinare le impostazioni di notifica degli avvisi oppure, se si preferisce, è possibile accettare le impostazioni predefinite. È possibile regolare queste impostazioni in un secondo momento nel **Impostazioni › Avvisi**.

> Quando la capacità libera nel pool raggiunge la percentuale specificata, viene inviata una notifica di avviso utilizzando il metodo specificato nella configurazione di avviso.

Perché non posso aumentare la mia capacità di conservazione?

Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, potrebbe non essere possibile aumentare la capacità di conservazione.

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata a un pool per supportare potenziali guasti del disco. Quando viene creato un pool, il sistema riserva automaticamente una quantità

predefinita di capacità di conservazione in base al numero di dischi nel pool. Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, non è possibile aumentare la capacità di conservazione senza aggiungere capacità al pool aggiungendo unità o eliminando volumi.

È possibile modificare la capacità di conservazione da **Pools & Volume Groups**. Selezionare il pool che si desidera modificare. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni), quindi selezionare la scheda **Settings** (Impostazioni).

> La capacità di conservazione viene specificata come un numero di dischi, anche se la capacità di conservazione effettiva viene distribuita tra i dischi del pool.

Esiste un limite al numero di dischi che è possibile rimuovere da un pool?

System Manager definisce i limiti per il numero di dischi che è possibile rimuovere da un pool.

- Non è possibile ridurre il numero di dischi in un pool a meno di 11 dischi.
- Non è possibile rimuovere le unità se nel pool non è disponibile una capacità libera sufficiente per contenere i dati delle unità rimosse quando tali dati vengono ridistribuiti alle altre unità del pool.
- È possibile rimuovere un massimo di 60 dischi alla volta. Se si selezionano più di 60 dischi, l'opzione Rimuovi dischi viene disattivata. Se è necessario rimuovere più di 60 dischi, ripetere l'operazione di rimozione dei dischi.

Quali tipi di supporto sono supportati per un disco?

Sono supportati i seguenti tipi di supporti: Disco rigido (HDD) e disco a stato solido (SSD).

Perché alcuni dischi non vengono visualizzati?

Nella finestra di dialogo Add Capacity (Aggiungi capacità), non tutti i dischi sono disponibili per l'aggiunta di capacità a un pool o a un gruppo di volumi esistente.

I dischi non sono idonei per uno dei seguenti motivi:

- Un disco deve essere non assegnato e non abilitato alla sicurezza. I dischi già parte di un altro pool, di un altro gruppo di volumi o configurati come hot spare non sono idonei. Se un disco non è assegnato ma è abilitato per la protezione, è necessario cancellarlo manualmente affinché sia idoneo.
- Un disco in uno stato non ottimale non è idoneo.
- Se la capacità di un disco è troppo piccola, non è idonea.
- Il tipo di disco deve corrispondere all'interno di un pool o di un gruppo di volumi. Non è possibile combinare i seguenti elementi:
  - Dischi rigidi (HDD) con dischi a stato solido (SSD)
  - NVMe con unità SAS
  - Dischi con blocchi di volumi da 512 byte e 4 KiB
- Se un pool o un gruppo di volumi contiene tutti i dischi con funzionalità di protezione, i dischi con funzionalità di protezione non sono elencati.
- Se un pool o un gruppo di volumi contiene tutti i dischi FIPS (Federal Information Processing Standard), i

dischi non FIPS non sono elencati.

- Se un pool o un gruppo di volumi contiene tutte le unità compatibili con Data Assurance (da) e nel pool o nel gruppo di volumi è presente almeno un volume abilitato da, un'unità che non supporta da non è idonea, quindi non può essere aggiunta a tale pool o gruppo di volumi. Tuttavia, se nel pool o nel gruppo di volumi non è presente alcun volume abilitato da, è possibile aggiungere un'unità che non supporta da a a tale pool o gruppo di volumi. Se si decide di combinare questi dischi, tenere presente che non è possibile creare volumi abilitati da.

> È possibile aumentare la capacità dell'array di storage aggiungendo nuove unità o eliminando pool o gruppi di volumi.

Come posso mantenere la protezione contro le perdite di scaffali/cassetti?

Per mantenere la protezione dalle perdite di shelf/cassetto per un pool o un gruppo di volumi, utilizzare i criteri specificati nella tabella seguente.

Livello	Criteri per la protezione contro le perdite di scaffali/cassetti	Numero minimo di ripiani/cassetti richiesti
Piscina	Per gli shelf, il pool non deve contenere più di due dischi in un singolo shelf. Per i cassetti, il pool deve includere un numero uguale di unità da ciascun cassetto.	6 per gli shelf 5 per cassetti
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo shelf o cassetto.	3
RAID 3 o RAID 5	Ciascuna unità del gruppo di volumi si trova in uno shelf o in un cassetto separato.	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in uno shelf o in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di scaffali/cassetti.	Non applicabile

> La protezione contro le perdite di shelf/cassetto non viene mantenuta se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf o a un cassetto di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

Qual è il posizionamento ottimale del disco per pool e gruppi di volumi?

Quando si creano pool e gruppi di volumi, assicurarsi di bilanciare la selezione del disco

tra gli slot superiori e inferiori.

Per i controller EF600 e EF300, gli slot 0-11 sono collegati a un bridge PCI, mentre gli slot 12-23 sono collegati a un bridge PCI diverso. Per ottenere prestazioni ottimali, è necessario bilanciare la selezione del disco in modo da includere un numero quasi uguale di dischi dagli slot superiore e inferiore. Questo posizionamento garantisce che i volumi non raggiungano un limite di larghezza di banda prima del necessario.

Qual è il livello RAID migliore per la mia applicazione?

Per massimizzare le performance di un gruppo di volumi, è necessario selezionare il livello RAID appropriato. È possibile determinare il livello RAID appropriato conoscendo le percentuali di lettura e scrittura per le applicazioni che accedono al gruppo di volumi. Utilizzare la pagina Performance (prestazioni) per ottenere queste percentuali.

Livelli RAID e performance applicative

RAID si basa su una serie di configurazioni, denominate *livelli*, per determinare il modo in cui i dati di ridondanza e dell'utente vengono scritti e recuperati dai dischi. Ogni livello RAID offre diverse funzionalità di performance. Le applicazioni con un'elevata percentuale di lettura sono in grado di funzionare correttamente utilizzando volumi RAID 5 o RAID 6, a causa delle eccezionali prestazioni di lettura delle configurazioni RAID 5 e RAID 6.

Le applicazioni con una bassa percentuale di lettura (elevata intensità di scrittura) non funzionano altrettanto sui volumi RAID 5 o RAID 6. Le prestazioni degradate sono il risultato del modo in cui un controller scrive i dati e i dati di ridondanza sui dischi di un gruppo di volumi RAID 5 o RAID 6.

Selezionare un livello RAID in base alle seguenti informazioni.

RAID 0

- **Descrizione**
  - Non ridondante, modalità striping.
- **Come funziona**
  - RAID 0 esegue lo striping dei dati su tutti i dischi del gruppo di volumi.
- **Caratteristiche di protezione dei dati**
  - RAID 0 non è consigliato per esigenze di alta disponibilità. RAID 0 è migliore per i dati non critici.
  - Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi.
- **Requisiti del numero di unità**
  - Per RAID livello 0 è richiesto un minimo di un disco.
  - I gruppi di volumi RAID 0 possono avere più di 30 dischi.
  - È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 1 o RAID 10

- **Descrizione**
  - Modalità striping/mirror.
- **Come funziona**

    - RAID 1 utilizza il mirroring del disco per scrivere i dati su due dischi duplicati contemporaneamente.
    - RAID 10 utilizza lo striping dei dischi per eseguire lo striping dei dati su un set di coppie di dischi mirrorati.
- **Caratteristiche di protezione dei dati**
    - RAID 1 e RAID 10 offrono performance elevate e la migliore disponibilità dei dati.
    - RAID 1 e RAID 10 utilizzano il mirroring del disco per eseguire una copia esatta da un disco a un altro.
    - Se uno dei dischi di una coppia di dischi si guasta, lo storage array può passare istantaneamente all'altro disco senza alcuna perdita di dati o di servizio.
    - Un guasto a un singolo disco causa il degrado dei volumi associati. L'unità mirror consente di accedere ai dati.
    - Un errore di coppia di dischi in un gruppo di volumi causa il malfunzionamento di tutti i volumi associati e la perdita di dati.
- **Requisiti del numero di unità**
    - Per RAID 1 sono necessari almeno due dischi: Un disco per i dati dell'utente e un disco per i dati mirrorati.
    - Se si selezionano quattro o più dischi, RAID 10 viene configurato automaticamente nel gruppo di volumi: Due dischi per i dati dell'utente e due dischi per i dati mirrorati.
    - È necessario disporre di un numero pari di dischi nel gruppo di volumi. Se non si dispone di un numero pari di dischi e si dispone di altri dischi non assegnati, passare a **Pools & Volume Groups** per aggiungere ulteriori dischi al gruppo di volumi e riprovare l'operazione.
    - I gruppi di volumi RAID 1 e RAID 10 possono avere più di 30 dischi. È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 5

- **Descrizione**
    - Modalità i/o elevata.
- **Come funziona**
    - I dati dell'utente e le informazioni ridondanti (parità) vengono sottoposti a striping tra i dischi.
    - La capacità equivalente di un disco viene utilizzata per le informazioni ridondanti.
- **Caratteristiche di protezione dei dati**
    - Se un singolo disco si guasta in un gruppo di volumi RAID 5, tutti i volumi associati diventano degradati. Le informazioni ridondanti consentono di accedere ai dati.
    - Se due o più dischi si guastano in un gruppo di volumi RAID 5, tutti i volumi associati si guastano e tutti i dati vengono persi.
- **Requisiti del numero di unità**
    - È necessario disporre di un minimo di tre dischi nel gruppo di volumi.
    - In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

RAID 6

- **Descrizione**
    - Modalità i/o elevata.

- **Come funziona**
  - I dati dell'utente e le informazioni ridondanti (doppia parità) vengono sottoposti a striping tra i dischi.
  - La capacità equivalente di due dischi viene utilizzata per le informazioni ridondanti.
- **Caratteristiche di protezione dei dati**
  - Se uno o due dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati diventano degradati, ma le informazioni ridondanti consentono di continuare ad accedere ai dati.
  - Se tre o più dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati si guastano e tutti i dati vengono persi.
- **Requisiti del numero di unità**
  - È necessario disporre di un minimo di cinque dischi nel gruppo di volumi.
  - In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

> Non è possibile modificare il livello RAID di un pool. L'interfaccia utente configura automaticamente i pool come RAID 6.

Livelli RAID e protezione dei dati

RAID 1, RAID 5 e RAID 6 scrivono i dati di ridondanza sul disco per la tolleranza di errore. I dati di ridondanza possono essere una copia dei dati (mirrorati) o un codice di correzione degli errori derivato dai dati. È possibile utilizzare i dati di ridondanza per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto.

È possibile configurare un singolo livello RAID in un singolo gruppo di volumi. Tutti i dati di ridondanza per quel gruppo di volumi vengono memorizzati all'interno del gruppo di volumi. La capacità del gruppo di volumi è la capacità aggregata dei dischi membri meno la capacità riservata ai dati di ridondanza. La quantità di capacità necessaria per la ridondanza dipende dal livello RAID utilizzato.

Cos'è Data Assurance?

Data Assurance (da) implementa lo standard T10 Protection Information (PI), che aumenta l'integrità dei dati verificando e correggendo gli errori che potrebbero verificarsi quando i dati vengono trasferiti lungo il percorso di i/O.

L'utilizzo tipico della funzione Data Assurance consente di controllare la parte del percorso i/o tra i controller e i dischi. Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi.

Quando questa funzione è attivata, l'array di storage aggiunge i codici di controllo degli errori (noti anche come CRC (Cyclic Redundancy Checks) a ciascun blocco di dati del volume. Dopo lo spostamento di un blocco di dati, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono scritti su disco né restituiti all'host. Se si desidera utilizzare la funzione da, selezionare un pool o un gruppo di volumi in grado di supportare da quando si crea un nuovo volume (cercare "Sì" accanto a "da" nella tabella dei candidati del gruppo di volumi e pool).

Assicurarsi di assegnare questi volumi abilitati da a un host utilizzando un'interfaccia i/o in grado di supportare da. Le interfacce i/o in grado di da includono Fibre Channel, SAS, iSCSI su TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE e iSER su InfiniBand (estensioni iSCSI per RDMA/IB). DA non è supportato da SRP su InfiniBand.

Che cos'è il supporto sicuro (Drive Security)?

Drive Security è una funzione che impedisce l'accesso non autorizzato ai dati su dischi abilitati alla sicurezza quando vengono rimossi dallo storage array. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).

Cosa devo sapere sull'aumento della capacità riservata?

In genere, è necessario aumentare la capacità quando si riceve un avviso che indica che la capacità riservata rischia di diventare piena. È possibile aumentare la capacità riservata solo con incrementi di 8 GiB.

- È necessario disporre di una capacità libera sufficiente nel pool o nel gruppo di volumi in modo da poterla espandere, se necessario.

  Se non esiste capacità libera in alcun pool o gruppo di volumi, è possibile aggiungere capacità non assegnata sotto forma di unità inutilizzate a un pool o a un gruppo di volumi.

- Il volume nel pool o nel gruppo di volumi deve avere uno stato ottimale e non deve essere in alcun stato di modifica.
- La capacità libera deve essere presente nel pool o nel gruppo di volumi che si desidera utilizzare per aumentare la capacità.
- Non è possibile aumentare la capacità riservata per un volume di snapshot di sola lettura. Solo i volumi Snapshot in lettura/scrittura richiedono una capacità riservata.

Per le operazioni di snapshot, la capacità riservata è in genere il 40% del volume di base. Per le operazioni di mirroring asincrono, la capacità riservata è in genere il 20% del volume di base. Utilizzare una percentuale più elevata se si ritiene che il volume di base subirà molte modifiche o se la durata prevista per l'operazione di copia del servizio di un oggetto di storage sarà molto lunga.

Perché non è possibile scegliere un altro importo da diminuire di?

È possibile ridurre la capacità riservata solo della quantità utilizzata per aumentarla. La capacità riservata per i volumi membro può essere rimossa solo nell'ordine inverso rispetto a quello in cui sono stati aggiunti.

Non è possibile ridurre la capacità riservata per un oggetto di storage se si verifica una delle seguenti condizioni:

- Se l'oggetto storage è un volume di coppia mirrorato.
- Se l'oggetto di storage contiene un solo volume per la capacità riservata. L'oggetto di storage deve contenere almeno due volumi per la capacità riservata.
- Se l'oggetto di storage è un volume di snapshot disattivato.
- Se l'oggetto di storage contiene una o più immagini snapshot associate.

È possibile rimuovere i volumi per la capacità riservata solo nell'ordine inverso rispetto a quello in cui sono stati aggiunti.

Non è possibile ridurre la capacità riservata per un volume snapshot di sola lettura perché non dispone di

capacità riservata associata. Solo i volumi Snapshot in lettura/scrittura richiedono una capacità riservata.

Perché è necessaria una capacità riservata per ciascun volume membro?

Ogni volume membro di un gruppo di coerenza snapshot deve disporre di una propria capacità riservata per salvare le modifiche apportate dall'applicazione host nel volume di base senza influire sull'immagine snapshot del gruppo di coerenza di riferimento. La capacità riservata fornisce all'applicazione host l'accesso in scrittura a una copia dei dati contenuti nel volume membro designato come Read-write.

Un'immagine snapshot di un gruppo di coerenza non è accessibile direttamente in lettura o scrittura agli host. L'immagine snapshot viene invece utilizzata per salvare solo i dati acquisiti dal volume di base.

Durante la creazione di un volume snapshot di un gruppo di coerenza designato come lettura/scrittura, System Manager crea una capacità riservata per ciascun volume membro del gruppo di coerenza. Questa capacità riservata fornisce all'applicazione host l'accesso in scrittura a una copia dei dati contenuti nell'immagine snapshot del gruppo di coerenza.

Come si visualizzano e interpretano tutte le statistiche della cache SSD?

È possibile visualizzare statistiche nominali e statistiche dettagliate per la cache SSD. Le statistiche nominali sono un sottoinsieme delle statistiche dettagliate.

Le statistiche dettagliate possono essere visualizzate solo quando si esportano tutte le statistiche SSD in un `.csv` file. Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Statistiche nominali

Per visualizzare le statistiche della cache SSD, selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups]). Selezionare la cache SSD per cui si desidera visualizzare le statistiche, quindi selezionare **More › View Statistics** (Visualizza statistiche). Le statistiche nominali vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD).

L'elenco seguente include le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate.

Statistica nominale	Descrizione
Letture/scritture	Il numero totale di letture host da o scritture host nei volumi abilitati per la cache SSD. Confrontare le letture relative alle scritture. Le letture devono essere maggiori delle scritture per un funzionamento efficace della cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Riscontri cache	Numero di accessi alla cache.

Statistica nominale	Descrizione
Riscontri cache (%)	Derivato da riscontri cache / (letture + scritture). La percentuale di cache hit deve essere superiore al 50% per un'operazione effettiva della cache SSD. Un piccolo numero potrebbe indicare diverse cose: • Il rapporto tra letture e scritture è troppo piccolo • Le letture non vengono ripetute • La capacità della cache è troppo piccola
Allocazione della cache (%)	La quantità di storage cache SSD allocata, espressa come percentuale dello storage cache SSD disponibile per questo controller. Derivato da byte allocati/byte disponibili. La percentuale di allocazione della cache viene normalmente visualizzata come 100%. Se questo numero è inferiore al 100%, significa che la cache non è stata riscaldata o che la capacità della cache SSD è superiore a tutti i dati a cui si accede. In quest'ultimo caso, una capacità di cache SSD inferiore potrebbe fornire lo stesso livello di performance. Si noti che ciò non indica che i dati memorizzati nella cache sono stati inseriti nella cache SSD; si tratta semplicemente di una fase di preparazione prima che i dati possano essere inseriti nella cache SSD.
Utilizzo della cache (%)	La quantità di storage SSD cache che contiene dati provenienti da volumi abilitati, espressa come percentuale di storage SSD cache allocata. Questo valore rappresenta l'utilizzo o la densità della cache SSD derivata dai byte dei dati utente / byte allocati. La percentuale di utilizzo della cache normalmente è inferiore al 100%, forse molto inferiore. Questo numero mostra la percentuale di capacità della cache SSD che è piena di dati della cache. Questo numero è inferiore al 100% perché ogni unità di allocazione della cache SSD, il blocco SSD cache, è divisa in unità più piccole denominate sottoblocchi, che vengono riempite in modo indipendente. Un numero più elevato è generalmente migliore, ma i guadagni in termini di performance possono essere significativi anche con un numero inferiore.

Statistiche dettagliate

Le statistiche dettagliate sono costituite dalle statistiche nominali e da statistiche aggiuntive. Queste statistiche aggiuntive vengono salvate insieme alle statistiche nominali, ma a differenza delle statistiche nominali, non vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare le statistiche dettagliate solo dopo aver esportato le statistiche in un `.csv` file.

Durante la visualizzazione di `.csv` fare attenzione che le statistiche dettagliate sono elencate dopo le statistiche nominali:

Statistiche dettagliate	Descrizione
Blocchi di lettura	Il numero di blocchi nelle letture dell'host.
Blocchi di scrittura	Il numero di blocchi in scritture host.

Statistiche dettagliate	Descrizione
Blocchi completi	Il numero di blocchi nei riscontri della cache. I blocchi completi indicano il numero di blocchi che sono stati letti interamente dalla cache SSD. La cache SSD è vantaggiosa solo per le performance di quelle operazioni che sono riscontri completi della cache.
Riscontri parziali	Il numero di letture host in cui almeno un blocco, ma non tutti i blocchi, si trovavano nella cache SSD. Un hit parziale è una cache SSD **miss** in cui le letture sono state soddisfatte dal volume di base.
Riscontri parziali - blocchi	Il numero di blocchi in riscontri parziali. I riscontri parziali della cache e i blocchi di hit parziali della cache derivano da un'operazione che contiene solo una parte dei dati nella cache SSD. In questo caso, l'operazione deve ottenere i dati dal volume del disco rigido (HDD) memorizzato nella cache. La cache SSD non offre alcun beneficio in termini di performance per questo tipo di hit. Se il numero di blocchi di hit della cache parziale è superiore a quello dei blocchi di hit della cache completa, un tipo di caratteristica i/o diverso (file system, database o server Web) potrebbe migliorare le performance. Si prevede che ci sarà un maggior numero di riscontri parziali e mancati rispetto ai riscontri cache mentre la cache SSD è in fase di riscaldamento.
Mancati	Il numero di letture host in cui nessuno dei blocchi si trova nella cache SSD. Una mancanza di cache SSD si verifica quando le letture sono state soddisfatte dal volume di base. Si prevede che ci sarà un maggior numero di riscontri parziali e mancati rispetto ai riscontri cache mentre la cache SSD è in fase di riscaldamento.
Mancati - blocchi	Il numero di blocchi in mancati.
Azioni di compilazione (letture host)	Il numero di letture host in cui sono stati copiati i dati dal volume di base alla cache SSD.
Azioni di compilazione (letture host) - blocchi	Il numero di blocchi in azioni popolate (letture host).
Azioni di compilazione (scritture host)	Il numero di scritture host in cui sono stati copiati i dati dal volume di base alla cache SSD. Il conteggio delle operazioni di compilazione (scritture host) potrebbe essere zero per le impostazioni di configurazione della cache che non riempiono la cache come risultato di un'operazione di scrittura i/O.
Azioni di compilazione (scritture host) - blocchi	Il numero di blocchi nelle azioni di compilazione (scritture host).
Invalidare le azioni	Il numero di volte in cui i dati sono stati invalidati o rimossi dalla cache SSD. Viene eseguita un'operazione di invalidazione della cache per ogni richiesta di scrittura dell'host, per ogni richiesta di lettura dell'host con accesso forzato alle unità (FUA), per ogni richiesta di verifica e in altre circostanze.

Statistiche dettagliate	Descrizione
Azioni di riciclo	Il numero di volte in cui il blocco SSD cache è stato riutilizzato per un altro volume di base e/o un intervallo LBA (Logical Block Addressing) diverso. Per un funzionamento efficace della cache, il numero di cicli di riciclo deve essere ridotto rispetto al numero combinato di operazioni di lettura e scrittura. Se il numero di Recycle Actions è vicino al numero combinato di letture e scritture, la cache SSD sta per essere thrash. La capacità della cache deve essere aumentata o il carico di lavoro non è favorevole per l'utilizzo con la cache SSD.
Byte disponibili	Il numero di byte disponibili nella cache SSD per l'utilizzo da parte di questo controller.
Byte allocati	Il numero di byte allocati dalla cache SSD da questo controller. I byte allocati dalla cache SSD potrebbero essere vuoti o contenere dati provenienti da volumi di base.
Byte dei dati utente	Il numero di byte allocati nella cache SSD che contengono i dati dei volumi di base. I byte disponibili, allocati e dati utente vengono utilizzati per calcolare la percentuale di allocazione della cache e la percentuale di utilizzo della cache.

Che cos'è la capacità di ottimizzazione per i pool?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra performance, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Pool Settings (Impostazioni pool) consente di regolare la capacità di ottimizzazione del pool. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

> Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) è disponibile solo per i sistemi storage EF600 e EF300.

Qual è la capacità di ottimizzazione per i gruppi di volumi?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo di volumi (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra prestazioni, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Volume Group Settings (Impostazioni gruppo di volumi) consente di regolare la capacità di ottimizzazione di un gruppo di volumi. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

> Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) è disponibile solo per i sistemi storage EF600 e EF300.

Quali sono le funzionalità di provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management o il comando SCSI Unmap. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Cosa occorre sapere sulla funzionalità dei volumi con provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management o il comando SCSI Unmap. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Il provisioning delle risorse è attivato per impostazione predefinita nei sistemi in cui i dischi supportano DULBE. È possibile disattivare l'impostazione predefinita da **Pools & Volume Groups**.

Volumi e carichi di lavoro

Panoramica su volumi e carichi di lavoro

È possibile creare un volume come container in cui applicazioni, database e file system memorizzano i dati. Quando si crea un volume, è anche possibile selezionare un carico di lavoro per personalizzare la configurazione dello storage array per un'applicazione specifica.

Cosa sono i volumi e i carichi di lavoro?

Un *volume* è il componente logico creato con capacità specifica per l'accesso dell'host. Anche se un volume può essere costituito da più di un disco, un volume viene visualizzato come un componente logico per l'host. Una volta definito un volume, è possibile aggiungerlo a un workload. Un *workload* è un oggetto storage che supporta un'applicazione, come SQL Server o Exchange, che è possibile utilizzare per ottimizzare lo storage per tale applicazione.

Scopri di più:

- "Come funzionano i volumi"
- "Come funzionano i carichi di lavoro"
- "Terminologia relativa ai volumi"
- "Come viene allocata la capacità per i volumi"
- "Azioni che è possibile eseguire sui volumi"

Come crei volumi e carichi di lavoro?

Innanzitutto, si crea un carico di lavoro. Accedere al **Storage › Volumes** (Storage[volumi]) e aprire una procedura guidata che ti guiderà attraverso i passaggi. Quindi, si crea un volume dalla capacità disponibile in un pool o in un gruppo di volumi, quindi si assegna il carico di lavoro creato.

Scopri di più:

- "Workflow per la creazione di volumi"
- "Creare carichi di lavoro"
- "Creare volumi"
- "Aggiungere volumi al carico di lavoro"

Informazioni correlate

Scopri di più sui concetti relativi ai volumi:

- "Integrità dei dati e sicurezza dei dati per i volumi"
- "Cache SSD e volumi"
- "Monitoraggio di volumi sottili"

Concetti

Come funzionano i volumi

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

È possibile creare volumi dalla capacità di storage disponibile sull'array di storage e semplificare l'organizzazione e l'utilizzo delle risorse del sistema. Questo concetto è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso semplice e rapido.

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

Tipi di volume che è possibile creare da pool e gruppi di volumi

I volumi traggono la propria capacità da pool o gruppi di volumi. È possibile creare i seguenti tipi di volumi dai pool o dai gruppi di volumi presenti nell'array di storage.

- **Dai pool** — è possibile creare volumi da un pool come *volumi con provisioning completo (thick)* o *volumi con thin provisioning.*

> L'interfaccia di System Manager non fornisce un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

- **Da gruppi di volumi** — è possibile creare volumi da un gruppo di volumi solo come *volumi con provisioning completo (thick)*.

I volumi spessi e i volumi thin traggono la capacità dall'array di storage in diversi modi:

- La capacità di un volume spesso viene allocata al momento della creazione del volume.
- La capacità di un volume thin viene allocata come dati quando viene scritta nel volume.

Il thin provisioning consente di evitare sprechi di capacità allocata e consente alle aziende di risparmiare sui costi iniziali dello storage. Tuttavia, il provisioning completo offre il vantaggio di una minore latenza, poiché tutto lo storage viene allocato contemporaneamente quando vengono creati volumi spessi.

> I sistemi storage EF600 e EF300 non supportano il thin provisioning.

Caratteristiche dei volumi

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

- **Dimensione segmento** — Un segmento è la quantità di dati in kilobyte (KiB) che viene memorizzata su un disco prima che lo storage array passi al disco successivo nello stripe (gruppo RAID). La dimensione del segmento è uguale o inferiore alla capacità del gruppo di volumi. La dimensione del segmento è fissa e non può essere modificata per i pool.
- **Capacità** — consente di creare un volume dalla capacità libera disponibile in un pool o in un gruppo di volumi. Prima di creare un volume, il pool o il gruppo di volumi deve già esistere e disporre di capacità libera sufficiente per creare il volume.

- **Controller ownership** — tutti gli storage array possono avere uno o due controller. Su un array a controller singolo, il carico di lavoro di un volume viene gestito da un singolo controller. Su un array a controller doppio, un volume avrà un controller preferito (A o B) che "possiede" il volume. In una configurazione a controller doppio, la proprietà del volume viene regolata automaticamente utilizzando la funzione di bilanciamento automatico del carico per correggere eventuali problemi di bilanciamento del carico quando i carichi di lavoro si spostano tra i controller. Il bilanciamento automatico del carico fornisce il bilanciamento automatizzato del carico di lavoro i/o e garantisce che il traffico i/o in entrata dagli host sia gestito dinamicamente e bilanciato tra entrambi i controller.
- **Assegnazione del volume** — è possibile consentire agli host di accedere a un volume sia quando si crea il volume che in un secondo momento. Tutti gli accessi host vengono gestiti tramite un numero di unità logica (LUN). Gli host rilevano le LUN che, a loro volta, sono assegnate ai volumi. Se si assegna un volume a più host, utilizzare il software di clustering per assicurarsi che il volume sia disponibile per tutti gli host.

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

- **Descrivi name** — puoi assegnare un nome a un volume qualsiasi, ma ti consigliamo di renderlo descrittivo.

Durante la creazione del volume, a ciascun volume viene allocata la capacità e viene assegnato un nome, una dimensione del segmento (solo gruppi di volumi), una proprietà del controller e un'assegnazione volume-a-host. I dati dei volumi vengono automaticamente bilanciati in base alle esigenze dei controller.

Come funzionano i carichi di lavoro

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

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

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

Tipi di carichi di lavoro

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

- **Specifico dell'applicazione**. Quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Applicazioni di videosorveglianza
- VMware ESXi™ (per volumi da utilizzare con il file system della macchina virtuale)

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

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

Viste delle applicazioni e dei workload

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

- È possibile selezionare la scheda **applicazioni e carichi di lavoro** nella sezione volumi per visualizzare i volumi dell'array di storage raggruppati per carico di lavoro e il tipo di applicazione a cui è associato il carico di lavoro.
- È possibile selezionare la scheda **applicazioni e carichi di lavoro** nel riquadro Performance per visualizzare le metriche delle performance (latenza, IOPS e MB) per gli oggetti logici. Gli oggetti sono raggruppati in base all'applicazione e al carico di lavoro associato. Raccogliendo questi dati sulle performance a intervalli regolari, è possibile stabilire misurazioni di riferimento e analizzare i trend, che possono aiutare a indagare i problemi relativi alle performance di i/O.

Terminologia relativa ai volumi

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

Tutti i tipi di volume

Termine	Descrizione
Capacità allocata	Si utilizza la capacità allocata per creare volumi e per le operazioni dei servizi di copia. La capacità allocata e quella riportata sono le stesse per i volumi spessi, ma sono diverse per i volumi thin. Per un volume spesso, lo spazio fisicamente allocato è uguale allo spazio che viene segnalato all'host. Per un volume thin, la capacità riportata è la capacità che viene segnalata agli host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocato per la scrittura dei dati.

Termine	Descrizione
Applicazione	Un'applicazione è un software come SQL Server o Exchange. È possibile definire uno o più workload per supportare ciascuna applicazione. Per alcune applicazioni, il sistema consiglia automaticamente una configurazione del volume che ottimizzi lo storage. Caratteristiche come il tipo di i/o, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume.
Capacità	La capacità è la quantità di dati che è possibile memorizzare in un volume.
Proprietà del controller	Controller ownership (proprietà del controller): Definisce il controller designato come controller principale o proprietario del volume. Un volume può avere un controller preferito (A o B) che "possiede" il volume. La proprietà del volume viene regolata automaticamente utilizzando la funzione di bilanciamento automatico del carico per correggere eventuali problemi di bilanciamento del carico quando i carichi di lavoro si spostano tra i controller. Il bilanciamento automatico del carico fornisce il bilanciamento automatizzato del carico di lavoro i/o e garantisce che il traffico i/o in entrata dagli host sia gestito e bilanciato dinamicamente tra entrambi i controller.
Prefetch di lettura della cache dinamica	Il prefetch di lettura dinamico della cache consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i 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. Per un volume thin, il prefetch dinamico di lettura della cache è sempre disattivato e non può essere modificato.
Area di capacità libera	Un'area di capacità libera è la capacità libera che può derivare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità disponibile durante la creazione del volume. Quando si crea un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume viene limitata alla maggiore area di capacità libera del gruppo di volumi. Ad esempio, se un gruppo di volumi ha una capacità libera totale di 15 GiB e l'area di capacità libera più grande è di 10 GiB, il volume più grande che è possibile creare è di 10 GiB. Consolidando la capacità libera, è possibile creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi.
Host	Un host è un server che invia i/o a un volume su un array di storage.
Cluster host	Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.

Termine	Descrizione
Disco hot spare	Le unità hot spare sono supportate solo con i gruppi di volumi. Un disco hot spare non contiene dati e funge da standby in caso di guasto di un disco nei volumi RAID 1, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. L'unità hot spare aggiunge un altro livello di ridondanza allo storage array.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi.
Scansione dei supporti	Una scansione dei supporti consente di rilevare gli errori dei supporti prima che vengano rilevati durante una normale lettura o scrittura sui dischi. Una scansione dei supporti viene eseguita come operazione in background ed esegue la scansione di tutti i dati e le informazioni di ridondanza in volumi utente definiti.
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.
Piscina	Un pool è un insieme di dischi raggruppati in modo logico. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. I volumi vengono creati da un pool o da un gruppo di volumi.
Capacità del pool o del gruppo di volumi	La capacità di pool, volume o gruppo di volumi è la capacità di un array di storage assegnato a un pool o a un gruppo di volumi. Questa capacità viene utilizzata per creare volumi e soddisfare le diverse esigenze di capacità delle operazioni dei servizi di copia e degli oggetti di storage.
Cache di lettura	La cache di lettura è un buffer che memorizza i dati letti dai dischi. I dati di un'operazione di lettura potrebbero essere già presenti nella cache di un'operazione precedente, eliminando così la necessità di accedere ai dischi. I dati rimangono nella cache di lettura fino a quando non vengono scaricati.
Capacità riportata	La capacità riportata è la capacità che viene riportata all'host e a cui l'host può accedere. La capacità riportata e la capacità allocata sono le stesse per i volumi spessi, ma sono diverse per i volumi thin. Per un volume spesso, lo spazio fisicamente allocato è uguale allo spazio che viene segnalato all'host. Per un volume thin, la capacità riportata è la capacità che viene segnalata agli host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocato per la scrittura dei dati.

Termine	Descrizione
Dimensione del segmento	Un segmento è la quantità di dati in kilobyte (KiB) memorizzati su un disco prima che l'array di storage passi al disco successivo nello stripe (gruppo RAID). La dimensione del segmento è uguale o inferiore alla capacità del gruppo di volumi. La dimensione del segmento è fissa e non può essere modificata per i pool.
Striping	Lo striping è un modo per memorizzare i dati nell'array di storage. Lo striping suddivide il flusso di dati in blocchi di una certa dimensione (chiamati "dimensione del blocco") e quindi scrive questi blocchi uno per uno sui dischi. Questo metodo di storage dei dati viene utilizzato per distribuire e memorizzare i dati su più dischi fisici. Lo striping è sinonimo di RAID 0 e distribuisce i dati su tutti i dischi di un gruppo RAID senza parità.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all'host di accedere allo storage sull'array di storage.
Assegnazione del volume	L'assegnazione del volume indica la modalità di assegnazione dei LUN host a un volume.
Nome del volume	Il nome di un volume è una stringa di caratteri assegnata al volume al momento della creazione. È possibile accettare il nome predefinito o fornire un nome più descrittivo che indichi il tipo di dati memorizzati nel volume.
Gruppo di volumi	Un gruppo di volumi è un contenitore per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità e un livello RAID definiti. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. I volumi vengono creati da un gruppo di volumi o da un pool.
Carico di lavoro	Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.
Cache di scrittura	La cache di scrittura è un buffer che memorizza i dati dell'host che non sono ancora stati scritti sui dischi. I dati rimangono nella cache di scrittura fino a quando non vengono scritti sui dischi. Il caching in scrittura può aumentare le performance di i/O.

Termine	Descrizione
Caching 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.
Caching in scrittura senza batterie	Il caching in scrittura senza batterie consente di continuare il caching in scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta del caching in scrittura senza batterie non è generalmente consigliata, in quanto i dati potrebbero andare persi in caso di interruzione dell'alimentazione. In genere, il caching in scrittura viene disattivato temporaneamente dal controller fino a quando le batterie non vengono caricate o non viene sostituita una batteria guasta.

Specifico per i volumi thin

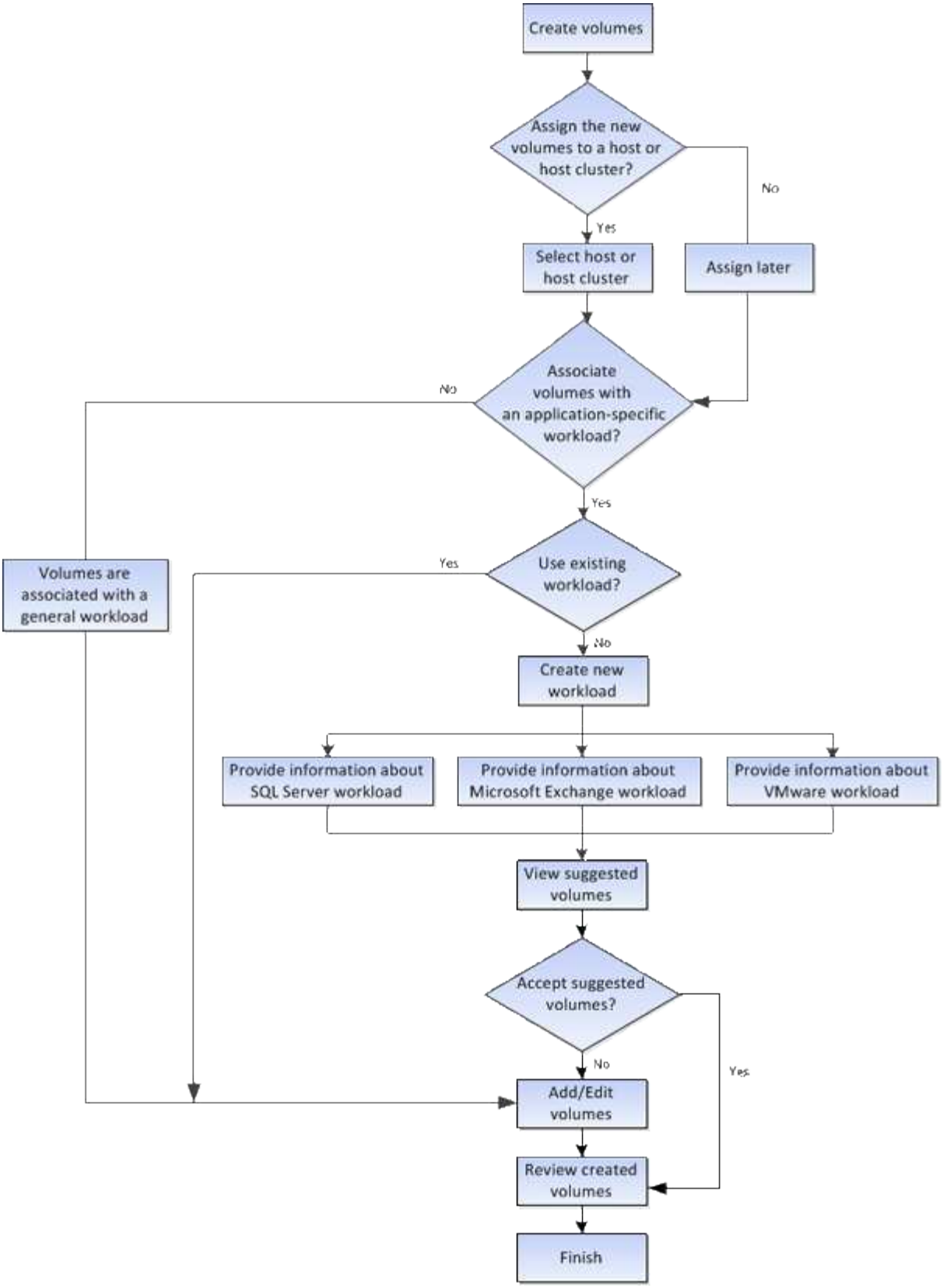
System Manager non offre un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

I thin volumi non sono disponibili sul sistema storage EF600 o EF300.

Termine	Descrizione
Limite di capacità allocata	Il limite di capacità allocata è il limite massimo per quanto può crescere la capacità fisica allocata per un volume sottile.
Capacità scritta	La capacità scritta è la quantità di capacità che è stata scritta dalla capacità riservata allocata per i thin volumi.
Soglia di avviso	È possibile impostare un avviso di soglia da emettere quando la capacità allocata per un volume thin raggiunge la percentuale di pieno (soglia di avviso).

Workflow per la creazione di volumi

In System Manager, è possibile creare volumi seguendo questa procedura.



Integrità dei dati e sicurezza dei dati per i volumi

È possibile abilitare i volumi a utilizzare la funzione Data Assurance (da) e la funzione Drive Security. Queste funzionalità vengono presentate a livello di pool e gruppo di volumi.

Data Assurance

Data Assurance (da) implementa lo standard T10 Protection Information (PI), che aumenta l'integrità dei dati verificando e correggendo gli errori che potrebbero verificarsi quando i dati vengono trasferiti lungo il percorso di i/O. L'utilizzo tipico della funzione Data Assurance consente di controllare la parte del percorso i/o tra i controller e i dischi. Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi.

Quando questa funzione è attivata, l'array di storage aggiunge i codici di controllo degli errori (noti anche come CRC (Cyclic Redundancy Checks) a ciascun blocco di dati del volume. Dopo lo spostamento di un blocco di dati, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono scritti su disco né restituiti all'host. Se si desidera utilizzare la funzione da, selezionare un pool o un gruppo di volumi in grado di supportare da quando si crea un nuovo volume (cercare "Sì" accanto a "da" nella tabella dei candidati del gruppo di volumi e pool).

Sicurezza del disco

Drive Security è una funzione che impedisce l'accesso non autorizzato ai dati su dischi abilitati alla sicurezza quando vengono rimossi dallo storage array. Questi dischi possono essere dischi con crittografia completa del disco (FDE) o dischi certificati per soddisfare gli standard di elaborazione delle informazioni federali 140-2 livello 2 (dischi FIPS).

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.

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*. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.

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).

     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.

Cache SSD e volumi

È possibile aggiungere un volume alla cache SSD per migliorare le performance di sola lettura. La cache SSD è costituita da un set di dischi a stato solido (SSD) che vengono raggruppati logicamente nell'array di storage.

Volumi

Semplici meccanismi di i/o dei volumi vengono utilizzati per spostare i dati da e verso la cache SSD. Dopo che i dati sono stati memorizzati nella cache e memorizzati negli SSD, le successive letture di tali dati vengono eseguite sulla cache SSD, eliminando così la necessità di accedere al volume HDD.

La cache SSD è una cache secondaria da utilizzare con la cache primaria nella DRAM (Dynamic Random-Access Memory) del controller.

- Nella cache primaria, i dati vengono memorizzati nella DRAM dopo la lettura da parte di un host.
- Nella cache SSD, i dati vengono copiati dai volumi e memorizzati su due volumi RAID interni (uno per controller) che vengono creati automaticamente quando si crea una cache SSD.

I volumi RAID interni vengono utilizzati per l'elaborazione della cache interna. Questi volumi non sono accessibili o visualizzati nell'interfaccia utente. Tuttavia, questi due volumi vengono conteggiati rispetto al numero totale di volumi consentiti nell'array di storage.

> Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.

Funzione di protezione del disco

Per utilizzare la cache SSD su un volume che utilizza anche Drive Security (è abilitato per la protezione), le funzionalità di protezione del disco del volume e della cache SSD devono corrispondere. Se non corrispondono, il volume non sarà abilitato alla protezione.

Azioni che è possibile eseguire sui volumi

È possibile eseguire diverse azioni su un volume: Aumento della capacità, eliminazione, copia, inizializzazione, ridistribuzione, modifica della proprietà, modifica delle impostazioni della cache e modifica delle impostazioni di scansione dei supporti.

Aumentare la capacità

È possibile espandere la capacità di un volume in due modi:

- Utilizzare la capacità libera disponibile nel pool o nel gruppo di volumi.

  Per aggiungere capacità a un volume, selezionare il **Storage › Pools and Volume Groups › Add Capacity** (Storage[Pools and Volume Groups > Add Capacity]).

- Aggiungere capacità non assegnata (sotto forma di unità inutilizzate) al pool o al gruppo di volumi del

volume. Utilizzare questa opzione quando non esiste capacità libera nel pool o nel gruppo di volumi.

Per aggiungere capacità non assegnata al pool o al gruppo di volumi, selezionare **Storage › Pool e gruppi di volumi › Add Capacity** (Aggiungi capacità).

Se la capacità libera non è disponibile nel pool o nel gruppo di volumi, non è possibile aumentare la capacità del volume. È necessario aumentare prima le dimensioni del pool o del gruppo di volumi o eliminare i volumi inutilizzati.

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Eliminare

In genere, i volumi vengono eliminati se sono stati creati con parametri o capacità errati, se non soddisfano più le esigenze di configurazione dello storage o se si tratta di immagini snapshot non più necessarie per il backup o il test delle applicazioni. L'eliminazione di un volume aumenta la capacità libera nel pool o nel gruppo di volumi.

L'eliminazione dei volumi causa la perdita di tutti i dati su tali volumi. L'eliminazione di un volume comporta anche l'eliminazione di eventuali snapshot, pianificazioni e volumi snapshot associati e la rimozione di eventuali relazioni di mirroring.

Copia

Quando si copiano i volumi, si crea una copia point-in-time di due volumi separati, il volume di origine e il volume di destinazione, sullo stesso array di storage. È possibile copiare i volumi selezionando il **Storage › Volumes › Copy Services › Copy volume**.

Inizializzare

L'inizializzazione di un volume cancella tutti i dati dal volume. Un volume viene inizializzato automaticamente quando viene creato per la prima volta. Tuttavia, il Recovery Guru potrebbe consigliare di inizializzare manualmente un volume per eseguire il ripristino in seguito a determinate condizioni di errore. Quando si inizializza un volume, il volume mantiene le impostazioni relative a WWN, assegnazioni host, capacità allocata e capacità riservata. Inoltre, mantiene le stesse impostazioni di sicurezza e di Data Assurance (da).

È possibile inizializzare i volumi selezionando **Storage › Volumes › More › Initialize Volumes** (Storage[volumi > Altro > Inizializza volumi]).

Ridistribuire

Ridistribuisci i volumi per spostarli di nuovo nei proprietari di controller preferiti. In genere, i driver multipath spostano i volumi dal proprietario del controller preferito quando si verifica un problema lungo il percorso dei dati tra l'host e l'array di storage.

La maggior parte dei driver multipath host tenta di accedere a ciascun volume su un percorso verso il proprietario del controller preferito. Tuttavia, se questo percorso preferito non è disponibile, il driver multipath sull'host esegue il failover su un percorso alternativo. Questo failover potrebbe causare la modifica della proprietà del volume nel controller alternativo. Dopo aver risolto la condizione che ha causato il failover, alcuni host potrebbero spostare automaticamente la proprietà del volume nel proprietario del controller preferito, ma in alcuni casi potrebbe essere necessario ridistribuire manualmente i volumi.

È possibile ridistribuire i volumi selezionando il **Storage › Volumes › More › redistribuisci volumi**.

Modificare la proprietà del volume

La modifica della proprietà di un volume modifica la proprietà preferita del controller del volume. Il proprietario preferito del controller di un volume è elencato in **Storage › Volumes › View/Edit Settings › Advanced tab** (Storage[volumi > Visualizza/Modifica impostazioni > scheda Advanced]).

È possibile modificare la proprietà di un volume selezionando **Storage › Volumes › More › Change Ownership** (Storage[volumi > Altro > Modifica proprietà]).

Mirroring e proprietà del volume

Se il volume primario della coppia mirrorata è di proprietà del controller A, anche il volume secondario sarà di proprietà del controller A dell'array di storage remoto. La modifica del proprietario del volume primario modifica automaticamente il proprietario del volume secondario per garantire che entrambi i volumi siano di proprietà dello stesso controller. Le attuali modifiche di proprietà sul lato primario si propagano automaticamente alle corrispondenti modifiche di proprietà correnti sul lato secondario.

Se un gruppo di coerenza mirror contiene un volume secondario locale e la proprietà del controller viene modificata, il volume secondario viene automaticamente ritrasferito al proprietario del controller originale alla prima operazione di scrittura. Non è possibile modificare la proprietà del controller di un volume secondario utilizzando l'opzione **Cambia proprietà**.

Copia della proprietà di volumi e volumi

Durante un'operazione di copia del volume, lo stesso controller deve possedere sia il volume di origine che il volume di destinazione. A volte, all'avvio dell'operazione di copia del volume, entrambi i volumi non dispongono dello stesso controller preferito. Pertanto, la proprietà del volume di destinazione viene automaticamente trasferita al controller preferito del volume di origine. Quando la copia del volume viene completata o interrotta, la proprietà del volume di destinazione viene ripristinata nel controller preferito.

Se la proprietà del volume di origine viene modificata durante l'operazione di copia del volume, viene modificata anche la proprietà del volume di destinazione. In alcuni ambienti del sistema operativo, potrebbe essere necessario riconfigurare il driver host multipath prima di poter utilizzare un percorso i/O. Alcuni driver multipath richiedono una modifica per riconoscere il percorso i/O. Per ulteriori informazioni, consultare la documentazione del driver.

Modificare le impostazioni della cache

La memoria cache è un'area di storage volatile temporaneo (RAM) sul controller che ha un tempo di accesso più rapido rispetto ai supporti del disco. Se si utilizza la memoria cache, è possibile aumentare le prestazioni di i/o complessive per i seguenti motivi:

- 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.

Selezionare il **Storage › Volumes › More › Change cache settings** (Storage[volumi > Altro > Modifica impostazioni cache) per modificare le seguenti impostazioni della cache:

- **Cache in lettura e scrittura** — la cache in 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.

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.

- **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.
- **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.

  Questa impostazione è disponibile solo se è stato attivato il caching in scrittura. Questa impostazione non è disponibile per i volumi thin.

- **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.

  Per un volume thin, il prefetch dinamico di lettura della cache è sempre disattivato e non può essere modificato.

Modificare le impostazioni di scansione dei supporti

Le scansioni dei supporti rilevano e riparano gli errori dei supporti sui blocchi di dischi che vengono raramente letti dalle applicazioni. Questa scansione può impedire la perdita di dati in caso di guasto di altri dischi nel pool o nel gruppo di volumi, poiché i dati relativi ai dischi guasti vengono ricostruiti utilizzando informazioni di ridondanza e dati provenienti da altri dischi nel pool o nel gruppo di volumi.

Le scansioni dei supporti vengono eseguite continuamente a una velocità costante in base alla capacità da sottoporre a scansione e alla durata della scansione. Le scansioni in background possono essere temporaneamente sospese da un'attività in background con priorità più alta (ad esempio, ricostruzione), ma vengono rieseguite alla stessa velocità costante.

È possibile attivare e impostare la durata dell'esecuzione della scansione dei supporti selezionando **Storage › Volumes › More › Change media scan settings** (Menu:archiviazione[volumi > Altro > Modifica impostazioni scansione supporti]).

La scansione di un volume viene eseguita solo quando l'opzione di scansione dei supporti è attivata per l'array di storage e per quel volume. Se è attivata anche la verifica della ridondanza per quel volume, le informazioni di ridondanza nel volume verranno controllate per verificarne la coerenza con i dati, a condizione che il volume disponga di ridondanza. La scansione dei supporti con controllo della ridondanza è attivata per impostazione predefinita per ciascun volume al momento della creazione.

Se durante la scansione si verifica un errore irreversibile del supporto, i dati verranno riparati utilizzando le informazioni di ridondanza, se disponibili. Ad esempio, le informazioni di ridondanza sono disponibili in volumi RAID 5 ottimali o in volumi RAID 6 ottimali o con un solo disco guasto. Se l'errore irreversibile non può essere riparato utilizzando le informazioni di ridondanza, il blocco di dati viene aggiunto al registro del settore illeggibile. Nel registro eventi vengono riportati errori del supporto correggibili e non correggibili.

Se il controllo di ridondanza rileva un'incoerenza tra i dati e le informazioni di ridondanza, viene riportato nel registro eventi.

Come viene allocata la capacità per i volumi

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

Utilizzo della capacità per creare ed espandere i volumi

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

- Quando si crea un volume dalla capacità non assegnata, è possibile creare contemporaneamente un pool o un gruppo di volumi e il volume.
- Quando si crea un volume dalla capacità libera, si crea un volume aggiuntivo su un pool o un gruppo di volumi già esistente.

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Tipi di capacità per volumi thick e thin

È possibile creare volumi thick o thin. La capacità riportata e la capacità allocata sono le stesse per i volumi spessi, ma sono diverse per i volumi thin.

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

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

- Per un volume thin, la capacità riportata è la capacità che viene segnalata agli host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocato per la scrittura dei dati.

  La capacità riportata può essere superiore alla capacità allocata sull'array di storage. I thin volumi possono essere dimensionati per adattarsi alla crescita senza tenere conto delle risorse attualmente disponibili.

> Gestore di sistema di SANtricity non fornisce un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

Limiti di capacità per i volumi spessi

La capacità minima per un volume spesso è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi.

Quando si aumenta la capacità riportata per un volume spesso, tenere presenti le seguenti linee guida:

- È possibile specificare fino a tre cifre decimali (ad esempio, 65.375 GiB).
- La capacità deve essere inferiore o uguale al massimo disponibile nel gruppo di volumi.

  Quando si crea un volume, viene preallocata una certa capacità aggiuntiva per la migrazione DSS (Dynamic Segment Size). La migrazione DSS è una funzione del software che consente di modificare le dimensioni dei segmenti di un volume.

- Alcuni sistemi operativi host supportano volumi superiori a 2 TIB (la capacità massima indicata è determinata dal sistema operativo host). Infatti, alcuni sistemi operativi host supportano fino a 128 volumi TIB. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Limiti di capacità per i volumi thin

È possibile creare volumi thin con una grande capacità segnalata e una capacità allocata relativamente piccola, il che è vantaggioso per l'utilizzo e l'efficienza dello storage. I thin volumi possono contribuire a semplificare l'amministrazione dello storage, in quanto la capacità allocata può aumentare in base alle esigenze dell'applicazione, senza interrompere l'applicazione, consentendo un migliore utilizzo dello storage.

Oltre alla capacità riportata e allocata, i thin volumi contengono anche capacità scritta. La capacità scritta è la quantità di capacità che è stata scritta dalla capacità riservata allocata per i thin volumi.

La tabella seguente elenca i limiti di capacità per un volume sottile.

Tipo di capacità	Dimensione minima	Dimensione massima
Segnalato	32 MiB	256 TIB
Allocato	4 MiB	64 TIB

Per un volume sottile, se è stata raggiunta la capacità massima di 256 TIB, non è possibile aumentarla. Assicurarsi che la capacità riservata del volume thin sia impostata su una dimensione superiore alla capacità massima indicata.

Il sistema espande automaticamente la capacità allocata in base al limite di capacità allocata. Il limite di capacità allocata consente di limitare la crescita automatica del thin volume al di sotto della capacità riportata. Quando la quantità di dati scritti si avvicina alla capacità allocata, è possibile modificare il limite di capacità allocata.

Per modificare il limite di capacità allocata, selezionare **Storage › Volumes › Thin Volume Monitoring tab › Change Limit** (Storage[volumi > scheda monitoraggio volume sottile > Modifica limite]).

Poiché System Manager non assegna la capacità completa quando crea un volume thin, nel pool potrebbe esistere una capacità libera insufficiente. Lo spazio insufficiente può bloccare le scritture nel pool, non solo per i volumi thin, ma anche per altre operazioni che richiedono capacità dal pool (ad esempio, immagini di snapshot o volumi di snapshot). Tuttavia, è comunque possibile eseguire operazioni di lettura dal pool. Se si verifica questa situazione, viene visualizzato un avviso relativo alla soglia.

Monitoraggio di volumi sottili

È possibile monitorare lo spazio dei thin volumi e generare avvisi appropriati per evitare condizioni di capacità insufficiente.

Gli ambienti con thin provisioning possono allocare più spazio logico rispetto allo storage fisico sottostante. È possibile selezionare il **Storage › Volumes › Thin Volume Monitoring** (Storage[volumi > monitoraggio volume thin]) per monitorare la crescita dei volumi thin prima che raggiungano il limite massimo di capacità allocata.

È possibile utilizzare la vista monitoraggio thin per eseguire le seguenti operazioni:

- Definire il limite che limita la capacità allocata a cui un volume sottile può espandersi automaticamente.
- Impostare il punto percentuale in cui un avviso (soglia di avviso superata) viene inviato all'area Notifiche della pagina iniziale quando un volume sottile si trova vicino al limite massimo di capacità allocata.

Per aumentare la capacità di un volume sottile, aumentare la capacità riportata.

System Manager non offre un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

I thin volumi non sono disponibili sul sistema storage EF600 o EF300.

Confronto tra volumi spessi e volumi thin

Un volume thick viene sempre sottoposto a provisioning completo, il che significa che tutta la capacità viene allocata al momento della creazione del volume. Un thin volume viene sempre sottoposto a thin provisioning, il che significa che la capacità viene allocata durante la scrittura dei dati nel volume.

System Manager non offre un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

Tipo di volume	Descrizione
Volumi spessi	• I volumi thick vengono creati da un pool o da un gruppo di volumi. • Con i volumi spessi, viene fornita in anticipo una grande quantità di spazio di storage in previsione delle future esigenze di storage. • I volumi spessi vengono creati con l'intera dimensione del volume pre-allocato sullo storage fisico al momento della creazione del volume. Questa pre-allocazione significa che la creazione di un volume da 100 GiB consuma effettivamente 100 GiB di capacità allocata sui dischi. Tuttavia, lo spazio potrebbe rimanere inutilizzato, causando un sottoutilizzo della capacità dello storage. • Quando si creano volumi spessi, assicurarsi di non allocare eccessivamente la capacità per un singolo volume. L'allocazione eccessiva della capacità per un singolo volume può consumare rapidamente tutto lo storage fisico nel sistema. • Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirroring asincrono), quindi non allocare tutta la capacità a volumi spessi. Lo spazio insufficiente può bloccare le scritture nel pool o nel gruppo di volumi. Se si verifica questa situazione, viene visualizzato un avviso di soglia per la capacità libera.
Volumi sottili	• I thin volumi vengono creati solo da un pool, non da un gruppo di volumi. • I volumi thin devono essere RAID 6. • I thin volumi non sono disponibili sul sistema storage EF600 o EF300. • È necessario utilizzare la CLI per creare volumi thin. • A differenza dei volumi thick, lo spazio richiesto per il volume thin non viene allocato durante la creazione, ma viene fornito on-demand in un secondo momento. • Un volume sottile consente di allocarne le dimensioni in modo eccessivo. In altri termini, è possibile assegnare una dimensione del LUN superiore a quella del volume. È quindi possibile espandere il volume in base alle necessità (se necessario, aggiungendo dischi nel processo) senza espandere le dimensioni del LUN e quindi senza scollegare gli utenti. • È possibile utilizzare la funzione di recupero dello spazio a blocchi (UNMAP) per il thin provisioning per recuperare i blocchi di un volume con thin provisioning sull'array di storage mediante un comando SCSI UNMAP emesso dall'host. Un array di storage che supporta il thin provisioning può riassegnare lo spazio recuperato per soddisfare le richieste di allocazione per alcuni altri volumi con thin provisioning all'interno dello stesso array di storage, consentendo un migliore reporting del consumo di spazio su disco e un utilizzo più efficiente delle risorse.

Limitazioni dei volumi sottili

I thin volumi supportano tutte le operazioni come thick volumi, con le seguenti eccezioni:

- Non è possibile modificare le dimensioni dei segmenti di un volume sottile.

- Non è possibile attivare la verifica della ridondanza di pre-lettura per un volume sottile.
- Non è possibile utilizzare un volume sottile come volume di destinazione in un'operazione Copy Volume.
- È possibile modificare il limite di capacità allocata e la soglia di avviso di un volume thin solo sul lato primario di una coppia di mirroring asincrono. Le modifiche apportate a questi parametri sul lato primario vengono propagate automaticamente sul lato secondario.

Configurare lo storage

Creare carichi di lavoro

È possibile creare carichi di lavoro per qualsiasi tipo di applicazione.

A proposito di questa attività

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

System Manager consiglia una configurazione del volume ottimizzata solo per i seguenti tipi di applicazione:

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Videosorveglianza
- VMware ESXi ™ (per volumi da utilizzare con il file system della macchina virtuale)

Tenere presenti le seguenti linee guida:

- *Quando si utilizza un carico di lavoro specifico dell'applicazione*, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. È possibile rivedere la configurazione del volume consigliata, quindi modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).
- *Quando si utilizzano altri tipi di applicazioni*, specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare **Create › workload** (Crea[carico di lavoro]).

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

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

Al termine

È possibile aggiungere capacità di storage al carico di lavoro creato. Utilizzare l'opzione **Create Volume** (Crea volume) per creare uno o più volumi per un'applicazione e per allocare quantità specifiche di capacità a

ciascun volume.

Creare volumi

È possibile creare volumi per aggiungere capacità di storage a un carico di lavoro specifico dell'applicazione e rendere visibili i volumi creati a un host o a un cluster host specifico. Inoltre, la sequenza di creazione dei volumi offre opzioni per allocare quantità specifiche di capacità a ciascun volume che si desidera creare.

A proposito di questa attività

La maggior parte dei tipi di applicazioni utilizza per impostazione predefinita una configurazione di volume definita dall'utente. Alcuni tipi di applicazioni hanno una configurazione smart applicata alla creazione del volume. Ad esempio, se si creano volumi per l'applicazione Microsoft Exchange, viene chiesto quante caselle di posta sono necessarie, quali sono i requisiti medi di capacità delle caselle di posta e quante copie del database si desidera. System Manager utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze.

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

Fase 1: Selezionare l'host per un volume

È possibile creare volumi per aggiungere capacità di storage a un carico di lavoro specifico dell'applicazione e rendere visibili i volumi creati a un host o a un cluster host specifico. Inoltre, la sequenza di creazione dei volumi offre opzioni per allocare quantità specifiche di capacità a ciascun volume che si desidera creare.

Prima di iniziare

- Nel riquadro host sono presenti host o cluster di host validi.
- Sono stati definiti gli identificatori delle porte host per l'host.
- Prima di creare un volume abilitato da, la connessione host che si intende utilizzare deve supportare da. Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

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

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

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).

2. Selezionare **Create › Volume** (Crea[Volume]).

   Viene visualizzata la finestra di dialogo Create Volumes (Crea volumi).

3. Dall'elenco a discesa, selezionare un host o un cluster host specifico al quale assegnare i volumi oppure scegliere di assegnare l'host o il cluster host in un secondo momento.
4. Per continuare la sequenza di creazione del volume per l'host o il cluster host selezionato, fare clic su **Avanti** e passare a. Fase 2: Selezionare un carico di lavoro per un volume.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

Fase 2: Selezionare un carico di lavoro per un volume

Selezionare un carico di lavoro per personalizzare la configurazione dell'array di storage per un'applicazione specifica, ad esempio Microsoft SQL Server, Microsoft Exchange, applicazioni di videosorveglianza o VMware. È possibile selezionare "Other application" (altra applicazione) se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.

A proposito di questa attività

Questa attività descrive come creare volumi per un carico di lavoro esistente.

- *Quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione*, il sistema potrebbe consigliare una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. È possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).
- *Quando si creano volumi utilizzando "altre"* applicazioni (o applicazioni senza supporto specifico per la creazione di volumi), si specifica manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Fasi

1. Effettuare una delle seguenti operazioni:
   - Selezionare l'opzione **Create Volumes for a existing workload** (Crea volumi per un carico di lavoro esistente) per creare volumi per un carico di lavoro esistente.
   - Selezionare l'opzione **Create a new workload** (Crea nuovo carico di lavoro) per definire un nuovo carico di lavoro per un'applicazione supportata o per "altre" applicazioni.
     - Dall'elenco a discesa, selezionare il nome dell'applicazione per cui si desidera creare il nuovo workload.

       Selezionare una delle "altre" voci se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.

     - Immettere un nome per il carico di lavoro che si desidera creare.
2. Fare clic su **Avanti**.
3. Se il carico di lavoro è associato a un tipo di applicazione supportato, inserire le informazioni richieste; in caso contrario, visitare il sito Fase 3: Aggiunta o modifica di volumi.

Fase 3: Aggiunta o modifica di volumi

System Manager potrebbe suggerire una configurazione del volume in base all'applicazione o al carico di lavoro selezionato. Questa configurazione del volume è ottimizzata in base al tipo di applicazione supportata

dal carico di lavoro. È possibile accettare la configurazione del volume consigliata o modificarla in base alle esigenze. Se è stata selezionata una delle "altre" applicazioni, è necessario specificare manualmente i volumi e le caratteristiche che si desidera creare.

Prima di iniziare

- I pool o i gruppi di volumi devono disporre di capacità libera sufficiente.
- Il numero massimo di volumi consentito in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello di sistema di storage:
  - 2,048 volumi (serie EF600 ed E5700)
  - 1,024 volumi (EF300)
  - 512 volumi (serie E2800)
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.

  Selezione di un pool o di un gruppo di volumi sicuri

  Se si desidera creare un volume abilitato da, selezionare un pool o un gruppo di volumi che supporti da (cercare **Sì** accanto a "da" nella tabella dei candidati del pool e del gruppo di volumi).

  Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi in System Manager. LA protezione DA verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. La selezione di un pool o di un gruppo di volumi da-capable per il nuovo volume garantisce il rilevamento e la correzione degli errori.

  Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

- Per creare un volume abilitato alla protezione, è necessario creare una chiave di sicurezza per l'array di storage.

  Selezione di un pool o di un gruppo di volumi sicuri

  Se si desidera creare un volume abilitato alla protezione, selezionare un pool o un gruppo di volumi che supporti la protezione (cercare **Sì** accanto a "abilitato alla protezione" nella tabella dei candidati del gruppo di volumi e del pool).

  Le funzionalità di sicurezza dei dischi vengono presentate a livello di pool e gruppo di volumi in System Manager. I dischi con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Un disco abilitato alla sicurezza crittografa i dati durante la scrittura e decrta i dati durante la lettura utilizzando una *chiave di crittografia* univoca.

  Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.

- Per creare un volume con provisioning di risorse, tutti i dischi devono essere dischi NVMe con l'opzione Deallocated o Unwritten Logical Block Error (DULBE).

A proposito di questa attività

I volumi vengono creati da pool o gruppi di volumi. La finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica

volumi) mostra tutti i pool e i gruppi di volumi idonei nell'array di storage. Per ciascun pool e gruppo di volumi idonei, vengono visualizzati il numero di dischi disponibili e la capacità libera totale.

Per alcuni carichi di lavoro specifici dell'applicazione, ciascun pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e la capacità libera rimanente in GiB. Per gli altri carichi di lavoro, la capacità proposta viene visualizzata quando si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

Fasi

1. Scegliere una di queste azioni in base alla selezione di un altro carico di lavoro o di un carico di lavoro specifico dell'applicazione:
    - **Altro** — fare clic su **Aggiungi nuovo volume** in ogni pool o gruppo di volumi che si desidera utilizzare per creare uno o più volumi.

Dettagli del campo

Campo	Descrizione
Volume Name (Nome volume)	System Manager assegna un nome predefinito a un volume durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 o 8 GiB, a seconda del tipo di disco. Qualsiasi capacità che non sia un multiplo di 4 o 8 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB o 8-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • 512 — 512 byte • 4K — 4,096 byte

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

Campo	Descrizione
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.
Provisioning delle risorse (solo EF300 e EF600)	**Sì** viene visualizzato accanto a "risorse fornite" solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

- **Carico di lavoro specifico dell'applicazione** — fare clic su **Avanti** per accettare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato.

Dettagli del campo

Campo	Descrizione
Volume Name (Nome volume)	System Manager assegna un nome predefinito a un volume durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 o 8 GiB, a seconda del tipo di disco. Qualsiasi capacità che non sia un multiplo di 4 o 8 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB o 8-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Tipo di volume	Il tipo di volume indica il tipo di volume creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • 512 — 512 byte • 4K — 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — System Manager determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage quando si modifica la dimensione del segmento per un volume, le prestazioni di i/o ne risentono, ma i dati rimangono disponibili.

Campo	Descrizione
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi nel pool o nel gruppo di volumi sono protetti. La sicurezza del disco impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione di sicurezza del disco è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.
Provisioning delle risorse (solo EF300 e EF600)	**Sì** viene visualizzato accanto a "risorse fornite" solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

2. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti** e passare a. Fase 4: Esaminare la configurazione del volume.

Fase 4: Esaminare la configurazione del volume

Esaminare un riepilogo dei volumi che si intende creare e apportare le modifiche necessarie.

Fasi

1. Esaminare i volumi che si desidera creare. Fare clic su **Indietro** per apportare le modifiche desiderate.
2. Quando si è soddisfatti della configurazione del volume, fare clic su **fine**.

Risultati

System Manager crea i nuovi volumi nei pool e nei gruppi di volumi selezionati, quindi visualizza i nuovi volumi nella tabella All Volumes (tutti i volumi).

Al termine

- Eseguire tutte le modifiche del sistema operativo necessarie sull'host dell'applicazione in modo che le applicazioni possano utilizzare il volume.
- Eseguire il sistema basato su host `hot_add` o un'utility specifica del sistema operativo (disponibile presso un fornitore di terze parti), quindi eseguire `SMdevices` utility per correlare i nomi dei volumi con i nomi degli array di storage host.

  Il `hot_add` e a. `SMdevices` le utility sono incluse nel `SMutils` pacchetto. Il `SMutils` il pacchetto è un insieme di utility per verificare ciò che l'host vede dall'array di storage. È incluso nell'installazione del software SANtricity.

Aggiungere volumi al carico di lavoro

È possibile aggiungere uno o più volumi a un carico di lavoro nuovo o esistente per i volumi attualmente non associati a un carico di lavoro.

A proposito di questa attività

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

3. Selezionare **Aggiungi al carico di lavoro**.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

4. Eseguire una delle seguenti operazioni:
   - **Aggiungi volumi a un carico di lavoro esistente** — selezionare questa opzione per aggiungere volumi a un carico di lavoro esistente.

     Utilizzare l'elenco a discesa per selezionare un carico di lavoro. Il tipo di applicazione associato al carico di lavoro viene assegnato ai volumi aggiunti a questo carico di lavoro.

   - **Aggiungi volumi a un nuovo carico di lavoro** — selezionare questa opzione per definire un nuovo carico di lavoro per un tipo di applicazione e aggiungere volumi al nuovo carico di lavoro.
5. Selezionare **Avanti** per continuare con la sequenza di aggiunta al carico di lavoro.

   Viene visualizzata la finestra di dialogo Select Volumes (Seleziona volumi).

6. Selezionare i volumi che si desidera aggiungere al carico di lavoro.
7. Esaminare i volumi che si desidera aggiungere al carico di lavoro selezionato.
8. Quando si è soddisfatti della configurazione del carico di lavoro, fare clic su **fine**.

Gestire i volumi

Aumentare la capacità di un volume

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

Prima di iniziare

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associati al volume.
- Il volume è ottimale e non in alcun stato di modifica.
- La capacità massima riportata di 256 TIB non è stata raggiunta per i volumi thin.
- Nel volume non sono in uso dischi hot spare. (Si applica solo ai volumi nei gruppi di volumi).

A proposito di questa attività

Tenere presente eventuali requisiti di capacità futuri per altri volumi in questo pool o gruppo di volumi. Assicurarsi di disporre di una capacità libera sufficiente per creare immagini snapshot, volumi snapshot o mirror remoti.

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

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare il volume per il quale si desidera aumentare la capacità, quindi selezionare **aumenta capacità**.

   Viene visualizzata la finestra di dialogo Conferma aumento capacità.

3. Selezionare **Sì** per continuare.

   Viene visualizzata la finestra di dialogo aumenta capacità riportata.

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

4. Utilizzare la casella **aumenta capacità segnalata aggiungendo…** per aggiungere capacità alla capacità corrente disponibile indicata. È possibile modificare il valore della capacità in modo che venga visualizzato in megibyte (MiB), gibibyte (GiB) o tebibyte (TIB).
5. Fare clic su **aumenta**.

Risultati

- System Manager aumenta la capacità del volume in base alla selezione effettuata.
- Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di aumento della capacità attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Al termine

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in

uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Inizializzare i volumi

Un volume viene inizializzato automaticamente quando viene creato per la prima volta. Tuttavia, il Recovery Guru potrebbe consigliare di inizializzare manualmente un volume per eseguire il ripristino in seguito a determinate condizioni di errore. Utilizzare questa opzione solo sotto la guida del supporto tecnico. È possibile selezionare uno o più volumi da inizializzare.

Prima di iniziare

- Tutte le operazioni di i/o sono state interrotte.
- Tutti i dispositivi o i file system sui volumi che si desidera inizializzare devono essere smontati.
- Il volume si trova in uno stato ottimale e non sono in corso operazioni di modifica sul volume.

> Non è possibile annullare l'operazione dopo l'avvio. Tutti i dati del volume vengono cancellati. Non provare a eseguire questa operazione a meno che il Recovery Guru non lo suggerisca. Prima di iniziare questa procedura, contattare il supporto tecnico.

A proposito di questa attività

Quando si inizializza un volume, il volume mantiene le impostazioni relative a WWN, assegnazioni host, capacità allocata e capacità riservata. Inoltre, mantiene le stesse impostazioni di sicurezza e di Data Assurance (da).

Impossibile inizializzare i seguenti tipi di volumi:

- Volume di base di un volume di snapshot
- Volume primario in una relazione mirror
- Volume secondario in relazione mirror
- Volume di origine in una copia del volume
- Volume di destinazione in una copia del volume
- Volume che ha già un'inizializzazione in corso

Questo argomento si applica solo ai volumi standard creati da pool o gruppi di volumi.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare un volume qualsiasi, quindi **More › Initialize Volumes** (Altro[Inizializza volumi]).

   Viene visualizzata la finestra di dialogo Inizializza volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

3. Selezionare uno o più volumi da inizializzare e confermare che si desidera eseguire l'operazione.

Risultati

System Manager esegue le seguenti operazioni:

- Cancella tutti i dati dai volumi inizializzati.

- Cancella gli indici dei blocchi, il che fa sì che i blocchi non scritti vengano letti come se fossero riempiti a zero (il volume sembra essere completamente vuoto).

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di inizializzazione attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Ridistribuire i volumi

Ridistribuisci i volumi per spostarli di nuovo nei proprietari di controller preferiti. In genere, i driver multipath spostano i volumi dal proprietario del controller preferito quando si verifica un problema lungo il percorso dei dati tra l'host e l'array di storage.

Prima di iniziare

- I volumi che si desidera ridistribuire non sono in uso o si verificano errori di i/O.
- Un driver multipath viene installato su tutti gli host che utilizzano i volumi che si desidera ridistribuire, altrimenti si verificheranno errori di i/O.

  Se si desidera ridistribuire i volumi senza un driver multipath sugli host, tutte le attività di i/o sui volumi *mentre è in corso l'operazione di ridistribuzione* devono essere interrotte per evitare errori dell'applicazione.

A proposito di questa attività

La maggior parte dei driver multipath host tenta di accedere a ciascun volume su un percorso verso il proprietario del controller preferito. Tuttavia, se questo percorso preferito non è disponibile, il driver multipath sull'host esegue il failover su un percorso alternativo. Questo failover potrebbe causare la modifica della proprietà del volume nel controller alternativo. Dopo aver risolto la condizione che ha causato il failover, alcuni host potrebbero spostare automaticamente la proprietà del volume nel proprietario del controller preferito, ma in alcuni casi potrebbe essere necessario ridistribuire manualmente i volumi.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare il **More › redistribuisci volumi**.

   Viene visualizzata la finestra di dialogo redistribuisci volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage il cui proprietario preferito del controller non corrisponde al proprietario corrente.

3. Selezionare uno o più volumi da ridistribuire e confermare che si desidera eseguire l'operazione.

Risultati

System Manager sposta i volumi selezionati nei rispettivi proprietari di controller preferiti oppure potrebbe essere visualizzata una finestra di dialogo ridistribuisci volumi non necessari.

Modificare la proprietà del controller di un volume

È possibile modificare la proprietà del controller preferito di un volume, in modo che l'i/o per le applicazioni host venga indirizzato attraverso il nuovo percorso.

Prima di iniziare

Se non si utilizza un driver multipath, tutte le applicazioni host che attualmente utilizzano il volume devono

essere chiuse. Questa azione impedisce gli errori dell'applicazione quando il percorso di i/o cambia.

A proposito di questa attività

È possibile modificare la proprietà del controller per uno o più volumi in un pool o un gruppo di volumi.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare un volume qualsiasi, quindi **More › Change ownership** (Altro[Modifica proprietà]).

   Viene visualizzata la finestra di dialogo Change Volume Ownership (Modifica proprietà volume). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

3. Utilizzare l'elenco a discesa **Preferred Owner** (Proprietario preferito) per modificare il controller preferito per ciascun volume che si desidera modificare e confermare che si desidera eseguire l'operazione.

Risultati

- System Manager modifica la proprietà del controller del volume. L'i/o al volume viene ora indirizzato attraverso questo percorso i/O.
- Il volume potrebbe non utilizzare il nuovo percorso i/o fino a quando il driver multipath non viene riconfigurato per riconoscere il nuovo percorso. Questa operazione richiede in genere meno di cinque minuti.

Elimina volume

In genere, i volumi vengono eliminati se sono stati creati con parametri o capacità errati, se non soddisfano più le esigenze di configurazione dello storage o se si tratta di immagini snapshot non più necessarie per il backup o il test delle applicazioni.

L'eliminazione di un volume aumenta la capacità libera nel pool o nel gruppo di volumi. È possibile selezionare uno o più volumi da eliminare.

Prima di iniziare

Sui volumi che si intende eliminare, assicurarsi di quanto segue:

- Viene eseguito il backup di tutti i dati.
- All Input/Output (i/o) viene interrotto.
- Tutti i dispositivi e i file system vengono smontati.

A proposito di questa attività

Non è possibile eliminare un volume che presenta una delle seguenti condizioni:

- Il volume è in fase di inizializzazione.
- Il volume è in fase di ricostruzione.
- Il volume fa parte di un gruppo di volumi che contiene un disco sottoposto a un'operazione copyback.
- Il volume sta subendo un'operazione di modifica, ad esempio una modifica delle dimensioni dei segmenti, a meno che il volume non sia ora nello stato Failed (guasto).
- Il volume contiene qualsiasi tipo di prenotazione persistente.
- Il volume è un volume di origine o un volume di destinazione in un volume di copia con stato Pending (in sospeso), in Progress (in corso) o Failed (non riuscito).

L'eliminazione di un volume causa la perdita di tutti i dati presenti su tali volumi.

Quando un volume supera una determinata dimensione (attualmente 128 TB), l'eliminazione viene eseguita in background e lo spazio liberato potrebbe non essere immediatamente disponibile.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Volumes.

3. Selezionare uno o più volumi da eliminare e confermare che si desidera eseguire l'operazione.
4. Fare clic su **Delete** (Elimina).

Risultati

System Manager esegue le seguenti operazioni:

- Elimina le immagini snapshot, le pianificazioni e i volumi di snapshot associati.
- Rimuove le relazioni di mirroring.
- Aumenta la capacità libera nel pool o nel gruppo di volumi.

Modificare il limite di capacità allocata per un volume sottile

Per i thin volumi in grado di allocare lo spazio on-demand, è possibile modificare il limite che limita la capacità allocata alla quale un thin volume può espandersi automaticamente.

È inoltre possibile modificare il punto percentuale in cui un avviso (soglia di avviso superata) viene inviato all'area Notifiche della pagina iniziale quando un volume sottile si trova vicino al limite di capacità allocata. È possibile scegliere di attivare o disattivare questa notifica di avviso.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Il sistema espande automaticamente la capacità allocata in base al limite di capacità allocata. Il limite di capacità allocata consente di limitare la crescita automatica del thin volume al di sotto della capacità riportata. Quando la quantità di dati scritti si avvicina alla capacità allocata, è possibile modificare il limite di capacità allocata.

Quando si modifica il limite di capacità allocata e la soglia di avviso di un volume sottile, è necessario tenere conto dello spazio che deve essere consumato dai dati utente e dai dati dei servizi di copia del volume.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare la scheda **Thin Volume Monitoring**.

   Viene visualizzata la vista Thin Volume Monitoring (monitoraggio volume sottile).

3. Selezionare il volume sottile che si desidera modificare, quindi selezionare **Modifica limite**.

Viene visualizzata la finestra di dialogo Change Limit (Modifica limite). In questa finestra di dialogo vengono visualizzati il limite di capacità allocata e la soglia di avviso per il volume sottile selezionato.

4. Modificare il limite di capacità allocata e la soglia di avviso in base alle necessità.

Dettagli del campo

Impostazione	Descrizione
Modifica limite di capacità allocata in…	La soglia alla quale le operazioni di scrittura non vengono eseguite, impedendo al thin volume di consumare risorse aggiuntive. Questa soglia è una percentuale delle dimensioni della capacità del volume riportate.
Avvisami quando… (soglia di avviso)	Selezionare questa casella di controllo se si desidera che il sistema generi un avviso quando un volume sottile si trova vicino al limite di capacità allocata. L'avviso viene inviato all'area Notifiche della home page. Questa soglia è una percentuale delle dimensioni della capacità del volume riportate. Deselezionare la casella di controllo per disattivare la notifica di avviso della soglia di avviso.

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

Gestire le impostazioni

Modificare le impostazioni di un volume

È possibile modificare le impostazioni di un volume, ad esempio il nome, l'assegnazione dell'host, la dimensione del segmento, la priorità di modifica, la memorizzazione nella cache, e così via.

Prima di iniziare

Il volume che si desidera modificare si trova nello stato ottimale.

> Alcune operazioni potrebbero non essere disponibili mentre sono in corso modifiche alle impostazioni del volume

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare il volume che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Settings (Impostazioni volume). Le impostazioni di configurazione del volume selezionato vengono visualizzate in questa finestra di dialogo.

3. Selezionare la scheda **Basic** per modificare il nome del volume e l'assegnazione dell'host.

Dettagli del campo

Impostazione	Descrizione
Nome	Visualizza il nome del volume. Modificare il nome di un volume quando il nome corrente non è più significativo o applicabile.
Capacità	Visualizza la capacità riportata e allocata per il volume selezionato. La capacità riportata e la capacità allocata sono le stesse per i volumi spessi, ma sono diverse per i volumi thin. Per un volume spesso, lo spazio fisicamente allocato è uguale allo spazio che viene segnalato all'host. Per un volume thin, la capacità riportata è la capacità che viene segnalata agli host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocato per la scrittura dei dati.
Gruppo pool/Volume	Visualizza il nome e il livello RAID del pool o del gruppo di volumi. Indica se il pool o il gruppo di volumi sono abilitati per la protezione e la protezione.
Host	Visualizza l'assegnazione del volume. Si assegna un volume a un cluster host o host in modo che sia possibile accedervi per le operazioni di i/O. Questa assegnazione consente a un host o a un cluster di host di accedere a un determinato volume o a una serie di volumi in un array di storage. • **Assegnato a** — identifica l'host o il cluster di host che ha accesso al volume selezionato. • **LUN** — Un numero di unità logica (LUN) è il numero assegnato allo spazio degli indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi. Per le interfacce NVMe, questa colonna visualizza l'ID dello spazio dei nomi. Uno spazio dei nomi è uno storage NVM formattato per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che si riferisce a un volume nell'array di storage. L'ID dello spazio dei nomi è l'identificatore univoco del controller NVMe per lo spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.

Impostazione	Descrizione
Identificatori	Visualizza gli identificatori del volume selezionato. • **WWID (World-Wide Identifier)** — identificatore esadecimale univoco del volume. • **Extended Unique Identifier (EUI)** — identificatore EUI-64 per il volume. • **SSID (Subsystem Identifier)** — identificativo del sottosistema dell'array di storage di un volume.

4. Selezionare la scheda **Avanzate** per modificare le impostazioni di configurazione aggiuntive per un volume in un pool o in un gruppo di volumi.

Dettagli del campo

Impostazione	Descrizione
Informazioni su applicazioni e carichi di lavoro	Durante la creazione dei volumi, è possibile creare carichi di lavoro specifici dell'applicazione o altri carichi di lavoro. Se applicabile, il nome del carico di lavoro, il tipo di applicazione e il tipo di volume vengono visualizzati per il volume selezionato. Se lo si desidera, è possibile modificare il nome del carico di lavoro.
Impostazioni della qualità del servizio	**Disable data assurance (Disattiva data assurance) in modo permanente** — questa impostazione viene visualizzata solo se il volume è abilitato per Data Assurance (da). DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. Utilizzare questa opzione per disattivare in modo permanente il da sul volume selezionato. Se disattivato, il da non può essere riattivato su questo volume. **Enable pre-Read Redundancy check** — questa impostazione viene visualizzata solo se il volume è un volume spesso. I controlli di ridondanza di pre-lettura determinano se i dati su un volume sono coerenti ogni volta che viene eseguita una lettura. Un volume con questa funzione attivata restituisce errori di lettura se i dati risultano incoerenti dal firmware del controller.
Proprietà del controller	Definisce il controller designato come controller principale o proprietario del volume. La proprietà del controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per l'i/o totale.

Impostazione	Descrizione
Dimensionamento dei segmenti	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — System Manager determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage quando si modifica la dimensione del segmento per un volume, le prestazioni di i/o ne risentono, ma i dati rimangono disponibili.
Priorità di modifica	Mostra l'impostazione della priorità di modifica, che viene visualizzata solo per i volumi in un gruppo di volumi. La priorità di modifica definisce il tempo di elaborazione allocato per le operazioni di modifica del volume in relazione alle prestazioni del sistema. È possibile aumentare la priorità di modifica del volume, anche se ciò potrebbe influire sulle prestazioni del sistema. Spostare le barre di scorrimento per selezionare un livello di priorità. **Modifica dei tassi di priorità** — il tasso di priorità più basso offre benefici alle prestazioni del sistema, ma l'operazione di modifica richiede più tempo. Il tasso di priorità più elevato è utile per l'operazione di modifica, ma le prestazioni del sistema potrebbero essere compromesse.

Impostazione	Descrizione
Caching	Mostra l'impostazione del caching, che è possibile modificare per influire sulle prestazioni i/o complessive di un volume.
Cache SSD	Mostra l'impostazione della cache SSD, che è possibile attivare sui volumi compatibili per migliorare le prestazioni di sola lettura. I volumi sono compatibili se condividono le stesse funzionalità di Drive Security e Data Assurance. **La funzione SSD cache utilizza uno o più dischi a stato solido (SSD) per implementare una cache di lettura**. Le performance applicative sono migliorate grazie ai tempi di lettura più rapidi per gli SSD. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. È sufficiente selezionare il volume che si desidera memorizzare nella cache, quindi il caching è automatico e dinamico.

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

   System Manager modifica le impostazioni del volume in base alle selezioni effettuate.

Al termine

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento delle operazioni di modifica attualmente in esecuzione per il volume selezionato.

Modificare le impostazioni del carico di lavoro

È possibile modificare il nome di un workload e visualizzarne il tipo di applicazione associato. Modificare il nome di un workload quando il nome corrente non è più significativo o applicabile.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

3. Selezionare il carico di lavoro che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Applications & workload Settings (Impostazioni applicazioni e carichi di lavoro).

4. **Opzionale:** modificare il nome del carico di lavoro fornito dall'utente.
5. Fare clic su **Save** (Salva).

Modificare le impostazioni della cache per un volume

È possibile modificare le impostazioni della cache di lettura e di scrittura per influire sulle prestazioni i/o generali di un volume.

A proposito di questa attività

Quando si modificano le impostazioni della cache di un volume, tenere presenti le seguenti linee guida:

- Dopo aver aperto la finestra di dialogo Change cache Settings (Modifica impostazioni cache), potrebbe essere visualizzata un'icona accanto alle proprietà della cache selezionate. Questa icona indica che il controller ha temporaneamente sospeso le operazioni di caching.

  Questa azione potrebbe verificarsi quando una nuova batteria è in carica, quando un controller è stato rimosso o se il controller ha rilevato una mancata corrispondenza nelle dimensioni della cache. Una volta deselezionata la condizione, le proprietà della cache selezionate nella finestra di dialogo diventano attive. Se le proprietà della cache selezionate non diventano attive, contattare il supporto tecnico.

- È possibile modificare le impostazioni della cache per un singolo volume o per più volumi su un array di storage. È possibile modificare le impostazioni della cache per tutti i volumi standard o per tutti i volumi thin contemporaneamente.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare un volume qualsiasi, quindi **More › Change cache settings** (Altro[Modifica impostazioni cache]).

   Viene visualizzata la finestra di dialogo Change cache Settings (Modifica impostazioni cache). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

3. Selezionare la scheda **Basic** per modificare le impostazioni per il caching in lettura e il caching in scrittura.

   Dettagli del campo

Impostazione della cache	Descrizione
Read Caching (cache lettura)	La cache di lettura è un buffer che memorizza i dati letti dai dischi. I dati di un'operazione di lettura potrebbero essere già presenti nella cache di un'operazione precedente, eliminando così la necessità di accedere ai dischi. I dati rimangono nella cache di lettura fino a quando non vengono scaricati.
Cache di scrittura	La cache di scrittura è un buffer che memorizza i dati dell'host che non sono ancora stati scritti sui dischi. I dati rimangono nella cache di scrittura fino a quando non vengono scritti sui dischi. Il caching in scrittura può aumentare le performance di i/O. La cache viene automaticamente scaricata dopo la disattivazione di **Write caching** per un volume.

4. Selezionare la scheda **Advanced** (Avanzate) per modificare le impostazioni avanzate per i volumi spessi. Le impostazioni avanzate della cache sono disponibili solo per i volumi thick.

Dettagli del campo

Impostazione della cache	Descrizione
Precaricamento della cache di lettura dinamica	Il prefetch di lettura dinamico della cache consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i 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. Per un volume thin, il prefetch dinamico di lettura della cache è sempre disattivato e non può essere modificato.
Cache di scrittura senza batterie	Il caching in scrittura senza batterie consente di continuare il caching in scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta del caching in scrittura senza batterie non è generalmente consigliata, in quanto i dati potrebbero andare persi in caso di interruzione dell'alimentazione. In genere, il caching in scrittura viene disattivato temporaneamente dal controller fino a quando le batterie non vengono caricate o non viene sostituita una batteria guasta. **Possibile perdita di dati** — se si seleziona questa opzione e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione **Write caching without batteries**. Questa impostazione è disponibile solo se è stato attivato il caching in scrittura. Questa impostazione non è disponibile per i volumi thin.
Cache di scrittura con mirroring	Il caching in scrittura con mirroring si verifica quando i dati scritti nella memoria cache di un controller vengono scritti anche nella memoria cache dell'altro controller. Pertanto, se un controller si guasta, l'altro può completare tutte le operazioni di scrittura in sospeso. Il mirroring della cache di scrittura è disponibile solo se il caching di scrittura è attivato e sono presenti due controller. Il caching in scrittura con mirroring è l'impostazione predefinita alla creazione del volume. Questa impostazione è disponibile solo se è stato attivato il caching in scrittura. Questa impostazione non è disponibile per i volumi thin.

5. Fare clic su **Save** (Salva) per modificare le impostazioni della cache.

Modificare le impostazioni di scansione dei supporti per un volume

Una scansione dei supporti è un'operazione in background che esegue la scansione di tutti i dati e delle informazioni di ridondanza nel volume. Utilizzare questa opzione per attivare o disattivare le impostazioni di scansione dei supporti per uno o più volumi o per modificare la durata della scansione.

Prima di iniziare

Comprendere quanto segue:

- Le scansioni dei supporti vengono eseguite continuamente a una velocità costante in base alla capacità da sottoporre a scansione e alla durata della scansione. Le scansioni in background possono essere temporaneamente sospese da un'attività in background con priorità più alta (ad esempio ricostruzione), ma vengono rieseguite alla stessa velocità costante.
- La scansione di un volume viene eseguita solo quando l'opzione di scansione dei supporti è attivata per l'array di storage e per quel volume. Se è attivata anche la verifica della ridondanza per quel volume, le informazioni di ridondanza nel volume verranno controllate per verificarne la coerenza con i dati, a condizione che il volume disponga di ridondanza. La scansione dei supporti con controllo della ridondanza è attivata per impostazione predefinita per ciascun volume al momento della creazione.
- Se durante la scansione si verifica un errore irreversibile del supporto, i dati verranno riparati utilizzando le informazioni di ridondanza, se disponibili.

  Ad esempio, le informazioni di ridondanza sono disponibili in volumi RAID 5 ottimali o in volumi RAID 6 ottimali o con un solo disco guasto. Se l'errore irreversibile non può essere riparato utilizzando le informazioni di ridondanza, il blocco di dati viene aggiunto al registro del settore illeggibile. Nel registro eventi vengono riportati errori del supporto correggibili e non correggibili.

  Se il controllo di ridondanza rileva un'incoerenza tra i dati e le informazioni di ridondanza, viene riportato nel registro eventi.

A proposito di questa attività

Le scansioni dei supporti rilevano e riparano gli errori dei supporti sui blocchi di dischi che vengono raramente letti dalle applicazioni. Ciò può impedire la perdita di dati in caso di guasto di un disco, poiché i dati dei dischi guasti vengono ricostruiti utilizzando le informazioni di ridondanza e i dati di altri dischi nel gruppo di volumi o nel pool.

È possibile eseguire le seguenti operazioni:

- Attivare o disattivare la scansione dei supporti in background per l'intero array di storage
- Modificare la durata della scansione per l'intero array di storage
- Attivare o disattivare la scansione dei supporti per uno o più volumi
- Attivare o disattivare il controllo di ridondanza per uno o più volumi

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare un volume qualsiasi, quindi **More › Change media scan settings** (Altro[Modifica impostazioni di scansione dei supporti]).

Viene visualizzata la finestra di dialogo Change Drive Media Scan Settings (Modifica impostazioni scansione supporti unità). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

3. Per attivare la scansione dei supporti, selezionare la casella di controllo **scansione supporti durante…**.

   La disattivazione della casella di controllo scansione supporti consente di sospendere tutte le impostazioni di scansione dei supporti.

4. Specificare il numero di giorni in cui si desidera eseguire la scansione del supporto.
5. Selezionare la casella di controllo **Media Scan** per ciascun volume su cui si desidera eseguire una scansione dei supporti.

   System Manager attiva l'opzione Redundancy Check per ciascun volume su cui si sceglie di eseguire una scansione dei supporti. Se esistono singoli volumi per i quali non si desidera eseguire un controllo di ridondanza, deselezionare la casella di controllo **controllo di ridondanza**.

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

   System Manager applica le modifiche alle scansioni dei supporti in background in base alla selezione effettuata.

Utilizzare i servizi di copia

Panoramica del volume di copia

La funzione Copy Volume (Copia volume) consente di creare una copia point-in-time di un volume creando due volumi separati, il volume di origine e il volume di destinazione, sullo stesso array di storage.

Questa funzione esegue una copia byte per byte dal volume di origine al volume di destinazione, rendendo i dati sul volume di destinazione identici ai dati sul volume di origine.

Copia dei dati per un maggiore accesso

Con la modifica dei requisiti di storage per un volume, è possibile utilizzare la funzione Copy Volume (Copia volume) per copiare i dati da pool o gruppi di volumi che utilizzano dischi di capacità inferiore in pool o gruppi di volumi che utilizzano dischi di capacità superiore. Ad esempio, è possibile utilizzare la funzione Copy Volume (Copia volume) per effettuare le seguenti operazioni:

- Spostare i dati su dischi più grandi.
- Passare a dischi con una velocità di trasferimento dei dati superiore.
- Passa ai dischi utilizzando nuove tecnologie per ottenere performance superiori.
- Modificare un volume sottile in un volume spesso.

Modificare un volume sottile in un volume spesso

Se si desidera modificare un volume thin in un volume thick, utilizzare l'operazione Copy Volume (Copia volume) per creare una copia del volume thin. La destinazione di un'operazione Copy Volume è sempre un volume spesso.

System Manager non offre un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare l'interfaccia della riga di comando (CLI).

Dati di backup

La funzione Copy Volume consente di eseguire il backup di un volume copiando i dati da un volume a un altro nello stesso array di storage. È possibile utilizzare il volume di destinazione come backup per il volume di origine, per il test del sistema o per eseguire il backup su un altro dispositivo, ad esempio un'unità a nastro.

Ripristinare i dati del volume Snapshot nel volume di base

Se è necessario ripristinare i dati nel volume di base dal volume snapshot associato, è possibile utilizzare la funzione Copy Volume (Copia volume) per copiare i dati dal volume snapshot al volume di base. È possibile creare una copia del volume dei dati sul volume di snapshot, quindi copiare i dati nel volume di base.

Volumi di origine e di destinazione

La tabella seguente specifica i tipi di volumi che è possibile utilizzare per i volumi di origine e di destinazione con la funzione Copy Volume (Copia volume).

Tipo di volume	Volume di origine della copia del volume offline	Volume online di origine della copia del volume	Volume di destinazione online e offline
Volume denso in un pool	Sì	Sì	Sì
Volume spesso in un gruppo di volumi	Sì	Sì	Sì
Volume sottile	Sì[1]	Sì	No
Volume Snapshot	Sì[2]	No	No
Volume di base Snapshot	Sì	No	No
Volume primario mirror remoto	Sì[3]	No	Sì

[1] il volume di destinazione deve avere una capacità uguale o superiore alla capacità del volume sottile riportata.

[2] non è possibile utilizzare la copia del volume snapshot fino al completamento dell'operazione di copia online.

[3] se il volume di origine è un volume primario, la capacità del volume di destinazione deve essere uguale o superiore alla capacità utilizzabile del volume di origine.

Tipi di operazioni Copy Volume

È possibile eseguire un'operazione *offline* Copy Volume o un'operazione *online* Copy Volume. Un'operazione offline legge i dati da un volume di origine e li copia in un volume di destinazione. Un'operazione online utilizza un volume di snapshot come origine e

copia i dati in un volume di destinazione.

Per garantire l'integrità dei dati, tutte le attività i/o sul volume di destinazione vengono sospese durante uno dei due tipi di operazioni Copy Volume. Questa sospensione si verifica perché lo stato dei dati sul volume di destinazione non è coerente fino al completamento della procedura.

Di seguito sono descritte le operazioni del volume di copia offline e online.

Operazione di copia del volume offline

La relazione del volume di copia offline è tra un volume di origine e un volume di destinazione. Una copia offline legge i dati dal volume di origine e li copia in un volume di destinazione, sospendendo tutti gli aggiornamenti al volume di origine con la copia in corso. Tutti gli aggiornamenti del volume di origine vengono sospesi per evitare la creazione di incoerenze cronologiche nel volume di destinazione.

Informazioni sulle operazioni di copia offline	
Richieste di lettura e scrittura	• I volumi di origine che partecipano a una copia offline sono disponibili per l'attività i/o di sola lettura mentre un'operazione Copy Volume ha lo stato in corso o in sospeso. • Le richieste di scrittura sono consentite una volta completata la copia offline. • Per evitare messaggi di errore protetti da scrittura, non accedere a un volume di origine che partecipa a un'operazione Copy Volume con lo stato in corso.
Journaling file system	• Se il volume di origine è stato formattato con un file system di journaling, qualsiasi tentativo di inviare una richiesta di lettura al volume di origine potrebbe essere rifiutato dai controller degli array di storage e potrebbe essere visualizzato un messaggio di errore. • Il driver del file system di journaling invia una richiesta di scrittura prima di tentare di emettere la richiesta di lettura. Il controller rifiuta la richiesta di scrittura e la richiesta di lettura potrebbe non essere emessa a causa della richiesta di scrittura rifiutata. Questa condizione potrebbe causare la visualizzazione di un messaggio di errore che indica che il volume di origine è protetto da scrittura. • Per evitare che questo problema si verifichi, non tentare di accedere a un volume di origine che partecipa a una copia offline mentre l'operazione Copy Volume ha lo stato in corso.

Operazione di copia online del volume

La relazione del volume di copia online è tra un volume di snapshot e un volume di destinazione. È possibile avviare un'operazione Copy Volume (Copia volume) mentre il volume di origine è online e disponibile per la scrittura dei dati. Questa funzione si ottiene creando uno snapshot del volume e utilizzando lo snapshot come volume di origine effettivo per la copia.

Quando si avvia un'operazione Copy Volume (Copia volume) per un volume di origine, System Manager crea un'immagine snapshot del volume di base e una relazione di copia tra l'immagine snapshot del volume di base e un volume di destinazione. L'utilizzo dell'immagine snapshot come volume di origine consente all'array di storage di continuare a scrivere nel volume di origine mentre la copia è in corso.

Durante un'operazione di copia online, si verifica un impatto sulle performance dovuto alla procedura copy-on-write. Una volta completata la copia online, le prestazioni del volume di base vengono ripristinate.

Informazioni utili sulle operazioni di copia online	
Che tipo di volumi è possibile utilizzare?	• Il volume per il quale viene creata l'immagine point-in-time è noto come volume di base e deve essere un volume standard o un volume sottile sull'array di storage. • Un volume di destinazione può essere un volume standard in un gruppo di volumi o un volume standard in un pool. Un volume di destinazione non può essere un volume sottile o un volume di base in un gruppo di snapshot. • È possibile utilizzare la funzione online Copy Volume per copiare i dati da un thin volume a un volume standard in un pool che risiede nello stesso array di storage. Tuttavia, non è possibile utilizzare la funzione Copy Volume (Copia volume) per copiare i dati da un volume standard a un volume thin.
Performance di base dei volumi	• Se il volume snapshot utilizzato come origine della copia è attivo, le prestazioni del volume di base sono ridotte a causa delle operazioni di copia su scrittura. Una volta completata la copia, lo snapshot viene disattivato e le prestazioni del volume di base vengono ripristinate. Anche se lo snapshot è disattivato, il volume di capacità riservata e la relazione di copia rimangono intatti.
Tipi di volumi creati	• Durante l'operazione di copia online vengono creati un volume snapshot e un volume di capacità riservata. • Il volume Snapshot non è un volume effettivo contenente dati, ma un riferimento ai dati contenuti in un volume in un momento specifico. • Per ogni snapshot creato, viene creato un volume di capacità riservata per conservare i dati dello snapshot. Il volume di capacità riservata viene utilizzato solo per gestire l'immagine snapshot.
Volume di capacità riservato	• Prima di modificare un blocco di dati sul volume di origine, il contenuto del blocco da modificare viene copiato nel volume di capacità riservata per la conservazione in sicurezza. • Poiché il volume a capacità riservata memorizza le copie dei dati originali in tali blocchi di dati, ulteriori modifiche apportate a tali blocchi di dati scrivono solo nel volume di origine. • L'operazione di copia online utilizza meno spazio su disco rispetto a una copia fisica completa, poiché gli unici blocchi di dati memorizzati nel volume a capacità riservata sono quelli modificati dall'ora dello snapshot.

Volume di copia

È possibile copiare i dati da un volume a un altro nello stesso array di storage e creare un duplicato fisico point-in-time (clone) di un volume di origine.

Prima di iniziare

- Tutte le attività di i/o sul volume di origine e sul volume di destinazione devono essere interrotte.
- Tutti i file system sul volume di origine e sul volume di destinazione devono essere smontati.
- Se in precedenza è stato utilizzato il volume di destinazione in un'operazione Copy Volume, non è più necessario eseguire il backup dei dati o di tali dati.

A proposito di questa attività

Il volume di origine è il volume che accetta i/o host e memorizza i dati dell'applicazione. Quando viene avviato un volume di copia, i dati del volume di origine vengono copiati interamente nel volume di destinazione.

Il volume di destinazione è un volume standard che mantiene una copia dei dati dal volume di origine. Il volume di destinazione è identico al volume di origine al termine dell'operazione Copy Volume (Copia volume). Il volume di destinazione deve avere la stessa capacità o una capacità superiore del volume di origine; tuttavia, può avere un livello RAID diverso.

Ulteriori informazioni sulle copie online e offline

Copia online

Una copia online crea una copia point-in-time di qualsiasi volume all'interno di un array di storage, mentre è ancora possibile scrivere sul volume con la copia in corso. Questa funzione si ottiene creando uno snapshot del volume e utilizzando lo snapshot come volume di origine effettivo per la copia. Il volume per il quale viene creata l'immagine point-in-time è noto come volume di base e può essere un volume standard o un volume sottile nell'array di storage.

Copia offline

Una copia offline legge i dati dal volume di origine e li copia in un volume di destinazione, sospendendo tutti gli aggiornamenti al volume di origine con la copia in corso. Tutti gli aggiornamenti del volume di origine vengono sospesi per evitare la creazione di incoerenze cronologiche nel volume di destinazione. La relazione di copia del volume offline è tra un volume di origine e un volume di destinazione.

Un'operazione Copy Volume sovrascrive i dati sul volume di destinazione e non riesce a tutti i volumi snapshot associati al volume di destinazione, se presenti.

Fasi

1. Selezionare **Storage › Volumes** (Storage[volumi]).
2. Selezionare il volume che si desidera utilizzare come origine per l'operazione Copy Volume (Copia volume), quindi selezionare **Copy Services › Copy volume** (Copia volume).

   Viene visualizzata la finestra di dialogo Copy Volume-Select Target (Copia destinazione selezione volume).

3. Selezionare il volume di destinazione in cui si desidera copiare i dati.

   La tabella riportata in questa finestra di dialogo elenca tutti i volumi di destinazione idonei.

4. Utilizzare la barra di scorrimento per impostare la priorità di copia per l'operazione Copy Volume (Copia volume).

   La priorità di copia determina la quantità di risorse di sistema utilizzate per completare l'operazione Copy Volume rispetto alle richieste i/o di servizio.

Ulteriori informazioni sui tassi di priorità delle copie

Sono disponibili cinque percentuali di priorità delle copie:

- Più basso
- Basso
- Medio
- Alto
- Massimo

Se la priorità di copia è impostata sul tasso più basso, l'attività di i/o viene assegnata priorità e l'operazione Copy Volume richiede più tempo. Se la priorità di copia è impostata sulla velocità massima, l'operazione Copy Volume (Copia volume) ha la priorità, ma l'attività i/o per l'array di storage potrebbe risentirne.

5. Selezionare se si desidera creare una copia online o offline. Per creare una copia online, selezionare la casella di controllo **Mantieni il volume di origine online durante l'operazione di copia**.
6. Effettuare una delle seguenti operazioni:
   - Per eseguire un'operazione di copia *online*, fare clic su **Avanti** per passare alla finestra di dialogo **capacità riservata**.
   - Per eseguire un'operazione di copia *offline*, fare clic su **fine** per avviare la copia offline.
7. Se si sceglie di creare una copia online, impostare la capacità riservata necessaria per memorizzare i dati e altre informazioni per la copia online, quindi fare clic su **fine** per avviare la copia online.

   La tabella dei candidati al volume visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.

   Allocare la capacità riservata utilizzando le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base, e di solito questa capacità è sufficiente.
   - Tuttavia, la capacità riservata varia in base al numero di modifiche apportate ai dati originali. Più a lungo è attivo un oggetto di storage, maggiore sarà la capacità riservata.

Risultati

System Manager copia tutti i dati dal volume di origine al volume di destinazione. Al termine dell'operazione Copy Volume (Copia volume), il volume di destinazione diventa automaticamente di sola lettura per gli host.

Al termine

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione Copy Volume (Copia volume). Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Eseguire un'operazione di copia del volume

È possibile visualizzare un'operazione Copy Volume (Copia volume) in corso e interrompere, modificare la priorità, eseguire nuovamente la copia o annullare

un’operazione Copy Volume (Copia volume).

Fasi

1. Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso).

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

2. Individuare l’operazione Copy Volume (Copia volume) su cui si desidera eseguire l’azione, quindi fare clic sul collegamento nella colonna **Actions** (azioni) per eseguire una delle seguenti operazioni.

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

Azione	Descrizione
Arrestare	È possibile interrompere un’operazione Copy Volume (Copia volume) quando l’operazione ha lo stato in corso, Pending (in sospeso) o Failed (non riuscito). Quando il volume di copia viene arrestato, tutti gli host mappati hanno accesso in scrittura al volume di origine. Se i dati vengono scritti nel volume di origine, i dati nel volume di destinazione non corrispondono più ai dati nel volume di origine.
Modificare la priorità	È possibile modificare la priorità di un’operazione Copy Volume (Copia volume) mentre l’operazione ha lo stato in corso per selezionare la velocità di completamento dell’operazione Copy Volume (Copia volume).
Copia di nuovo	È possibile copiare di nuovo un volume quando si è interrotta un’operazione Copy Volume e si desidera avviarla di nuovo o quando un’operazione Copy Volume (Copia volume) non ha avuto esito positivo o si è interrotta. L’operazione Copy Volume (Copia volume) viene avviata dall’inizio. L’azione di ricopia sovrascrive i dati esistenti sul volume di destinazione e non riesce a tutti i volumi di snapshot associati al volume di destinazione, se presenti.
Chiaro	È possibile rimuovere l’operazione Copy Volume (Copia volume) quando l’operazione ha lo stato in corso, Pending (in sospeso) o Failed (non riuscito). Assicurarsi di eseguire questa operazione prima di selezionare **Cancella**. Nessuna finestra di dialogo di conferma.

FAQ

Che cos’è un volume?

Un volume è un container in cui applicazioni, database e file system memorizzano i dati. Si tratta del componente logico creato per consentire all’host di accedere allo storage sull’array di storage.

Un volume viene creato dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Anche se un volume può essere costituito da più di un disco, un volume viene visualizzato come un componente logico per l'host.

Perché viene visualizzato un errore di overallocation della capacità quando si dispone di capacità libera sufficiente in un gruppo di volumi per creare volumi?

Il gruppo di volumi selezionato potrebbe avere una o più aree a capacità libera. Un'area di capacità libera è la capacità libera che può derivare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità disponibile durante la creazione del volume.

Quando si crea un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume viene limitata alla maggiore area di capacità libera del gruppo di volumi. Ad esempio, se un gruppo di volumi ha una capacità libera totale di 15 GiB e l'area di capacità libera più grande è di 10 GiB, il volume più grande che è possibile creare è di 10 GiB.

Se un gruppo di volumi dispone di aree di capacità libera, il grafico del gruppo di volumi contiene un link che indica il numero di aree di capacità libera esistenti. Selezionare il collegamento per visualizzare una finestra a comparsa che indica la capacità di ciascuna area.

Consolidando la capacità libera, è possibile creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi. È possibile consolidare la capacità libera esistente su un gruppo di volumi selezionato utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, il suggerimento "consolidare la capacità libera" viene visualizzato nella home page dell'area di notifica. Fare clic sul collegamento **consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile selezionare il **Pools & Volume Groups › Uncommon Tasks › consolida capacità libera del gruppo di volumi** per avviare la finestra di dialogo.

Se si desidera utilizzare un'area di capacità libera specifica invece dell'area di capacità libera più grande, utilizzare l'interfaccia a riga di comando (CLI).

In che modo il carico di lavoro selezionato influisce sulla creazione di volumi?

Durante la creazione del volume, vengono richieste informazioni sull'utilizzo di un carico di lavoro. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze. In alternativa, è possibile saltare questo passaggio nella sequenza di creazione del volume.

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

- **Specifico dell'applicazione** — quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.

- Microsoft® SQL Server™
- Microsoft® Exchange Server™
- Applicazioni di videosorveglianza
- VMware ESXi™ (per volumi da utilizzare con il file system della macchina virtuale)

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

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

Perché questi volumi non sono associati a un carico di lavoro?

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

Perché non è possibile eliminare il carico di lavoro selezionato?

Questo carico di lavoro è costituito da un gruppo di volumi creati utilizzando l'interfaccia della riga di comando (CLI) o migrati (importati/esportati) da un array di storage diverso. Di conseguenza, i volumi di questo carico di lavoro non sono associati a un carico di lavoro specifico dell'applicazione, pertanto non è possibile eliminare il carico di lavoro.

In che modo i carichi di lavoro specifici dell'applicazione mi aiutano a gestire lo storage array?

Le caratteristiche del volume del carico di lavoro specifico dell'applicazione determinano il modo in cui il carico di lavoro interagisce con i componenti dell'array di storage e aiutano a determinare le performance dell'ambiente in una determinata configurazione.

Un'applicazione è un software come SQL Server o Exchange. È possibile definire uno o più workload per supportare ciascuna applicazione. Per alcune applicazioni, il sistema consiglia automaticamente una configurazione del volume che ottimizzi lo storage. Caratteristiche come il tipo di i/o, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume.

In che modo fornire queste informazioni aiuta a creare storage?

Le informazioni sul carico di lavoro vengono utilizzate per ottimizzare le caratteristiche del volume, ad esempio il tipo di i/o, la dimensione del segmento e la cache di lettura/scrittura per il carico di lavoro selezionato. Queste caratteristiche ottimizzate determinano il modo in cui il carico di lavoro interagisce con i componenti dell'array di storage.

In base alle informazioni sul carico di lavoro fornite, System Manager crea i volumi appropriati e li inserisce nei pool o nei gruppi di volumi disponibili attualmente nel sistema. Il sistema crea i volumi e ne ottimizza le

caratteristiche in base alle Best practice correnti per il carico di lavoro selezionato.

Prima di completare la creazione dei volumi per un determinato carico di lavoro, è possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Per informazioni sulle Best practice, consultare la documentazione specifica dell'applicazione.

Cosa devo fare per riconoscere la capacità espansa?

Se si aumenta la capacità di un volume, l'host potrebbe non riconoscere immediatamente l'aumento della capacità del volume.

La maggior parte dei sistemi operativi riconosce la capacità del volume espanso e si espande automaticamente dopo l'avvio dell'espansione del volume. Tuttavia, alcuni potrebbero non farlo. Se il sistema operativo non riconosce automaticamente la capacità del volume espanso, potrebbe essere necessario eseguire una nuova scansione o un riavvio del disco.

Una volta espansa la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso.

Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Perché non vengono visualizzati tutti i pool e/o i gruppi di volumi?

Qualsiasi pool o gruppo di volumi in cui non è possibile spostare il volume non viene visualizzato nell'elenco.

I pool o i gruppi di volumi non sono idonei per uno dei seguenti motivi:

- Le funzionalità di Data Assurance (da) di un pool o di un gruppo di volumi non corrispondono.
- Un pool o un gruppo di volumi non si trova in uno stato ottimale.
- La capacità di un pool o di un gruppo di volumi è troppo ridotta.

Che cos'è la dimensione del segmento?

Un segmento è la quantità di dati in kilobyte (KiB) memorizzati su un disco prima che l'array di storage passi al disco successivo nello stripe (gruppo RAID). Le dimensioni dei segmenti si applicano solo ai gruppi di volumi, non ai pool.

La dimensione del segmento è definita dal numero di blocchi di dati in esso contenuti. Quando si determina la dimensione del segmento, è necessario conoscere il tipo di dati da memorizzare in un volume. Se un'applicazione utilizza generalmente IOPS (Random Read and Scritture) di piccole dimensioni, un segmento di dimensioni inferiori funziona meglio. In alternativa, se l'applicazione dispone di grandi letture e scritture sequenziali (throughput), una dimensione di segmento elevata è generalmente migliore.

Sia che un'applicazione utilizzi piccole letture e scritture casuali o grandi letture e scritture sequenziali, l'array di storage offre prestazioni migliori se la dimensione del segmento è maggiore della dimensione tipica del blocco di dati. In genere, questo rende più semplice e rapido l'accesso dei dischi ai dati, il che è importante per migliorare le performance degli array di storage.

Ambienti in cui le performance IOPS sono importanti

In un ambiente IOPS (i/o Operations per second), lo storage array offre prestazioni migliori se si utilizza una dimensione di segmento superiore alla dimensione tipica del blocco di dati (“chunk”) che viene letta/scritta su un disco. In questo modo, ogni chunk viene scritto su un singolo disco.

Ambienti in cui il throughput è importante

In un ambiente di throughput, la dimensione del segmento deve essere pari a una frazione del totale dei dischi per i dati e la dimensione tipica del blocco di dati (dimensione i/o). In questo modo, i dati vengono distribuiti come singolo stripe tra i dischi del gruppo di volumi, con conseguente velocità di lettura e scrittura.

Che cos’è la proprietà preferita del controller?

Preferred controller ownership (proprietà preferita del controller): Definisce il controller designato come controller principale o proprietario del volume.

La proprietà del controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per l’i/o totale.

Ad esempio, se un controller legge principalmente grandi blocchi di dati sequenziali e l’altro controller ha piccoli blocchi di dati con letture e scritture frequenti, i carichi sono molto diversi. La conoscenza dei volumi che contengono il tipo di dati consente di bilanciare i trasferimenti di i/o in modo uniforme su entrambi i controller.

Quando si desidera utilizzare la selezione dell’host di assegnazione in un secondo momento?

Se si desidera accelerare il processo di creazione dei volumi, è possibile saltare la fase di assegnazione dell’host in modo che i volumi appena creati vengano inizializzati offline.

I volumi appena creati devono essere inizializzati. Il sistema può inizializzarli utilizzando una delle due modalità, ovvero un processo di inizializzazione in background del formato IMMEDIATAMENTE disponibile (IAF) o un processo offline.

Quando si esegue il mapping di un volume a un host, tutti i volumi di inizializzazione del gruppo vengono forzati a passare all’inizializzazione in background. Questo processo di inizializzazione in background consente l’i/o host simultaneo, che a volte può richiedere molto tempo.

Quando nessuno dei volumi in un gruppo di volumi viene mappato, viene eseguita l’inizializzazione offline. Il processo offline è molto più veloce del processo in background.

Cosa occorre sapere sui requisiti relativi alle dimensioni dei blocchi host?

Per i sistemi EF300 e EF600, è possibile impostare un volume in modo che supporti una dimensione di blocco di 512 byte o 4 KiB (chiamata anche "dimensione del settore"). È necessario impostare il valore corretto durante la creazione del volume. Se possibile, il sistema suggerisce il valore predefinito appropriato.

Prima di impostare le dimensioni del blocco del volume, leggere le seguenti limitazioni e linee guida.

- Alcuni sistemi operativi e macchine virtuali (in particolare VMware, al momento) richiedono una dimensione di blocco di 512 byte e non supportano 4KiB, quindi assicurarsi di conoscere i requisiti dell’host prima di creare un volume. In genere, è possibile ottenere le migliori prestazioni impostando un volume in modo

che presenti una dimensione di blocco di 4 KiB; tuttavia, assicurarsi che l'host supporti blocchi da 4 KiB (o "4Kn").

- Il tipo di dischi selezionati per il pool o il gruppo di volumi determina anche le dimensioni dei blocchi di volume supportate, come indicato di seguito:
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 512 byte, è possibile creare solo volumi con blocchi da 512 byte.
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 4 KiB, è possibile creare volumi con blocchi da 512 byte o 4 KiB.
- Se l'array dispone di una scheda di interfaccia host iSCSI, tutti i volumi sono limitati a blocchi da 512 byte (indipendentemente dalla dimensione del blocco del gruppo di volumi). Ciò è dovuto a un'implementazione hardware specifica.
- Una volta impostata, non è possibile modificare le dimensioni di un blocco. Se è necessario modificare le dimensioni di un blocco, è necessario eliminare il volume e ricrearlo.

Host e cluster di host

Panoramica degli host e dei cluster di host

È possibile configurare host e cluster di host, che definiscono le connessioni tra lo storage array e i server di dati.

Cosa sono gli host e i cluster di host?

Un *host* è un server che invia i/o a un volume su un array di storage. Un *cluster di host* è un gruppo di host che è possibile creare per assegnare gli stessi volumi a più host.

Scopri di più:

- "Terminologia dell'host"
- "Volumi di accesso"
- "Numero massimo di LUN"

Come si configurano gli host e i cluster di host?

Per definire le connessioni host, è possibile consentire a un HCA (host Context Agent) di rilevare automaticamente gli host oppure accedere al **Storage › hosts** per configurare manualmente l'host. Se si desidera che due o più host condividano l'accesso allo stesso set di volumi, è possibile definire un cluster e assegnare i volumi a tale cluster.

Scopri di più:

- "Creazione automatica e manuale degli host"
- "Modalità di assegnazione dei volumi agli host e ai cluster di host"
- "Workflow per la creazione dell'host e l'assegnazione del volume"
- "Crea host automaticamente"
- "Creare l'host manualmente"
- "Creare un cluster host"

- "Assegnare volumi agli host"

Informazioni correlate

Scopri di più sulle attività relative agli host:

- "Impostare il bilanciamento automatico del carico"
- "Impostare il reporting sulla connettività host"
- "Modificare il tipo di host predefinito"

Concetti

Terminologia dell'host

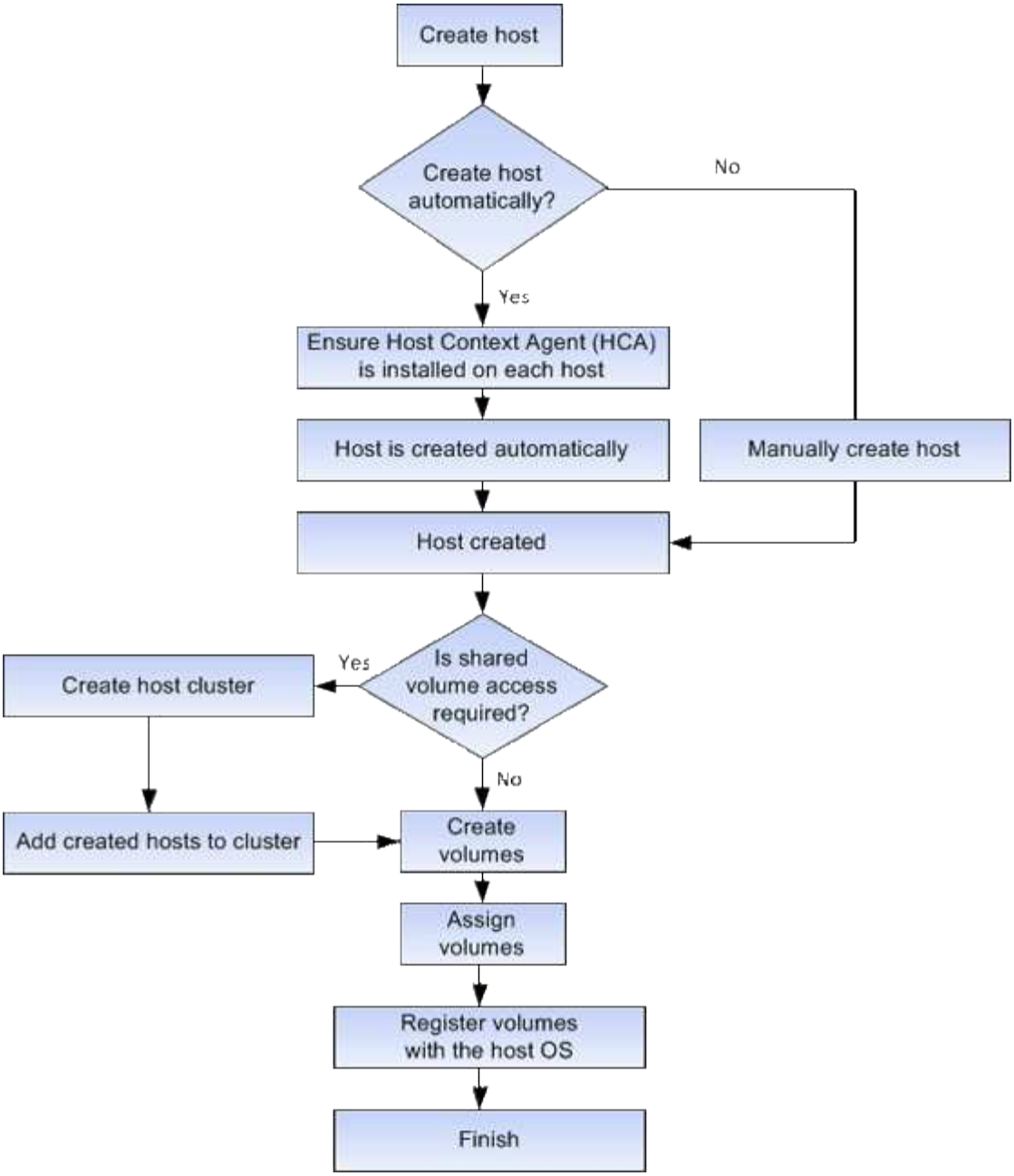
Scopri come si applicano i termini host al tuo storage array.

Componente	Definizione
Host	Un host è un server che invia i/o a un volume su un array di storage.
Nome host	Il nome host deve essere uguale al nome di sistema dell'host.
Cluster host	Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.
Protocollo di interfaccia host	Un protocollo di interfaccia host è la connessione (ad esempio Fibre Channel, iSCSI, ecc.) tra i controller e gli host.
HBA o scheda di interfaccia di rete (NIC)	Un HBA (host bus adapter) è una scheda che risiede in un host e contiene una o più porte host.
Porta host	Una porta host è una porta di un HBA (host Bus Adapter) che fornisce la connessione fisica a un controller e viene utilizzata per le operazioni di i/O.
Identificatore della porta host	Un identificatore di porta host è un nome univoco a livello mondiale associato a ciascuna porta host di un HBA (host Bus Adapter). • Gli identificatori delle porte host di Internet Small computer System Interface (iSCSI) devono contenere da 1 a 233 caratteri. Gli identificatori delle porte host iSCSI vengono visualizzati nel formato IQN standard (ad es. `iqn.xxx.com.xxx:8b3ad`). • Gli identificatori delle porte host non iSCSI, ad esempio Fibre Channel e SAS (Serial Attached SCSI), vengono visualizzati come delimitati dai due punti dopo ogni due caratteri (ad es. `xx:yy:zz`). Gli identificatori delle porte host Fibre Channel devono contenere 16 caratteri.

Componente	Definizione
Tipo di sistema operativo host	Il tipo di sistema operativo host è un'impostazione di configurazione che definisce il modo in cui i controller dell'array di storage reagiscono all'i/o a seconda del sistema operativo (o della variante) dell'host. In breve, questo tipo di host viene chiamato anche *host type*.
Porta host del controller	Una porta host del controller è una porta del controller che fornisce la connessione fisica a un host e viene utilizzata per le operazioni di i/O.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi.

Workflow per la creazione dell'host e l'assegnazione del volume

La figura seguente illustra come configurare l'accesso all'host.



Creazione automatica e manuale degli host

La creazione di un host è una delle operazioni necessarie per consentire all'array di storage di sapere quali host sono collegati e di consentire l'accesso i/o ai volumi. È possibile creare un host automaticamente o manualmente.

Creazione automatica

La creazione automatica dell'host per gli host basati su SCSI (non NVMe-of) viene avviata dall'HCA (host Context Agent). HCA è un'utility che è possibile installare su ciascun host collegato allo storage array. Ogni host su cui è installato l'HCA invia le informazioni di configurazione ai controller degli array di storage attraverso il percorso i/O. In base alle informazioni sull'host, i controller creano automaticamente l'host e le porte host associate e impostano il tipo di host. Se necessario, è possibile apportare ulteriori modifiche alla configurazione dell'host utilizzando System Manager.

Una volta che l'HCA ha eseguito il rilevamento automatico, l'host viene visualizzato automaticamente nella pagina host con i seguenti attributi:

- Il nome host derivato dal nome di sistema dell'host.
- Le porte di identificazione host associate all'host.
- Il tipo di sistema operativo host dell'host.

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

Creazione manuale

È possibile creare manualmente un host per uno dei seguenti motivi:

1. Si è scelto di non installare l'utility HCA sugli host.
2. Assicurarsi che gli identificatori della porta host rilevati dai controller degli array di storage siano associati correttamente agli host.

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

Modalità di assegnazione dei volumi agli host e ai cluster di host

Affinché un host o un cluster host invii i/o a un volume, è necessario assegnare il volume all'host o al cluster host.

È possibile selezionare un host o un cluster di host quando si crea un volume oppure assegnare un volume a un host o cluster di host in un secondo momento. Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.

L'assegnazione di volumi agli host è flessibile e consente di soddisfare le esigenze di storage specifiche.

- **Host standalone, non parte di un cluster di host** — è possibile assegnare un volume a un singolo host. È possibile accedere al volume solo da un host.
- **Cluster di host** — è possibile assegnare un volume a un cluster di host. Tutti gli host del cluster host possono accedere al volume.
- **Host all'interno di un cluster di host** — è possibile assegnare un volume a un singolo host che fa parte di un cluster di host. Anche se l'host fa parte di un cluster di host, è possibile accedere al volume solo dal singolo host e non da altri host del cluster di host.

Quando vengono creati i volumi, i LUN (Logical Unit Number) vengono assegnati automaticamente. Il LUN funge da "indirizzo" tra l'host e il controller durante le operazioni di i/O. Una volta creato il volume, è possibile modificare i LUN.

Volumi di accesso

Un volume di accesso è un volume configurato in fabbrica sull'array di storage utilizzato per la comunicazione con l'array di storage e l'host attraverso la connessione i/o dell'host. Il volume di accesso richiede un LUN (Logical Unit Number).

Il volume di accesso viene utilizzato in due istanze:

- **Automatic host Creation** — il volume di accesso viene utilizzato dall'utility host Context Agent (HCA) per inviare informazioni host (nome, porte, tipo di host) a System Manager per la creazione automatica dell'host.
- **Gestione in-band** — il volume di accesso viene utilizzato per una connessione in-band per gestire lo storage array. Questa operazione può essere eseguita solo se si gestisce lo storage array con l'interfaccia a riga di comando (CLI).

> La gestione in-band non è disponibile per i sistemi storage EF600 o EF300.

Un volume di accesso viene creato automaticamente la prima volta che si assegna un volume a un host. Ad esempio, se si assegnano Volume_1 e Volume_2 a un host, quando si visualizzano i risultati dell'assegnazione, vengono visualizzati tre volumi (Volume_1, Volume_2 e Access).

Se non si creano automaticamente host o non si gestisce un array di storage in-band con la CLI, non è necessario il volume di accesso ed è possibile liberare il LUN eliminando il volume di accesso. Questa azione rimuove l'assegnazione del volume al LUN e tutte le connessioni di gestione in-band all'host.

Numero massimo di LUN

Lo storage array dispone di un numero massimo di LUN (Logical Unit Number) che possono essere utilizzati per ciascun host.

Il numero massimo dipende dal sistema operativo dell'host. L'array di storage tiene traccia del numero di LUN utilizzati. Se si tenta di assegnare un volume a un host che supera il numero massimo di LUN, l'host non può accedere al volume.

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 VMware, Altri tre sistemi operativi Linux sono in esecuzione, è necessario selezionare Factory Default (predefinito) come tipo di sistema operativo host

predefinito.

Configurare l’accesso all’host

Crea host automaticamente

È possibile consentire all’HCA (host Context Agent) di rilevare automaticamente gli host, quindi verificare che le informazioni siano corrette. La creazione di un host è una delle operazioni necessarie per consentire all’array di storage di sapere quali host sono collegati e di consentire l’accesso i/o ai volumi.

Prima di iniziare

Assicurarsi che host Context Agent (HCA) sia installato e in esecuzione su ogni host connesso allo storage array. Gli host con HCA installato e connesso allo storage array vengono creati automaticamente. Per installare l’HCA, installare Gestione storage SANtricity sull’host e selezionare l’opzione host. HCA non è disponibile su tutti i sistemi operativi supportati. Se non è disponibile, è necessario creare l’host manualmente.

Fasi

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

   La tabella elenca gli host creati automaticamente.

2. Verificare che le informazioni fornite dall’HCA siano corrette (nome, tipo di host, identificatori della porta host).

   Per modificare le informazioni, selezionare l’host, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

3. **Opzionale:** se si desidera che l’host creato automaticamente sia in un cluster, creare un cluster host e aggiungere l’host o gli host.

Risultati

Una volta creato automaticamente un host, il sistema visualizza i seguenti elementi nella tabella degli host:

- Il nome host derivato dal nome di sistema dell’host.
- Le porte di identificazione host associate all’host.
- Il tipo di sistema operativo host dell’host.

Creare l’host manualmente

Per gli host che non possono essere rilevati automaticamente, è possibile creare manualmente un host. La creazione di un host è una delle operazioni necessarie per consentire all’array di storage di sapere quali host sono collegati e di consentire l’accesso i/o ai volumi.

A proposito di questa attività

Tenere presenti queste linee guida quando si crea un host:

- È necessario definire le porte di identificazione host associate all’host.
- Assicurarsi di fornire lo stesso nome del nome di sistema assegnato all’host.
- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Fare clic sul **Create › host** (Crea[host]).

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

3. Selezionare le impostazioni per l’host in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare il sistema operativo in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia host	(Facoltativo) se si dispone di più tipi di interfaccia host supportati sull'array di storage, selezionare il tipo di interfaccia host che si desidera utilizzare.
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare interfaccia i/o** In genere, le porte host devono essere state registrate ed essere disponibili dall'elenco a discesa. È possibile selezionare gli identificatori della porta host dall'elenco. • **Aggiunta manuale** Se nell'elenco non viene visualizzato un identificatore di porta host, significa che la porta host non ha effettuato l'accesso. È possibile utilizzare un'utility HBA o l'utility iSCSI Initiator per individuare gli identificatori delle porte host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dall'utility (uno alla volta) nel campo **host ports** (Porte host). È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori associati all'host. Ciascun identificatore viene visualizzato nel campo **host ports** (Porte host). Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto.

Impostazione	Descrizione
Iniziatore CHAP	(Facoltativo) se si seleziona o si immette manualmente una porta host con un IQN iSCSI e si desidera richiedere un host che tenta di accedere allo storage array per l'autenticazione mediante Challenge Handshake Authentication Protocol (CHAP), selezionare la casella di controllo **CHAP Initiator**. Per ogni porta host iSCSI selezionata o inserita manualmente, procedere come segue: • Immettere lo stesso segreto CHAP impostato su ciascun iniziatore host iSCSI per l'autenticazione CHAP. Se si utilizza l'autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di validarsi nell'array di storage e a un array di storage di validarsi nell'host), è necessario impostare anche il segreto CHAP per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lasciare vuoto il campo se non si richiede l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato da System Manager è CHAP.

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

Risultati

Una volta creato correttamente l'host, il sistema crea un nome predefinito per ciascuna porta host configurata per l'host (etichetta utente).

L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per `host IPT is IPT_1`.

Creare un cluster host

Si crea un cluster host quando due o più host richiedono l'accesso i/o agli stessi volumi.

A proposito di questa attività

Tenere presenti queste linee guida quando si crea un cluster host:

- Questa operazione non viene avviata a meno che non siano disponibili due o più host per la creazione del cluster.
- Gli host nei cluster di host possono avere sistemi operativi diversi (eterogenei).
- Gli host NVMe nei cluster di host non possono essere misti con host non NVMe.
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.

  Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare **Create › host Cluster** (Crea[cluster host]).

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

3. Selezionare le impostazioni appropriate per il cluster host.

   Dettagli del campo

Impostazione	Descrizione
Nome	Digitare il nome del nuovo cluster host.
Selezionare gli host per condividere l'accesso al volume	Selezionare due o più host dall'elenco a discesa. Vengono visualizzati nell'elenco solo gli host che non fanno già parte di un cluster di host.

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

   Se gli host selezionati sono collegati a tipi di interfaccia che hanno diverse funzionalità di Data Assurance (da), viene visualizzata una finestra di dialogo con il messaggio che da non sarà disponibile sul cluster host. Questa non disponibilità impedisce l'aggiunta di volumi abilitati da al cluster host. Selezionare **Sì** per continuare o **No** per annullare.

   DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente all'array di storage di verificare la presenza di errori che potrebbero verificarsi quando i dati vengono spostati tra gli host e i dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Risultati

Il nuovo cluster di host viene visualizzato nella tabella con gli host assegnati nelle righe sottostanti.

Assegnare volumi agli host

È necessario assegnare un volume a un host o a un cluster di host in modo che possa essere utilizzato per le operazioni di i/O. Questa assegnazione consente a un host o a un cluster host di accedere a uno o più volumi in un array di storage.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano volumi agli host:

- È possibile assegnare un volume a un solo host o cluster di host alla volta.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un LUN univoco.
- Per i nuovi gruppi di volumi, se si attende la creazione e l'inizializzazione di tutti i volumi prima di assegnarli a un host, il tempo di inizializzazione del volume viene ridotto. Tenere presente che una volta mappato un volume associato al gruppo di volumi, *tutti* i volumi torneranno all'inizializzazione più lenta. È possibile

controllare l'avanzamento dell'inizializzazione dal **Home › operazioni in corso**.

L'assegnazione di un volume non riesce nelle seguenti condizioni:

- Vengono assegnati tutti i volumi.
- Il volume è già assegnato a un altro host o cluster di host.

La possibilità di assegnare un volume non è disponibile nelle seguenti condizioni:

- Non esistono host o cluster di host validi.
- Non sono stati definiti identificatori di porta host per l'host.
- Sono state definite tutte le assegnazioni dei volumi.

Durante questa attività vengono visualizzati tutti i volumi non assegnati, ma le funzioni per gli host con o senza Data Assurance (da) si applicano come segue:

- Per un host da-capable, è possibile selezionare i volumi che sono da-enabled o non da-enabled.
- Per un host che non supporta da, se si seleziona un volume abilitato da, viene visualizzato un avviso che indica che il sistema deve disattivare automaticamente da sul volume prima di assegnarlo all'host.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare l'host o il cluster host a cui si desidera assegnare i volumi, quindi fare clic su **Assign Volumes** (Assegna volumi).

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

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

Risultati

Dopo aver assegnato correttamente uno o più volumi a un host o a un cluster di host, il sistema esegue le seguenti operazioni:

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

Gestire host e cluster

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 VMware, 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**.

Annullare l'assegnazione dei volumi

Annullare l'assegnazione dei volumi dagli host o dai cluster di host se non è più necessario l'accesso i/o a tale volume dall'host o dal cluster di host.

A proposito di questa attività

Tenere presenti queste linee guida quando si annulla l'assegnazione di un volume:

- Se si rimuove l'ultimo volume assegnato da un cluster host e il cluster host dispone anche di host con volumi assegnati specifici, assicurarsi di rimuovere o spostare tali assegnazioni prima di rimuovere l'ultima assegnazione per il cluster host.
- Se un cluster host, un host o una porta host viene assegnata a un volume registrato nel sistema operativo, è necessario annullare la registrazione prima di poter rimuovere questi nodi.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare l'host o il cluster host che si desidera modificare, quindi fare clic su **Annulla assegnazione volumi**.

   Viene visualizzata una finestra di dialogo che mostra tutti i volumi attualmente assegnati.

3. Selezionare la casella di controllo accanto a ciascun volume che si desidera annullare l'assegnazione

oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.

4. Fare clic su **Annulla assegnazione**.

Risultati

- I volumi non assegnati sono disponibili per una nuova assegnazione.
- Fino a quando le modifiche non vengono configurate sull'host, il volume viene ancora riconosciuto dal sistema operativo host.

Eliminare l'host o il cluster host

È possibile eliminare un host o un cluster di host.

A proposito di questa attività

Tenere presenti queste linee guida quando si elimina un host o un cluster host:

- Tutte le assegnazioni di volume specifiche vengono eliminate e i volumi associati sono disponibili per una nuova assegnazione.
- Se l'host fa parte di un cluster host che dispone di assegnazioni specifiche, il cluster host non viene influenzato. Tuttavia, se l'host fa parte di un cluster di host che non ha altre assegnazioni, il cluster di host e qualsiasi altro host o identificativo di porta host associato ereditano eventuali assegnazioni predefinite.
- Tutti gli identificatori di porta host associati all'host diventano indefiniti.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare l'host o il cluster host che si desidera eliminare, quindi fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo di conferma.

3. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Se si elimina un host, il sistema esegue le seguenti operazioni:

- Elimina l'host e, se applicabile, lo rimuove dal cluster host.
- Rimuove l'accesso a tutti i volumi assegnati.
- Riporta i volumi associati a uno stato non assegnato.
- Restituisce gli identificatori di porta host associati all'host a uno stato non associato.

Se si elimina un cluster host, il sistema esegue le seguenti operazioni:

- Elimina il cluster host e gli host associati (se presenti).
- Rimuove l'accesso a tutti i volumi assegnati.
- Riporta i volumi associati a uno stato non assegnato.
- Restituisce gli identificatori di porta host associati agli host a uno stato non associato.

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.

Gestire le impostazioni

Modificare le impostazioni di un host

È possibile modificare il nome, il tipo di sistema operativo host e i cluster host associati per un host.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare l'host che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti dell'host.

3. Se non è già selezionata, fare clic sulla scheda **Proprietà**.
4. Modificare le impostazioni in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome dell'host fornito dall'utente. Specificare un nome per l'host.
Cluster host associato	È possibile scegliere una delle seguenti opzioni: • **None** — l'host rimane un host standalone. Se l'host è stato associato a un cluster host, il sistema rimuove l'host dal cluster. • **<Host Cluster>** — il sistema associa l'host al cluster selezionato.
Tipo di sistema operativo host	È possibile modificare il tipo di sistema operativo in esecuzione sull'host definito.

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

Modificare le impostazioni di un cluster host

È possibile modificare il nome del cluster host oppure aggiungere o rimuovere host in un cluster host.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare il cluster host che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti del cluster host.

3. Modificare le impostazioni del cluster host in base alle esigenze.

   Dettagli del campo

Impostazione	Descrizione
Nome	È possibile specificare il nome fornito dall'utente del cluster host. Specificare un nome per un cluster.
Host associati	Per aggiungere un host, fare clic sulla casella **Associated Hosts** (host associati), quindi selezionare un nome host dall'elenco a discesa. Non è possibile inserire manualmente un nome host. Per eliminare un host, fare clic sulla * X* accanto al nome host.

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

Modificare gli identificatori delle porte host per un host

Modificare gli identificatori della porta host quando si desidera modificare l'etichetta utente su un identificatore della porta host, aggiungere un nuovo identificatore della porta host all'host o eliminare un identificatore della porta host dall'host.

A proposito di questa attività

Quando si modificano gli identificatori delle porte host, tenere presenti le seguenti linee guida:

- **Add** — quando si aggiunge una porta host, si associa l'identificatore della porta host all'host creato per connettersi allo storage array. È possibile inserire manualmente le informazioni sulla porta utilizzando un'utility HBA (host bus adapter).
- **Edit** — è possibile modificare le porte host per spostare (associare) una porta host a un host diverso. È possibile che l'host bus adapter o l'iSCSI Initiator siano stati spostati in un host diverso, quindi è necessario spostare (associare) la porta host nel nuovo host.
- **Delete** — è possibile eliminare le porte host per rimuovere (disassociare) le porte host da un host.

Fasi

1. Selezionare **Storage › Hosts** (Storage[host]).
2. Selezionare l'host a cui associare le porte, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Se si desidera aggiungere porte a un host in un cluster di host, espandere il cluster di host e selezionare l'host desiderato. Non è possibile aggiungere porte a livello di cluster host.

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti dell'host.

3. Fare clic sulla scheda **host Ports** (Porte host).

   La finestra di dialogo mostra gli identificatori di porta host correnti.

4. Modificare le impostazioni dell'identificatore della porta host in base alle esigenze.

Impostazione	Descrizione
Porta host	È possibile scegliere una delle seguenti opzioni: • **Add** — utilizzare Add per associare un nuovo identificatore di porta host all'host. La lunghezza del nome dell'identificatore della porta host è determinata dalla tecnologia dell'interfaccia host. I nomi degli identificatori delle porte host Fibre Channel e Infiniband devono contenere 16 caratteri. I nomi degli identificatori delle porte host iSCSI hanno un massimo di 223 caratteri. La porta deve essere univoca. Un numero di porta già configurato non è consentito. • **Delete** — utilizzare Delete per rimuovere (disassociare) un identificatore di porta host. L'opzione Delete (Elimina) non rimuove fisicamente la porta host. Questa opzione rimuove l'associazione tra la porta host e l'host. A meno che non si rimuovano host bus adapter o iSCSI Initiator, la porta host viene ancora riconosciuta dal controller. Se si elimina un identificatore di porta host, questo non viene più associato a questo host. Inoltre, l'host perde l'accesso a uno qualsiasi dei volumi assegnati tramite questo identificatore di porta host.
Etichetta	Per modificare il nome dell'etichetta della porta, fare clic sull'icona **Modifica** (matita). Il nome dell'etichetta della porta deve essere univoco. Un nome di etichetta già configurato non è consentito.
Segreto CHAP	Viene visualizzato solo per gli host iSCSI. È possibile impostare o modificare il segreto CHAP per gli iniziatori (host iSCSI). 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 chiamata CHAP secret (segreto CHAP).

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

FAQ

Cosa sono gli host e i cluster di host?

Un host è un server che invia i/o a un volume su un array di storage. Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.

Si definisce un host separatamente. Può essere un'entità indipendente o essere aggiunta a un cluster host. È possibile assegnare volumi a un singolo host oppure un host può far parte di un cluster di host che condivide l'accesso a uno o più volumi con altri host del cluster di host.

Il cluster host è un'entità logica creata in Gestore di sistema di SANtricity. Prima di poter assegnare i volumi, è necessario aggiungere gli host al cluster host.

Perché dovrei creare un cluster host?

È necessario creare un cluster host se si desidera che due o più host condividano l'accesso allo stesso set di volumi. In genere, i singoli host dispongono di un software di clustering installato su di essi per coordinare l'accesso ai volumi.

Come si fa a sapere quale tipo di sistema operativo host è corretto?

Il campo host Operating System Type (tipo di sistema operativo host) contiene il sistema operativo dell'host. È possibile selezionare il tipo di host consigliato dall'elenco a discesa o consentire all'HCA (host Context Agent) di configurare l'host e il tipo di sistema operativo appropriato.

I tipi di host visualizzati nell'elenco a discesa dipendono dal modello di array di storage e dalla versione del firmware. Le versioni più recenti visualizzano prima le opzioni più comuni, che sono le più probabili. L'aspetto in questo elenco non implica che l'opzione sia completamente supportata.

> Per ulteriori informazioni sul supporto degli host, fare riferimento a. "Tool di matrice di interoperabilità NetApp".

Alcuni dei seguenti tipi di host potrebbero essere visualizzati nell'elenco:

Tipo di sistema operativo host	Sistema operativo e driver multipath
Linux DM-MP (kernel 3.10 o successivo)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.10 o successivo.
VMware ESXi	Supporta i sistemi operativi VMware ESXi che eseguono l'architettura NMP (Native Multipathing Plug-in) utilizzando il modulo SATP_ALUA Storage Array Type Policy integrato da VMware.
Windows (in cluster o non in cluster)	Supporta configurazioni in cluster o non in cluster di Windows che non eseguono il driver di multipathing atto.
ATTO Cluster (tutti i sistemi operativi)	Supporta tutte le configurazioni del cluster utilizzando il driver multipathing della tecnologia atto, Inc.
Linux (Veritas DMP)	Supporta i sistemi operativi Linux che utilizzano una soluzione multipathing Veritas DMP.
Linux (atto)	Supporta i sistemi operativi Linux che utilizzano un driver multipathing per la tecnologia atto, Inc.
Mac OS (atto)	Supporta le versioni di Mac OS che utilizzano un driver multipathing per la tecnologia atto, Inc.
Windows (atto)	Supporta i sistemi operativi Windows che utilizzano un driver multipathing per la tecnologia atto, Inc.

Tipo di sistema operativo host	Sistema operativo e driver multipath
FlexArray (ALUA)	Supporta un sistema NetApp FlexArray che utilizza ALUA per il multipathing.
SVC IBM	Supporta una configurazione IBM SAN Volume Controller.
Impostazione predefinita di fabbrica	Riservato all'avvio iniziale dello storage array. Se il tipo di sistema operativo host in uso è impostato su Factory Default, modificarlo in modo che corrisponda al sistema operativo host e al driver multipath in esecuzione sull'host connesso.
Linux DM-MP (kernel 3.9 o precedente)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.9 o precedente.
Cluster di finestre (obsoleto)	Se il tipo di sistema operativo host è impostato su questo valore, utilizzare l'impostazione Windows (in cluster o non in cluster).

Una volta installato l'HCA e collegato lo storage all'host, l'HCA invia la topologia host ai controller di storage attraverso il percorso i/O. In base alla topologia dell'host, i controller di storage definiscono automaticamente l'host e le porte host associate, quindi impostano il tipo di host.

> Se l'HCA non seleziona il tipo di host consigliato, è necessario impostare manualmente il tipo di host.

Cosa sono gli HBA e le porte dell'adattatore?

Un HBA (host bus adapter) è una scheda che risiede in un host e contiene una o più porte host. Una porta host è una porta di un HBA (host Bus Adapter) che fornisce la connessione fisica a un controller e viene utilizzata per le operazioni di i/O.

Le porte dell'adattatore sull'HBA sono denominate porte host. La maggior parte degli HBA dispone di una o due porte host. L'HBA dispone di un WWID (World Wide Identifier) univoco e ogni porta host HBA dispone di un WWID univoco. Gli identificatori delle porte host vengono utilizzati per associare l'HBA appropriato all'host fisico quando si crea manualmente l'host tramite Gestore di sistema SANtricity o si crea automaticamente l'host utilizzando l'agente di contesto host.

Come faccio ad associare le porte host a un host?

Se si crea manualmente un host, è necessario utilizzare l'utility HBA (host bus adapter) appropriata disponibile sull'host per determinare gli identificatori di porta host associati a ciascun HBA installato nell'host.

Quando si dispone di queste informazioni, selezionare gli identificatori di porta host che hanno effettuato l'accesso allo storage array dall'elenco fornito nella finestra di dialogo Create host (Crea host).

> Assicurarsi di selezionare gli identificatori di porta host appropriati per l'host che si sta creando. Se si associano identificatori di porta host errati, potrebbe verificarsi un accesso non intenzionale da un altro host a questi dati.

Se si creano automaticamente host utilizzando l'HCA (host Context Agent) installato su ciascun host, l'HCA deve associare automaticamente gli identificatori di porta host a ciascun host e configurarli in modo appropriato.

Come si creano i segreti CHAP?

Se si imposta l'autenticazione CHAP (Challenge Handshake Authentication Protocol) su qualsiasi host iSCSI connesso allo storage array, è necessario immettere nuovamente il segreto CHAP dell'iniziatore per ciascun host iSCSI.

A tale scopo, è possibile utilizzare System Manager come parte dell'operazione Create host o tramite l'opzione View/Edit Settings (Visualizza/Modifica impostazioni).

Se si utilizza l'autenticazione reciproca CHAP, è necessario definire anche un segreto CHAP di destinazione per l'array di storage nella pagina Settings (Impostazioni) e immettere di nuovo il segreto CHAP di destinazione su ciascun host iSCSI.

Qual è il cluster predefinito?

Il cluster predefinito è un'entità definita dal sistema che consente a qualsiasi identificatore di porta host non associato che abbia eseguito l'accesso all'array di storage di accedere ai volumi assegnati al cluster predefinito. Un identificatore di porta host non associato è una porta host che non è logicamente associata a un particolare host, ma che è fisicamente installata in un host e collegata all'array di storage.

> Se si desidera che gli host abbiano accesso specifico a determinati volumi nell'array di storage, è necessario *non* utilizzare il cluster predefinito. È invece necessario associare gli identificatori delle porte host ai rispettivi host. Questa attività può essere eseguita manualmente durante l'operazione Create host (Crea host) o automaticamente utilizzando l'HCA (host Context Agent) installato su ciascun host. Quindi, assegnare i volumi a un singolo host o a un cluster host.

È necessario *solo* utilizzare il cluster predefinito in situazioni speciali in cui l'ambiente di storage esterno favorisce l'accesso a tutti gli host e a tutti gli identificatori di porta host connessi allo storage array a tutti i volumi (modalità all-access) senza rendere specifici gli host noti allo storage array o all'interfaccia utente.

Inizialmente, è possibile assegnare i volumi solo al cluster predefinito tramite l'interfaccia della riga di comando (CLI). Tuttavia, dopo aver assegnato almeno un volume al cluster predefinito, questa entità (chiamata cluster predefinito) viene visualizzata nell'interfaccia utente, dove è possibile gestire questa entità.

Che cos'è il 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.

Snapshot

Panoramica delle istantanee

La funzione Snapshot consente di creare immagini point-in-time dei volumi di array di storage da utilizzare per il backup o il test.

Cosa sono le immagini Snapshot?

Una *immagine snapshot* è una copia logica dei dati del volume, acquisita in un determinato momento. Come un punto di ripristino, le immagini Snapshot consentono di eseguire il rollback a un set di dati sicuramente funzionante. Sebbene l'host possa accedere all'immagine snapshot, non può leggerla o scriverla direttamente.

Scopri di più:

- "Come funziona lo storage Snapshot"
- "Terminologia Snapshot"
- "Volumi di base, capacità riservata e gruppi di snapshot"
- "Pianificazioni di Snapshot e gruppi di coerenza"
- "Volumi Snapshot"

Come si creano le istantanee?

È possibile creare manualmente un'immagine snapshot da un volume di base o da un gruppo di coerenza snapshot. Questa procedura è disponibile dal **Storage › Snapshot**.

Scopri di più:

- "Requisiti e linee guida per le snapshot"
- "Workflow per la creazione di immagini e volumi snapshot"
- "Creare un'immagine istantanea"
- "Programmare le immagini snapshot"
- "Creare un gruppo di coerenza snapshot"
- "Creare un volume di snapshot"

Come faccio a eseguire il rollback dei dati da uno snapshot?

Un *rollback* è il processo che consente di riportare i dati di un volume di base a un punto temporale precedente. È possibile eseguire il rollback dei dati snapshot dal **Storage › Snapshot**.

Scopri di più:

- "Rollback di Snapshot"
- "Avviare il rollback di un'immagine snapshot per un volume di base"
- "Avviare un rollback dell'immagine snapshot per un membro del gruppo di coerenza"

Informazioni correlate

Scopri di più sulle attività correlate alle snapshot:

- "Modificare la capacità riservata per un volume di snapshot"
- "Modificare la capacità riservata per un gruppo di snapshot"

Concetti

Come funziona lo storage Snapshot

La funzione Snapshot utilizza la tecnologia copy-on-write per memorizzare le immagini snapshot e utilizzare la capacità riservata allocata.

Modalità di utilizzo delle immagini Snapshot

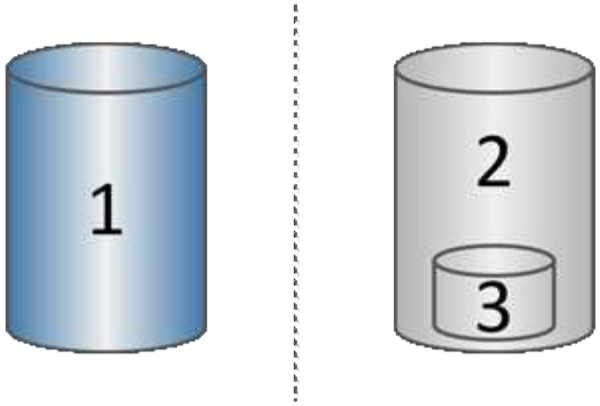
Un'immagine snapshot è una copia logica di sola lettura del contenuto del volume, acquisita in un determinato momento. È possibile utilizzare le snapshot per proteggersi dalla perdita di dati.

Le immagini Snapshot sono utili anche per gli ambienti di test. Creando una copia virtuale dei dati, è possibile eseguire il test dei dati utilizzando lo snapshot senza alterare il volume effettivo. Inoltre, gli host non dispongono dell'accesso in scrittura alle immagini snapshot, pertanto le snapshot sono sempre una risorsa di backup sicura.

Creazione di snapshot

Man mano che vengono create le snapshot, la funzione Snapshot memorizza i dati delle immagini come segue:

- Quando viene creata un'immagine snapshot, questa corrisponde esattamente al volume di base. La funzione Snapshot utilizza la tecnologia copy-on-write. Una volta eseguita la snapshot, la prima scrittura su qualsiasi blocco o gruppo di blocchi sul volume di base causa la copia dei dati originali nella capacità riservata prima di scrivere i nuovi dati nel volume di base.
- Le snapshot successive includono solo blocchi di dati modificati. Prima che i dati vengano sovrascritti sul volume di base, la funzione Snapshot utilizza la tecnologia copy-on-write per salvare le immagini richieste dei settori interessati nella capacità riservata di snapshot.



[1] Volume di base (capacità del disco fisico); [2] Snapshot (capacità del disco logico); [3] capacità riservata (capacità del disco fisico)

- La capacità riservata memorizza i blocchi di dati originali per le parti del volume di base che sono state modificate dopo l'esecuzione dello snapshot e include un indice per il tracciamento delle modifiche. In genere, la dimensione della capacità riservata corrisponde per impostazione predefinita al 40% del volume di base. (Se hai bisogno di una maggiore capacità riservata, puoi aumentare la capacità riservata).
- Le immagini Snapshot vengono memorizzate in un ordine specifico, in base alla data e all'ora. Solo l'immagine snapshot meno recente di un volume base è disponibile per l'eliminazione manuale.

Ripristino dello snapshot

Per ripristinare i dati in un volume di base, è possibile utilizzare un volume snapshot o un'immagine snapshot:

- **Volume Snapshot** — se è necessario recuperare i file cancellati, creare un volume di snapshot da un'immagine snapshot sicuramente funzionante e assegnarlo all'host.
- **Immagine Snapshot** — se è necessario ripristinare un volume di base a uno specifico punto in tempo, utilizzare un'immagine snapshot precedente per eseguire il rollback dei dati nel volume di base.

Terminologia Snapshot

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

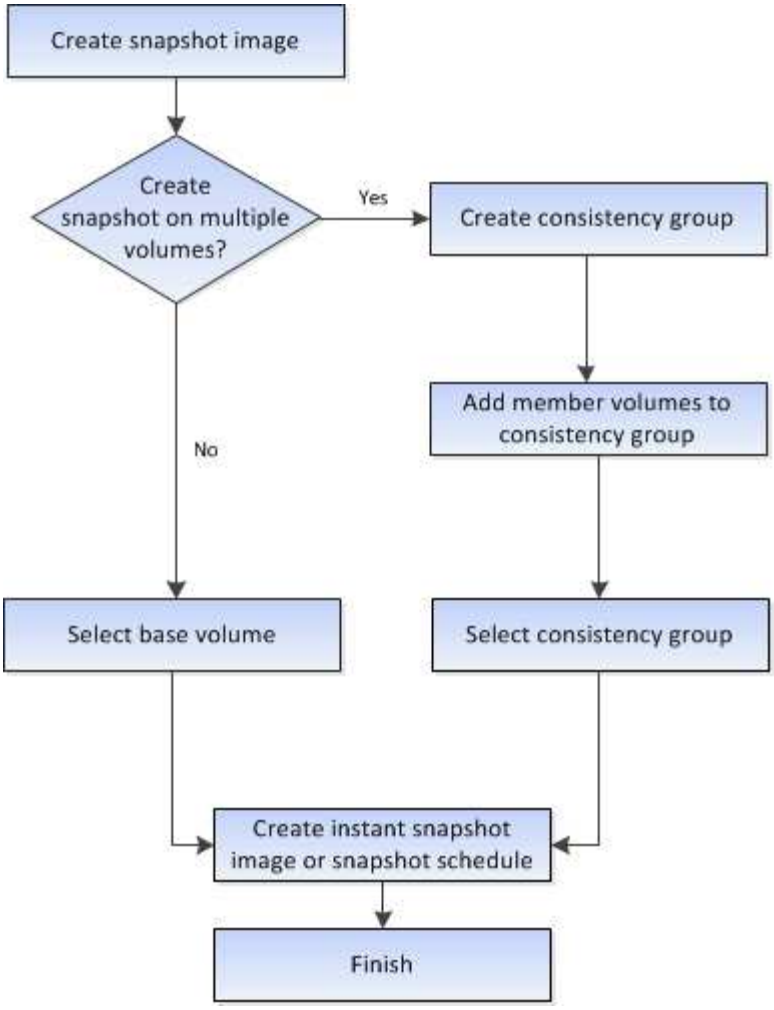
Termine	Descrizione
Funzione Snapshot	La funzione Snapshot consente di creare e gestire le immagini dei volumi.
Immagine Snapshot	Un'immagine snapshot è una copia logica dei dati del volume, acquisita in un determinato momento. Come un punto di ripristino, le immagini Snapshot consentono di eseguire il rollback a un set di dati sicuramente funzionante. Sebbene l'host possa accedere all'immagine snapshot, non può leggerla o scriverla direttamente.
Volume di base	Un volume di base è l'origine da cui viene creata un'immagine snapshot. Può essere un volume spesso o sottile e viene in genere assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un pool di dischi.

Termine	Descrizione
Volume Snapshot	Un volume di snapshot consente all'host di accedere ai dati nell'immagine di snapshot. Il volume Snapshot contiene la propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine snapshot originale.
Gruppo di snapshot	Un gruppo di snapshot è una raccolta di immagini snapshot da un singolo volume di base.
Volume di capacità riservato	Un volume a capacità riservata tiene traccia dei blocchi di dati del volume di base sovrascritti e del contenuto preservato di tali blocchi.
Calendario di Snapshot	Un programma di snapshot è un calendario per la creazione automatica di immagini snapshot. Attraverso il programma, è possibile controllare la frequenza delle creazioni di immagini.
Gruppo di coerenza Snapshot	Un gruppo di coerenza snapshot è un insieme di volumi che vengono trattati come una singola entità quando viene creata un'immagine snapshot. Ciascuno di questi volumi dispone di una propria immagine snapshot, ma tutte le immagini vengono create nello stesso momento.
Volume membro del gruppo di coerenza Snapshot	Ciascun volume appartenente a un gruppo di coerenza snapshot viene definito volume membro. Quando si aggiunge un volume a un gruppo di coerenza snapshot, System Manager crea automaticamente un nuovo gruppo di snapshot che corrisponde a questo volume membro.
Eseguire il rollback	Un rollback è il processo di restituzione dei dati in un volume di base a un punto precedente.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.

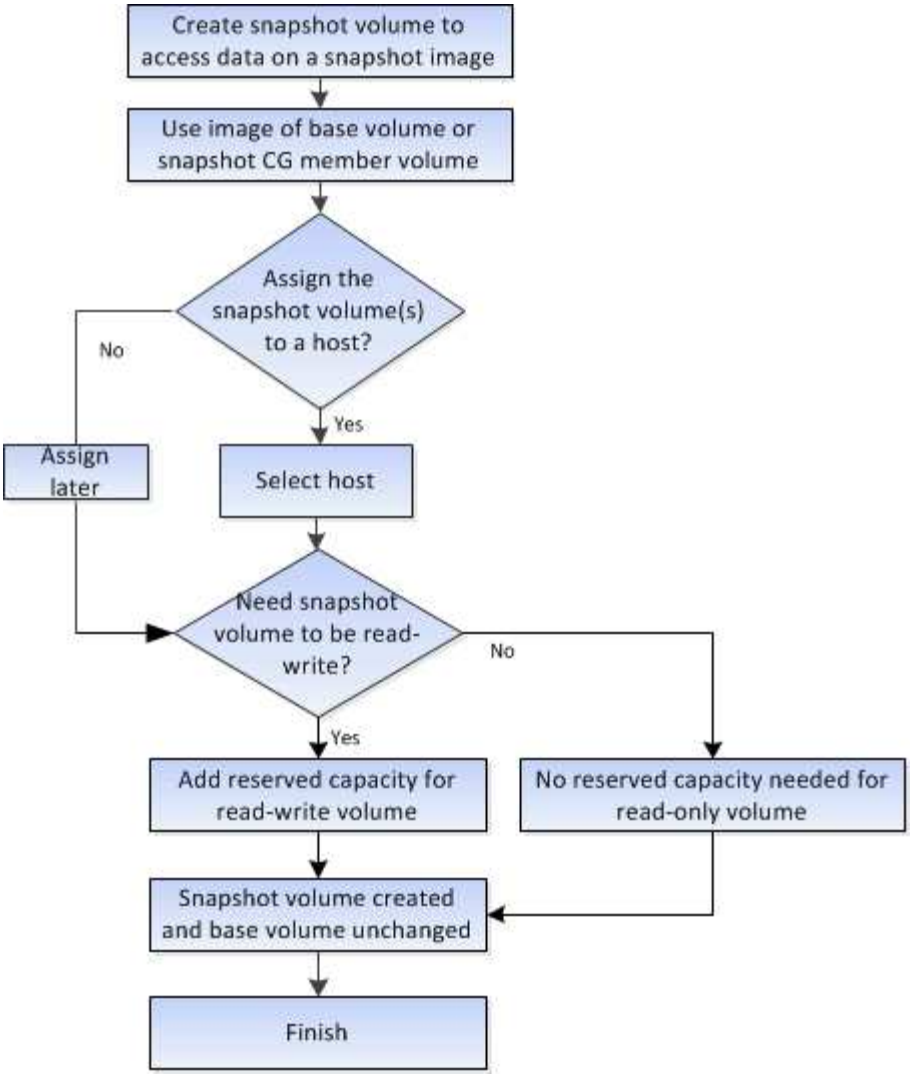
Workflow per la creazione di immagini snapshot e volumi di snapshot

In System Manager, è possibile creare immagini snapshot e volumi snapshot seguendo questa procedura.

Workflow per la creazione di immagini snapshot



Workflow per la creazione di volumi di snapshot



Requisiti e linee guida per le snapshot

Quando si creano e si utilizzano snapshot, consultare i seguenti requisiti e linee guida.

Immagini Snapshot e gruppi di snapshot

- Ogni immagine snapshot è associata esattamente a un gruppo di snapshot.
- Un gruppo di snapshot viene creato la prima volta che si crea un'immagine snapshot pianificata o istantanea per un oggetto associato. In questo modo si crea capacità riservata.

  È possibile visualizzare i gruppi di snapshot dalla pagina Pools & Volume Groups.

- Le immagini snapshot pianificate non si verificano quando lo storage array è offline o spento.
- Se si elimina un gruppo di snapshot con una pianificazione di snapshot, viene eliminata anche la pianificazione di snapshot.
- Se si dispone di un volume snapshot non più necessario, è possibile riutilizzarlo, insieme a qualsiasi capacità riservata associata, invece di eliminarlo. In questo modo viene creato un volume di snapshot diverso dello stesso volume di base. È possibile riassociare il volume di snapshot o il volume di snapshot del gruppo di coerenza di snapshot con la stessa immagine di snapshot o un'immagine di snapshot diversa, purché l'immagine di snapshot si trovi nello stesso volume di base.

Gruppo di coerenza Snapshot

- Un gruppo di coerenza di snapshot contiene un gruppo di snapshot per ogni volume membro del gruppo di coerenza di snapshot.
- È possibile associare un gruppo di coerenza snapshot a un solo programma.
- Se si elimina un gruppo di coerenza snapshot con una pianificazione snapshot, viene eliminata anche la pianificazione snapshot.
- Non è possibile gestire singolarmente un gruppo di snapshot associato a un gruppo di coerenza di snapshot. È invece necessario eseguire le operazioni di gestione (creazione di un'immagine snapshot, eliminazione di un'immagine snapshot o di un gruppo di snapshot e rollback dell'immagine snapshot) a livello di gruppo di coerenza snapshot.

Volume di base

- Un volume Snapshot deve avere le stesse impostazioni di sicurezza e Data Assurance (da) del volume di base associato.
- Non è possibile creare un volume di snapshot di un volume di base guasto.
- Se il volume di base risiede in un gruppo di volumi, i volumi membri di qualsiasi gruppo di coerenza snapshot associato possono risiedere in un pool o in un gruppo di volumi.
- Se un volume di base risiede in un pool, tutti i volumi membri di qualsiasi gruppo di coerenza snapshot associato devono risiedere nello stesso pool del volume di base.

Capacità riservata

- La capacità riservata è associata a un solo volume di base.
- L'utilizzo di una pianificazione può causare un gran numero di immagini snapshot. Assicurarsi di disporre di una capacità riservata sufficiente per gli snapshot pianificati.
- Il volume di capacità riservata per un gruppo di coerenza snapshot deve avere le stesse impostazioni di sicurezza e Data Assurance (da) del volume di base associato per il volume membro del gruppo di coerenza snapshot.

Immagini snapshot in sospeso

La creazione di un'immagine Snapshot potrebbe rimanere in sospeso nelle seguenti condizioni:

- Il volume di base che contiene questa immagine snapshot è membro di un gruppo di mirror asincrono.
- Il volume di base è attualmente in fase di sincronizzazione. La creazione dell'immagine snapshot viene completata non appena l'operazione di sincronizzazione viene completata.

Numero massimo di immagini snapshot

- Se un volume è membro di un gruppo di coerenza snapshot, System Manager crea un gruppo di snapshot per quel volume membro. Questo gruppo di snapshot conta per il numero massimo consentito di gruppi di snapshot per volume di base.
- Se si tenta di creare un'immagine snapshot su un gruppo di snapshot o un gruppo di coerenza snapshot, ma il gruppo associato ha raggiunto il numero massimo di immagini snapshot, sono disponibili due opzioni:
  - Abilitare l'eliminazione automatica per il gruppo di snapshot o il gruppo di coerenza di snapshot.
  - Eliminare manualmente una o più immagini di snapshot dal gruppo di snapshot o dal gruppo di coerenza di snapshot e riprovare l'operazione.

Eliminazione automatica

Se il gruppo di snapshot o il gruppo di coerenza snapshot è abilitato per l'eliminazione automatica, System Manager elimina l'immagine snapshot meno recente quando il sistema ne crea una nuova per il gruppo.

Operazione di rollback

- Non è possibile eseguire le seguenti azioni quando è in corso un'operazione di rollback:
  - Eliminare l'immagine snapshot utilizzata per il rollback.
  - Creare una nuova immagine snapshot per un volume di base che partecipa a un'operazione di rollback.
  - Modificare la policy Repository-Full del gruppo di snapshot associato.
- Non è possibile avviare un'operazione di rollback quando è in corso una di queste operazioni:
  - Espansione della capacità (aggiunta di capacità a un pool o a un gruppo di volumi)
  - Espansione dei volumi (aumento della capacità di un volume)
  - Modifica del livello RAID per un gruppo di volumi
  - Modifica delle dimensioni dei segmenti per un volume
- Non è possibile avviare un'operazione di rollback se il volume di base partecipa a una copia del volume.
- Non è possibile avviare un'operazione di rollback se il volume base è un volume secondario in un mirror remoto.
- Un'operazione di rollback non riesce se una delle capacità utilizzate nel volume di repository snapshot associato presenta settori illeggibili.

Volumi di base, capacità riservata e gruppi di snapshot

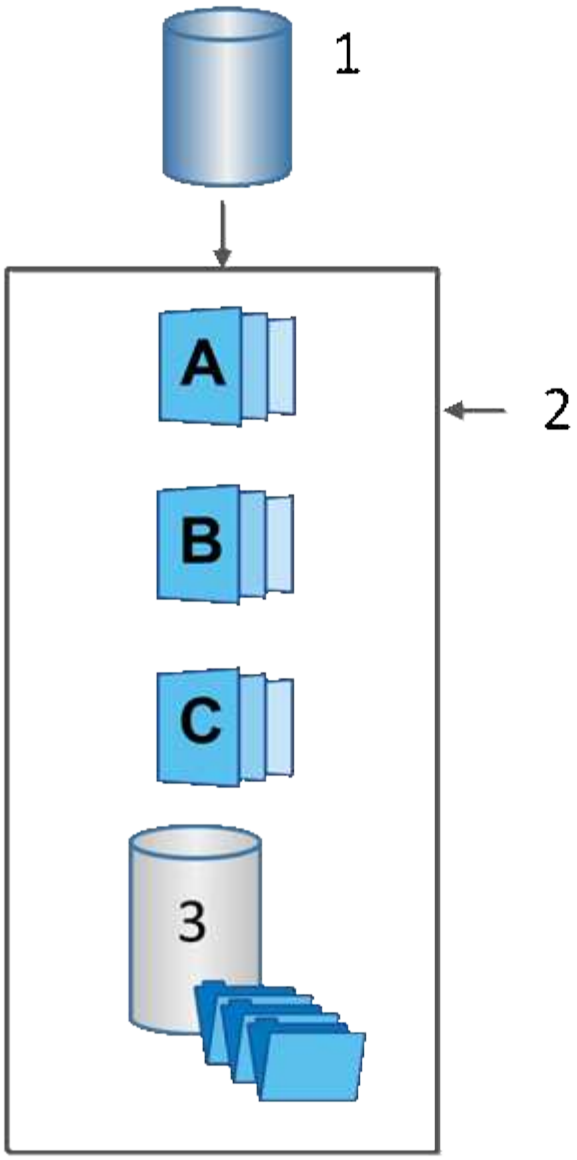
La funzione Snapshot utilizza volumi di base, capacità riservata e gruppi di snapshot.

Volumi di base

Un *volume base* è il volume utilizzato come origine per un'immagine snapshot. Un volume di base può essere un volume spesso o un volume sottile e può risiedere in un pool o in un gruppo di volumi.

Per creare snapshot del volume di base, è possibile creare un'immagine istantanea in qualsiasi momento oppure automatizzare il processo definendo una pianificazione regolare per gli snapshot.

La figura seguente mostra la relazione tra gli oggetti snapshot e il volume di base.



[1] Volume di base; [2] oggetti Snapshot nel gruppo (immagini e capacità riservata); [3] capacità riservata per il gruppo di snapshot.

Capacità riservata e gruppi di snapshot

System Manager organizza le immagini snapshot in *gruppi di snapshot*. Quando System Manager stabilisce il gruppo di snapshot, crea automaticamente la *capacità riservata* associata per conservare le immagini snapshot per il gruppo e tenere traccia delle modifiche successive apportate agli snapshot aggiuntivi.

Se il volume di base risiede in un gruppo di volumi, la capacità riservata può trovarsi in un pool o in un gruppo di volumi. Se il volume di base risiede in un pool, la capacità riservata deve trovarsi nello stesso pool del volume di base.

I gruppi di snapshot non richiedono alcuna azione da parte dell'utente, ma è possibile regolare la capacità riservata di un gruppo di snapshot in qualsiasi momento. Inoltre, potrebbe essere richiesto di creare capacità riservata quando vengono soddisfatte le seguenti condizioni:

- Ogni volta che si crea uno snapshot di un volume di base che non dispone ancora di un gruppo di

snapshot, System Manager crea automaticamente un gruppo di snapshot. Questa azione crea inoltre capacità riservata per il volume di base utilizzato per memorizzare le immagini snapshot successive.

- Ogni volta che si crea una pianificazione di snapshot per un volume di base, System Manager crea automaticamente un gruppo di snapshot.

Eliminazione automatica

Quando si lavora con gli snapshot, utilizzare l'opzione predefinita per attivare l'eliminazione automatica. L'eliminazione automatica elimina automaticamente l'immagine snapshot meno recente quando il gruppo di snapshot raggiunge il limite di 32 immagini. Se si disattiva l'eliminazione automatica, i limiti del gruppo di snapshot vengono superati e si devono eseguire azioni manuali per configurare le impostazioni del gruppo di snapshot e gestire la capacità riservata.

Pianificazioni di Snapshot e gruppi di coerenza di Snapshot

Utilizzare le pianificazioni per la raccolta di immagini snapshot e i gruppi di coerenza snapshot per gestire più volumi di base.

Per gestire facilmente le operazioni di snapshot per i volumi di base, è possibile utilizzare le seguenti funzionalità:

- **Snapshot schedule** — automatizza le snapshot per un singolo volume di base.
- **Snapshot Consistency group** — Gestisci più volumi di base come un'unica entità.

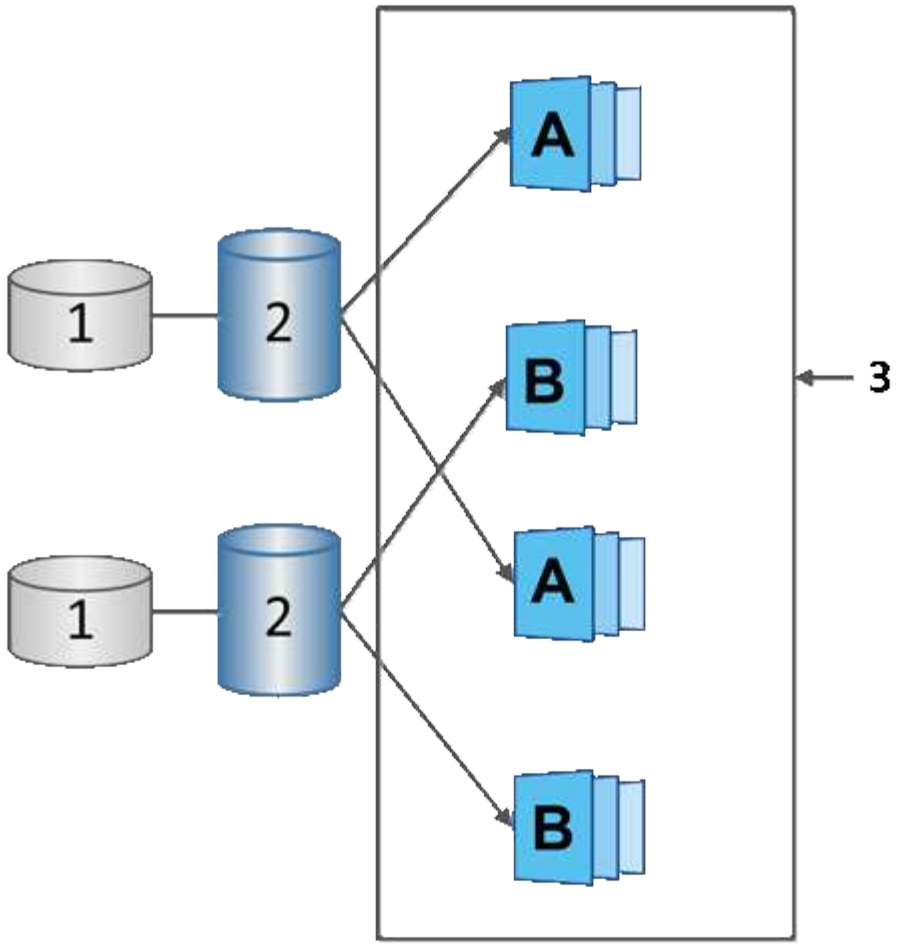
Calendario di Snapshot

Se si desidera creare automaticamente snapshot per un volume di base, è possibile creare una pianificazione. Ad esempio, è possibile definire un programma che prenda le immagini snapshot ogni sabato a mezzanotte, il primo di ogni mese o in qualsiasi data e ora decida. Una volta raggiunto il numero massimo di 32 snapshot per una singola pianificazione, è possibile sospendere gli snapshot pianificati, creare una capacità più riservata o eliminare gli snapshot. Le istantanee possono essere eliminate manualmente o automatizzando il processo di eliminazione. Una volta eliminata un'immagine snapshot, è disponibile ulteriore capacità riservata per il riutilizzo.

Gruppo di coerenza Snapshot

Si crea un gruppo di coerenza snapshot quando si desidera assicurarsi che le immagini snapshot vengano acquisite su più volumi contemporaneamente. Le azioni dell'immagine Snapshot vengono eseguite sull'intero gruppo di coerenza Snapshot. Ad esempio, è possibile pianificare snapshot sincronizzati di tutti i volumi con lo stesso indicatore data e ora. I gruppi di coerenza Snapshot sono ideali per le applicazioni che si estendono su più volumi, ad esempio le applicazioni di database che memorizzano i log su un volume e i file di database su un altro volume.

I volumi inclusi in un gruppo di coerenza snapshot sono denominati volumi membri. Quando si aggiunge un volume a un gruppo di coerenza, System Manager crea automaticamente una nuova capacità riservata che corrisponde a quel volume membro. È possibile definire una pianificazione per creare automaticamente un'immagine snapshot di ciascun volume membro.



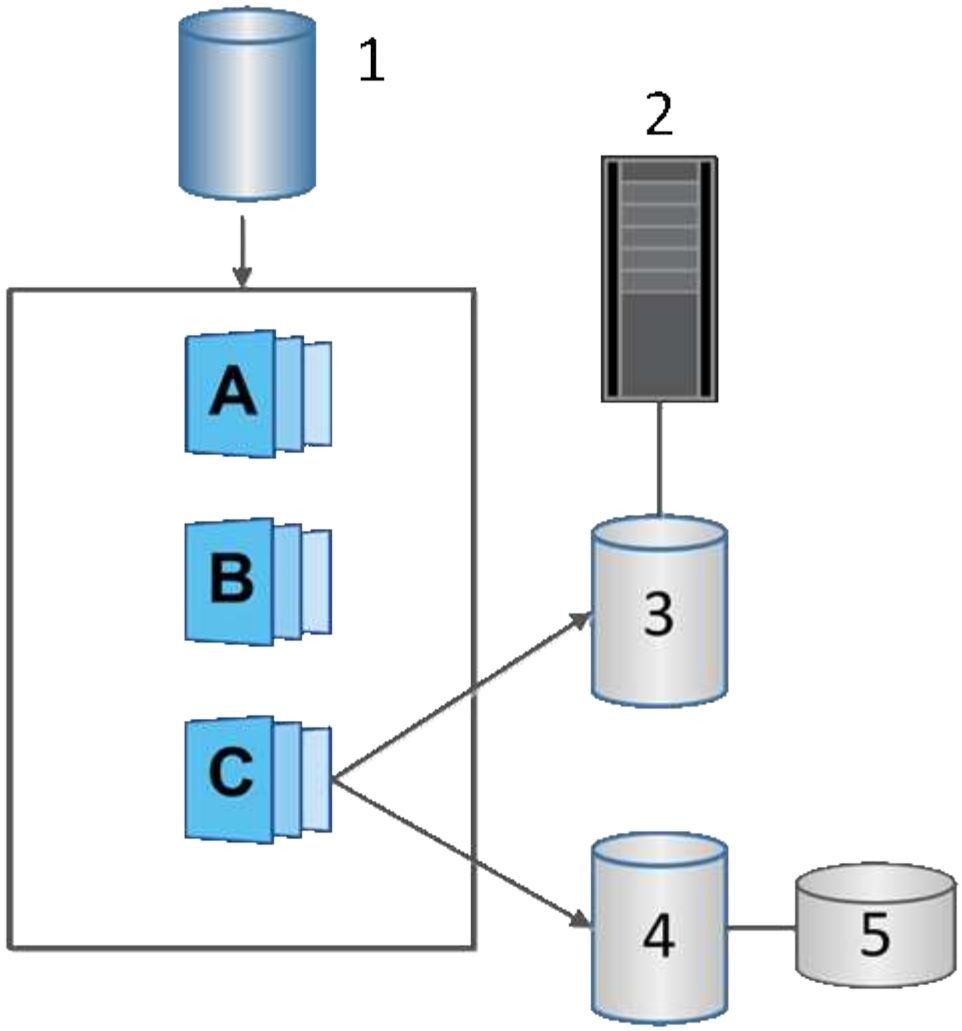
[1] capacità riservata; [2] volume membro; [3] immagini snapshot del gruppo di coerenza

Volumi Snapshot

È possibile creare un volume di snapshot e assegnarlo a un host se si desidera leggere o scrivere i dati di snapshot. Il volume Snapshot condivide le stesse caratteristiche del volume di base (livello RAID, caratteristiche i/o e così via).

Quando si crea un volume snapshot, è possibile designarlo come *Read-only* o *Read-write accessible*.

Quando si creano volumi snapshot di sola lettura, non è necessario aggiungere capacità riservata. Quando si creano volumi snapshot di lettura/scrittura, è necessario aggiungere capacità riservata per fornire l'accesso in scrittura.



[1] Volume base; [2] host; [3] Volume snapshot di sola lettura; [4] Volume snapshot di lettura/scrittura; [5] capacità riservata

Rollback di Snapshot

Un'operazione di rollback riporta un volume di base a uno stato precedente, determinato dallo snapshot selezionato.

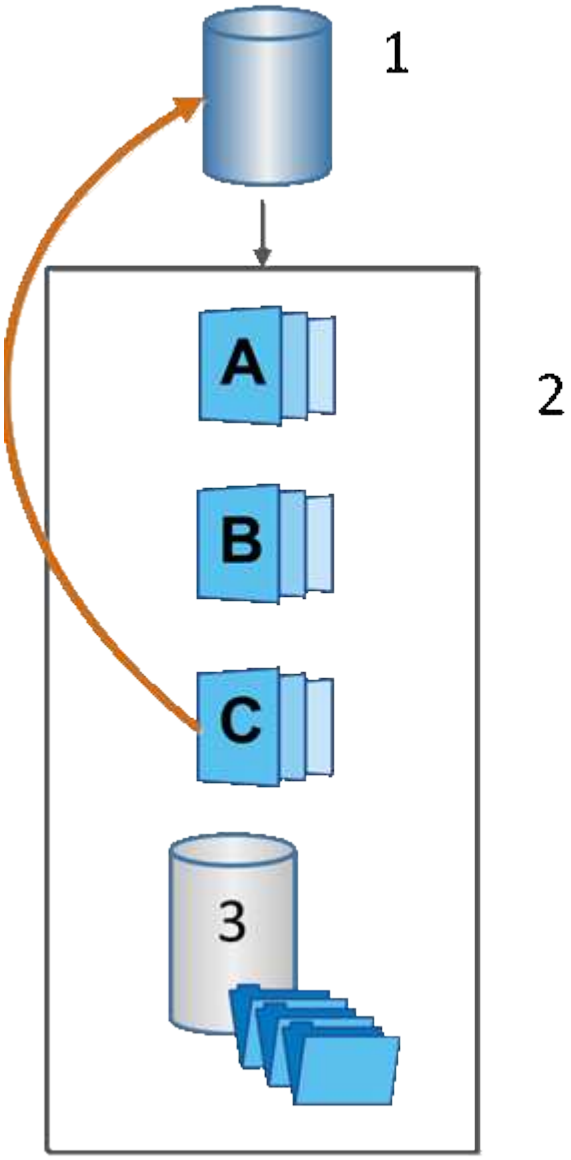
Per il rollback, è possibile selezionare un'immagine snapshot da una delle seguenti origini:

- **Rollback dell'immagine Snapshot**, per un ripristino completo di un volume di base.
- **Rollback del gruppo di coerenza Snapshot**, che può essere utilizzato per eseguire il rollback di uno o più volumi.

Durante il rollback, la funzione Snapshot conserva tutte le immagini snapshot del gruppo. Consente inoltre all'host di accedere al volume di base durante questo processo, se necessario per le operazioni di i/O.

Quando viene avviato un rollback, un processo in background esegue la ricerca degli indirizzi LBA (Logical Block Address) per il volume di base, quindi trova i dati copy-on-write nell'immagine snapshot di rollback da ripristinare. Poiché il volume di base è accessibile all'host per le operazioni di lettura e scrittura e tutti i dati precedentemente scritti sono immediatamente disponibili, il volume di capacità riservata deve essere

sufficientemente grande da contenere tutte le modifiche durante l'elaborazione del rollback. Il trasferimento dei dati continua come operazione in background fino al completamento del rollback.



[1] Volume di base; [2] oggetti Snapshot in un gruppo; [3] capacità riservata del gruppo Snapshot

Creare snapshot e oggetti snapshot

Creare un'immagine snapshot

È possibile creare manualmente un'immagine snapshot da un volume di base o da un gruppo di coerenza snapshot. Questo è anche chiamato *snapshot istantaneo* o *immagine istantanea*.

Prima di iniziare

- Il volume di base deve essere ottimale.
- Il disco deve essere ottimale.

- Impossibile designare il gruppo di snapshot come “reserved.”
- Il volume di capacità riservata deve avere le stesse impostazioni di Data Assurance (da) del volume di base associato per il gruppo di snapshot.

Fasi

1. Per creare un’immagine istantanea, eseguire una delle seguenti operazioni:
   - Selezionare **Storage › Volumes** (Storage[volumi]). Selezionare l’oggetto (volume di base o gruppo di coerenza snapshot), quindi selezionare **Copy Services › Create Instant snapshot**.
   - Selezionare **Storage › Snapshot**. Selezionare la scheda **Snapshot Images**, quindi selezionare **Create › Instant snapshot**.

     Viene visualizzata la finestra di dialogo Create Snapshot Image (Crea immagine istantanea). Selezionare l’oggetto (volume di base o gruppo di coerenza dello snapshot), quindi fare clic su **Avanti**. Se è stata creata un’immagine snapshot precedente per il volume o il gruppo di coerenza snapshot, il sistema crea immediatamente l’istantanea. In caso contrario, se si crea per la prima volta un’immagine snapshot per il volume o il gruppo di coerenza snapshot, viene visualizzata la finestra di dialogo Confirm Create Snapshot Image (Conferma creazione immagine istantanea).

2. Fare clic su **Create** (Crea) per accettare la notifica della necessità di capacità riservata e passare alla fase Reserve Capacity (capacità riservata).

   Viene visualizzata la finestra di dialogo capacità riservata.

3. Utilizzare la casella di selezione per regolare la percentuale di capacità, quindi fare clic su **Avanti** per accettare il volume candidato evidenziato nella tabella.

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

4. Selezionare le impostazioni per l’immagine istantanea in base alle esigenze e confermare che si desidera eseguire l’operazione.

Dettagli del campo

Impostazione	Descrizione
Impostazioni dell'immagine Snapshot	Limite dell'immagine Snapshot
Mantenere la casella di controllo selezionata se si desidera eliminare automaticamente le immagini snapshot dopo il limite specificato; utilizzare la casella di selezione per modificare il limite. Se si deseleziona questa casella di controllo, la creazione dell'immagine snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservate**
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di snapshot è quasi piena. Quando la capacità riservata per il gruppo di snapshot supera la soglia specificata, utilizzare l'avviso anticipato per aumentare la capacità riservata o eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Policy per la capacità massima riservata	Scegliere una delle seguenti policy: • **Purge Oldest snapshot image** (Elimina immagine snapshot meno recente) — il sistema rimuove automaticamente l'immagine snapshot meno recente nel gruppo di snapshot, che rilascia la capacità riservata dell'immagine snapshot per poterla riutilizzare all'interno del gruppo. • **Rifiuta scritture nel volume base** — quando la capacità riservata raggiunge la massima percentuale definita, il sistema rifiuta qualsiasi richiesta di scrittura i/o nel volume base che ha attivato l'accesso alla capacità riservata.

Risultati

- System Manager visualizza la nuova immagine istantanea nella tabella Snapshot Images (immagini istantanee). La tabella elenca la nuova immagine in base alla data e all'ora e al volume di base o al gruppo di coerenza dello snapshot associato.
- La creazione dello snapshot potrebbe rimanere in sospeso a causa delle seguenti condizioni:

- Il volume di base che contiene questa immagine snapshot è membro di un gruppo di mirror asincrono.
- Il volume di base è attualmente in fase di sincronizzazione. La creazione dell'immagine snapshot viene completata non appena l'operazione di sincronizzazione viene completata.

Programmare le immagini snapshot

Viene creata una pianificazione di snapshot per abilitare il ripristino in caso di problemi con il volume di base ed eseguire backup pianificati. È possibile creare snapshot di volumi di base o gruppi di coerenza snapshot in base a una pianificazione giornaliera, settimanale o mensile, in qualsiasi momento della giornata.

Prima di iniziare

Il volume di base deve essere ottimale.

A proposito di questa attività

Questa attività descrive come creare una pianificazione di snapshot per un gruppo di coerenza di snapshot o un volume di base esistente.

> È inoltre possibile creare una pianificazione di snapshot contemporaneamente alla creazione di un'immagine di snapshot di un volume di base o di un gruppo di coerenza di snapshot.

Fasi

1. Eseguire una delle seguenti operazioni per creare una pianificazione di snapshot:
   - Selezionare **Storage › Volumes** (Storage[volumi]).

     Selezionare l'oggetto (volume o gruppo di coerenza snapshot) per questa pianificazione snapshot, quindi selezionare **Copy Services › Create snapshot schedule**.

   - Selezionare **Storage › Snapshot**.

     Selezionare la scheda **programmi**, quindi fare clic su **Crea**.

2. Selezionare l'oggetto (volume o gruppo di coerenza dello snapshot) per questa pianificazione dello snapshot, quindi fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Crea pianificazione snapshot.

3. Eseguire una delle seguenti operazioni:
   - **Utilizzare una pianificazione precedentemente definita da un altro oggetto snapshot**.

     Assicurarsi che vengano visualizzate le opzioni avanzate. Fare clic su **Mostra altre opzioni**. Fare clic su **Importa pianificazione**, selezionare l'oggetto con la pianificazione che si desidera importare, quindi fare clic su **Importa**.

   - **Modificare le opzioni di base o avanzate**.

     Nella parte superiore destra della finestra di dialogo, fare clic su **Mostra altre opzioni** per visualizzare tutte le opzioni, quindi fare riferimento alla seguente tabella.

Dettagli del campo

Campo	Descrizione
Impostazioni di base	Selezionare i giorni
Selezionare i singoli giorni della settimana per le immagini snapshot.	Ora di inizio
Dall'elenco a discesa, selezionare una nuova ora di inizio per le istantanee giornaliere (le selezioni vengono fornite in incrementi di mezz'ora). Per impostazione predefinita, l'ora di inizio è mezz'ora prima dell'ora corrente.	Fuso orario
Dall'elenco a discesa, selezionare il fuso orario dell'array.	**Impostazioni avanzate**
Giorno / mese	Scegliere una delle seguenti opzioni: • **Daily / Weekly** — Seleziona i singoli giorni per gli snapshot di sincronizzazione. È inoltre possibile selezionare la casella di controllo **Select All days** (Seleziona tutti i giorni) in alto a destra se si desidera una pianificazione giornaliera. • **Mensile / annuale** — selezionare i singoli mesi per le snapshot di sincronizzazione. Nel campo **on day(s)**, immettere i giorni del mese per le sincronizzazioni da eseguire. Le voci valide sono da **1** a **31** e **Last**. È possibile separare più giorni con una virgola o un punto e virgola. Utilizzare un trattino per le date inclusive. Ad esempio: 1,3,4,10-15,ultimo. Se si desidera una pianificazione mensile, è anche possibile selezionare la casella di controllo **Seleziona tutti i mesi** in alto a destra.
Ora di inizio	Dall'elenco a discesa, selezionare una nuova ora di inizio per le istantanee giornaliere (le selezioni vengono fornite in incrementi di mezz'ora). Per impostazione predefinita, l'ora di inizio è mezz'ora prima dell'ora corrente.
Fuso orario	Dall'elenco a discesa, selezionare il fuso orario dell'array.

Campo	Descrizione
Snapshot al giorno/ora tra snapshot	Selezionare il numero di immagini snapshot da creare al giorno. Se si selezionano più immagini, selezionare anche il tempo tra le immagini snapshot. Per più immagini snapshot, assicurarsi di disporre di una capacità riservata adeguata.
Creare subito un'immagine snapshot?	Selezionare questa casella di controllo per creare un'immagine istantanea oltre alle immagini automatiche che si stanno pianificando.
Data di inizio/fine o Nessuna data di fine	Inserire la data di inizio delle sincronizzazioni. Inserire anche una data di fine o selezionare **Nessuna data di fine**.

4. Eseguire una delle seguenti operazioni:
   - Se l'oggetto è un gruppo di coerenza snapshot, fare clic su **Create** per accettare le impostazioni e creare la pianificazione.
   - Se l'oggetto è un volume, fare clic su **Avanti** per allocare la capacità riservata per le immagini snapshot.

     La tabella dei candidati al volume visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.
5. Utilizzare la casella di selezione per allocare la capacità riservata per le immagini snapshot. Eseguire una delle seguenti operazioni:
   - **Accettare le impostazioni predefinite.**

     Utilizzare questa opzione consigliata per allocare la capacità riservata per le immagini snapshot con le impostazioni predefinite.
   - **Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati.**

     Se si modifica l'impostazione predefinita della capacità riservata, fare clic su **Refresh Candidates** (Aggiorna candidati) per aggiornare l'elenco dei candidati per la capacità riservata specificata.

     Allocare la capacità riservata utilizzando le seguenti linee guida:
     - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base. Di solito questa capacità è sufficiente.
     - La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nei volumi, alla quantità e alla durata della raccolta di immagini snapshot.
6. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Edit Settings (Modifica impostazioni).
7. Modificare le impostazioni per la pianificazione snapshot in base alle esigenze, quindi fare clic su **fine**.

Dettagli del campo

Impostazione	Descrizione
Limite immagine Snapshot	Attiva l'eliminazione automatica delle immagini snapshot quando…
Mantenere la casella di controllo selezionata se si desidera eliminare automaticamente le immagini snapshot dopo il limite specificato; utilizzare la casella di selezione per modificare il limite. Se si deseleziona questa casella di controllo, la creazione dell'immagine snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservate**
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per una pianificazione è quasi piena. Quando la capacità riservata per la pianificazione supera la soglia specificata, utilizzare l'avviso anticipato per aumentare la capacità riservata o eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Policy per la capacità massima riservata	Scegliere una delle seguenti policy: • **Rimuovi l'immagine snapshot meno recente** — il sistema rimuove automaticamente l'immagine snapshot meno recente, rilasciando la capacità riservata dell'immagine snapshot per poterla riutilizzare all'interno del gruppo di snapshot. • **Rifiuta scritture nel volume base** — quando la capacità riservata raggiunge la massima percentuale definita, il sistema rifiuta qualsiasi richiesta di scrittura i/o nel volume base che ha attivato l'accesso alla capacità riservata.

Creare un gruppo di coerenza snapshot

Per garantire copie coerenti, è possibile creare un set di volumi multipli denominato *snapshot Consistency group*.

Questo gruppo consente di creare immagini snapshot di tutti i volumi contemporaneamente per garantire la coerenza. Ciascun volume appartenente a un gruppo di coerenza snapshot viene definito *volume membro*.

Quando si aggiunge un volume a un gruppo di coerenza snapshot, il sistema crea automaticamente un nuovo gruppo di snapshot che corrisponde a questo volume membro.

A proposito di questa attività

La sequenza di creazione del gruppo di coerenza Snapshot consente di selezionare i volumi membro per il gruppo e di allocare la capacità ai volumi membro.

Il processo per creare un gruppo di coerenza snapshot è una procedura multi-step.

Fase 1: Aggiunta di membri al gruppo di coerenza snapshot

Selezionare i membri per specificare una raccolta di volumi che comprendono il gruppo di coerenza snapshot. Tutte le azioni eseguite sul gruppo di coerenza snapshot si estendono uniformemente ai volumi membro selezionati.

Prima di iniziare

I volumi dei membri devono essere ottimali.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **gruppi di coerenza Snapshot**.
3. Selezionare il **Create › Snapshot Consistency group** (Crea[Gruppo di coerenza snapshot]

   Viene visualizzata la finestra di dialogo Create Snapshot Consistency Group.

4. Selezionare i volumi da aggiungere come volumi membri al gruppo di coerenza snapshot.
5. Fare clic su **Avanti** e passare a. Fase 2: Riservare la capacità per il gruppo di coerenza snapshot.

Fase 2: Riservare la capacità per il gruppo di coerenza snapshot

Associare la capacità riservata al gruppo di coerenza snapshot. System Manager suggerisce i volumi e la capacità in base alle proprietà del gruppo di coerenza snapshot. È possibile accettare la configurazione di capacità riservata consigliata o personalizzare lo storage allocato.

A proposito di questa attività

Nella finestra di dialogo capacità riservata, la tabella dei candidati al volume visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.

Fasi

1. Utilizzare la casella di selezione per allocare la capacità riservata per il gruppo di coerenza snapshot. Eseguire una delle seguenti operazioni:
   - **Accettare le impostazioni predefinite**.

     Utilizzare questa opzione consigliata per allocare la capacità riservata per ciascun volume membro con le impostazioni predefinite.

   - **Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati.**

     Allocare la capacità riservata utilizzando le seguenti linee guida.

    - L’impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base. Di solito questa capacità è sufficiente.
    - La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nei volumi, alla quantità e alla durata della raccolta di immagini snapshot.
2. **Opzionale:** se si modifica l’impostazione predefinita della capacità riservata, fare clic su **Aggiorna candidati** per aggiornare l’elenco dei candidati per la capacità riservata specificata.
3. Fare clic su **Avanti** e passare a. Fase 3: Modificare le impostazioni per il gruppo di coerenza snapshot.

Fase 3: Modificare le impostazioni per il gruppo di coerenza snapshot

Accettare o scegliere le impostazioni di eliminazione automatica e le soglie di avviso della capacità riservata per il gruppo di coerenza snapshot.

A proposito di questa attività

La sequenza di creazione del gruppo di coerenza Snapshot consente di selezionare i volumi membro per il gruppo e di allocare la capacità ai volumi membro.

Fasi

1. Accettare o modificare le impostazioni predefinite per il gruppo di coerenza snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del gruppo di coerenza Snapshot	Nome
Specificare il nome del gruppo di coerenza snapshot.	Attiva l'eliminazione automatica delle immagini snapshot quando…
Mantenere la casella di controllo selezionata se si desidera eliminare automaticamente le immagini snapshot dopo il limite specificato; utilizzare la casella di selezione per modificare il limite. Se si deseleziona questa casella di controllo, la creazione dell'immagine snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservate**
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di coerenza snapshot è quasi piena. Quando la capacità riservata per il gruppo di coerenza snapshot supera la soglia specificata, utilizzare la notifica anticipata per aumentare la capacità riservata o eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Policy per la capacità massima riservata	Scegliere una delle seguenti policy: • **Purge Oldest snapshot image** (Elimina immagine snapshot meno recente) — il sistema rimuove automaticamente l'immagine snapshot meno recente nel gruppo di coerenza snapshot, che rilascia la capacità riservata dell'immagine snapshot per il riutilizzo all'interno del gruppo. • **Rifiuta scritture nel volume base** — quando la capacità riservata raggiunge la massima percentuale definita, il sistema rifiuta qualsiasi richiesta di scrittura i/o nel volume base che ha attivato l'accesso alla capacità riservata.

2. Una volta completata la configurazione del gruppo di coerenza snapshot, fare clic su **fine**.

Creare un volume di snapshot

Si crea un volume di snapshot per fornire l'accesso host a un'immagine di snapshot di un volume o di un gruppo di coerenza di snapshot. È possibile designare il volume di snapshot come di sola lettura o di lettura/scrittura.

A proposito di questa attività

La sequenza di creazione del volume di snapshot consente di creare un volume di snapshot da un'immagine di snapshot e fornisce opzioni per allocare la capacità riservata se il volume è in lettura/scrittura. Un volume di snapshot può essere designato come uno dei seguenti:

- Un volume snapshot di sola lettura fornisce a un'applicazione host l'accesso in lettura a una copia dei dati contenuti nell'immagine snapshot, ma senza la possibilità di modificare l'immagine. Un volume snapshot di sola lettura non dispone di capacità riservata associata.
- Un volume di snapshot in lettura/scrittura fornisce all'applicazione host l'accesso in scrittura a una copia dei dati contenuti nell'immagine snapshot. Dispone di una propria capacità riservata che viene utilizzata per salvare eventuali modifiche successive apportate dall'applicazione host nel volume di base senza influire sull'immagine snapshot di riferimento.

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

Fase 1: Esaminare i membri per un volume di snapshot

Selezionare un'immagine snapshot di un volume di base o un gruppo di coerenza snapshot. Se si seleziona un'immagine snapshot del gruppo di coerenza snapshot, i volumi membri del gruppo di coerenza snapshot vengono visualizzati per la revisione.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).
3. Selezionare **Crea**.

   Viene visualizzata la finestra di dialogo Create Snapshot Volume (Crea volume snapshot).

4. Selezionare l'immagine snapshot (volume o gruppo di coerenza snapshot) che si desidera convertire in un volume snapshot, quindi fare clic su **Avanti**. Utilizzare una voce di testo nel campo **Filter** per restringere l'elenco.

   Se la selezione riguardava un'immagine snapshot di un gruppo di coerenza snapshot, viene visualizzata la finestra di dialogo Review Members (membri revisione).

   Nella finestra di dialogo Review Members (membri revisione), esaminare l'elenco dei volumi selezionati per la conversione in volumi snapshot, quindi fare clic su **Next** (Avanti).

5. Passare a. Fase 2: Assegnare il volume snapshot all'host.

Fase 2: Assegnare il volume snapshot all'host

Selezionare un host o un cluster host specifico per assegnarlo al volume di snapshot. Questa assegnazione concede a un host o a un cluster host l'accesso al volume di snapshot. Se necessario, è possibile scegliere di assegnare un host in un secondo momento.

Prima di iniziare

- Nella pagina host sono presenti host o cluster di host validi.
- Gli identificatori delle porte host devono essere stati definiti per l'host.
- Prima di creare un volume abilitato da, verificare che la connessione host pianificata supporti la funzione Data Assurance (da). Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

A proposito di questa attività

Quando si assegnano i volumi, tenere presenti le seguenti linee guida:

- Il sistema operativo di un host può avere limiti specifici sul numero di volumi a cui l'host può accedere.
- È possibile definire un'assegnazione host per ciascun volume di snapshot nell'array di storage.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume di snapshot. È necessario utilizzare un LUN univoco.

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

Fasi

1. Nella finestra di dialogo **Assegna all'host**, selezionare l'host o il cluster host che si desidera assegnare al nuovo volume. Se si desidera creare il volume senza assegnare un host, selezionare **Assegna in seguito** dall'elenco a discesa.
2. Selezionare la modalità di accesso. Scegliere una delle seguenti opzioni:
   - **Read/write** — questa opzione fornisce all'host l'accesso in lettura/scrittura al volume di snapshot e richiede una capacità riservata.
   - **Sola lettura** — questa opzione fornisce all'host l'accesso in sola lettura al volume snapshot e non richiede capacità riservata.
3. Fare clic su **Avanti** ed eseguire una delle seguenti operazioni:
   - Se il volume snapshot è in lettura/scrittura, viene visualizzata la finestra di dialogo Review Capacity (capacità di revisione). Passare a. Fase 3: Riservare la capacità per un volume di snapshot.
   - Se il volume snapshot è di sola lettura, viene visualizzata la finestra di dialogo Edit Priority (Modifica priorità). Passare a. Fase 4: Modificare le impostazioni di un volume di snapshot.

Fase 3: Riservare la capacità per un volume di snapshot

Associare la capacità riservata a un volume snapshot di lettura/scrittura. System Manager suggerisce i volumi e la capacità in base alle proprietà del volume di base o del gruppo di coerenza dello snapshot. È possibile accettare la configurazione di capacità riservata consigliata o personalizzare lo storage allocato.

A proposito di questa attività

È possibile aumentare o diminuire la capacità riservata per il volume di snapshot in base alle necessità. Se la capacità riservata dello snapshot è superiore a quella necessaria, è possibile ridurne le dimensioni per liberare spazio necessario per altri volumi logici.

Fasi

1. Utilizzare la casella di selezione per allocare la capacità riservata per il volume di snapshot.

   La tabella Volume Candidate (candidato volume) visualizza solo i candidati che supportano la capacità

riservata specificata.

Eseguire una delle seguenti operazioni:

- **Accettare le impostazioni predefinite**.

  Utilizzare questa opzione consigliata per allocare la capacità riservata per il volume di snapshot con le impostazioni predefinite.

- **Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati**.

  Se si modifica l'impostazione predefinita della capacità riservata, fare clic su **Refresh Candidates** (Aggiorna candidati) per aggiornare l'elenco dei candidati per la capacità riservata specificata.

  Allocare la capacità riservata utilizzando le seguenti linee guida.

  - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base, e di solito questa capacità è sufficiente.
  - La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nei volumi, alla quantità e alla durata della raccolta di immagini snapshot.

2. **Opzionale:** se si crea il volume di snapshot per un gruppo di coerenza di snapshot, l'opzione "Change Candidate" viene visualizzata nella tabella Reserved Capacity Candidates. Fare clic su **Change Candidate** (Cambia candidato) per selezionare un candidato alternativo a capacità riservata.
3. Fare clic su **Avanti** e passare a. Fase 4: Modificare le impostazioni di un volume di snapshot.

Fase 4: Modificare le impostazioni di un volume di snapshot

Modificare le impostazioni di un volume di snapshot, ad esempio il nome, il caching, le soglie di avviso della capacità riservata e così via.

A proposito di questa attività

È possibile aggiungere il volume alla cache del disco a stato solido (SSD) per migliorare le prestazioni di sola lettura. La cache SSD è costituita da un set di unità SSD che vengono raggruppate logicamente nell'array di storage.

Fasi

1. Accettare o modificare le impostazioni per il volume di snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del volume Snapshot	Nome
Specificare il nome del volume di snapshot.	Abilitare la cache SSD
Scegliere questa opzione per abilitare il caching in sola lettura sugli SSD.	**Impostazioni di capacità riservate**
Avvisami quando…	**Viene visualizzato solo per un volume snapshot di lettura/scrittura**. Utilizzare la casella di selezione per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di snapshot è quasi piena. Quando la capacità riservata per il gruppo di snapshot supera la soglia specificata, utilizzare l'avviso anticipato per aumentare la capacità riservata o eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.

2. Esaminare la configurazione del volume di snapshot. Fare clic su **Indietro** per apportare le modifiche desiderate.
3. Quando si è soddisfatti della configurazione del volume snapshot, fare clic su **fine**.

Gestire le pianificazioni di snapshot

Modificare le impostazioni per una pianificazione snapshot

Per una pianificazione snapshot, è possibile modificare gli orari di raccolta automatica o la frequenza di raccolta.

A proposito di questa attività

È possibile importare le impostazioni da una pianificazione di snapshot esistente oppure modificarle in base alle esigenze.

Poiché una pianificazione di snapshot è associata a un gruppo di snapshot o a un gruppo di coerenza di snapshot, la capacità riservata potrebbe essere influenzata dalle modifiche alle impostazioni di pianificazione.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **programmi**.
3. Selezionare il programma di snapshot che si desidera modificare, quindi fare clic su **Edit** (Modifica).

Viene visualizzata la finestra di dialogo Modifica pianificazione snapshot.

4. Effettuare una delle seguenti operazioni:
   - **Utilizzare un programma definito in precedenza da un altro oggetto di snapshot** — fare clic su **Importa pianificazione**, selezionare l'oggetto con il programma che si desidera importare, quindi fare clic su **Importa**.
   - **Modificare le impostazioni del programma** — fare riferimento ai dettagli dei campi riportati di seguito.

     Dettagli del campo

Impostazione	Descrizione
Giorno / mese	Scegliere una delle seguenti opzioni: • **Daily / Weekly** — Seleziona i singoli giorni per gli snapshot di sincronizzazione. È inoltre possibile selezionare la casella di controllo **Select All days** (Seleziona tutti i giorni) in alto a destra se si desidera una pianificazione giornaliera. • **Mensile / annuale** — selezionare i singoli mesi per le snapshot di sincronizzazione. Nel campo **on day(s)**, immettere i giorni del mese per le sincronizzazioni da eseguire. Le voci valide sono da **1** a **31** e **Last**. È possibile separare più giorni con una virgola o un punto e virgola. Utilizzare un trattino per le date inclusive. Ad esempio: 1,3,4,10-15,ultimo. Se si desidera una pianificazione mensile, è anche possibile selezionare la casella di controllo **Seleziona tutti i mesi** in alto a destra.
Ora di inizio	Dall'elenco a discesa, selezionare una nuova ora di inizio per le istantanee giornaliere. Le selezioni sono disponibili con incrementi di mezz'ora. Per impostazione predefinita, l'ora di inizio è mezz'ora prima dell'ora corrente.
Fuso orario	Dall'elenco a discesa, selezionare il fuso orario dell'array di storage.
Snapshot al giorno Tempo tra le snapshot	Selezionare il numero di immagini snapshot da creare al giorno. Se si selezionano più punti, selezionare anche l'intervallo di tempo tra i punti di ripristino. Per più punti di ripristino, assicurarsi di disporre di una capacità riservata adeguata.
Data di inizio Data di fine Nessuna data di fine	Inserire la data di inizio delle sincronizzazioni. Inserire anche una data di fine o selezionare **Nessuna data di fine**.

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

Attivare e sospendere la pianificazione delle snapshot

È possibile sospendere temporaneamente la raccolta pianificata di immagini snapshot quando è necessario risparmiare spazio di storage. Questo metodo è più efficiente dell'eliminazione e della successiva ricreazione della pianificazione di snapshot.

A proposito di questa attività

Lo stato della pianificazione snapshot rimane sospeso fino a quando non si utilizza l'opzione **Activate** per riprendere l'attività snapshot pianificata.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Se non è già visualizzato, fare clic sulla scheda **programmi**.

   I programmi sono elencati nella pagina.

3. Selezionare un programma di snapshot attivo che si desidera sospendere, quindi fare clic su **Activate/Suspend** (attiva/Sospendi).

   Lo stato della colonna state (Stato) diventa **Suspended** (sospeso) e la pianificazione delle istantanee interrompe la raccolta di tutte le immagini snapshot.

4. Per riprendere la raccolta delle immagini snapshot, selezionare la pianificazione delle istantanee sospese che si desidera riprendere, quindi fare clic su **Activate / Suspend** (attiva / Sospendi).

   Lo stato della colonna Stato diventa **attivo**.

Elimina pianificazione snapshot

Se non si desidera più raccogliere immagini snapshot, è possibile eliminare una pianificazione snapshot esistente.

A proposito di questa attività

Quando si elimina una pianificazione di snapshot, le immagini di snapshot associate non vengono eliminate insieme ad essa. Se si ritiene che la raccolta di immagini snapshot possa essere ripresa a un certo punto, è necessario sospendere la pianificazione delle istantanee piuttosto che eliminarla.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **programmi**.
3. Selezionare il programma di snapshot che si desidera eliminare e confermare l'operazione.

Risultati

Il sistema rimuove tutti gli attributi di pianificazione dal volume di base o dal gruppo di coerenza dello snapshot.

Gestire le immagini Snapshot

Consente di visualizzare le impostazioni dell'immagine snapshot

È possibile visualizzare le proprietà, lo stato, la capacità riservata e gli oggetti associati

assegnati a ciascuna immagine istantanea.

A proposito di questa attività

Gli oggetti associati a un'immagine snapshot includono il volume di base o il gruppo di coerenza dello snapshot per il quale l'immagine snapshot è un punto di ripristino, il gruppo di snapshot associato ed eventuali volumi di snapshot creati dall'immagine snapshot. Utilizzare le impostazioni di snapshot per determinare se si desidera copiare o convertire l'immagine di snapshot.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **Snapshot Images** (immagini istantanee).
3. Selezionare l'immagine istantanea che si desidera visualizzare, quindi fare clic su **View Settings** (Impostazioni vista).

   Viene visualizzata la finestra di dialogo Snapshot Image Settings (Impostazioni immagine istantanea).

4. Visualizzare le impostazioni dell'immagine istantanea.

Avviare il rollback dell'immagine snapshot per un volume di base

È possibile eseguire un'operazione di rollback per modificare il contenuto di un volume di base in modo che corrisponda al contenuto salvato in un'immagine snapshot.

L'operazione di rollback non modifica il contenuto delle immagini snapshot associate al volume di base.

Prima di iniziare

- È disponibile una capacità riservata sufficiente per avviare un'operazione di rollback.
- L'immagine snapshot selezionata è ottimale e il volume selezionato è ottimale.
- Il volume selezionato non dispone di un'operazione di rollback già in corso.

A proposito di questa attività

La sequenza di avvio del rollback consente di avviare il rollback su un'immagine snapshot di un volume di base, fornendo al contempo opzioni per aggiungere capacità di storage. Non è possibile avviare più di un'operazione di rollback per un volume di base alla volta.

> L'host può accedere immediatamente al nuovo volume di base rollback, ma il volume di base esistente non consente l'accesso in lettura/scrittura all'host dopo l'inizio del rollback. È possibile creare uno snapshot del volume di base appena prima di iniziare il rollback per conservare il volume di base pre-rollback per il ripristino.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Images** (immagini istantanee).
3. Selezionare l'immagine istantanea, quindi selezionare **Rollback › Start**.

   Viene visualizzata la finestra di dialogo Confirm Start Rollback (Conferma avvio ripristino).

4. **Opzionale:** selezionare l'opzione **aumenta capacità** se necessario.

   Viene visualizzata la finestra di dialogo aumenta capacità riservata.

a. Utilizzare la casella di selezione per regolare la percentuale di capacità.

   Se la capacità libera non esiste nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage dispone di capacità non assegnata, è possibile aggiungere capacità. È possibile creare un nuovo pool o gruppo di volumi e riprovare a eseguire questa operazione utilizzando la nuova capacità libera del pool o del gruppo di volumi.

b. Fare clic su **aumenta**.

5. Confermare che si desidera eseguire questa operazione, quindi fare clic su **Rollback**.

Risultati

System Manager esegue le seguenti operazioni:

- Ripristina il volume con il contenuto salvato nell'immagine istantanea selezionata.
- Rende i volumi rollback immediatamente disponibili per l'accesso all'host. Non è necessario attendere il completamento dell'operazione di rollback.

Al termine

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di rollback.

Se l'operazione di rollback non riesce, l'operazione viene interrotta. È possibile riprendere l'operazione in pausa e, se il problema persiste, seguire la procedura Recovery Guru per risolvere il problema o contattare il supporto tecnico.

Avviare il rollback dell'immagine snapshot per i volumi membri del gruppo di coerenza snapshot

È possibile eseguire un'operazione di rollback per modificare il contenuto dei volumi membri del gruppo di coerenza snapshot in modo che corrisponda al contenuto salvato in un'immagine snapshot.

L'operazione di rollback non modifica il contenuto delle immagini snapshot associate al gruppo di coerenza snapshot.

Prima di iniziare

- È disponibile una capacità riservata sufficiente per avviare un'operazione di rollback.
- L'immagine snapshot selezionata è ottimale e il volume selezionato è ottimale.
- Il volume selezionato non dispone di un'operazione di rollback già in corso.

A proposito di questa attività

La sequenza di avvio del rollback consente di avviare il rollback su un'immagine snapshot di un gruppo di coerenza snapshot, fornendo al contempo opzioni per aggiungere capacità di storage. Non è possibile avviare più di un'operazione di rollback per un gruppo di coerenza snapshot alla volta.

> L'host ha accesso immediato ai nuovi volumi di rollback, ma i volumi membri esistenti non consentono più l'accesso in lettura/scrittura all'host dopo l'avvio del rollback. È possibile creare un'immagine snapshot dei volumi membro appena prima di iniziare il rollback per conservare i volumi di base pre-rollback a scopo di recovery.

Il processo per avviare il rollback di un'immagine snapshot di un gruppo di coerenza snapshot è una procedura multi-step.

Fase 1: Selezionare i membri

È necessario selezionare i volumi membro da ripristinare.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Images** (immagini istantanee).
3. Selezionare l'immagine snapshot del gruppo di coerenza snapshot, quindi selezionare **Rollback › Start**.

   Viene visualizzata la finestra di dialogo Avvia ripristino.

4. Selezionare il volume membro o i volumi.
5. Fare clic su **Avanti** ed eseguire una delle seguenti operazioni:
   - Se uno qualsiasi dei volumi membro selezionati è associato a più di un oggetto di capacità riservata che memorizza immagini snapshot, viene visualizzata la finestra di dialogo Review Capacity (capacità di revisione). Passare a. Fase 2: Rivedere la capacità.
   - Se nessuno dei volumi membro selezionati è associato a più di un oggetto di capacità riservata che memorizza immagini snapshot, viene visualizzata la finestra di dialogo Edit Priority (Modifica priorità). Passare a. Fase 3: Modificare la priorità.

Fase 2: Rivedere la capacità

Se sono stati selezionati volumi membro associati a più di un oggetto di capacità riservata, come un gruppo di snapshot e un volume di capacità riservata, è possibile rivedere e aumentare la capacità riservata per i volumi di rollback.

Fasi

1. Accanto a qualsiasi volume membro con capacità riservata molto bassa (o zero), fare clic sul collegamento **aumento capacità** nella colonna **Modifica**.

   Viene visualizzata la finestra di dialogo aumenta capacità riservata.

2. Utilizzare la casella di selezione per regolare la percentuale di capacità, quindi fare clic su **aumento**.

   Se la capacità libera non esiste nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage dispone di capacità non assegnata, è possibile aggiungere capacità. È possibile creare un nuovo pool o gruppo di volumi e riprovare a eseguire questa operazione utilizzando la nuova capacità libera di tale pool o gruppo di volumi.

3. Fare clic su **Avanti** e passare a. Fase 3: Modificare la priorità.

   Viene visualizzata la finestra di dialogo Edit Priority (Modifica priorità).

Fase 3: Modificare la priorità

Se necessario, è possibile modificare la priorità dell'operazione di rollback.

A proposito di questa attività

La priorità di rollback determina quante risorse di sistema sono dedicate all'operazione di rollback a scapito delle prestazioni del sistema.

Fasi

1. Utilizzare il dispositivo di scorrimento per regolare la priorità di rollback in base alle esigenze.
2. Confermare l'operazione, quindi fare clic su **fine**.

Risultati

System Manager esegue le seguenti operazioni:

- Ripristina i volumi dei membri del gruppo di coerenza snapshot con il contenuto salvato nell'immagine snapshot selezionata.
- Rende i volumi rollback immediatamente disponibili per l'accesso all'host. Non è necessario attendere il completamento dell'operazione di rollback.

Al termine

Selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di rollback.

Se l'operazione di rollback non riesce, l'operazione viene interrotta. È possibile riprendere l'operazione in pausa e, se il problema persiste, seguire la procedura Recovery Guru per risolvere il problema o contattare il supporto tecnico.

Riprendere il rollback dell'immagine snapshot

Se si verifica un errore durante un'operazione di rollback dell'immagine snapshot, l'operazione viene automaticamente messa in pausa. È possibile riprendere un'operazione di rollback in stato di pausa.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **Snapshot Images** (immagini istantanee).
3. Evidenziare il rollback in pausa, quindi selezionare **rollback › Riprendi**.

   L'operazione riprende.

Risultati

System Manager esegue le seguenti operazioni:

- Se l'operazione di rollback riprende, è possibile visualizzare l'avanzamento dell'operazione di rollback nella finestra Operations in Progress (operazioni in corso).
- Se l'operazione di rollback non riesce, l'operazione viene nuovamente interrotta. Seguire la procedura Recovery Guru per risolvere il problema o contattare il supporto tecnico.

Annulla il rollback dell'immagine snapshot

È possibile annullare un rollback attivo in corso (copia attiva dei dati), un rollback in sospeso (in una coda in attesa di avvio delle risorse) o un rollback che è stato sospeso a causa di un errore.

A proposito di questa attività

Quando si annulla un'operazione di rollback in corso, il volume di base torna a uno stato inutilizzabile e viene visualizzato come non riuscito. Pertanto, è consigliabile annullare un'operazione di rollback solo quando sono

disponibili opzioni di ripristino per il ripristino del contenuto del volume di base.

> Se il gruppo di snapshot su cui risiede l'immagine snapshot presenta una o più immagini snapshot che sono state eliminate automaticamente, l'immagine snapshot utilizzata per l'operazione di rollback potrebbe non essere disponibile per i rollback futuri.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **Snapshot Images** (immagini istantanee).
3. Selezionare il rollback attivo o in pausa, quindi selezionare **rollback › Annulla**.

   Viene visualizzata la finestra di dialogo Confirm Cancel Rollback (Conferma annullamento ripristino).

4. Fare clic su **Sì** per confermare.

Risultati

System Manager interrompe l'operazione di rollback. Il volume di base è utilizzabile ma potrebbe avere dati incoerenti o non intatti.

Al termine

Dopo aver annullato un'operazione di rollback, è necessario eseguire una delle seguenti operazioni:

- Reinizializzare il contenuto del volume di base.
- Eseguire una nuova operazione di rollback per ripristinare il volume di base utilizzando la stessa immagine snapshot utilizzata nell'operazione Annulla rollback o un'immagine snapshot diversa per eseguire la nuova operazione di rollback.

Eliminare l'immagine istantanea

Le immagini snapshot vengono eliminate per eliminare l'immagine snapshot meno recente da un gruppo di snapshot o da un gruppo di coerenza snapshot.

A proposito di questa attività

È possibile eliminare una singola immagine snapshot oppure le immagini snapshot da gruppi di coerenza snapshot che hanno lo stesso timestamp di creazione. È inoltre possibile eliminare le immagini snapshot da un gruppo di snapshot.

Non è possibile eliminare un'immagine snapshot se non si tratta dell'immagine snapshot meno recente per il volume di base o il gruppo di coerenza snapshot associato.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **Snapshot Images** (immagini istantanee).
3. Selezionare l'immagine istantanea che si desidera eliminare e confermare che si desidera eseguire l'operazione.

   Se è stata selezionata un'immagine snapshot di un gruppo di coerenza snapshot, selezionare ciascun volume membro che si desidera eliminare e confermare che si desidera eseguire l'operazione.

4. Fare clic su **Delete** (Elimina).

Risultati

System Manager esegue le seguenti operazioni:

- Elimina l'immagine snapshot dall'array di storage.
- Rilascia la capacità riservata per il riutilizzo all'interno del gruppo di snapshot o del gruppo di coerenza di snapshot.
- Disattiva tutti i volumi snapshot associati esistenti per l'immagine snapshot eliminata.
- Dall'eliminazione di un gruppo di coerenza snapshot, sposta qualsiasi volume membro associato all'immagine snapshot eliminata in uno stato interrotto.

Gestire i gruppi di coerenza di Snapshot

Aggiungere un volume membro a un gruppo di coerenza snapshot

È possibile aggiungere un nuovo volume membro a un gruppo di coerenza snapshot esistente. Quando si aggiunge un nuovo volume membro, è necessario riservare la capacità anche per il volume membro.

Prima di iniziare

- Il volume membro deve essere ottimale.
- Il gruppo di coerenza snapshot deve avere un numero inferiore al numero massimo di volumi consentiti (come definito dalla configurazione).
- Ogni volume di capacità riservato deve avere le stesse impostazioni di sicurezza e Data Assurance (da) del volume membro associato.

A proposito di questa attività

È possibile aggiungere volumi standard o thin al gruppo di coerenza snapshot. Il volume di base può risiedere in un pool o in un gruppo di volumi.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Consistency Groups** (gruppi di coerenza snapshot).

   Viene visualizzata la tabella che mostra tutti i gruppi di coerenza snapshot associati all'array di storage.

3. Selezionare il gruppo di coerenza snapshot che si desidera modificare, quindi fare clic su **Aggiungi membri**.

   Viene visualizzata la finestra di dialogo Add Members (Aggiungi membri).

4. Selezionare i volumi membri che si desidera aggiungere, quindi fare clic su **Avanti**.

   Viene visualizzata la fase capacità riservata. La tabella Volume Candidate (candidato volume) visualizza solo i candidati che supportano la capacità riservata specificata.

5. Utilizzare la casella di selezione per allocare la capacità riservata per il volume membro. Eseguire una delle seguenti operazioni:
   - **Accettare le impostazioni predefinite.**

     Utilizzare questa opzione consigliata per assegnare la capacità riservata al volume membro con le

impostazioni predefinite.

- **Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati.**

  Se si modifica l'impostazione predefinita della capacità riservata, fare clic su **Refresh Candidates** (Aggiorna candidati) per aggiornare l'elenco dei candidati per la capacità riservata specificata.

  Allocare la capacità riservata utilizzando le seguenti linee guida.

  - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base, e di solito questa capacità è sufficiente.
  - La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nei volumi, alla quantità e alla durata della raccolta di immagini snapshot.

6. Fare clic su **fine** per aggiungere i volumi membro.

Rimuovere un volume membro da un gruppo di coerenza snapshot

È possibile rimuovere un volume membro da un gruppo di coerenza snapshot esistente.

A proposito di questa attività

Quando si rimuove un volume membro da un gruppo di coerenza snapshot, System Manager elimina automaticamente gli oggetti snapshot associati a tale volume membro.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **gruppi di coerenza Snapshot**.
3. Espandere il gruppo di coerenza snapshot che si desidera modificare selezionando il segno più (+) accanto.
4. Selezionare il volume membro che si desidera rimuovere, quindi fare clic su **Rimuovi**.
5. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Remove** (Rimuovi).

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutte le immagini snapshot e i volumi snapshot associati al volume membro.
- Elimina il gruppo di snapshot associato al volume membro.
- Il volume membro non viene altrimenti modificato o eliminato.

Modificare le impostazioni di un gruppo di coerenza snapshot

Modificare le impostazioni di un gruppo di coerenza snapshot quando si desidera modificarne il nome, le impostazioni di eliminazione automatica o il numero massimo di immagini snapshot consentite.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **gruppi di coerenza Snapshot**.

3. Selezionare il gruppo di coerenza snapshot che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Snapshot Consistency Group Setting.

4. Modificare le impostazioni del gruppo di coerenza snapshot in base alle esigenze.

   Dettagli del campo

Impostazione	Descrizione
Impostazioni del gruppo di coerenza Snapshot	Nome
È possibile modificare il nome del gruppo di coerenza snapshot.	Eliminazione automatica
Mantenere la casella di controllo selezionata se si desidera eliminare automaticamente le immagini snapshot dopo il limite specificato; utilizzare la casella di selezione per modificare il limite. Se si deseleziona questa casella di controllo, la creazione dell'immagine snapshot si interrompe dopo 32 immagini.	Limite dell'immagine Snapshot
È possibile modificare il numero massimo di immagini snapshot consentite per un gruppo di snapshot.	Calendario di Snapshot
Questo campo indica se una pianificazione è associata al gruppo di coerenza snapshot.	**Oggetti associati**
Volumi dei membri	È possibile visualizzare la quantità di volumi membri associati al gruppo di coerenza snapshot.

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

Elimina gruppo di coerenza snapshot

È possibile eliminare i gruppi di coerenza snapshot non più necessari.

Prima di iniziare

Verificare che le immagini per tutti i volumi membri non siano più necessarie per scopi di backup o test.

A proposito di questa attività

Questa operazione elimina tutte le immagini snapshot o i programmi associati al gruppo di coerenza snapshot.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Consistency Groups** (gruppi di coerenza snapshot).
3. Selezionare il gruppo di coerenza snapshot che si desidera eliminare, quindi selezionare **attività non comuni › Elimina**.

   Viene visualizzata la finestra di dialogo Confirm Delete Snapshot Consistency Group.

4. Confermare che si desidera eseguire questa operazione, quindi fare clic su **Delete** (Elimina).

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutte le immagini snapshot e i volumi snapshot esistenti dal gruppo di coerenza snapshot.
- Elimina tutte le immagini snapshot associate esistenti per ciascun volume membro nel gruppo di coerenza snapshot.
- Elimina tutti i volumi snapshot associati esistenti per ogni volume membro nel gruppo di coerenza snapshot.
- Elimina tutta la capacità riservata associata per ciascun volume membro nel gruppo di coerenza snapshot (se selezionato).

Gestire i volumi di snapshot

Convertire il volume Snapshot in modalità lettura/scrittura

È possibile convertire un volume snapshot di sola lettura o un volume snapshot di gruppo di coerenza snapshot in modalità di lettura/scrittura, se necessario.

Un volume Snapshot convertito in accessibile in lettura/scrittura contiene la propria capacità riservata. Questa capacità viene utilizzata per salvare eventuali modifiche successive apportate dall'applicazione host al volume di base senza influire sull'immagine snapshot di riferimento.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).

   Viene visualizzata la tabella Snapshot Volumes (volumi snapshot) che mostra tutti i volumi snapshot associati all'array di storage.

3. Selezionare il volume snapshot di sola lettura che si desidera convertire, quindi fare clic su **Convert to**

Read/Write (Converti in lettura/scrittura).

Viene visualizzata la finestra di dialogo Converti in lettura/scrittura con il passo **Reserve Capacity** attivato. La tabella Volume Candidate (candidato volume) visualizza solo i candidati che supportano la capacità riservata specificata.

4. Per allocare la capacità riservata per il volume snapshot di lettura/scrittura, eseguire una delle seguenti operazioni:
   - **Accettare le impostazioni predefinite** — utilizzare questa opzione consigliata per allocare la capacità riservata per il volume di snapshot con le impostazioni predefinite.
   - **Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati** — allocare la capacità riservata utilizzando le seguenti linee guida.
     - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume di base, e di solito questa capacità è sufficiente.
     - La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume.
5. Selezionare **Avanti** per rivedere o modificare le impostazioni.

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

6. Accettare o specificare le impostazioni per il volume di snapshot come appropriato, quindi selezionare **fine** per convertire il volume di snapshot.

   Dettagli del campo

Impostazione	Descrizione
Impostazioni di capacità riservate	Avvisami quando…

Modificare le impostazioni del volume per un volume di snapshot

È possibile modificare le impostazioni di un volume snapshot o di un volume snapshot di coerenza snapshot per rinominarlo, attivare o disattivare il caching SSD o modificare l'assegnazione di host, cluster host o LUN (Logical Unit Number).

Fasi

1. Selezionare **Storage › Snapshot**.
2. Fare clic sulla scheda **Snapshot Volumes**.
3. Selezionare il volume di snapshot che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo Snapshot Volume Settings (Impostazioni volume snapshot).

4. Visualizzare o modificare le impostazioni per il volume di snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Volume Snapshot	Nome
È possibile modificare il nome del volume di snapshot.	Assegnato a.
È possibile modificare l'assegnazione dell'host o del cluster host per il volume di snapshot.	LUN
È possibile modificare l'assegnazione del LUN per il volume snapshot.	Cache SSD
È possibile attivare/disattivare il caching in sola lettura sui dischi a stato solido (SSD).	**Oggetti associati**
Immagine Snapshot	È possibile visualizzare le immagini Snapshot associate al volume Snapshot. Un'immagine snapshot è una copia logica dei dati del volume, acquisita in un determinato momento. Come un punto di ripristino, le immagini Snapshot consentono di eseguire il rollback a un set di dati sicuramente funzionante. Sebbene l'host possa accedere all'immagine snapshot, non può leggerla o scriverla direttamente.
Volume di base	È possibile visualizzare il volume di base associato al volume di snapshot. Un volume di base è l'origine da cui viene creata un'immagine snapshot. Può essere un volume spesso o sottile e viene in genere assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un pool di dischi.
Gruppo di snapshot	È possibile visualizzare il gruppo di snapshot associato al volume di snapshot. Un gruppo di snapshot è una raccolta di immagini snapshot da un singolo volume di base.

Copia del volume Snapshot

È possibile eseguire un processo Copy Volume su un volume snapshot o su un volume snapshot di un gruppo di coerenza snapshot.

A proposito di questa attività

È possibile copiare un volume di snapshot nel volume di destinazione come avviene in una normale operazione Copy Volume. Tuttavia, i volumi Snapshot non possono rimanere online durante il processo di copia del volume.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).

   Viene visualizzata la tabella Snapshot Volumes (volumi snapshot) che mostra tutti i volumi snapshot associati all'array di storage.

3. Selezionare il volume di snapshot che si desidera copiare, quindi selezionare **Copy Volume** (Copia volume).

   Viene visualizzata la finestra di dialogo Copy Volume (Copia volume) che richiede di selezionare una destinazione.

4. Selezionare il volume di destinazione da utilizzare come destinazione della copia, quindi fare clic su **fine**.

Ricreare il volume di snapshot

È possibile ricreare un volume di snapshot o un volume di snapshot del gruppo di coerenza snapshot precedentemente disattivato. La ricreazione di un volume snapshot richiede meno tempo rispetto alla creazione di un nuovo volume.

Prima di iniziare

- Lo stato del volume snapshot deve essere ottimale o Disattivato.
- Tutti i volumi snapshot membri devono essere in uno stato Disabled (Disattivato) prima di poter ricreare il volume snapshot del gruppo di coerenza snapshot.

A proposito di questa attività

Non è possibile ricreare un singolo volume snapshot membro; è possibile ricreare solo il volume snapshot del gruppo di coerenza snapshot generale.

> Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot fa parte di una relazione di copia online, non è possibile eseguire l'opzione di ricreazione sul volume.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).

   Viene visualizzata la tabella Snapshot Volumes (volumi snapshot) che mostra tutti i volumi snapshot associati all'array di storage.

3. Selezionare il volume di snapshot che si desidera ricreare, quindi selezionare **Uncommon Tasks › Recreate**.

   Viene visualizzata la finestra di dialogo Recreate Snapshot Volume.

4. Selezionare una delle seguenti opzioni:
   - **Immagine snapshot esistente creata dal volume <name>**

Selezionare questa opzione per indicare un'immagine snapshot esistente da cui ricreare il volume di snapshot.

- **Una nuova immagine istantanea del volume <name>**

  Selezionare questa opzione per creare una nuova immagine snapshot da cui ricreare il volume snapshot.

5. Fare clic su **Ricrea**.

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutto `write` dati su qualsiasi volume di repository di snapshot associato.
- I parametri del volume snapshot o del volume snapshot Consistency Group Snapshot rimangono gli stessi dei parametri del volume precedentemente disattivati.
- Conserva i nomi originali del volume snapshot o del volume snapshot del gruppo di coerenza snapshot.

Disattiva il volume Snapshot

È possibile disattivare un volume snapshot o uno snapshot in un gruppo di coerenza snapshot quando non è più necessario o se si desidera interromperne temporaneamente l'utilizzo.

A proposito di questa attività

Utilizzare l'opzione Disable (Disattiva) se si verifica una delle seguenti condizioni:

- Il volume snapshot o il volume snapshot del gruppo di coerenza snapshot sono stati completati per il momento.
- Si intende ricreare il volume snapshot o il volume snapshot del gruppo di coerenza snapshot (designato come Read-write) in un secondo momento e conservare la capacità riservata associata in modo da non dover creare nuovamente.
- Si desidera aumentare le prestazioni dello storage array interrompendo l'attività di scrittura su un volume snapshot di lettura/scrittura.

Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot è designato come Read-write, questa opzione consente anche di interrompere qualsiasi ulteriore attività di scrittura nel volume di capacità riservata associato. Se si decide di ricreare il volume snapshot o il volume snapshot del gruppo di coerenza snapshot, è necessario scegliere un'immagine snapshot dallo stesso volume di base.

> Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot fa parte di una relazione di copia online, non è possibile eseguire l'opzione Disable (Disattiva) sul volume.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).

   System Manager visualizza tutti i volumi di snapshot associati all'array di storage.

3. Selezionare il volume di snapshot che si desidera disattivare, quindi selezionare **attività non comuni ›**

Disattiva.

4. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Disable** (Disattiva).

Risultati

- Il volume snapshot rimane associato al volume di base.
- Il volume Snapshot conserva il proprio World Wide Name (WWN).
- In caso di lettura/scrittura, il volume Snapshot conserva la capacità riservata associata.
- Il volume Snapshot conserva le assegnazioni e gli accessi degli host. Tuttavia, le richieste di lettura/scrittura non riescono.
- Il volume snapshot perde la sua associazione con l'immagine snapshot.

Elimina volume snapshot

È possibile eliminare un volume di snapshot o un volume di snapshot del gruppo di coerenza snapshot che non è più necessario per il backup o il test delle applicazioni software.

È inoltre possibile specificare se si desidera eliminare il volume di capacità riservata dello snapshot associato a `read-write` volume snapshot o mantenere il volume di capacità riservato snapshot come volume non assegnato.

A proposito di questa attività

L'eliminazione di un volume di base elimina automaticamente qualsiasi volume snapshot associato o volume snapshot del gruppo di coerenza. Non è possibile eliminare un volume snapshot che si trova in una copia di un volume con lo stato **in corso**.

Fasi

1. Selezionare **Storage › Snapshot**.
2. Selezionare la scheda **Snapshot Volumes** (volumi snapshot).

   System Manager visualizza tutti i volumi di snapshot associati all'array di storage.

3. Selezionare il volume di snapshot che si desidera eliminare, quindi selezionare **attività non comuni › Elimina**.
4. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

System Manager esegue le seguenti operazioni:

- Elimina tutti i volumi snapshot membri (per un volume snapshot di gruppo di coerenza snapshot).
- Rimuove tutte le assegnazioni host associate.

FAQ

Perché non vengono visualizzati tutti i volumi, gli host o i cluster di host?

I volumi Snapshot con un volume di base abilitato da non possono essere assegnati a un host che non supporta Data Assurance (da). È necessario disattivare il da sul volume di

base prima di poter assegnare un volume snapshot a un host che non supporta il da.

Prendere in considerazione le seguenti linee guida per l'host a cui si sta assegnando il volume di snapshot:

- Un host non è in grado di supportare da se è collegato all'array di storage attraverso un'interfaccia i/o che non è in grado di supportare da.
- Un cluster host non è in grado di supportare da se ha almeno un membro host che non è in grado di supportare da.

> Non è possibile disattivare il da su un volume associato a snapshot (gruppi di coerenza, gruppi di snapshot, immagini snapshot e volumi di snapshot), copie di volumi, e specchi. Tutti gli oggetti snapshot e capacità riservata associati devono essere cancellati prima che il da possa essere disattivato sul volume di base.

Che cos'è un'immagine snapshot?

Un'immagine snapshot è una copia logica del contenuto del volume, acquisita in un determinato momento. Le immagini Snapshot utilizzano uno spazio di storage minimo.

I dati dell'immagine Snapshot vengono memorizzati come segue:

- Quando viene creata un'immagine snapshot, questa corrisponde esattamente al volume di base. Dopo aver eseguito lo snapshot, quando si verifica la prima richiesta di scrittura per qualsiasi blocco o gruppo di blocchi sul volume di base, i dati originali vengono copiati nella capacità riservata dello snapshot prima che i nuovi dati vengano scritti nel volume di base.
- Le snapshot successive includono solo i blocchi di dati modificati dopo la creazione della prima immagine snapshot. Ogni successiva operazione copy-on-write salva i dati originali che stanno per essere sovrascritti sul volume di base nella capacità riservata dello snapshot prima che i nuovi dati vengano scritti nel volume di base.

Perché utilizzare le immagini Snapshot?

È possibile utilizzare le snapshot per proteggere e consentire il ripristino da perdite o danneggiamenti accidentali o dannosi dei dati.

Selezionare un volume di base o un gruppo di volumi di base, denominato gruppo di coerenza snapshot, quindi acquisire le immagini snapshot in uno o più dei seguenti modi:

- È possibile creare un'immagine snapshot di un singolo volume di base o di un gruppo di coerenza snapshot costituito da più volumi di base.
- È possibile acquisire snapshot manualmente o creare una pianificazione per un volume di base o un gruppo di coerenza snapshot per acquisire automaticamente immagini snapshot periodiche.
- È possibile creare un volume di snapshot accessibile dall'host di un'immagine snapshot.
- È possibile eseguire un'operazione di rollback per ripristinare un'immagine snapshot.

Il sistema conserva più immagini Snapshot come punti di ripristino che è possibile utilizzare per eseguire il rollback a set di dati sicuramente funzionanti in specifici momenti del tempo. La possibilità di eseguire il rollback offre protezione contro l'eliminazione accidentale dei dati e la corruzione dei dati.

Quali tipi di volumi possono essere utilizzati per le snapshot?

I volumi standard e i volumi thin sono gli unici tipi di volumi che è possibile utilizzare per memorizzare le immagini snapshot. Non è possibile utilizzare volumi non standard. Il volume di base può risiedere in un pool o in un gruppo di volumi.

Perché dovrei creare un gruppo di coerenza delle snapshot?

Si crea un gruppo di coerenza snapshot quando si desidera assicurarsi che le immagini snapshot vengano acquisite su più volumi contemporaneamente.

Ad esempio, un database costituito da più volumi che devono rimanere coerenti per scopi di recovery richiederebbe un gruppo di coerenza snapshot per raccogliere snapshot coordinate di tutti i volumi e utilizzarli per ripristinare l'intero database.

I volumi inclusi in un gruppo di coerenza snapshot sono denominati *volumi membro*.

È possibile eseguire le seguenti operazioni di snapshot su un gruppo di coerenza di snapshot:

- Creare un'immagine snapshot di un gruppo di coerenza snapshot per ottenere immagini simultanee dei volumi membri.
- Creare una pianificazione per il gruppo di coerenza snapshot in modo da acquisire automaticamente le immagini simultanee periodiche dei volumi membri.
- Creare un volume snapshot accessibile all'host di un'immagine di gruppo di coerenza snapshot.
- Eseguire un'operazione di rollback per un gruppo di coerenza snapshot.

Che cos'è un volume snapshot e quando ha bisogno di capacità riservata?

Un volume di snapshot consente all'host di accedere ai dati nell'immagine di snapshot. Il volume Snapshot contiene la propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine snapshot originale. Le immagini Snapshot non sono accessibili in lettura o scrittura agli host. Se si desidera leggere o scrivere nei dati di snapshot, creare un volume di snapshot e assegnarlo a un host.

È possibile creare due tipi di volumi di snapshot. Il tipo di volume di snapshot determina se utilizza la capacità riservata.

- **Sola lettura** — Un volume di snapshot creato in sola lettura fornisce a un'applicazione host l'accesso in lettura a una copia dei dati contenuti nell'immagine snapshot. Un volume snapshot di sola lettura non utilizza la capacità riservata.
- **Read-write** — Un volume di snapshot creato come Read-write consente di apportare modifiche al volume di snapshot senza influire sull'immagine di snapshot a cui si fa riferimento. Un volume di snapshot in lettura/scrittura utilizza la capacità riservata per memorizzare queste modifiche. È possibile convertire un volume snapshot di sola lettura in lettura/scrittura in qualsiasi momento.

Che cos'è un gruppo di snapshot?

Un gruppo di snapshot è un insieme di immagini snapshot point-in-time di un singolo volume di base associato.

System Manager organizza le immagini snapshot in *gruppi di snapshot*. I gruppi di snapshot non richiedono alcuna azione da parte dell'utente, ma è possibile regolare la capacità riservata di un gruppo di snapshot in qualsiasi momento. Inoltre, potrebbe essere richiesto di creare capacità riservata quando vengono soddisfatte le seguenti condizioni:

- Ogni volta che si crea uno snapshot di un volume di base che non dispone ancora di un gruppo di snapshot, System Manager crea automaticamente un gruppo di snapshot. In questo modo si crea una capacità riservata per il volume di base utilizzato per memorizzare le immagini snapshot successive.
- Ogni volta che si crea una pianificazione di snapshot per un volume di base, System Manager crea automaticamente un gruppo di snapshot.

Perché è necessario disattivare un volume di snapshot?

È possibile disattivare un volume di snapshot quando si desidera assegnare un volume di snapshot diverso all'immagine di snapshot. È possibile riservare il volume snapshot disattivato per un utilizzo successivo.

Se il volume snapshot o il volume snapshot del gruppo di coerenza non sono più necessari e non si intende ricrearlo in un secondo momento, eliminare il volume invece di disattivarlo.

Che cos'è lo stato Disabled?

Un volume di snapshot nello stato Disabled (Disattivato) non è attualmente assegnato a un'immagine di snapshot. Per attivare il volume di snapshot, è necessario utilizzare l'operazione di ricreazione per assegnare una nuova immagine di snapshot al volume di snapshot disattivato.

Le caratteristiche del volume di snapshot sono definite dall'immagine snapshot ad esso assegnata. L'attività di lettura/scrittura viene sospesa su un volume di snapshot in stato Disabled (Disattivato).

Perché dovrei sospendere un programma di snapshot?

Quando un programma viene sospeso, non vengono eseguite le creazioni dell'immagine snapshot pianificate. È possibile sospendere una pianificazione di snapshot per risparmiare spazio di storage e quindi riprendere le snapshot pianificate in un secondo momento.

Se non è necessaria la pianificazione snapshot, è necessario eliminarla invece di sospenderla.

Mirroring

Panoramica

Panoramica del mirroring asincrono

La funzione di mirroring asincrono offre un meccanismo basato su firmware a livello di controller per la replica dei dati tra uno storage array locale e uno storage array remoto.

Che cos'è il mirroring asincrono?

Mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato in base alla larghezza di banda. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, man mano che le risorse di rete diventano disponibili.

Il mirroring asincrono viene creato per volume ma gestito a livello di gruppo, consentendo di associare un volume remoto mirrorato distinto a qualsiasi volume primario di un determinato array di storage. Questo tipo di mirroring è ideale per soddisfare la richiesta di operazioni non-stop e, in generale, è molto più efficiente in termini di rete per i processi periodici.

Scopri di più:

- "Come funziona il mirroring asincrono"
- "Terminologia del mirroring asincrono"
- "Stato del mirror asincrono"
- "Proprietà del volume"
- "Modifica del ruolo di un gruppo di coerenza mirror"

Come si configura il mirroring asincrono?

È necessario utilizzare l'interfaccia di Unified Manager per eseguire la configurazione iniziale del mirroring tra gli array. Una volta configurato, è possibile gestire coppie mirrorate e gruppi di coerenza in System Manager.

Scopri di più:

- "Requisiti per l'utilizzo del mirroring asincrono"
- "Workflow per il mirroring asincrono di un volume"
- "Creazione di coppia asincrona con mirroring (in Unified Manager)"

Informazioni correlate

Scopri di più sui concetti relativi al mirroring asincrono:

- "Cosa occorre sapere prima di creare un gruppo di coerenza mirror"
- "Cosa occorre sapere prima di creare una coppia mirrorata"
- "Differenze tra il mirroring asincrono e il mirroring sincrono"

Panoramica del mirroring sincrono

La funzione Synchronous Mirroring offre una replica dei dati online e in tempo reale tra array di storage su una distanza remota.

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Che cos'è il mirroring sincrono?

Mirroring sincrono replica i volumi di dati in tempo reale per garantire la disponibilità continua. I controller degli array di storage gestiscono l'operazione di mirroring, che è trasparente per i computer host e le applicazioni software.

Questo tipo di mirroring è ideale per scopi di business continuity come il disaster recovery.

Scopri di più:

- "Come funziona il mirroring sincrono"
- "Terminologia del mirroring sincrono"
- "Stato del mirroring sincrono"
- "Proprietà del volume"
- "Cambiamento di ruolo tra i volumi in una coppia mirrorata"

Come si configura il mirroring sincrono?

È necessario utilizzare l'interfaccia di Unified Manager per eseguire la configurazione iniziale del mirroring tra gli array. Una volta configurato, è possibile gestire le coppie mirrorate in System Manager.

Scopri di più:

- "Requisiti per l'utilizzo del mirroring sincrono"
- "Workflow per il mirroring sincrono di un volume"
- "Creazione di una coppia sincrona con mirroring (in Unified Manager)"

Informazioni correlate

Scopri di più sui concetti relativi al mirroring sincrono:

- "Cosa occorre sapere prima di creare una coppia mirrorata"
- "Differenze tra il mirroring asincrono e il mirroring sincrono"

Concetti di Async

Come funziona il mirroring asincrono

Il mirroring asincrono copia i volumi di dati su richiesta o in base a una pianificazione, riducendo al minimo o evitando i downtime che potrebbero derivare da danneggiamento o perdita dei dati.

Il mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato in base alla larghezza di banda. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, man mano che le risorse di rete diventano disponibili.

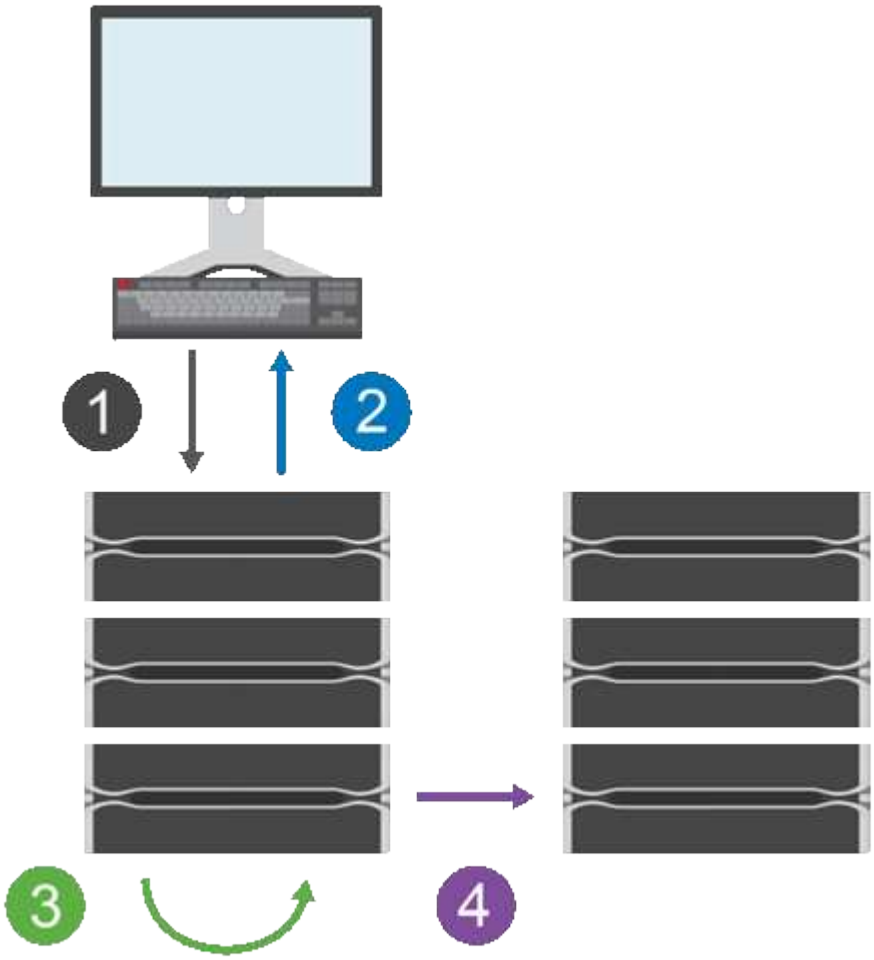
Questo tipo di mirroring è ideale per soddisfare la richiesta di operazioni non-stop e, in generale, è molto più efficiente in termini di rete per processi periodici, come backup e archiviazione. I motivi per cui si utilizza il mirroring asincrono sono i seguenti:

- Consolidamento del backup remoto.
- Protezione da disastri locali o su vasta area.
- Sviluppo e test delle applicazioni su un'immagine point-in-time dei dati live.

Sessione di mirroring asincrono

Il mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine. Il mirroring asincrono consente l'aggiornamento immediato del sito primario e l'aggiornamento del sito secondario in base alla larghezza di banda. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, man mano che le risorse di rete diventano disponibili.

Una sessione di mirroring asincrono attiva prevede quattro passaggi principali.



1. Un'operazione di scrittura viene eseguita per prima cosa sull'array di storage del volume primario.
2. Lo stato dell'operazione viene restituito all'host.
3. Tutte le modifiche apportate al volume principale vengono registrate e monitorate.
4. Tutte le modifiche vengono inviate all'array di storage del volume secondario come processo in background.

Questi passi vengono ripetuti in base agli intervalli di sincronizzazione definiti oppure i passi possono essere ripetuti manualmente se non sono definiti intervalli.

Il mirroring asincrono trasferisce i dati al sito remoto solo a intervalli prestabiliti, in modo che l'i/o locale non venga influenzato quasi tanto dalle connessioni di rete lente. Poiché questo trasferimento non è legato all'i/o locale, non influisce sulle prestazioni dell'applicazione. Pertanto, il mirroring asincrono può utilizzare connessioni più lente, come iSCSI, e funzionare su distanze più lunghe tra i sistemi storage locali e remoti.

Gli array di storage devono disporre di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).

Mirrorare gruppi di coerenza e coppie mirrorate

Si crea un gruppo di coerenza mirror per stabilire la relazione di mirroring tra l'array di storage locale e l'array di storage remoto. La relazione di mirroring asincrono consiste in una coppia mirrorata: Un volume primario su un array di storage e un volume secondario su un altro array di storage.

L'array di storage contenente il volume primario si trova in genere nel sito primario e serve gli host attivi. L'array di storage contenente il volume secondario si trova in genere in un sito secondario e contiene una replica dei dati. Il volume secondario in genere contiene una copia di backup dei dati e viene utilizzato per il disaster recovery.

Impostazioni di sincronizzazione

Quando si crea una coppia mirrorata, si definiscono anche la priorità di sincronizzazione e il criterio di risincronizzazione utilizzati dalla coppia mirrorata per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

Quando si crea un gruppo di coerenza mirror, si definiscono anche la priorità di sincronizzazione e il criterio di risincronizzazione per tutte le coppie mirrorate all'interno del gruppo. Le coppie mirrorate utilizzano la priorità di sincronizzazione e il criterio di risincronizzazione per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

I volumi primari e secondari di una coppia mirrorata possono non essere sincronizzati quando l'array di storage del volume primario non è in grado di scrivere i dati nel volume secondario. Questa condizione può essere causata dai seguenti problemi:

- Problemi di rete tra gli array di storage locali e remoti.
- Un volume secondario guasto.
- La sincronizzazione viene sospesa manualmente sulla coppia mirrorata.
- Conflitto di ruoli del gruppo mirror.

È possibile sincronizzare i dati sull'array di storage remoto manualmente o automaticamente.

Capacità riservata e mirroring asincrono

La capacità riservata viene utilizzata per tenere traccia delle differenze tra il volume primario e il volume secondario quando la sincronizzazione non avviene. Tiene inoltre traccia delle statistiche di sincronizzazione per ogni coppia mirrorata.

Ogni volume in una coppia mirrorata richiede una propria capacità riservata.

Configurazione e gestione

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Una volta attivato il mirroring, è possibile gestire le coppie mirrorate e le impostazioni di sincronizzazione in System Manager.

Terminologia del mirroring asincrono

Scopri come si applicano i termini del mirroring asincrono al tuo storage array.

Termine	Descrizione
Storage array locale	L'array di storage locale è l'array di storage su cui si sta agendo. Quando nella colonna Local role (ruolo locale) viene visualizzato **Primary**, l'array di storage contiene il volume che detiene il ruolo primario nella relazione mirror. Quando nella colonna ruolo locale viene visualizzato **secondario**, l'array di storage contiene il volume che contiene il ruolo secondario nella relazione mirror.
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un contenitore per una o più coppie mirrorate. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror.
Coppia mirrorata	Una coppia mirrorata è composta da due volumi, un volume primario e un volume secondario. Nel mirroring asincrono, una coppia mirrorata appartiene sempre a un gruppo di coerenza mirror. Le operazioni di scrittura vengono eseguite prima nel volume primario e poi replicate nel volume secondario. Ogni coppia mirrorata in un gruppo di coerenza mirror condivide le stesse impostazioni di sincronizzazione.
Volume primario	Il volume principale di una coppia mirrorata è il volume di origine da mirrorare.
Storage array remoto	L'array di storage remoto è generalmente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.
Cambiamento di ruolo	Il cambiamento di ruolo consiste nell'assegnare il ruolo primario al volume secondario e viceversa.
Volume secondario	Il volume secondario di una coppia mirrorata si trova in genere in un sito secondario e contiene una replica dei dati.
Sincronizzazione	La sincronizzazione avviene alla sincronizzazione iniziale tra lo storage array locale e lo storage array remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario non vengono sincronizzati dopo un'interruzione della comunicazione. Quando il collegamento di comunicazione funziona di nuovo, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Workflow per il mirroring asincrono di un volume

Il mirroring asincrono viene configurato utilizzando il seguente flusso di lavoro.

1. Eseguire la configurazione iniziale in Unified Manager:
    a. Selezionare lo storage array locale come origine per il trasferimento dei dati.

b. Creare o selezionare un gruppo di coerenza mirror esistente, che è un contenitore per il volume primario sull'array locale e il volume secondario sull'array remoto. I volumi primario e secondario sono denominati "coppia mirrorata". Se si crea il gruppo di coerenza mirror per la prima volta, specificare se si desidera eseguire sincronizzazioni manuali o pianificate.

c. Selezionare un volume primario dall'array di storage locale, quindi determinarne la capacità riservata. La capacità riservata è la capacità fisica allocata da utilizzare per l'operazione di copia.

d. Selezionare un array di storage remoto come destinazione del trasferimento, un volume secondario, quindi determinarne la capacità riservata.

e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.

2. Verificare l'avanzamento della sincronizzazione iniziale:

   a. In Unified Manager, avviare System Manager per l'array locale.

   b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale".

3. **Opzionale:** è possibile riprogrammare o eseguire manualmente i trasferimenti di dati successivi in System Manager. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.

> Poiché la replica asincrona è periodica, il sistema può consolidare i blocchi modificati e conservare la larghezza di banda della rete. L'impatto sul throughput di scrittura e sulla latenza di scrittura è minimo.

Requisiti per l'utilizzo del mirroring asincrono

Se si prevede di utilizzare il mirroring asincrono, tenere presenti i seguenti requisiti.

Unified Manager

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Unified Manager viene installato su un sistema host insieme al proxy dei servizi Web.

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Storage array

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.

- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.

Connessioni supportate

Il mirroring asincrono può utilizzare connessioni FC o iSCSI o entrambe per la comunicazione tra sistemi storage locali e remoti. Al momento della creazione di un gruppo di coerenza mirror, l'amministratore può selezionare FC o iSCSI per quel gruppo se entrambi sono connessi all'array di storage remoto. Non esiste un failover da un tipo di canale all'altro.

Il mirroring asincrono utilizza le porte i/o lato host dell'array di storage per trasferire i dati mirrorati dal lato primario al lato secondario.

- **Mirroring tramite interfaccia Fibre Channel (FC)**

  Ogni controller dello storage array dedica la porta host FC con il numero più alto alle operazioni di mirroring.

  Se il controller dispone di porte FC di base e porte FC HIC (host Interface Card), la porta con il numero più alto si trova su un HIC. Tutti gli host connessi alla porta dedicata vengono disconnessi e non vengono accettate richieste di accesso all'host. Le richieste di i/o su questa porta vengono accettate solo dai controller che partecipano alle operazioni di mirroring.

  Le porte di mirroring dedicate devono essere collegate a un ambiente fabric FC che supporti le interfacce del servizio di directory e del servizio di nomi. In particolare, FC-al e point-to-point non sono supportati come opzioni di connettività tra i controller che partecipano a relazioni mirror.

- **Mirroring tramite interfaccia iSCSI**

  A differenza di FC, iSCSI non richiede una porta dedicata. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare alcuna delle porte iSCSI front-end dello storage array per l'utilizzo con il mirroring asincrono; tali porte sono condivise sia per il traffico mirror asincrono che per le connessioni i/o host-to-array.

  Il controller mantiene un elenco di sistemi storage remoti con i quali l'iSCSI Initiator tenta di stabilire una sessione. La prima porta che stabilisce correttamente una connessione iSCSI viene utilizzata per tutte le comunicazioni successive con l'array di storage remoto. Se la comunicazione non riesce, viene tentata una nuova sessione utilizzando tutte le porte disponibili.

  Le porte iSCSI sono configurate a livello di array porta per porta. La comunicazione tra controller per la messaggistica di configurazione e il trasferimento dei dati utilizza le impostazioni globali, incluse le impostazioni per:

  - VLAN: Per comunicare, i sistemi locali e remoti devono avere la stessa impostazione VLAN
  - Porta di ascolto iSCSI
  - Frame jumbo
  - Priorità Ethernet

  > La comunicazione tra controller iSCSI deve utilizzare una porta di connessione host e non la porta Ethernet di gestione.

  Il mirroring asincrono utilizza le porte i/o lato host dell'array di storage per trasferire i dati mirrorati dal lato

primario al lato secondario. Poiché il mirroring asincrono è destinato a reti a latenza più elevata, a costi inferiori, le connessioni iSCSI (e quindi basate su TCP/IP) sono la soluzione ideale per l'IT. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare alcuna delle porte iSCSI front-end dell'array per l'utilizzo con il mirroring asincrono; tali porte sono condivise sia per il traffico mirror asincrono che per le connessioni i/o host-to-array

Volumi mirrorati candidati

- Il livello RAID, i parametri di caching e le dimensioni dei segmenti possono essere diversi sui volumi primario e secondario di una coppia di mirroring asincrono.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

- Il volume secondario deve essere grande almeno quanto il volume primario.
- Un volume può partecipare a una sola relazione di mirroring.
- I candidati al volume devono condividere le stesse funzionalità di sicurezza dei dati.
  - Se il volume primario è in grado di supportare FIPS, il volume secondario deve essere in grado di supportare FIPS.
  - Se il volume primario è compatibile con FDE, il volume secondario deve essere compatibile con FDE.
  - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Capacità riservata

- Un volume a capacità riservata è necessario per un volume primario e per un volume secondario in una coppia mirrorata per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono ulteriore capacità riservata, è necessario assicurarsi di disporre di capacità libera su entrambi gli array di storage nella relazione mirror.

Funzione di protezione del disco

- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono disporre di impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono utilizzare lo stesso tipo di disco. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

Stato del mirror asincrono

Lo stato del mirror definisce lo stato dei gruppi di coerenza mirror e delle coppie di volumi mirrorati.

Stato dei gruppi di coerenza mirror

Stato	Descrizione
Sincronizzazione (sincronizzazione iniziale)	L'avanzamento della sincronizzazione iniziale dei dati completata tra le coppie di volumi mirrorati. Durante una sincronizzazione iniziale, i volumi possono passare ai seguenti stati: Degraded/Failed/Optimal/Unknown (degradato/non riuscito/ottimale/sconosciuto).
Sincronizzazione (sincronizzazione a intervalli)	L'avanzamento della sincronizzazione periodica dei dati completata tra le coppie di volumi mirrorati.
Sistema sospeso	Sincronizzazione dei dati sospesi dal sistema di storage su tutte le coppie mirrorate a livello di gruppo di coerenza mirror. Almeno una coppia mirrorata nel gruppo di coerenza mirror si trova in uno stato interrotto o non riuscito.
Utente sospeso	Sincronizzazione dei dati sospesi dall'utente su tutte le coppie mirrorate a livello di gruppo di coerenza mirror. Questo stato consente di ridurre l'impatto delle performance sull'applicazione host che potrebbe verificarsi mentre i dati modificati sull'array di storage locale vengono copiati nell'array di storage remoto.
In pausa	Il processo di sincronizzazione dei dati è stato temporaneamente sospeso a causa di un errore di accesso all'array di storage remoto.
Orfano	Un volume di coppia di mirroring orfano esiste quando un volume membro in un gruppo di mirror di coerenza è stato rimosso da un lato del gruppo di mirror di coerenza (lato primario o lato secondario) ma non dall'altro lato. I volumi di coppia di mirroring orfani vengono rilevati quando viene ripristinata la comunicazione tra array e i due lati della configurazione di mirroring riconciliano i parametri di mirroring. È possibile rimuovere una coppia mirrorata per correggere uno stato di coppia mirrorata orfana.
Cambiamento di ruolo in sospeso/in corso	Una modifica di ruolo tra i gruppi di coerenza mirror è in sospeso o in corso. La modifica dell'inversione del ruolo (in un ruolo primario o secondario) influisce su tutte le coppie mirrorate asincrone all'interno del gruppo di coerenza del mirror selezionato. È possibile annullare una modifica del ruolo in sospeso, ma non una modifica del ruolo in corso.

Stato	Descrizione
Conflitto di ruolo	Si è verificato un conflitto di ruolo tra gruppi di coerenza mirror a causa di un problema di comunicazione tra l'array di storage locale e l'array di storage remoto durante un'operazione di modifica del ruolo. Una volta risolto il problema di comunicazione, si verifica un conflitto di ruolo. Utilizzare Recovery Guru per risolvere questo errore. Una promozione forzata non è consentita quando si risolve un conflitto di ruolo.

Stato delle coppie mirrorate

Lo stato di una coppia mirrorata indica se i dati sul volume primario e sul volume secondario sono sincronizzati.

Stato	Descrizione
Sincronizzazione	L'avanzamento della sincronizzazione iniziale o periodica dei dati completata tra le coppie mirrorate. Esistono due tipi di sincronizzazione: La sincronizzazione iniziale e la sincronizzazione periodica. L'avanzamento iniziale della sincronizzazione viene visualizzato anche nella finestra di dialogo Long Running Operations.
Ottimale	I volumi nella coppia mirrorata sono sincronizzati, il che indica che la connessione tra gli array di storage è operativa e che ciascun volume si trova nella condizione operativa desiderata.
Incompleto	La coppia di mirroring asincrono è incompleta sull'array di storage remoto perché la sequenza di creazione della coppia di mirroring è stata avviata su un array di storage non supportato da System Manager e la coppia di mirroring non è stata completata sul secondario. Il processo di creazione della coppia mirrorata viene completato quando un volume viene aggiunto al gruppo di coerenza mirror sull'array di storage remoto. Questo volume diventa il volume secondario nella coppia di mirroring asincrono. La coppia mirrorata viene completata automaticamente se lo storage array remoto viene gestito da System Manager.
Non riuscito	L'operazione di mirroring asincrono non è in grado di funzionare normalmente a causa di un errore nei volumi primari, secondari o nella capacità riservata del mirror.

Stato	Descrizione
Orfano	Un volume di coppia di mirroring orfano esiste quando un volume membro in un gruppo di mirror di coerenza è stato rimosso da un lato del gruppo di mirror di coerenza (lato primario o lato secondario) ma non dall'altro lato. I volumi di coppia di mirroring orfani vengono rilevati quando viene ripristinata la comunicazione tra i due array di storage e i due lati della configurazione di mirroring riconciliano i parametri di mirroring. È possibile rimuovere una coppia mirrorata per correggere uno stato di coppia mirrorata orfana.
Interrotto	La coppia mirrorata si trova in uno stato di arresto perché il gruppo di coerenza mirror si trova in uno stato di sospensione del sistema.

Proprietà del volume

È possibile modificare il proprietario del controller preferito in una coppia mirrorata.

Se il volume primario della coppia mirrorata è di proprietà del controller A, anche il volume secondario sarà di proprietà del controller A dell'array di storage remoto. La modifica del proprietario del volume primario modifica automaticamente il proprietario del volume secondario per garantire che entrambi i volumi siano di proprietà dello stesso controller. Le attuali modifiche di proprietà sul lato primario si propagano automaticamente alle corrispondenti modifiche di proprietà correnti sul lato secondario.

Ad esempio, un volume primario è di proprietà del controller A, quindi si cambia il proprietario del controller in controller B. In questo caso, la successiva scrittura remota modifica il proprietario del controller del volume secondario da controller A a B. Poiché le modifiche alla proprietà dei controller sul lato secondario sono controllate dal lato primario, non richiedono alcun intervento speciale da parte dell'amministratore dello storage.

Il controller viene ripristinato

Una reimpostazione del controller determina una modifica della proprietà del volume sul lato primario, dal proprietario del controller preferito al controller alternativo nell'array di storage.

A volte, una scrittura remota viene interrotta da un ripristino del controller o da un ciclo di alimentazione dello storage array prima di poter essere scritta sul volume secondario. In questo caso, il controller non deve eseguire una sincronizzazione completa della coppia mirrorata.

Quando una scrittura remota è stata interrotta durante un ripristino del controller, il nuovo proprietario del controller sul lato primario legge le informazioni memorizzate in un file di log nel volume di capacità riservata del proprietario del controller preferito. Il nuovo proprietario del controller copia quindi i blocchi di dati interessati dal problema dal volume primario al volume secondario, eliminando la necessità di una sincronizzazione completa dei volumi mirrorati.

Modifica del ruolo di un gruppo di coerenza mirror

È possibile modificare il ruolo tra coppie mirrorate in un gruppo di coerenza mirror. A tale scopo, è possibile eseguire il declassamento del gruppo di coerenza del mirror primario al ruolo secondario o promuovere il gruppo di coerenza del mirror secondario al ruolo

primario.

Esaminare le seguenti informazioni sull'operazione di cambiamento di ruolo:

- La modifica del ruolo influisce su tutte le coppie mirrorate all'interno del gruppo di coerenza mirror selezionato.
- Quando un gruppo di coerenza mirror viene retrocesso al ruolo secondario, tutte le coppie mirrorate all'interno di quel gruppo di coerenza mirror vengono anche retrocesse al ruolo secondario e viceversa.
- Quando il gruppo di coerenza del mirror primario viene retrocesso nel ruolo secondario, gli host assegnati ai volumi membri all'interno di tale gruppo non hanno più accesso in scrittura.
- Quando un gruppo di coerenza mirror viene promosso al ruolo primario, tutti gli host che accedono ai volumi membri all'interno di tale gruppo sono ora in grado di scriverli.
- Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, è possibile forzare la modifica del ruolo nell'array di storage locale.

Forza il cambiamento di ruolo

È possibile forzare una modifica del ruolo tra gruppi di coerenza mirror quando un problema di comunicazione tra l'array di storage locale e l'array di storage remoto impedisce la promozione dei volumi membri all'interno del gruppo di coerenza mirror secondario o la demozione dei volumi membri all'interno della coerenza mirror primaria gruppo.

È possibile forzare il gruppo di coerenza mirror sul lato secondario a passare al ruolo primario. Quindi, l'host di ripristino può accedere ai volumi membri promossi di recente all'interno del gruppo di coerenza mirror e le operazioni di business possono continuare.

Quando è consentita e non è consentita una promozione forzata?

La promozione forzata di un gruppo di coerenza mirror è consentita solo se tutti i volumi membri del gruppo di coerenza mirror sono stati sincronizzati e dispongono di punti di ripristino coerenti.

La promozione forzata di un gruppo di coerenza mirror non è consentita nelle seguenti condizioni:

- Tutti i volumi membri di un gruppo di coerenza mirror sono in fase di sincronizzazione iniziale.
- I volumi membri di un gruppo di coerenza mirror non dispongono di un'immagine point-in-time del punto di ripristino (ad esempio, a causa di un errore di capacità riservata completa).
- Il gruppo di coerenza mirror non contiene volumi membri.
- Il gruppo di coerenza mirror si trova negli stati Failed (non riuscito), role-Change-Pending (in attesa di modifica ruolo) o role-Change-in-Progress (Modifica in corso ruolo) oppure in caso di guasto di uno qualsiasi dei volumi membri associati o dei volumi di capacità riservati.

Conflitto di ruoli del gruppo mirror

Quando viene risolto un problema di comunicazione tra gli array di storage locali e remoti, si verifica una condizione di conflitto di ruolo di Mirror Group. Utilizzare Recovery Guru per risolvere questo errore. Una promozione forzata non è consentita quando si risolve un conflitto a doppio ruolo.

Per evitare la condizione di conflitto di ruolo del gruppo di mirroring e le successive fasi di ripristino, attendere che la connessione tra gli array di storage sia operativa per forzare la modifica del ruolo.

Stato in corso del cambiamento di ruolo

Se due array di storage in una configurazione di mirroring si disconnettono e il lato primario di un gruppo di coerenza di mirroring viene sottoposto a demartazione forzata su un ruolo secondario e il lato secondario di un gruppo di coerenza di mirroring viene promosso forzatamente a un ruolo primario, Quindi, quando viene ripristinata la comunicazione, i gruppi di coerenza mirror su entrambi gli array di storage vengono posizionati nello stato role-Change-in-Progress.

Il sistema completa il processo di modifica del ruolo trasferendo i registri delle modifiche, eseguendo una nuova sincronizzazione, impostando lo stato del gruppo di coerenza mirror su uno stato operativo normale e continuando con le sincronizzazioni periodiche.

Concetti di sincronizzazione

Come funziona il mirroring sincrono

Il mirroring sincrono replica i volumi di dati in tempo reale per garantire una disponibilità continua.

> Il mirroring sincrono non è disponibile sull'array di storage EF600 o EF300.

Il mirroring sincrono raggiunge un obiettivo RPO (Recovery Point Objective) pari a zero dati persi grazie alla disponibilità di una copia dei dati importanti in caso di disastro su uno dei due array di storage. La copia è identica ai dati di produzione in ogni momento perché ogni volta che viene eseguita una scrittura nel volume primario, viene eseguita una scrittura nel volume secondario. L'host non riceve una conferma che la scrittura è riuscita fino a quando il volume secondario non viene aggiornato correttamente con le modifiche apportate sul volume primario.

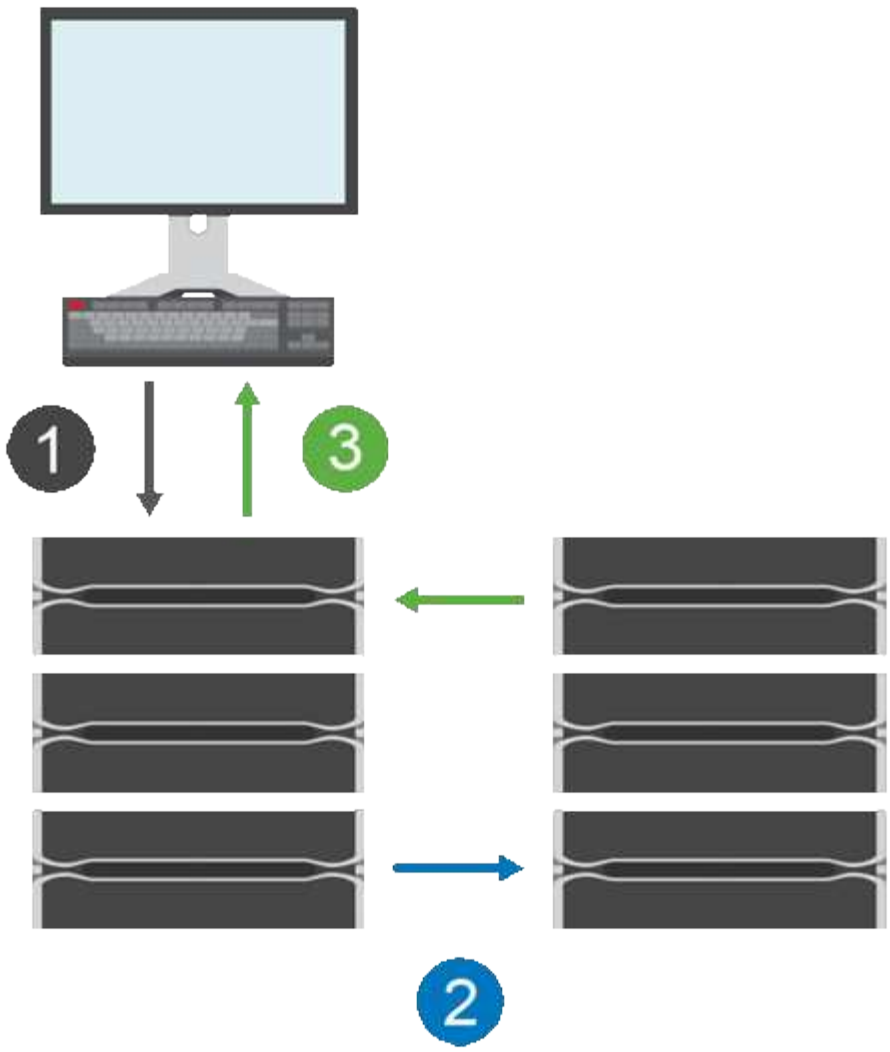
Questo tipo di mirroring è ideale per scopi di business continuity come il disaster recovery.

Relazione di mirroring sincrono

Una relazione di mirroring sincrono è costituita da un volume primario e da un volume secondario su storage array separati. L'array di storage contenente il volume primario si trova in genere nel sito primario e serve gli host attivi. L'array di storage contenente il volume secondario si trova in genere in un sito secondario e contiene una replica dei dati. Il volume secondario viene utilizzato se l'array di storage del volume primario non è disponibile a causa, ad esempio, di un'interruzione dell'alimentazione completa, di un incendio o di un guasto hardware nel sito primario.

Sessione di mirroring sincrono

Il processo di configurazione del mirroring sincrono prevede la configurazione dei volumi in coppie. Dopo aver creato una coppia mirrorata, costituita da un volume primario su un array di storage e da un volume secondario su un altro array di storage, è possibile avviare il mirroring sincrono. Di seguito sono illustrate le fasi del mirroring sincrono.



1. Una scrittura proviene dall'host.
2. La scrittura viene inviata al volume primario, propagata al sistema remoto e quindi inviata al volume secondario.
3. L'array di storage del volume primario invia un messaggio di completamento i/o al sistema host *dopo* che entrambe le operazioni di scrittura sono state completate correttamente.

La capacità riservata viene utilizzata per registrare le informazioni sulla richiesta di scrittura in entrata da un host.

Quando l'attuale proprietario del controller del volume primario riceve una richiesta di scrittura da un host, il controller registra prima le informazioni sulla scrittura nella capacità riservata del volume primario. Quindi, scrive i dati nel volume primario. Quindi, il controller avvia un'operazione di scrittura remota per copiare i blocchi di dati interessati nel volume secondario dell'array di storage remoto.

Poiché l'applicazione host deve attendere che la scrittura avvenga sull'array di storage locale e sulla rete dell'array di storage remoto, È necessaria una connessione molto rapida tra lo storage array locale e lo storage array remoto per mantenere la relazione di mirroring senza ridurre eccessivamente le performance di i/o locale.

Disaster recovery

Il mirroring sincrono mantiene una copia dei dati fisicamente distanti dal sito in cui risiedono i dati. Se si verifica

un disastro nel sito primario, ad esempio un'interruzione dell'alimentazione o un flusso, è possibile accedere rapidamente ai dati dal sito secondario.

Il volume secondario non è disponibile per ospitare le applicazioni durante l'operazione di mirroring sincrono, pertanto, in caso di disastro nell'array di storage locale, è possibile eseguire il failover nell'array di storage remoto. Per eseguire il failover, promuovere il volume secondario al ruolo primario. Quindi, l'host di ripristino può accedere al volume appena promosso e le operazioni di business possono continuare.

Impostazioni di sincronizzazione

Quando si crea una coppia mirrorata, si definiscono anche la priorità di sincronizzazione e il criterio di risincronizzazione utilizzati dalla coppia mirrorata per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

Se il collegamento di comunicazione tra i due array di storage smette di funzionare, gli host continuano a ricevere riconoscimenti dall'array di storage locale, impedendo una perdita di accesso. Quando il collegamento di comunicazione funziona di nuovo, i dati non replicati possono essere risincronati automaticamente o manualmente nell'array di storage remoto.

La risincronizzazione automatica dei dati dipende dalla policy di risincronizzazione della coppia mirrorata. Un criterio di risincronizzazione automatica consente alla coppia mirrorata di risincronizzarsi automaticamente quando il collegamento funziona di nuovo. Un criterio di risincronizzazione manuale richiede di riprendere manualmente la sincronizzazione dopo un problema di comunicazione. La risincronizzazione manuale è la policy consigliata.

È possibile modificare le impostazioni di sincronizzazione per una coppia mirrorata solo sull'array di storage che contiene il volume primario.

Dati non sincronizzati

I volumi primario e secondario non vengono sincronizzati quando l'array di storage del volume primario non è in grado di scrivere i dati nel volume secondario. Ciò può essere causato dai seguenti problemi:

- Problemi di rete tra gli array di storage locali e remoti
- Un volume secondario guasto
- La sincronizzazione viene sospesa manualmente sulla coppia mirrorata

Coppia mirrorata orfana

Un volume di coppia di mirroring orfano esiste quando un volume membro è stato rimosso da un lato (lato primario o secondario) ma non dall'altro.

I volumi di coppia di mirroring orfani vengono rilevati quando viene ripristinata la comunicazione tra array e i due lati della configurazione di mirroring riconciliano i parametri di mirroring.

È possibile rimuovere una coppia mirrorata per correggere uno stato di coppia mirrorata orfana.

Configurazione e gestione

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Una volta attivato il mirroring, è possibile gestire le coppie mirrorate e le impostazioni di sincronizzazione in System Manager.

Terminologia del mirroring sincrono

Scopri in che modo i termini del mirroring sincrono si applicano al tuo storage array.

Termine	Descrizione
Storage array locale	L'array di storage locale è l'array di storage su cui si sta agendo. Quando nella colonna Local role (ruolo locale) viene visualizzato **Primary**, l'array di storage contiene il volume che detiene il ruolo primario nella relazione mirror. Quando nella colonna ruolo locale viene visualizzato **secondario**, l'array di storage contiene il volume che contiene il ruolo secondario nella relazione mirror.
Coppia mirrorata	Una coppia mirrorata è composta da due volumi, un volume primario e un volume secondario.
Volume primario	Il volume principale di una coppia mirrorata è il volume di origine da mirrorare.
Recovery Point Objective (RPO) (obiettivo punto di ripristino)	Recovery Point Objective (RPO) rappresenta un obiettivo che indica la differenza considerata accettabile tra il volume primario e il volume secondario in una coppia mirrorata. Un RPO pari a zero indica che non è possibile tollerare alcuna differenza tra il volume primario e il volume secondario. Un RPO maggiore di zero indica che il volume secondario è meno attuale o è indietro rispetto al volume primario.
Storage array remoto	L'array di storage remoto è generalmente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host.
Cambiamento di ruolo	Il cambiamento di ruolo consiste nell'assegnare il ruolo primario al volume secondario e viceversa.
Volume secondario	Il volume secondario di una coppia mirrorata si trova in genere in un sito secondario e contiene una replica dei dati.
Sincronizzazione	La sincronizzazione avviene alla sincronizzazione iniziale tra lo storage array locale e lo storage array remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario non vengono sincronizzati dopo un'interruzione della comunicazione. Quando il collegamento di comunicazione funziona di nuovo, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Workflow per il mirroring sincrono di un volume

Il mirroring sincrono viene configurato utilizzando il seguente flusso di lavoro.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare un array di storage locale come origine per il trasferimento dei dati.
   b. Selezionare un volume primario dall'array di storage locale.
   c. Selezionare un array di storage remoto come destinazione per il trasferimento dei dati, quindi selezionare un volume secondario.
   d. Selezionare le priorità di sincronizzazione e risincronizzazione.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.
2. Verificare l'avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avviare System Manager per l'array locale.
   b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale". I due array tentano di rimanere sincronizzati con le normali operazioni. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.
3. **Opzionale:** è possibile modificare le impostazioni di sincronizzazione in System Manager.

> Poiché la replica sincrona è continua, il collegamento di replica tra i due siti deve fornire funzionalità di larghezza di banda sufficienti.

Requisiti per l'utilizzo del mirroring sincrono

Se si prevede di utilizzare il mirroring sincrono, tenere presenti i seguenti requisiti.

Unified Manager

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Unified Manager viene installato su un sistema host insieme al proxy dei servizi Web.

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Storage array

> Il mirroring sincrono non è disponibile sull'array di storage EF300 o EF600.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).

- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel.

Connessioni supportate

La comunicazione per il mirroring sincrono è supportata solo sui controller con porte host Fibre Channel (FC).

Il mirroring sincrono utilizza la porta host con il numero più alto su ciascun controller sia sull'array di storage locale che sull'array di storage remoto. La porta host 4 dell'HBA (Controller host Bus Adapter) è in genere riservata alla trasmissione di dati mirror.

Volumi mirrorati candidati

- Il livello RAID, i parametri di caching e le dimensioni dei segmenti possono essere diversi sui volumi primario e secondario di una coppia di mirroring sincrono.
- I volumi primari e secondari di una coppia sincrona con mirroring devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Il volume secondario deve essere grande almeno quanto il volume primario.
- Solo il volume primario può avere snapshot associati e/o essere il volume di origine o di destinazione in un'operazione di copia del volume.
- Un volume può partecipare a una sola relazione di mirroring.
- Esistono limiti al numero di volumi supportati in un determinato array di storage. Assicurarsi che il numero di volumi configurati sull'array di storage sia inferiore al limite supportato. Quando il mirroring sincrono è attivo, i due volumi di capacità riservata creati vengono conteggiati rispetto al limite di volume.

Capacità riservata

- La capacità riservata è necessaria per un volume primario e per un volume secondario per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- I volumi di capacità riservati vengono creati automaticamente quando viene attivato il mirroring sincrono. Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono capacità riservata, è necessario assicurarsi di disporre di una capacità libera sufficiente su entrambi gli array di storage che partecipano alla relazione di mirroring sincrono.

Funzione di protezione del disco

- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono disporre di impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono utilizzare lo stesso tipo di disco. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
  - Se il volume primario utilizza dischi FDE (Full Disk Encryption), il volume secondario deve utilizzare dischi FDE.
  - Se il volume primario utilizza dischi convalidati FIPS (Federal Information Processing Standards 140-2), il volume secondario deve utilizzare dischi validati FIPS 140-2.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

Stato del mirroring sincrono

Lo stato di una coppia sincrona con mirroring indica se i dati sul volume primario e sul volume secondario sono sincronizzati. Lo stato di un mirror è indipendente dallo stato dei componenti dei volumi nella coppia mirrorata.

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Le coppie sincrone mirrorate possono avere uno dei seguenti stati:

- **Ottimale**

  Indica che i volumi nella coppia mirrorata sono sincronizzati, il che significa che la connessione fabric tra gli array di storage è operativa e ciascun volume si trova nella condizione operativa desiderata.

- **Sincronizzazione**

  Mostra l'avanzamento della sincronizzazione dei dati tra le coppie mirrorate. Questo stato viene visualizzato anche durante la sincronizzazione iniziale.

  Dopo un'interruzione del collegamento di comunicazione, solo i blocchi di dati modificati sul volume primario durante l'interruzione del collegamento vengono copiati nel volume secondario.

- **Non sincronizzato**

  Indica che l'array di storage del volume primario non è in grado di scrivere i dati in entrata nell'array remoto. L'host locale può continuare a scrivere nel volume primario, ma non vengono eseguite operazioni di scrittura remote. Condizioni diverse possono impedire all'array di storage del volume primario di scrivere i dati in entrata nel volume secondario, ad esempio:

  - Il volume secondario non è accessibile.
  - L'array di storage remoto non è accessibile.
  - La connessione fabric tra gli array di storage non è accessibile.
  - Impossibile aggiornare il volume secondario con un nuovo WWID (World Wide Identifier).

- **Sospeso**

  Indica che l'operazione di mirroring sincrono è stata sospesa dall'utente. Quando una coppia mirrorata viene sospesa, non viene effettuato alcun tentativo di contatto con il volume secondario. Tutte le scritture nel volume primario vengono registrate in modo persistente nei volumi di capacità riservati del mirror.

- **Non riuscito**

  Indica che l'operazione di mirroring sincrono non è in grado di funzionare normalmente a causa di un errore del volume primario, del volume secondario o della capacità riservata del mirror.

Proprietà del volume

È possibile modificare il proprietario del controller preferito in una coppia mirrorata.

> Questa funzione non è disponibile per il mirroring sincrono sul sistema storage EF600 o EF300.

Se il volume primario della coppia mirrorata è di proprietà del controller A, anche il volume secondario sarà di proprietà del controller A dell'array di storage remoto. La modifica del proprietario del volume primario modifica automaticamente il proprietario del volume secondario per garantire che entrambi i volumi siano di proprietà dello stesso controller. Le attuali modifiche di proprietà sul lato primario si propagano automaticamente alle corrispondenti modifiche di proprietà correnti sul lato secondario.

Ad esempio, un volume primario è di proprietà del controller A, quindi si cambia il proprietario del controller in controller B. In questo caso, la successiva scrittura remota modifica il proprietario del controller del volume secondario da controller A a B. Poiché le modifiche alla proprietà dei controller sul lato secondario sono controllate dal lato primario, non richiedono alcun intervento speciale da parte dell'amministratore dello storage.

Il controller viene ripristinato

Una reimpostazione del controller determina una modifica della proprietà del volume sul lato primario, dal proprietario del controller preferito al controller alternativo nell'array di storage.

A volte, una scrittura remota viene interrotta da un ripristino del controller o da un ciclo di alimentazione dello storage array prima di poter essere scritta sul volume secondario. In questo caso, il controller non deve eseguire una sincronizzazione completa della coppia mirrorata.

Quando una scrittura remota è stata interrotta durante un ripristino del controller, il nuovo proprietario del controller sul lato primario legge le informazioni memorizzate in un file di log nel volume di capacità riservata del proprietario del controller preferito. Il nuovo proprietario del controller copia quindi i blocchi di dati interessati dal problema dal volume primario al volume secondario, eliminando la necessità di una sincronizzazione completa dei volumi mirrorati.

Cambiamento di ruolo tra i volumi in una coppia mirrorata

È possibile modificare il ruolo tra i volumi in una coppia mirrorata. A tale scopo, è possibile eseguire il demoting del volume primario al ruolo secondario o promuovere il volume secondario al ruolo primario.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Esaminare le seguenti informazioni sull'operazione di cambiamento di ruolo:

- Quando un volume primario viene retrocesso al ruolo secondario, il volume secondario in quella coppia mirrorata viene promosso al ruolo primario e viceversa.
- Quando il volume primario viene deportato al ruolo secondario, gli host assegnati a quel volume non dispongono più dell'accesso in scrittura.
- Quando il volume secondario viene promosso al ruolo primario, tutti gli host che accedono a quel volume sono ora in grado di scriverlo.
- Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, è possibile forzare la modifica del ruolo nell'array di storage locale.

Forza il cambiamento di ruolo

È possibile forzare una modifica del ruolo tra i volumi in una coppia mirrorata quando un problema di comunicazione tra l'array di storage locale e l'array di storage remoto impedisce la promozione del volume secondario o la riduzione del volume primario.

È possibile forzare il passaggio del volume sul lato secondario al ruolo primario. Quindi, l'host di ripristino può

accedere al volume appena promosso e le operazioni di business possono continuare.

> Una volta ripristinato l'array di storage remoto e risolti eventuali problemi di comunicazione, si verifica una condizione di conflitto tra mirroring sincrono e volume primario. Le fasi di ripristino includono la risincronizzazione dei volumi. Utilizzare Recovery Guru per risolvere questo errore.

Quando è consentita e non è consentita una promozione forzata?

La promozione forzata di un volume in una coppia mirrorata non è consentita nelle seguenti condizioni:

- Tutti i volumi di una coppia mirrorata sono in fase di sincronizzazione iniziale.
- La coppia mirrorata si trova negli stati Failed (non riuscito), role-Change-Pending (in attesa di modifica ruolo) o role-Change-in-Progress (Modifica in corso ruolo) o se uno dei volumi di capacità riservati associati presenta un errore.

Stato in corso del cambiamento di ruolo

Se due array di storage in una configurazione di mirroring si disconnettono e il volume primario di una coppia mirrorata viene forzato a un ruolo secondario e il volume secondario di una coppia mirrorata viene forzato a un ruolo primario, Quindi, quando viene ripristinata la comunicazione, i volumi su entrambi gli array di storage vengono posizionati nello stato role-Change-in-progress.

Il sistema completerà il processo di modifica del ruolo trasferendo i registri delle modifiche, eseguendo una nuova sincronizzazione, ripristinando lo stato della coppia mirrorata su uno stato operativo normale e continuando con le sincronizzazioni.

Gestire i gruppi di coerenza mirror asincrone

Verificare la comunicazione per i gruppi di coerenza mirror

È possibile verificare il collegamento di comunicazione per diagnosticare eventuali problemi di comunicazione tra l'array di storage locale e l'array di storage remoto associato a un gruppo di coerenza mirror.

Prima di iniziare

Il gruppo di coerenza mirror che si desidera testare deve esistere sugli array di storage locali e remoti.

A proposito di questa attività

È possibile eseguire quattro diversi test:

- **Connettività** — verifica che i due controller dispongano di un percorso di comunicazione. Il test di connettività invia un messaggio inter-array tra gli array di storage, quindi convalida l'esistenza del gruppo di coerenza mirror corrispondente sull'array di storage remoto. Inoltre, convalida che i volumi membri del gruppo di coerenza mirror sull'array di storage remoto corrispondano ai volumi membri del gruppo di coerenza mirror sull'array di storage locale.
- **Latency** — Invia un comando SCSI Test Unit a ciascun volume mirrorato dell'array di storage remoto associato al gruppo di coerenza mirror per verificare la latenza minima, media e massima.
- **Bandwidth** — Invia due messaggi tra array all'array di storage remoto per verificare la larghezza di banda minima, media e massima, nonché la velocità di collegamento negoziata della porta sull'array che esegue il test.
- **Port Connections** — Mostra la porta utilizzata per il mirroring sull'array di storage locale e la porta che

riceve i dati mirrorati sull'array di storage remoto.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups** (gruppi di coerenza mirror), quindi selezionare il gruppo di coerenza mirror che si desidera sottoporre a test.
3. Selezionare **Test di comunicazione**.

   Viene visualizzata la finestra di dialogo Test di comunicazione.

4. Selezionare uno o più test di comunicazione da eseguire tra gli array storage locali e remoti associati al gruppo di coerenza mirror selezionato, quindi fare clic su **Test**.
5. Esaminare le informazioni visualizzate nella finestra dei risultati.

Stato del test di comunicazione	Descrizione
Normale senza errori	Il gruppo di coerenza mirror sta comunicando correttamente.
Stato superato (ma non normale)	Verificare i possibili problemi di rete o di connessione e riprovare a eseguire il test.
Stato di errore	Viene indicato il motivo del guasto. Consultare il Recovery Guru per risolvere il problema.
Errore di connessione alla porta	Il motivo potrebbe essere che lo storage array locale non è collegato o che non è possibile contattare lo storage array remoto. Consultare il Recovery Guru per risolvere il problema.

Risultati

Al termine del test di comunicazione, questa finestra di dialogo mostra lo stato normale, superato o non riuscito.

Se il test di comunicazione restituisce uno stato Failed (non riuscito), il test continua a essere eseguito dopo la chiusura di questa finestra di dialogo fino a quando non viene ripristinata la comunicazione tra i gruppi di coerenza mirror.

Sospendere o riprendere la sincronizzazione per il gruppo di coerenza mirror

È possibile sospendere o riprendere la sincronizzazione dei dati su tutte le coppie mirrorate all'interno di un gruppo di coerenza mirror, che è più efficiente della sospensione o della ripresa della sincronizzazione su singole coppie mirrorate.

A proposito di questa attività

La sospensione e la ripresa della sincronizzazione sui gruppi contribuisce a ridurre l'impatto delle performance sull'applicazione host, che potrebbe verificarsi durante la copia di tutti i dati modificati sull'array di storage locale nell'array di storage remoto.

Lo stato del gruppo di coerenza mirror e delle relative coppie mirrorate rimane sospeso fino a quando non si utilizza l'opzione Resume (Riprendi) per riprendere l'attività di sincronizzazione.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirrored Consistency Group (Gruppo di coerenza mirrorato) che mostra tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror che si desidera sospendere o riprendere, quindi selezionare **More › Suspend** o **More › Resume**.

   Il sistema visualizza una conferma.

4. Selezionare **Sì** per confermare.

Risultati

System Manager esegue le seguenti operazioni:

- Sospende o riprende il trasferimento dei dati tra tutte le coppie mirrorate in un gruppo di coerenza mirror senza rimuovere la relazione mirror.
- Registra tutti i dati scritti sul lato primario del gruppo di coerenza del mirror mentre il gruppo di mirroring è sospeso e scrive automaticamente i dati sul lato secondario del gruppo di coerenza del mirror quando il gruppo di mirroring viene ripristinato. Non è richiesta una sincronizzazione completa.
- Per i gruppi di coerenza *sospesi* mirror, visualizza **sospesi dall'utente** nella tabella Mirror Consistency Groups.
- Per un gruppo di coerenza mirror *ripristinato*, i dati scritti nei volumi primari mentre il gruppo di coerenza mirror è stato sospeso vengono scritti immediatamente nei volumi secondari. La sincronizzazione periodica riprende se è stato impostato un intervallo di sincronizzazione automatico.

Modificare le impostazioni di sincronizzazione per un gruppo di coerenza mirror

È possibile modificare le impostazioni di sincronizzazione e le soglie di avviso utilizzate dal gruppo di coerenza del mirror sull'array di storage locale quando i dati vengono inizialmente sincronizzati o quando i dati vengono nuovamente sincronizzati durante le operazioni di mirroring asincrono.

A proposito di questa attività

La modifica delle impostazioni di sincronizzazione influisce sulle operazioni di sincronizzazione di tutte le coppie mirrorate all'interno del gruppo di coerenza mirror.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirrored Consistency Group (Gruppo di coerenza mirrorato) che mostra tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror che si desidera modificare, quindi selezionare **Altro › Modifica impostazioni**.

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

4. Modificare le impostazioni di sincronizzazione e avviso in base alle esigenze, quindi fare clic su **Save** (Salva).

Dettagli del campo

Campo	Descrizione
Sincronizza le coppie mirrorate…	Specificare se si desidera sincronizzare manualmente o automaticamente le coppie mirrorate sull'array di storage remoto. • **Manualmente** – selezionare questa opzione per sincronizzare manualmente le coppie mirrorate sull'array di storage remoto. • **Automatically, every** – selezionare questa opzione per sincronizzare automaticamente le coppie mirrorate sull'array di storage remoto specificando l'intervallo di tempo dall'inizio dell'aggiornamento precedente all'inizio dell'aggiornamento successivo. L'intervallo predefinito è 10 minuti.
Avvisami…	Se si imposta il metodo di sincronizzazione in modo che venga eseguito automaticamente, impostare i seguenti avvisi: • **Sincronizzazione** – consente di impostare il periodo di tempo dopo il quale System Manager invia un avviso che informa che la sincronizzazione non è stata completata. • **Punto di ripristino remoto** – impostare un limite di tempo dopo il quale System Manager invia un avviso che indica che i dati del punto di ripristino sull'array di storage remoto sono più vecchi del limite di tempo definito. Definire il limite di tempo dalla fine dell'aggiornamento precedente. • **Soglia capacità riservata** – consente di definire una quantità di capacità riservata alla quale System Manager invia un avviso che indica che si sta avvicinando alla soglia di capacità riservata. Definire la soglia in base alla percentuale della capacità rimanente.

Risultati

System Manager modifica le impostazioni di sincronizzazione per ogni coppia mirrorata nel gruppo di coerenza mirror.

Risincronizzare manualmente il gruppo di coerenza mirror

È possibile avviare manualmente la risincronizzazione per tutte le coppie mirrorate all'interno di un gruppo di coerenza mirror.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group (Gruppo di coerenza mirror) che visualizza tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror che si desidera risincronizzare, quindi selezionare **More › Manually resincronize** (Altro[risincronizzare manualmente]).

   Il sistema visualizza una conferma.

4. Selezionare **Sì** per confermare.

Risultati

Il sistema esegue le seguenti operazioni:

- Avvia la risincronizzazione dei dati su tutte le coppie mirrorate all'interno del gruppo di coerenza del mirror selezionato.
- Aggiorna i dati modificati dall'array di storage locale all'array di storage remoto.

Visualizzare la quantità di dati non sincronizzati tra gruppi di coerenza mirror

È possibile visualizzare la quantità di dati non sincronizzati tra i gruppi di coerenza mirror sull'array di storage locale e sull'array di storage remoto. Mentre il gruppo di coerenza mirror si trova in uno stato non sincronizzato, non viene eseguita alcuna attività di mirroring.

A proposito di questa attività

È possibile eseguire questa attività quando il gruppo di coerenza mirror selezionato contiene coppie mirrorate e quando la sincronizzazione non è attualmente in corso.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group (Gruppo di coerenza mirror) che visualizza tutti i gruppi di coerenza mirror associati all'array di storage.

3. Fare clic sul **Altro › Visualizza quantità di dati non sincronizzati**.

   Se esistono dati non sincronizzati, i valori della tabella lo riflettono. La colonna data amount (quantità dati) elenca la quantità di dati non sincronizzati in MiB.

Aggiornare l'indirizzo IP remoto

È possibile aggiornare l'indirizzo IP iSCSI dell'array di storage remoto per ristabilire la connessione con l'array di storage locale.

Prima di iniziare

Sia lo storage array locale che quello remoto devono essere configurati per il mirroring asincrono utilizzando una connessione iSCSI.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

La tabella Mirror Consistency Group visualizza tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror che si desidera aggiornare, quindi selezionare **More › Update remote IP address**.

   Viene visualizzata la finestra di dialogo Update Remote IP Address (Aggiorna indirizzo IP remoto).

4. Selezionare **Update** (Aggiorna) per aggiornare l'indirizzo IP iSCSI dell'array di storage remoto.

Risultati

Il sistema ripristina l'indirizzo IP dell'array di storage remoto per ristabilire la connessione con l'array di storage locale.

Impostare il ruolo del gruppo di coerenza mirror su primario o secondario

È possibile modificare il ruolo tra gruppi di coerenza mirror a scopo amministrativo o in caso di disastro nell'array di storage locale.

A proposito di questa attività

I gruppi di coerenza mirror creati sull'array di storage locale ricopriscono il ruolo principale. I gruppi di coerenza mirror creati sull'array di storage remoto ricopriscono il ruolo secondario. È possibile declassare il gruppo di coerenza mirror locale in un ruolo secondario o promuovere il gruppo di coerenza mirror remoto in un ruolo primario.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group (Gruppo di coerenza mirror) che visualizza tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror per il quale si desidera modificare il ruolo, quindi selezionare il **More › Change role to <Primary | Secondary>**.

   Il sistema visualizza una conferma.

4. Confermare che si desidera modificare il ruolo del gruppo di coerenza mirror, quindi fare clic su **Cambia ruolo**.

   > Il sistema visualizza la finestra di dialogo Cannot Contact Storage Array (Impossibile contattare lo storage array) quando viene richiesta una modifica del ruolo, ma non è possibile contattare lo storage array remoto. Fare clic su **Sì** per forzare la modifica del ruolo.

Risultati

System Manager esegue le seguenti operazioni:

- La tabella Mirror Consistency Group visualizza lo stato "in sospeso" o "in corso" accanto al gruppo di coerenza mirror sottoposto alla modifica del ruolo. È possibile annullare un'operazione di modifica del ruolo in sospeso facendo clic sul collegamento **Annulla** nella cella della tabella.
- Se è possibile contattare il gruppo di coerenza mirror associato, i ruoli tra i gruppi di coerenza mirror cambiano. System Manager promuove il gruppo di coerenza del mirror secondario in un ruolo primario o demotizza il gruppo di coerenza del mirror primario in un ruolo secondario (a seconda della selezione

effettuata). La modifica del ruolo influisce su tutte le coppie mirrorate all'interno del gruppo di coerenza mirror selezionato.

Elimina gruppo di coerenza mirror

È possibile eliminare gruppi di coerenza mirror che non sono più necessari sull'array di storage locale e sull'array di storage remoto.

Prima di iniziare

Tutte le coppie mirrorate devono essere rimosse dal gruppo di coerenza mirror.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group (Gruppo di coerenza mirror) che visualizza tutti i gruppi di coerenza mirror associati all'array di storage.

3. Selezionare il gruppo di coerenza mirror che si desidera eliminare, quindi selezionare **attività non comuni › Elimina**.

   Il sistema visualizza una conferma.

4. Selezionare **Sì** per eliminare il gruppo di coerenza mirror.

Risultati

System Manager esegue le seguenti operazioni:

- Elimina prima il gruppo di coerenza mirror sull'array di storage locale, quindi elimina il gruppo di coerenza mirror sull'array di storage remoto.
- Rimuove il gruppo di coerenza mirror dalla tabella Mirror Consistency Group.

Al termine

In alcuni casi, il gruppo di coerenza mirror potrebbe essere cancellato correttamente dall'array di storage locale, ma un errore di comunicazione impedisce l'eliminazione del gruppo di coerenza mirror dall'array di storage remoto. In questo caso, è necessario accedere all'array di storage remoto per eliminare il gruppo di coerenza mirror corrispondente.

Gestire le coppie mirrorate asincrone

Rimuovere la relazione di mirroring asincrona

Rimuovere una coppia mirrorata per rimuovere la relazione di mirroring dal volume primario sull'array di storage locale e dal volume secondario sull'array di storage remoto.

A proposito di questa attività

Esaminare le seguenti informazioni sulle coppie di mirroring orfane:

- Esiste una coppia di mirroring orfani quando un volume membro di un gruppo di mirror di coerenza è stato rimosso da un lato (lato dell'array di storage locale o lato dell'array di storage remoto) ma non dall'altro.
- Le coppie di mirroring orfane vengono rilevate quando viene ripristinata la comunicazione tra array e i due

lati della configurazione di mirroring riconciliano i parametri di mirroring.

- È possibile rimuovere una coppia mirrorata per correggere uno stato di coppia mirrorata orfana.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **coppia mirrorata**.

   Viene visualizzata la tabella delle coppie mirrorate, che mostra tutte le coppie mirrorate associate all'array di storage.

3. Selezionare la coppia mirrorata che si desidera rimuovere, quindi fare clic su **Rimuovi**.
4. Confermare la rimozione della coppia mirrorata, quindi fare clic su **Rimuovi**.

Risultati

System Manager esegue le seguenti operazioni:

- Rimuove la relazione di mirroring dal gruppo di coerenza di mirroring sull'array di storage locale e sull'array di storage remoto ed elimina la capacità riservata.
- Restituisce il volume primario e il volume secondario a volumi non mirrorati accessibili all'host.
- Aggiorna il riquadro di mirroring asincrono con la rimozione della coppia di mirroring asincrono.

Aumentare la capacità riservata

È possibile aumentare la capacità riservata, ovvero la capacità fisicamente allocata utilizzata per qualsiasi operazione di servizio di copia su un oggetto di storage.

Per le operazioni di snapshot, si tratta in genere del 40% del volume di base; per le operazioni di mirroring asincrono si tratta in genere del 20% del volume di base. In genere, si aumenta la capacità riservata quando si riceve un avviso che indica che la capacità riservata dell'oggetto di storage sta diventando piena.

Prima di iniziare

- Il volume nel pool o nel gruppo di volumi deve avere uno stato ottimale e non deve essere in alcun stato di modifica.
- La capacità libera deve essere presente nel pool o nel gruppo di volumi che si desidera utilizzare per aumentare la capacità.

  Se non esiste capacità libera in alcun pool o gruppo di volumi, è possibile aggiungere capacità non assegnata sotto forma di unità inutilizzate a un pool o a un gruppo di volumi.

A proposito di questa attività

È possibile aumentare la capacità riservata solo con incrementi di 8 GiB per i seguenti oggetti di storage:

- Gruppo di snapshot
- Volume Snapshot
- Volume membro del gruppo di coerenza
- Volume di coppia mirrorato

Utilizzare una percentuale elevata se si ritiene che il volume primario subirà molte modifiche o se la durata di una determinata operazione di servizio di copia sarà molto lunga.

Non è possibile aumentare la capacità riservata per un volume di snapshot di sola lettura. Solo i volumi Snapshot in lettura/scrittura richiedono una capacità riservata.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la scheda **capacità riservata**.
3. Selezionare l'oggetto di storage per il quale si desidera aumentare la capacità riservata, quindi fare clic su **aumenta capacità**.

   Viene visualizzata la finestra di dialogo aumenta capacità riservata.

4. Utilizzare la casella di selezione per regolare la percentuale di capacità.

   Se la capacità libera non esiste nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage dispone di capacità non assegnata, è possibile creare un nuovo pool o gruppo di volumi. È quindi possibile riprovare a eseguire questa operazione utilizzando la nuova capacità libera del pool o del gruppo di volumi.

5. Fare clic su **aumenta**.

Risultati

System Manager esegue le seguenti operazioni:

- Aumenta la capacità riservata per l'oggetto di storage.
- Visualizza la capacità riservata aggiunta di recente.

Modificare le impostazioni di capacità riservata per un volume di coppia mirrorata

È possibile modificare le impostazioni di un volume di coppia mirrorata per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per un volume di coppia mirrorata è quasi piena.

Fasi

1. Selezionare **Storage › Pools & Volume Groups** (Storage[Pools & Volume Groups])
2. Selezionare la scheda **capacità riservata**.
3. Selezionare il volume della coppia mirrorata che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni capacità riservata volume coppia mirrorata.

4. Modificare le impostazioni di capacità riservata per il volume di coppia mirrorata in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare la casella di selezione per regolare il punto percentuale in cui System Manager invia una notifica di avviso quando la capacità riservata per una coppia mirrorata è quasi piena. Quando la capacità riservata per la coppia mirrorata supera la soglia specificata, System Manager invia un avviso, consentendo di aumentare la capacità riservata. La modifica dell'impostazione Avviso per una coppia mirrorata modifica l'impostazione Avviso per tutte le coppie mirrorate che appartengono allo stesso gruppo di coerenza mirror.

5. Fare clic su **Save** (Salva) per applicare le modifiche.

Coppia mirrorata completa per volumi primari creati su sistemi legacy

Se è stato creato un volume primario su un array di storage legacy che non può essere gestito da System Manager, è possibile creare il volume secondario su questo array con System Manager.

A proposito di questa attività

È possibile eseguire il mirroring asincrono tra array legacy che utilizzano un'interfaccia diversa e array più recenti che possono essere gestiti da System Manager.

- Se si esegue il mirroring tra due array di storage che utilizzano System Manager, è possibile ignorare questa attività perché la coppia mirrorata è già stata completata nella sequenza di creazione della coppia mirrorata.
- Eseguire questa attività sull'array di storage remoto.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare la scheda **coppia mirrorata**.

   Viene visualizzata la tabella delle coppie mirrorate, che mostra tutte le coppie mirrorate associate all'array di storage.

3. Individuare il volume di coppia mirrorata con stato incomplete, quindi fare clic sul collegamento **complete mirrored pair** (Coppia mirrorata completa) visualizzato nella colonna Mirrored Pair (Coppia mirrorata).
4. Scegliere se si desidera completare la sequenza di creazione della coppia mirrorata automaticamente o manualmente selezionando uno dei seguenti pulsanti di opzione:
   - **Automatico** — Crea un nuovo volume secondario.

     Accettare le impostazioni predefinite per il lato remoto della coppia mirrorata selezionando un pool o un gruppo di volumi esistente in cui si desidera creare il volume secondario. Utilizzare questa opzione

consigliata per allocare la capacità riservata al volume secondario con le impostazioni predefinite.

- **Manuale** — selezionare un volume esistente.

  Definire i propri parametri per il volume secondario.

  i. Fare clic su **Avanti** per selezionare il volume secondario.
  ii. Selezionare un volume esistente che si desidera utilizzare come volume secondario, quindi fare clic su **Avanti** per allocare la capacità riservata.
  iii. Allocare la capacità riservata. Effettuare una delle seguenti operazioni:
    - Accettare le impostazioni predefinite.

      L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume di base, e di solito questa capacità è sufficiente.

    - Allocare le proprie impostazioni di capacità riservate per soddisfare le esigenze di storage dei dati relative al mirroring asincrono.

      La capacità richiesta varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume primario e al tempo necessario per mantenere la capacità. In generale, scegliere una capacità più elevata per la capacità riservata se si verifica una o entrambe le seguenti condizioni:

      - Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.
      - Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.

5. Selezionare **completo**.

Risultati

System Manager esegue le seguenti operazioni:

- Crea il volume secondario sull'array di storage remoto e alloca la capacità riservata per il lato remoto della coppia mirrorata.
- Avvia la sincronizzazione iniziale tra lo storage array locale e lo storage array remoto.
- Se il volume sottoposto a mirroring è un volume sottile, solo i blocchi allocati vengono trasferiti al volume secondario durante la sincronizzazione iniziale. Questo trasferimento riduce la quantità di dati che devono essere trasferiti per completare la sincronizzazione iniziale.
- Crea la capacità riservata per la coppia mirrorata sull'array di storage locale e sull'array di storage remoto.

Gestire le coppie di sincronizzazione mirrorate

Verifica della comunicazione per il mirroring sincrono

È possibile testare la comunicazione tra un array di storage locale e un array di storage remoto per diagnosticare possibili problemi di comunicazione per una coppia mirrorata che partecipa al mirroring sincrono.

A proposito di questa attività

Vengono eseguiti due diversi test:

- **Comunicazione** — verifica che i due array di storage dispongano di un percorso di comunicazione. Il test di comunicazione verifica che l'array di storage locale possa comunicare con l'array di storage remoto e che il volume secondario associato alla coppia mirrorata esista sull'array di storage remoto.
- **Latency** — Invia un comando SCSI test unit al volume secondario sull'array di storage remoto associato alla coppia mirrorata per verificare la latenza minima, media e massima.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare la coppia mirrorata che si desidera verificare, quindi selezionare **Test Communication** (verifica comunicazione).
3. Esaminare le informazioni visualizzate nella finestra dei risultati e, se necessario, seguire l'azione correttiva indicata.

> Se il test di comunicazione non riesce, il test continua a essere eseguito dopo la chiusura di questa finestra di dialogo fino a quando non viene ripristinata la comunicazione tra la coppia mirrorata.

Sospendere e riprendere la sincronizzazione per una coppia mirrorata

È possibile utilizzare l'opzione Sospendi e l'opzione Riprendi per controllare quando sincronizzare i dati sul volume primario e sul volume secondario in una coppia mirrorata.

A proposito di questa attività

Se una coppia mirrorata viene sospesa manualmente, la coppia mirrorata non viene sincronizzata fino a quando non viene ripresa manualmente.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare la coppia mirrorata che si desidera sospendere o riprendere, quindi selezionare **More › Suspend** (Altro[sospensione]) o **More › Resume** (Altro[Riprendi]).

   Il sistema visualizza una conferma.

3. Selezionare **Sì** per confermare.

Risultati

System Manager esegue le seguenti operazioni:

- Sospende o riprende il trasferimento dei dati tra la coppia mirrorata senza rimuovere la relazione di mirroring.
- Per una coppia di mirroring *sospesa*:
  - Visualizza **sospeso** nella tabella delle coppie mirrorate.
  - Registra tutti i dati scritti nel volume primario della coppia mirrorata mentre la sincronizzazione viene sospesa.
- Per una coppia con mirroring *ripresa*, scrive automaticamente i dati nel volume secondario della coppia con mirroring al ripristino della sincronizzazione. Non è richiesta una sincronizzazione completa.

Cambiare ruolo tra i volumi in una coppia mirrorata

È possibile eseguire un'inversione di ruolo tra i due volumi di una coppia mirrorata che partecipano al mirroring sincrono. Questa attività potrebbe essere necessaria per scopi amministrativi o in caso di disastro sull'array di storage locale.

A proposito di questa attività

È possibile ridurre il volume primario al ruolo secondario o promuovere il volume secondario al ruolo primario. Tutti gli host che accedono al volume primario dispongono dell'accesso in lettura/scrittura al volume. Quando il volume primario diventa un volume secondario, nel volume vengono scritte solo le scritture remote avviate dal controller primario.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare la coppia mirrorata contenente i volumi per i quali si desidera modificare il ruolo, quindi selezionare **More › Change role** (Altro[Cambia ruolo]).

   Il sistema visualizza una conferma.

3. Confermare che si desidera modificare il ruolo dei volumi, quindi selezionare **Cambia ruolo**.

> Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, il sistema visualizza la finestra di dialogo Impossibile contattare l'array di storage quando viene richiesta una modifica del ruolo, ma non è possibile contattare l'array di storage remoto. Fare clic su **Sì** per forzare la modifica del ruolo.

Risultati

System Manager esegue la seguente azione:

- Se è possibile contattare il volume associato nella coppia mirrorata, i ruoli tra i volumi cambiano. System Manager promuove il volume secondario nella coppia mirrorata nel ruolo primario o demotizza il volume primario nella coppia mirrorata nel ruolo secondario (a seconda della selezione effettuata).

Modificare le impostazioni di sincronizzazione per una coppia mirrorata

È possibile modificare la priorità di sincronizzazione e il criterio di risincronizzazione utilizzati dalla coppia mirrorata per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

A proposito di questa attività

È possibile modificare le impostazioni di sincronizzazione per una coppia mirrorata solo sull'array di storage che contiene il volume primario.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare la coppia mirrorata che si desidera modificare, quindi selezionare **Altro › Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo View/Edit Settings (Visualizza/Modifica impostazioni).

3. Utilizzare la barra di scorrimento per modificare la priorità di sincronizzazione.

   La priorità di sincronizzazione determina la quantità di risorse di sistema utilizzate per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione rispetto alle richieste di i/o del servizio.

   Ulteriori informazioni sulle velocità di sincronizzazione

   Sono disponibili cinque tassi di priorità di sincronizzazione:

   - Più basso
   - Basso
   - Medio
   - Alto
   - Massimo

   Se la priorità di sincronizzazione è impostata sul tasso più basso, l'attività di i/o ha la priorità e l'operazione di risincronizzazione richiede più tempo. Se la priorità di sincronizzazione è impostata sulla velocità massima, l'operazione di risincronizzazione viene assegnata alla priorità, ma l'attività di i/o per l'array di storage potrebbe risentirne.

4. Modificare il criterio di risincronizzazione in base alle esigenze.

   È possibile risincronizzare le coppie mirrorate sull'array di storage remoto manualmente o automaticamente.

   - **Manuale** (opzione consigliata) — selezionare questa opzione per richiedere la ripresa manuale della sincronizzazione dopo il ripristino della comunicazione su una coppia mirrorata. Questa opzione offre la migliore opportunità per il ripristino dei dati.
   - **Automatico** — selezionare questa opzione per avviare la risincronizzazione automaticamente dopo il ripristino della comunicazione su una coppia mirrorata.

5. Selezionare **Salva**.

Rimuovere la relazione di mirroring sincrono

Rimuovere una coppia mirrorata per rimuovere la relazione di mirroring dal volume primario sull'array di storage locale e dal volume secondario sull'array di storage remoto.

A proposito di questa attività

È inoltre possibile rimuovere una coppia mirrorata per correggere uno stato di coppia mirrorata orfana. Esaminare le seguenti informazioni sulle coppie di mirroring orfane:

- Esiste una coppia di mirroring orfano quando un volume membro è stato rimosso da un lato (locale/remoto) ma non dall'altro.
- Le coppie di mirroring orfane vengono rilevate quando viene ripristinata la comunicazione tra array.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare la coppia mirrorata che si desidera rimuovere, quindi selezionare il **operazioni non comuni ›**

Rimuovi.

Viene visualizzata la finestra di dialogo Rimuovi relazione mirror.

3. Confermare la rimozione della coppia mirrorata, quindi fare clic su **Rimuovi**.

Risultati

System Manager esegue le seguenti operazioni:

- Rimuove la relazione di mirroring dalla coppia mirrorata sull'array di storage locale e sull'array di storage remoto.
- Restituisce il volume primario e il volume secondario a volumi non mirrorati accessibili all'host.
- Aggiorna il riquadro Synchronous Mirroring con la rimozione della coppia di mirroring sincrono.

Disattivare il mirroring

Disattivare il mirroring asincrono

È possibile disattivare il mirroring asincrono sugli array di storage locali e remoti per ristabilire il normale utilizzo delle porte dedicate sugli array di storage.

Prima di iniziare

- È necessario eliminare tutte le relazioni mirror. Verificare che tutti i gruppi di coerenza mirror e le coppie mirrorate siano stati eliminati dagli array di storage locali e remoti.
- L'array di storage locale e l'array di storage remoto devono essere collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.

A proposito di questa attività

Quando si disattiva il mirroring asincrono, non può verificarsi alcuna attività di mirroring sugli array di storage locali e remoti.

Fasi

1. Selezionare **Storage › Mirroring asincrono**.
2. Selezionare **attività non comuni › Disattiva**.

   Il sistema visualizza una conferma.

3. Selezionare **Sì** per confermare.

Risultati

- I canali host HBA del controller dedicati alla comunicazione di mirroring asincrono possono ora accettare richieste di lettura e scrittura dell'host.
- Nessuno dei volumi di questo array di storage è in grado di partecipare a relazioni mirror come volumi primari o secondari.

Disattivare il mirroring sincrono

È possibile disattivare la funzione Synchronous Mirroring su uno storage array per ripristinare il normale utilizzo della porta host 4 dell'HBA (host bus adapter), riservata alla trasmissione dei dati mirror.

Prima di iniziare

È necessario eliminare tutte le relazioni mirror sincrone. Verificare che tutte le coppie mirrorate siano state eliminate dallo storage array.

Fasi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare **attività non comuni › Disattiva**.

   Il sistema visualizza una conferma.

3. Selezionare **Sì** per confermare.

Risultati

- La porta host HBA 4 del controller, dedicata alla comunicazione di mirroring sincrono, è ora in grado di accettare richieste di lettura e scrittura dell'host.
- I volumi di capacità riservati sull'array di storage vengono cancellati.

Domande frequenti su Async

In che modo il mirroring asincrono differisce dal mirroring sincrono?

La funzione di mirroring asincrono si differenzia dalla funzione di mirroring sincrono in un modo essenziale: Acquisisce lo stato del volume di origine in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine.

Con il mirroring sincrono, lo stato del volume primario non viene acquisito in un determinato momento, ma riflette tutte le modifiche apportate sul volume primario al volume secondario. Il volume secondario è identico al volume primario in ogni momento perché, con questo tipo di mirror, ogni volta che viene eseguita una scrittura nel volume primario, viene eseguita una scrittura nel volume secondario. L'host non riceve una conferma che la scrittura è riuscita fino a quando il volume secondario non viene aggiornato correttamente con le modifiche apportate sul volume primario.

Con il mirroring asincrono, l'array di storage remoto non è completamente sincronizzato con l'array di storage locale, quindi se l'applicazione deve passare all'array di storage remoto a causa di una perdita dell'array di storage locale, alcune transazioni potrebbero andare perse.

Confronto tra le funzionalità di mirroring:

Mirroring asincrono	Mirroring sincrono
Metodo di replica	• **Point-in-Time** Il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente. Le pianificazioni possono essere definite in base alla granularità dei minuti. Il tempo minimo tra le sincronizzazioni è di 10 minuti.

Mirroring asincrono	Mirroring sincrono
• **Continuo** Il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura host.	**Capacità riservata**
• **Multiplo** Per ogni coppia mirrorata è necessario un volume di capacità riservato.	• **Singolo** Per tutti i volumi mirrorati è necessario un singolo volume di capacità riservata.
Comunicazione	• **ISCSI e Fibre Channel** Supporta interfacce iSCSI e Fibre Channel tra array di storage.
• **Fibre Channel** Supporta solo interfacce Fibre Channel tra array di storage.	**Distanza**
• **Senza limiti** Supporto di distanze virtualmente illimitate tra lo storage array locale e lo storage array remoto, con la distanza generalmente limitata solo dalle funzionalità della rete e dalla tecnologia di estensione del canale.	• **Limitato** In genere, per soddisfare i requisiti di latenza e performance delle applicazioni, è necessario che l'array di storage locale si trovi entro circa 10 km (6.2 miglia).

Perché non è possibile accedere alla funzione di mirroring scelta?

Il mirroring viene configurato nell'interfaccia di Unified Manager.

> Il mirroring sincrono non è disponibile sull'array di storage EF600 o EF300.

Per abilitare e configurare il mirroring tra due array, verificare quanto segue:

- Il servizio Web Services Proxy deve essere in esecuzione. (Unified Manager viene installato su un sistema host insieme al proxy dei servizi Web).
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- I due array di storage che si desidera utilizzare per il mirroring devono essere rilevati in Unified Manager.
- Unified Manager deve disporre di certificati SSL validi per gli array di storage. È possibile accettare un certificato autofirmato o installare certificati CA firmati da Unified Manager.

Per istruzioni sulla configurazione, consultare quanto segue:

- "Creazione di coppia asincrona con mirroring (in Unified Manager)"
- "Creazione di una coppia sincrona con mirroring (in Unified Manager)"

Cosa è necessario sapere prima di creare un gruppo di coerenza mirror?

Seguire queste linee guida prima di creare un gruppo di coerenza mirror.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

È possibile creare un gruppo di coerenza in Unified Manager nella procedura guidata Crea coppie mirrorate.

Soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array di storage:

- I due storage array devono essere rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.

Mirroring asincrono - cosa occorre sapere prima di creare una coppia mirrorata?

Le coppie mirrorate vengono configurate nell'interfaccia di Unified Manager e quindi gestite in System Manager.

Prima di creare una coppia mirrorata, seguire queste linee guida.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.

- Sono stati installati Web Services Proxy e Unified Manager. Le coppie mirrorate vengono configurate nell'interfaccia di Unified Manager.
- I due array di storage vengono rilevati in Unified Manager.
- L'array di storage deve contenere almeno un gruppo di coerenza mirror. È possibile creare un gruppo di coerenza in Unified Manager nella procedura guidata Crea coppie mirrorate.

Cosa devo sapere prima di aumentare la mia capacità riservata su un volume a coppia mirrorata?

In genere, è necessario aumentare la capacità riservata quando si riceve un avviso che indica che la capacità riservata per una coppia mirrorata sta diventando piena. È possibile aumentare la capacità riservata solo con incrementi di 8 GiB.

Per le operazioni di mirroring asincrono, la capacità riservata è in genere il 20% del volume di base. Scegliere una capacità più ampia per la capacità riservata se si verifica una o entrambe le seguenti condizioni:

- Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.
- Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.

È possibile aumentare la capacità riservata per una coppia mirrorata eseguendo una delle seguenti operazioni:

- Regolare la percentuale di capacità per un volume di coppia mirrorata selezionando **Storage › Pools and Volumes Groups** (Storage[gruppi di pool e volumi]), quindi facendo clic sulla scheda **Reserved Capacity** (capacità riservata).
- Creare un nuovo volume utilizzando la capacità libera disponibile in un pool o in un gruppo di volumi.

  Se non esiste capacità libera in alcun pool o gruppo di volumi, è possibile aggiungere capacità non configurata sotto forma di unità inutilizzate a un pool o a un gruppo di volumi.

Perché non è possibile aumentare la capacità riservata con l'importo richiesto?

È possibile aumentare la capacità riservata solo con incrementi di 4 GiB.

Consultare le seguenti linee guida:

- È necessario disporre di una capacità libera sufficiente nel pool o nel gruppo di volumi in modo da poterla espandere, se necessario.

  Se non esiste capacità libera in alcun pool o gruppo di volumi, è possibile aggiungere capacità non assegnata sotto forma di unità inutilizzate a un pool o a un gruppo di volumi.

- Il volume nel pool o nel gruppo di volumi deve avere uno stato ottimale e non deve essere in alcun stato di modifica.
- La capacità libera deve essere presente nel pool o nel gruppo di volumi che si desidera utilizzare per aumentare la capacità.

Per le operazioni di mirroring asincrono, la capacità riservata è in genere il 20% del volume di base. Utilizzare una percentuale più elevata se si ritiene che il volume di base subirà molte modifiche o se la durata prevista per l'operazione di copia del servizio di un oggetto di storage sarà molto lunga.

Perché dovrei modificare questa percentuale?

La capacità riservata corrisponde in genere al 40% del volume di base per le operazioni di snapshot e al 20% del volume di base per le operazioni di mirroring asincrono.

Di solito questa capacità è sufficiente. La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume di base e alla durata dell'utilizzo del servizio di copia dell'oggetto di storage.

In generale, scegliere una percentuale maggiore per la capacità riservata se sussistono una o entrambe le seguenti condizioni:

- Se la durata di un'operazione di copia del servizio di un oggetto di storage specifico sarà molto lunga.
- Se una grande percentuale di blocchi di dati cambia sul volume di base a causa di un'intensa attività di i/O. Utilizza dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume di base.

Perché vengono visualizzati più candidati con capacità riservata?

Se in un pool o gruppo di volumi sono presenti più volumi che soddisfano la percentuale di capacità selezionata per l'oggetto di storage, verranno visualizzati più volumi candidati.

È possibile aggiornare l'elenco dei candidati consigliati modificando la percentuale di spazio su disco fisico che si desidera riservare sul volume di base per le operazioni del servizio di copia. I candidati migliori vengono visualizzati in base alla selezione effettuata.

Perché nella tabella vengono visualizzati i valori non disponibili?

La tabella elenca i valori non disponibili quando i dati presenti nell'array di storage remoto non sono disponibili per la visualizzazione.

Per visualizzare i dati dell'array di storage remoto, avviare System Manager da Unified Manager.

Perché non vengono visualizzati tutti i pool e i gruppi di volumi?

Quando si crea un volume secondario per la coppia con mirroring asincrono, il sistema visualizza un elenco di tutti i pool e gruppi di volumi idonei per la coppia con mirroring asincrono. Qualsiasi pool o gruppo di volumi non idoneo all'utilizzo non viene visualizzato nell'elenco.

I pool o i gruppi di volumi potrebbero non essere idonei per uno dei seguenti motivi.

- Le funzionalità di sicurezza di un pool o di un gruppo di volumi non corrispondono.
- Un pool o un gruppo di volumi non si trova in uno stato ottimale.
- La capacità di un pool o di un gruppo di volumi è troppo ridotta.

Mirroring asincrono - perché non vedo tutti i volumi?

Quando si seleziona un volume primario per una coppia mirrorata, un elenco mostra tutti i volumi idonei.

I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per

uno dei seguenti motivi:

- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Per i volumi thin, è necessario attivare l'espansione automatica.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

Mirroring asincrono - perché non vengono visualizzati tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario nell'array di storage remoto, un elenco mostra tutti i volumi idonei per la coppia mirrorata.

I volumi non idonei per l'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Gli attributi del volume thin tra il volume primario e il volume secondario non corrispondono.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.
  - Se il volume primario è abilitato da, il volume secondario deve essere abilitato da.
  - Se il volume primario non è abilitato da, il volume secondario non deve essere abilitato da.

Perché aggiornare l'indirizzo IP del mio array di storage remoto?

L'indirizzo IP dell'array di storage remoto viene aggiornato quando l'indirizzo IP di una porta iSCSI cambia e l'array di storage locale non è in grado di comunicare con l'array di storage remoto.

Quando si stabilisce una relazione di mirroring asincrono con una connessione iSCSI, gli array di storage locale e remoto memorizzano un record dell'indirizzo IP dell'array di storage remoto nella configurazione di mirroring asincrono. Se l'indirizzo IP di una porta iSCSI cambia, l'array di storage remoto che sta tentando di utilizzare tale porta rileva un errore di comunicazione.

L'array di storage con l'indirizzo IP modificato invia un messaggio a ciascun array di storage remoto associato ai gruppi di coerenza mirror configurati per il mirroring su una connessione iSCSI. Gli array di storage che ricevono questo messaggio aggiornano automaticamente l'indirizzo IP di destinazione remota.

Se lo storage array con l'indirizzo IP modificato non riesce a inviare il messaggio inter-array a uno storage array remoto, il sistema invia un avviso relativo al problema di connettività. Utilizzare l'opzione Update Remote IP Address (Aggiorna indirizzo IP remoto) per ristabilire la connessione con lo storage array locale.

Domande frequenti sulla sincronizzazione

In che modo il mirroring asincrono differisce dal mirroring sincrono?

La funzione di mirroring asincrono si differenzia dalla funzione di mirroring sincrono in un modo essenziale: Acquisisce lo stato del volume di origine in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine.

Con il mirroring sincrono, lo stato del volume primario non viene acquisito in un determinato momento, ma riflette tutte le modifiche apportate sul volume primario al volume secondario. Il volume secondario è identico al volume primario in ogni momento perché, con questo tipo di mirror, ogni volta che viene eseguita una scrittura nel volume primario, viene eseguita una scrittura nel volume secondario. L'host non riceve una conferma che la scrittura è riuscita fino a quando il volume secondario non viene aggiornato correttamente con le modifiche apportate sul volume primario.

Con il mirroring asincrono, l'array di storage remoto non è completamente sincronizzato con l'array di storage locale, quindi se l'applicazione deve passare all'array di storage remoto a causa di una perdita dell'array di storage locale, alcune transazioni potrebbero andare perse.

Confronto tra le funzionalità di mirroring:

Mirroring asincrono	Mirroring sincrono
Metodo di replica	• **Point-in-Time** Il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente. Le pianificazioni possono essere definite in base alla granularità dei minuti. Il tempo minimo tra le sincronizzazioni è di 10 minuti.
• **Continuo** Il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura host.	**Capacità riservata**
• **Multiplo** Per ogni coppia mirrorata è necessario un volume di capacità riservato.	• **Singolo** Per tutti i volumi mirrorati è necessario un singolo volume di capacità riservata.
Comunicazione	• **ISCSI e Fibre Channel** Supporta interfacce iSCSI e Fibre Channel tra array di storage.
• **Fibre Channel** Supporta solo interfacce Fibre Channel tra array di storage.	**Distanza**

Mirroring asincrono	Mirroring sincrono
• **Senza limiti** Supporto di distanze virtualmente illimitate tra lo storage array locale e lo storage array remoto, con la distanza generalmente limitata solo dalle funzionalità della rete e dalla tecnologia di estensione del canale.	• **Limitato** In genere, per soddisfare i requisiti di latenza e performance delle applicazioni, è necessario che l'array di storage locale si trovi entro circa 10 km (6.2 miglia).

Mirroring sincrono - perché non vengono visualizzati tutti i volumi?

Quando si seleziona un volume primario per una coppia mirrorata, un elenco mostra tutti i volumi idonei.

I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è un volume standard, ad esempio un volume snapshot o un volume thin.
- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.

Mirroring sincrono - perché non vengono visualizzati tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario nell'array di storage remoto, un elenco mostra tutti i volumi idonei per la coppia mirrorata.

I volumi non idonei per l'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è un volume standard, ad esempio un volume snapshot o un volume thin.
- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.
  - Se il volume primario è abilitato da, il volume secondario deve essere abilitato da.
  - Se il volume primario non è abilitato da, il volume secondario non deve essere abilitato da.

Mirroring sincrono - cosa occorre sapere prima di creare una coppia mirrorata?

Le coppie mirrorate vengono configurate nell'interfaccia di Unified Manager e quindi gestite in System Manager.

Prima di creare una coppia mirrorata, attenersi alle seguenti linee guida:

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.

- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Sono stati installati Web Services Proxy e Unified Manager. Le coppie mirrorate vengono configurate nell'interfaccia di Unified Manager.
- I due array di storage vengono rilevati in Unified Manager.

Qual è l'impatto della priorità di sincronizzazione sulle velocità di sincronizzazione?

La priorità di sincronizzazione definisce il tempo di elaborazione allocato per le attività di sincronizzazione in relazione alle prestazioni del sistema.

Il proprietario del controller del volume primario esegue questa operazione in background. Allo stesso tempo, il proprietario del controller elabora le scritture i/o locali nel volume primario e le scritture remote associate nel volume secondario. Poiché la risincronizzazione distoglie le risorse di elaborazione del controller dall'attività di i/o, la risincronizzazione può avere un impatto sulle prestazioni dell'applicazione host.

Tenere presenti queste linee guida per determinare il tempo necessario per una priorità di sincronizzazione e il modo in cui le priorità di sincronizzazione possono influire sulle prestazioni del sistema.

Informazioni sui tassi di priorità di sincronizzazione

Sono disponibili i seguenti tassi di priorità:

- Più basso
- Basso
- Medio
- Alto
- Massimo

Il tasso di priorità più basso supporta le prestazioni del sistema, ma la risincronizzazione richiede più tempo. Il tasso di priorità più elevato supporta la risincronizzazione, ma le prestazioni del sistema potrebbero essere compromesse.

Queste linee guida approssimano le differenze tra le priorità.

Tasso di priorità per la sincronizzazione completa	Tempo trascorso rispetto alla massima velocità di sincronizzazione
Più basso	Circa otto volte più a lungo rispetto al tasso di priorità più elevato.
Basso	Circa sei volte più a lungo rispetto al tasso di priorità più elevato.

Tasso di priorità per la sincronizzazione completa	Tempo trascorso rispetto alla massima velocità di sincronizzazione
Medio	Circa tre volte e mezzo fino al tasso di priorità più elevato.
Alto	Circa il doppio rispetto al tasso di priorità più elevato.

Le dimensioni del volume e i carichi della velocità di i/o dell'host influiscono sui confronti dei tempi di sincronizzazione.

Perché si consiglia di utilizzare una policy di sincronizzazione manuale?

La risincronizzazione manuale è consigliata perché consente di gestire il processo di risincronizzazione in modo da offrire la migliore opportunità di recupero dei dati.

Se si utilizza un criterio di risincronizzazione automatica e si verificano problemi di comunicazione intermittente durante la risincronizzazione, i dati sul volume secondario potrebbero essere temporaneamente danneggiati. Una volta completata la risincronizzazione, i dati vengono corretti.

Storage remoto

Panoramica delle funzionalità dello storage remoto

Se si dispone della funzione di storage remoto, è possibile importare i dati da un sistema di storage remoto all'array di storage.

Che cos'è la funzione di storage remoto?

La funzione *Remote Storage* consente di importare i dati da un sistema di storage remoto a un sistema di storage e-Series locale. Il sistema remoto può essere un altro sistema e-Series o un sistema di un altro vendor. Questa funzione è utile quando si desidera ottimizzare la migrazione dei dati con tempi di inattività minimi, ad esempio durante gli aggiornamenti delle apparecchiature.

> Per utilizzare lo storage remoto, questa funzione deve essere attivata nell'ID modello secondario (SMID).

Scopri di più:

- "Come funziona lo storage remoto"
- "Terminologia dello storage remoto"
- "Requisiti di storage remoto"
- "Requisiti del volume di storage remoto"

Come si importano i dati con questa funzione?

Utilizzando la procedura guidata Storage remoto, è possibile mappare un dispositivo di storage remoto (l'origine per l'importazione dei dati) a un volume di destinazione sul sistema e-Series. Questa procedura guidata è disponibile dal **Storage › Remote storage** (archiviazione remota).

Scopri di più:

- "Importa storage remoto"
- "Gestire l'avanzamento dell'importazione dei dati"

Concetti

Come funziona lo storage remoto

La funzione di storage remoto consente di importare i dati da un sistema di storage remoto a un sistema di storage e-Series locale. Questa funzione è utile quando si desidera ottimizzare la migrazione dei dati con tempi di inattività minimi, ad esempio durante gli aggiornamenti delle apparecchiature.

Per configurare la funzione di storage remoto, è necessario configurare l'hardware e utilizzare System Manager per creare un oggetto di storage remoto. Una volta completata la configurazione, viene avviato il processo di importazione.

Configurazione dell'hardware

Utilizzare il seguente flusso di lavoro per preparare le connessioni hardware.

Questi passaggi sono descritti più avanti nella guida utente per la funzione di storage remoto, disponibile nel centro di documentazione e-Series e SANtricity all'indirizzo "Panoramica dei volumi di storage remoto"e in "Report tecnico sullo storage remoto".

Sul sistema storage e-Series locale:

1. Assicurarsi che ciascun controller disponga di una connessione iSCSI al sistema di storage remoto. Con questa connessione, il sistema locale e-Series agisce come un iniziatore iSCSI che può essere configurato come host sul sistema remoto.
2. Creare un volume di destinazione per l'operazione di importazione. Assicurarsi che il volume abbia una capacità uguale o superiore al volume di origine sul sistema di storage remoto, abbia una dimensione di blocco corrispondente e non sia mappato. Vedere "Creare volumi".
3. Ottenere il nome qualificato iSCSI (IQN) per il sistema e-Series locale dalla relativa interfaccia di System Manager. L'IQN verrà utilizzato in seguito per configurare il sistema locale e-Series come host sul sistema di storage remoto. In System Manager, andare a: Menu:Impostazioni[sistema > Impostazioni iSCSI > IQN di destinazione].

Sul sistema di storage remoto:

1. Configurare il sistema locale e-Series come host sul sistema remoto, utilizzando il relativo IQN. Assicurarsi di impostare il tipo di host appropriato, come indicato di seguito:
   - Se il sistema remoto è un modello e-Series, vedere "Panoramica degli host e dei cluster di host". Utilizzare un tipo di host "Factory Default".
   - Se il sistema remoto proviene da un altro vendor, selezionare un tipo di host appropriato in base alle opzioni disponibili.
2. Arrestare tutti i sistemi i/o, smontare i file system e rimuovere eventuali assegnazioni agli host o alle applicazioni per il volume di origine.
3. Assegnare il volume all'host del sistema storage e-Series locale appena creato.

4. Per il volume di origine selezionato, raccogliere le seguenti informazioni dal sistema di storage remoto in modo da poter creare l'importazione:
    - Nome qualificato iSCSI (IQN)
    - Indirizzo IP iSCSI
    - Numero LUN del volume di origine

Configurazione di System Manager

Utilizzare il seguente flusso di lavoro per creare un oggetto storage remoto per l'importazione:

1. Utilizzando la procedura guidata Storage remoto nell'interfaccia di System Manager, mappare un dispositivo di storage remoto (l'origine per l'importazione dei dati) a un volume di destinazione sul sistema e-Series. Quando si seleziona **fine**, viene avviato il processo di importazione.
2. Monitorare l'importazione dalla finestra di dialogo View Operations (operazioni vista) o dal pannello Operations in Progress (operazioni in corso). Se necessario, è anche possibile sospendere e riprendere il processo.
3. In alternativa, interrompere la connessione tra i volumi di origine e di destinazione al termine dell'importazione o mantenere la connessione per le importazioni future.

Terminologia dello storage remoto

Scopri come si applicano i termini dello storage remoto al tuo storage array.

Termine	Descrizione
IQN	Identificatore IQN (iSCSI Qualified Name), che è un nome univoco per un iniziatore o una destinazione iSCSI.
LUN	Numero di unità logica, utilizzato per identificare un'unità logica che può essere presentata a un host per l'accesso.
Sistema di storage remoto	Il sistema storage in cui risiedono i dati. Il sistema di storage remoto può essere un modello e-Series o un sistema di un altro vendor.
Dispositivo di storage remoto	Il dispositivo fisico o logico in cui i dati vengono inizialmente memorizzati nel sistema remoto. In un sistema storage e-Series, questo viene definito "volume".
Oggetto storage remoto	Oggetto contenente informazioni che consentono al sistema e-Series di identificare e connettersi al sistema di storage remoto. Queste informazioni includono gli indirizzi IQN e IP per il sistema di storage remoto. L'oggetto storage remoto rappresenta la comunicazione tra il sistema storage remoto e il sistema e-Series.
Volume di storage remoto	Volume standard del sistema e-Series che consente l'accesso ai dati a un dispositivo di storage remoto.
Volume	Contenitore in cui vengono memorizzati i dati. Si tratta del componente logico creato per l'host per accedere ai dati.

Requisiti delle funzionalità dello storage remoto

Prima di utilizzare la funzione di storage remoto, esaminare i seguenti requisiti e limitazioni.

Protocolli supportati

Sono supportati i seguenti protocolli:

- ISCSI
- IPv4

Per informazioni aggiornate sul supporto e-Series e sulla configurazione, consultare "Tool di matrice di interoperabilità NetApp".

Requisiti hardware

Il sistema storage e-Series deve includere:

- Due controller (modalità duplex)
- Connessioni iSCSI per i controller e-Series per comunicare con il sistema di storage remoto attraverso una o più connessioni iSCSI
- SANtricity OS 11.71 o superiore
- Funzione di storage remoto attivata nell'ID modello secondario (SMID)

Il sistema remoto può essere un sistema storage e-Series o un sistema di un altro vendor. Deve includere:

- Interfacce compatibili con iSCSI

Restrizioni

La funzione di storage remoto presenta le seguenti restrizioni:

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

Requisiti del volume di storage remoto

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

Volume di storage remoto

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

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

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

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

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

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

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

Candidati al volume di destinazione

Il volume di destinazione è il volume di destinazione sul sistema e-Series locale. Il volume di destinazione deve soddisfare i seguenti criteri:

- Deve essere un volume RAID/DDP.
- Deve avere una capacità uguale o superiore al volume di storage remoto.
- Deve avere una dimensione del blocco uguale a quella del volume di storage remoto.
- Deve avere uno stato valido (ottimale).
- Non è possibile avere alcuna delle seguenti relazioni: Copia del volume, copie Snapshot, mirroring asincrono o sincrono.
- Non è possibile eseguire operazioni di riconfigurazione: Espansione dinamica del volume, espansione dinamica della capacità, dimensione dinamica dei segmenti, migrazione dinamica del RAID, riduzione dinamica della capacità, O deframmentazione.
- Impossibile eseguire il mapping a un host prima dell'inizio dell'importazione (tuttavia, è possibile eseguire il mapping dopo il completamento dell'importazione).

- Non è possibile attivare la funzione Flash Read cache (FRC).

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

Gestire lo storage remoto

Importa storage remoto

Per avviare un'importazione dello storage da un sistema remoto a un sistema storage e-Series locale, utilizzare la procedura guidata Importa storage remoto.

Prima di iniziare

- Il sistema storage e-Series deve essere configurato per comunicare con il sistema storage remoto.

> La configurazione dell'hardware è descritta nella guida dell'utente per la funzione di storage remoto, disponibile presso il centro di documentazione e-Series e SANtricity all'indirizzo "Configurare l'hardware"e in "Report tecnico sullo storage remoto".

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

Per un elenco completo dei requisiti, vedere "Requisiti dei volumi di storage remoto".

- **Consigliato:** eseguire il backup dei volumi sul sistema di storage remoto prima di avviare il processo di importazione.

A proposito di questa attività

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

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

Fasi

1. Selezionare **Storage › Remote storage** (archiviazione remota).
2. Fare clic su **Importa storage remoto**.

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

3. Nel **Passo 1a** del pannello Configura origine, immettere le informazioni di connessione. Se si desidera aggiungere un'altra connessione iSCSI, fare clic su **Add another IP address** (Aggiungi un altro indirizzo IP) per includere un indirizzo IP aggiuntivo per lo storage remoto. Al termine, fare clic su **Avanti**.

   Dettagli del campo

Impostazione	Descrizione
Nome	Immettere un nome per il dispositivo di storage remoto per identificarlo nell'interfaccia di System Manager. Un nome può includere fino a 30 caratteri e può contenere solo lettere, numeri e i seguenti caratteri speciali: Trattino basso (_), trattino (-) e il segno hash (n.). Un nome non può contenere spazi.
Proprietà della connessione iSCSI	Immettere le proprietà di connessione del dispositivo di storage remoto: • **ISCSI Qualified Name (IQN)**: Immettere l'IQN iSCSI. • **IP Address** (Indirizzo IP): Inserire l'indirizzo IPv4. • **Port** (porta): Immettere il numero di porta da utilizzare per le comunicazioni tra i dispositivi di origine e di destinazione. Per impostazione predefinita, il numero della porta è 3260.

   Dopo aver fatto clic su **Avanti**, viene visualizzato il **Passo 1b** del pannello Configura origine.

4. Nel campo **LUN**, selezionare il numero LUN del dispositivo di storage remoto da utilizzare come origine, quindi fare clic su **Avanti**.

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

5. Dalla tabella, selezionare un volume di destinazione nel sistema storage e-Series. Se necessario, utilizzare il dispositivo di scorrimento per modificare la priorità di importazione. Fare clic su **Avanti**. Confermare l'operazione nella finestra di dialogo successiva digitando `continue`, Quindi fare clic su **continua**.

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

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

6. Dal pannello Review (Revisione), verificare che le impostazioni siano corrette, quindi fare clic su **Finish** (fine) per avviare l'importazione.

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

7. Se necessario, fare clic su **Sì** per creare un'altra importazione di storage remoto. Facendo clic su **Yes** (Sì)

si torna al **Step 1a** del pannello Configure Source (Configura origine), dove è possibile selezionare la configurazione esistente o aggiungerne una nuova. Se non si desidera creare un'altra importazione, fare clic su **No** per uscire dalla finestra di dialogo.

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

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

Risultati

Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del sistema di storage remoto, dall'impostazione della priorità per l'importazione e dalla quantità di carico i/o su entrambi i sistemi storage e sui volumi associati.

Una volta completata l'importazione, il volume locale è un duplicato del dispositivo di storage remoto.

Al termine

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

Gestire l'avanzamento delle importazioni di storage remoto

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

A proposito di questa attività

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

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

Fasi

1. Dalla pagina Storage remoto, selezionare **View Operations** (Visualizza operazioni).

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

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

- **Disconnect** — selezionare **Disconnect** per interrompere la relazione tra i volumi di origine e di destinazione per un'operazione di importazione interrotta, completata o non riuscita.

Modificare le impostazioni di connessione per lo storage remoto

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

A proposito di questa attività

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

Fasi

1. Selezionare **Storage › Remote storage** (archiviazione remota).
2. Dall'elenco, selezionare l'oggetto di storage remoto che si desidera modificare.
3. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo Remote Storage Settings (Impostazioni storage remoto).

4. Fare clic sulla scheda **Connection Properties** (Proprietà connessione).

   Vengono visualizzati l'indirizzo IP configurato e le impostazioni della porta per l'importazione dello storage remoto.

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

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

Rimuovere l'oggetto storage remoto

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

Prima di iniziare

Assicurarsi che nessuna importazione sia associata all'oggetto di storage remoto che si intende rimuovere.

A proposito di questa attività

Quando si rimuove un oggetto di storage remoto, le connessioni tra i dispositivi locali e remoti vengono

rimosse.

Fasi

1. Selezionare **Storage › Remote storage** (archiviazione remota).
2. Dall'elenco, selezionare l'oggetto di storage remoto che si desidera rimuovere.
3. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Confirm Remove Remote Storage Connection (Conferma rimozione connessione storage remoto).

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

   L'oggetto di storage remoto selezionato viene rimosso.

FAQ

Cosa occorre sapere prima di creare una connessione di storage remoto?

Per configurare la funzione di storage remoto, è necessario collegare direttamente il dispositivo remoto e i sistemi storage di destinazione tramite iSCSI.

Per impostare la connessione al sistema iSCSI, fare riferimento a:

- "Configurare le porte iSCSI"
- "Report tecnico sullo storage remoto"

Perché viene richiesto di rimuovere i volumi remoti?

Quando raggiunge il numero massimo di volumi remoti, il sistema di storage rileva automaticamente eventuali volumi remoti inutilizzati e richiede di rimuoverli.

In alcuni casi, i volumi remoti non utilizzati non vengono ripuliti durante il processo di creazione. Prima di avviare ulteriori operazioni di importazione, verificare che i sistemi siano ottimali e che le connessioni di rete siano stabili.

Perché non vengono visualizzati tutti i volumi sull'array di destinazione?

Quando si configura un'importazione per la funzione di storage remoto, alcuni volumi potrebbero non essere visualizzati nell'elenco dei candidati di destinazione a causa delle dimensioni del blocco, della capacità o della disponibilità del volume.

Per apparire nell'elenco, i candidati al volume devono avere:

- Capacità uguale o superiore al volume remoto.
- Dimensione del blocco uguale al volume remoto.
- Stato corrente di ottimale.

I volumi candidati sono esclusi dall'elenco se hanno:

- Una delle seguenti relazioni: Copia del volume, snapshot o mirroring.

- Operazione di riconfigurazione in corso.
- Mappatura a un altro dispositivo (host o cluster host).
- Cache flash di lettura attivata.

Cosa occorre sapere sul volume remoto in un'importazione?

Quando si utilizza la funzione di storage remoto, tenere presente che il volume remoto è l'origine dei dati.

Quando l'importazione è in corso, i dati vengono trasferiti dal volume remoto al volume di destinazione sul sistema di storage di destinazione. Questi due volumi devono avere una dimensione di blocco corrispondente.

Cosa occorre sapere prima di avviare un'importazione dello storage remoto?

La funzione di storage remoto consente di copiare i dati da un sistema di storage remoto a un volume su un sistema di storage e-Series locale. Prima di utilizzare questa funzione, consultare le seguenti linee guida.

Configurazione

Prima di creare l'importazione dello storage remoto, è necessario completare le seguenti azioni e verificare le seguenti condizioni:

- Assicurarsi che ciascun controller del sistema storage locale e-Series disponga di una connessione iSCSI al sistema storage remoto.
- Nel sistema storage e-Series locale, creare un volume di destinazione per l'operazione di importazione. Assicurarsi che il volume abbia una capacità uguale o superiore al volume di origine, abbia una dimensione del blocco corrispondente al volume di origine e non sia mappato. Vedere "Creare volumi".
- Configurare il sistema storage e-Series locale come host sul sistema remoto utilizzando il nome iSCSI qualificato (IQN). È possibile visualizzare l'IQN dal **Impostazioni › sistema › Impostazioni iSCSI › IQN di destinazione**. Inoltre, assicurarsi di impostare il tipo di host appropriato in base al sistema in uso.
- Arrestare tutti i sistemi i/o, smontare i file system e rimuovere eventuali assegnazioni agli host o alle applicazioni per il volume selezionato sul sistema di storage remoto.
- Assegnare il volume al sistema di storage remoto all'host del sistema di storage e-Series locale appena creato.
- Raccogliere le seguenti informazioni dal sistema di storage remoto in modo da poter creare l'importazione:
  - Nome qualificato iSCSI (IQN)
  - Indirizzo IP iSCSI
  - Il numero LUN del dispositivo di storage remoto, in cui provengono i dati di origine
- Una volta avviato il processo di importazione, l'intero volume di destinazione locale viene sovrascritto con i dati copiati. I nuovi dati scritti nel volume di destinazione locale vengono propagati al volume sul dispositivo di storage remoto dopo la creazione dell'importazione. Pertanto, si consiglia di eseguire il backup dei volumi sul sistema di storage remoto prima di avviare il processo di importazione.

Processo di importazione

La procedura seguente illustra il processo di importazione.

1. Accedere all'interfaccia di System Manager, quindi alla pagina **Remote Storage**. Selezionare **Importa** per avviare una nuova creazione di importazione. Per istruzioni dettagliate, vedere "Importa storage remoto".

   Se si desidera eseguire un'importazione offline, non mappare il volume di destinazione fino al completamento dell'importazione.

2. Monitorare l'avanzamento dell'importazione.

   Una volta avviata l'importazione, è possibile mappare il volume di destinazione. Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del dispositivo di storage remoto (volume di origine), dall'impostazione della priorità per l'importazione e dalla quantità di carico i/o sui sistemi storage e sui volumi associati.

   Al termine dell'importazione, il volume di destinazione è un duplicato dell'origine.

3. Quando si è pronti a interrompere la relazione di mappatura, eseguire un'operazione **Disconnect** sull'oggetto di importazione dal pannello **Operations in Progress** (operazioni in corso).

Una volta disconnessa l'importazione, le prestazioni della destinazione locale tornano alla normalità e non sono più influenzate dalla connessione remota.

Restrizioni

La funzione di storage remoto presenta le seguenti restrizioni:

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

Ulteriori informazioni

Per ulteriori informazioni sulla funzione di storage remoto, visitare il sito "Report tecnico sullo storage remoto".

Componenti hardware

Panoramica dei componenti hardware

È possibile controllare lo stato dei componenti nella pagina hardware ed eseguire alcune funzioni correlate a tali componenti.

Quali componenti posso gestire?

È possibile controllare lo stato dei componenti ed eseguire alcune funzioni correlate a questi componenti:

- **Shelf** — Un *shelf* è un componente che contiene l'hardware per lo storage array (controller, alimentatori/ventole e dischi). Gli shelf sono disponibili in tre dimensioni per ospitare fino a 12, 24 o 60 dischi.
- **Controller** — Un *controller* è l'hardware e il firmware combinati che implementa le funzioni di storage array e gestione. Include la memoria cache, il supporto del disco e le porte per le connessioni host.
- **Dischi** — Un *disco* può essere un disco rigido (HDD) o un disco a stato solido (SSD). A seconda delle dimensioni dello shelf, è possibile installare fino a 12, 24 o 60 dischi nello shelf.

Scopri di più:

- "Pagina hardware"
- "Terminologia hardware"

Come si visualizzano i componenti hardware?

Accedere alla pagina hardware, che fornisce una rappresentazione grafica dei componenti fisici dell'array di storage. È possibile passare dalla vista anteriore a quella posteriore degli shelf degli array selezionando **Mostra retro dello shelf** o **Mostra parte anteriore dello shelf** dall'alto a destra della vista dello shelf.

Scopri di più:

- "Visualizzare lo stato e le impostazioni dei componenti dello shelf"
- "Visualizzare le impostazioni del controller"
- "Visualizzare lo stato e le impostazioni del disco"

Informazioni correlate

Scopri di più sui concetti relativi all'hardware:

- "stati del controller"
- "stati del disco"
- "Protezione contro la perdita di scaffali e protezione contro la perdita di cassetti"

Concetti

Pagina hardware e componenti

La pagina hardware fornisce una rappresentazione grafica dei componenti fisici dell'array di storage. Da qui, è possibile controllare lo stato dei componenti ed eseguire alcune funzioni correlate a tali componenti.

Shelf

Uno shelf è un componente che contiene l'hardware per lo storage array (controller, alimentatori/ventole e dischi). Esistono due tipi di shelf:

- **Controller shelf** — contiene i dischi, i contenitori di alimentazione/ventole e i controller.
- **Shelf di dischi** (o **shelf di espansione**) — contiene dischi, alimentatori/ventole e due moduli di input/output (IOM). Gli IOM, noti anche come ESM (Environmental Service Module), includono porte SAS che collegano lo shelf di dischi allo shelf di controller.

Gli shelf sono disponibili in tre dimensioni per ospitare fino a 12, 24 o 60 dischi. Ogni shelf include un numero ID assegnato dal firmware del controller. L'ID viene visualizzato in alto a sinistra nella vista dello shelf.

La vista shelf nella pagina hardware mostra i componenti anteriori o posteriori. È possibile passare da una vista all'altra selezionando **Mostra retro dello shelf** o **Mostra parte anteriore dello shelf** dall'alto a destra della vista dello shelf. È inoltre possibile selezionare **Mostra tutto in primo piano** o **Mostra tutto in secondo piano** dalla parte inferiore della pagina. Le viste anteriore e posteriore mostrano quanto segue:

- **Componenti anteriori** — dischi e alloggiamenti vuoti.
- **Componenti posteriori** — Controller e alimentatori/ventole (per shelf di controller) o IOM e alimentatori/ventole (per shelf di dischi).

È possibile eseguire le seguenti funzioni relative agli shelf:

- Accendere la luce di posizionamento dello shelf, in modo da individuare la posizione fisica dello shelf nel cabinet o nel rack.
- Modificare il numero ID visualizzato in alto a sinistra nella vista dello shelf.
- Visualizzare le impostazioni dello shelf, ad esempio i tipi di dischi installati e il numero di serie.
- Spostare le viste dello shelf verso l'alto o verso il basso in modo che corrispondano al layout fisico dell'array di storage.

Controller

Un controller è l'hardware e il firmware combinati che implementa le funzioni di storage array e gestione. Include la memoria cache, il supporto del disco e il supporto dell'interfaccia host.

È possibile eseguire le seguenti funzioni relative ai controller:

- Configurare le porte di gestione per gli indirizzi IP e la velocità.
- Configurare le connessioni host iSCSI (se si dispone di host iSCSI).
- Configurare un server NTP (Network Time Protocol) e un server DNS (Domain Name System).
- Visualizzare lo stato e le impostazioni del controller.
- Consentire agli utenti esterni alla rete locale di avviare una sessione SSH e modificare le impostazioni del controller.
- Impostare il controller offline, online o in modalità di servizio.

Dischi

Lo storage array può includere dischi rigidi (HDD) o dischi a stato solido (SSD). A seconda delle dimensioni dello shelf, è possibile installare fino a 12, 24 o 60 dischi nello shelf.

È possibile eseguire le seguenti funzioni relative ai dischi:

- Accendere la spia di localizzazione dell'unità, in modo da individuare la posizione fisica dell'unità nello shelf.

- Visualizzare lo stato e le impostazioni del disco.
- Riassegnare un disco (sostituire logicamente un disco guasto con un disco non assegnato) e ricostruire manualmente il disco, se necessario.
- Eseguire manualmente il failover di un disco per poterlo sostituire. (Il guasto di un disco consente di copiare il contenuto del disco prima di sostituirlo).
- Assegnare o annullare l'assegnazione di hot spare.
- Cancellare i dischi.

Terminologia hardware

I seguenti termini hardware si applicano agli array di storage.

Termini generali dell'hardware:

Componente	Descrizione
Baia	Un alloggiamento è uno slot nello shelf in cui è installato un disco o un altro componente.
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di System Manager.
Shelf di controller	Uno shelf di controller contiene un set di dischi e uno o più contenitori di controller. Un contenitore di controller contiene i controller, le schede di interfaccia host (HICS) e le batterie.
Disco	Un disco è un dispositivo elettromeccanico o un dispositivo di memoria a stato solido che fornisce il supporto di storage fisico per i dati.
Shelf di dischi	Uno shelf di dischi, chiamato anche shelf di espansione, contiene un set di dischi e due moduli di input/output (IOM). Gli IOM contengono porte SAS che collegano uno shelf di dischi a uno shelf di controller o ad altri shelf di dischi.
IOM (ESM)	IOM è un modulo di input/output che include porte SAS per il collegamento dello shelf di dischi allo shelf di controller. Nei precedenti modelli di controller, l'IOM era definito come ESM (Environmental Service Module).
Alimentazione/filtro a carboni attivi della ventola	Un contenitore di alimentazione/ventola è un gruppo che scorre in un ripiano. Include un alimentatore e una ventola integrata.
SFP	Un SFP è un ricetrasmettitore SFP (Small Form-Factor Pluggable).
Shelf	Uno shelf è un enclosure installato in un cabinet o in un rack. Contiene i componenti hardware per lo storage array. Esistono due tipi di shelf: Uno shelf di controller e uno shelf di dischi. Uno shelf di controller include controller e dischi. Uno shelf di dischi include i moduli di input/output (IOM) e i dischi.
Array di storage	Uno storage array include shelf, controller, dischi, software e firmware.

Termini del controller:

Componente	Descrizione
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di System Manager.
Shelf di controller	Uno shelf di controller contiene un set di dischi e uno o più contenitori di controller. Un contenitore di controller contiene i controller, le schede di interfaccia host (HICS) e le batterie.
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.
DNS	DNS (Domain Name System) è un sistema di denominazione per i dispositivi connessi a Internet o a una rete privata. Il server DNS mantiene una directory di nomi di dominio e li converte in indirizzi IP (Internet Protocol).
Configurazioni duplex	Il duplex è una configurazione a due moduli controller all'interno dello storage array. I sistemi duplex sono completamente ridondanti rispetto a controller, percorsi di volumi logici e percorsi di dischi. In caso di guasto di un controller, l'altro controller assume il controllo dell'i/o per mantenere la disponibilità. I sistemi duplex dispongono anche di ventole e alimentatori ridondanti.
Connessioni full-duplex/half-duplex	Full-duplex e half-duplex si riferiscono alle modalità di connessione. In modalità full-duplex, due dispositivi possono comunicare contemporaneamente in entrambe le direzioni. In modalità half-duplex, i dispositivi possono comunicare in una direzione alla volta (un dispositivo invia un messaggio, mentre l'altro lo riceve).
HIC	È possibile installare una scheda di interfaccia host (HIC) all'interno di un contenitore di controller. Le porte host integrate nel controller sono chiamate porte host baseboard. Le porte host integrate nell'HIC sono chiamate porte HIC.
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.
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.

Componente	Descrizione
MTU	Una MTU (Maximum Transmission Unit) è il pacchetto o frame di dimensioni maggiori che può essere inviato in una rete.
NTP	Network Time Protocol (NTP) è un protocollo di rete per la sincronizzazione del clock tra sistemi di computer in reti di dati.
Configurazioni simplex	Simplex è una configurazione a modulo controller singolo all'interno dell'array di storage. Un sistema simplex non offre la ridondanza del controller o del percorso del disco, ma dispone di ventole e alimentatori ridondanti.
VLAN	Una VLAN (Virtual Local Area Network) è una rete logica che si comporta come se fosse fisicamente separata dalle altre reti supportate dagli stessi dispositivi (switch, router, ecc.).

Termini del disco:

Componente	Descrizione
DA	Data Assurance (da) è una funzione che controlla e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Data Assurance può essere abilitato a livello di pool o gruppo di volumi, con host che utilizzano un'interfaccia i/o compatibile con da, ad esempio Fibre Channel.
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.
Shelf di dischi	Uno shelf di dischi, chiamato anche shelf di espansione, contiene un set di dischi e due moduli di input/output (IOM). Gli IOM contengono porte SAS che collegano uno shelf di dischi a uno shelf di controller o ad altri shelf di dischi.
DULBE	Deallocated or Unwritten Logical Block Error (DULBE) è un'opzione sui dischi NVMe che consente allo storage array EF300 o EF600 di supportare volumi con provisioning delle risorse.
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.
DISCO RIGIDO	I dischi rigidi (HDD) sono dispositivi di storage dei dati che utilizzano dischi metallici rotanti con rivestimento magnetico.
Dischi hot spare	Le hot spare fungono da unità di standby nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Si tratta di dischi completamente funzionanti che non contengono dati. Se un disco si guasta nel gruppo di volumi, il controller ricostruisce automaticamente i dati dal disco guasto a un hot spare.
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.

Componente	Descrizione
SAS	Serial Attached SCSI (SAS) è un protocollo seriale point-to-point che collega i controller direttamente ai dischi.
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.
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.

Termini iSCSI:

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.

Termine	Descrizione
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.

Termini NVMe:

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.
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.

Termine	Descrizione
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.

Gestire i componenti dello shelf

Visualizza i componenti hardware

La pagina hardware offre funzioni di ordinamento e filtraggio che semplificano la ricerca dei componenti.

Fasi

1. Selezionare **hardware**.
2. Utilizzare le funzioni descritte nella seguente tabella per visualizzare i componenti hardware.

Funzione	Descrizione
Viste di dischi, controller e componenti	Per passare dalla vista anteriore a quella posteriore, selezionare **Drives** (unità) o **Controllers & Components** (Controller e componenti) dall'estrema destra (il collegamento visualizzato dipende dalla vista corrente). La vista **Drives** mostra i dischi e gli eventuali alloggiamenti vuoti. La vista **Controller & Components** mostra i controller, i moduli IOM (ESM), i contenitori di alimentazione/ventole o gli alloggiamenti dei controller vuoti. Nella parte inferiore della pagina, è anche possibile selezionare **Mostra tutti i dischi**.
Filtri per la vista su disco	Se lo storage array contiene dischi con diversi tipi di attributi fisici e logici, la pagina **hardware** include i filtri di visualizzazione del disco. Questi campi di filtro consentono di individuare rapidamente unità specifiche limitando i tipi di unità visualizzati nella pagina. Sotto **Mostra dischi che sono…**, fare clic sul campo del filtro a sinistra (per impostazione predefinita, mostra **qualsiasi tipo di disco**) per visualizzare un elenco a discesa degli attributi fisici (ad esempio capacità e velocità). Fare clic sul campo del filtro a destra (per impostazione predefinita, mostra **in qualsiasi punto dello storage array**) per visualizzare un elenco a discesa degli attributi logici (ad esempio, l'assegnazione dei gruppi di volumi). È possibile utilizzare questi filtri insieme o separatamente. Se l'array di storage contiene dischi che condividono tutti gli stessi attributi fisici, il campo **qualsiasi tipo di disco** a sinistra non viene visualizzato. Se i dischi si trovano tutti nella stessa posizione logica, il campo **Anywhere in the storage array** (qualsiasi punto dell'array di storage) a destra non viene visualizzato.
Legenda	I componenti vengono visualizzati in determinati colori per illustrare i rispettivi stati di ruolo. Per espandere e comprimere le descrizioni di questi stati, fare clic su **Legenda**.

Funzione	Descrizione
Mostra i dettagli dell'icona di stato	Gli indicatori di stato possono includere descrizioni di testo per gli stati di disponibilità. Fare clic su **Show status icon details** (Mostra dettagli icona stato) per visualizzare o nascondere il testo dello stato.
Icone di shelf/shelf	Ogni vista shelf fornisce un elenco di comandi correlati, oltre a proprietà e stato. Fare clic su **Shelf** per visualizzare un elenco a discesa dei comandi. È inoltre possibile selezionare una delle icone in alto per visualizzare lo stato e le proprietà dei singoli componenti: Controller, IOM (ESM), alimentatori, ventole, temperatura, Batterie e SFP.
Ordine di shelf	Gli shelf possono essere riorganizzati nella pagina hardware. Utilizzare le frecce su e giù nella parte superiore destra di ciascuna vista dello shelf per modificare l'ordine superiore/inferiore degli shelf.

Mostra o nasconde lo stato del componente

È possibile visualizzare le descrizioni dello stato di dischi, controller, ventole e alimentatori.

Fasi

1. Selezionare **hardware**.
2. Per visualizzare i componenti posteriori o anteriori:
   - Se si desidera visualizzare i componenti del controller e del contenitore di alimentazione/ventola, ma i dischi sono visualizzati, fare clic su **Mostra retro dello shelf**.
   - Se si desidera visualizzare i dischi, ma vengono visualizzati i componenti del controller e del contenitore di alimentazione/ventola, fare clic su **Mostra parte anteriore dello shelf**.
3. Per visualizzare o nascondere le descrizioni dello stato a comparsa:
   - Se si desidera visualizzare una descrizione a comparsa delle icone di stato, fare clic su **Mostra dettagli icona di stato** in alto a destra nella vista dello shelf (selezionare la casella di controllo).
   - Per nascondere le descrizioni a comparsa, fare nuovamente clic su **Mostra dettagli icona stato** (deselezionare la casella di controllo).
4. Se si desidera visualizzare i dettagli completi dello stato, selezionare il componente nella vista shelf, quindi selezionare **View settings** (Visualizza impostazioni).
5. Per visualizzare le descrizioni dei componenti colorati, selezionare **Legenda**.

Consente di passare dalla vista anteriore a quella posteriore e viceversa

La pagina hardware può mostrare la vista frontale o posteriore degli scaffali.

A proposito di questa attività

La vista posteriore mostra i controller/IOM e i contenitori delle ventole di alimentazione. La vista frontale mostra i dischi.

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. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

4. In alternativa, è possibile selezionare **Mostra tutto in primo piano** o **Mostra tutto in secondo piano**, nella parte inferiore della pagina.

Modificare l'ordine di visualizzazione degli shelf

È possibile modificare l'ordine degli shelf visualizzati nella pagina hardware in modo che corrisponda all'ordine fisico degli shelf in un cabinet.

Fasi

1. Selezionare **hardware**.
2. Nella parte superiore destra della vista di uno shelf, selezionare le frecce verso l'alto o verso il basso per riordinare l'ordine degli shelf mostrato nella pagina hardware.

Accendere la luce di posizionamento degli scaffali

Per individuare la posizione fisica di uno shelf mostrato nella pagina hardware, è possibile accendere la luce di localizzazione dello shelf.

Fasi

1. Selezionare **hardware**.
2. Selezionare l'elenco a discesa per lo shelf del controller o lo shelf dell'unità, quindi selezionare **accendere la luce di localizzazione**.

   La spia di posizionamento dello scaffale si accende.

3. Una volta posizionato lo shelf, tornare alla finestra di dialogo e selezionare **Spegni**.

Modificare gli ID degli shelf

L'ID dello shelf è un numero che identifica in modo univoco uno shelf nell'array di storage. Gli shelf sono numerati consecutivamente, a partire da 00 o 01, nella parte superiore sinistra di ciascuna vista.

A proposito di questa attività

Il firmware del controller assegna automaticamente l'ID dello shelf, ma è possibile modificarlo se si desidera creare un diverso schema di ordinazione.

Fasi

1. Selezionare **hardware**.
2. Selezionare l'elenco a discesa per lo shelf del controller o per lo shelf del disco, quindi selezionare **Change ID** (Modifica ID).
3. Nella finestra di dialogo Change Shelf ID (Modifica ID shelf), selezionare l'elenco a discesa per visualizzare

i numeri disponibili.

Questa finestra di dialogo non visualizza gli ID attualmente assegnati agli shelf attivi.

4. Selezionare un numero disponibile, quindi fare clic su **Salva**.

   A seconda del numero selezionato, l'ordine dello shelf può essere riorganizzato nella pagina hardware. Se lo si desidera, è possibile utilizzare le frecce su/giù nella parte superiore destra di ogni shelf per regolare di nuovo l'ordine.

Visualizzare lo stato e le impostazioni dei componenti dello shelf

La pagina hardware fornisce lo stato e le impostazioni dei componenti dello shelf, inclusi alimentatori, ventole e batterie.

A proposito di questa attività

I componenti disponibili dipendono dal tipo di shelf:

- **Shelf di dischi** — contiene un set di dischi, alimentatori/ventole, moduli di input/output (IOM) e altri componenti di supporto in un unico shelf.
- **Ripiano controller** — contiene un set di dischi, uno o due contenitori controller, contenitori di alimentazione/ventole e altri componenti di supporto in un unico shelf.

Fasi

1. Selezionare **hardware**.
2. Selezionare l'elenco a discesa per lo shelf del controller o lo shelf dell'unità, quindi selezionare **View Settings** (Visualizza impostazioni).

   Viene visualizzata la finestra di dialogo Shelf Components Settings (Impostazioni componenti shelf), con schede che mostrano lo stato e le impostazioni relative ai componenti dello shelf. A seconda del tipo di shelf selezionato, alcune schede descritte nella tabella potrebbero non essere visualizzate.

Scheda	Descrizione
Shelf	La scheda **Shelf** mostra le seguenti proprietà: • **ID shelf** — identifica in modo univoco uno shelf nell'array di storage. Il firmware del controller assegna questo numero, ma è possibile modificarlo selezionando **Shelf › Cambia ID**. • **Ridondanza del percorso shelf** — specifica se le connessioni tra lo shelf e il controller hanno metodi alternativi (Sì) o meno (No). • **Tipi di dischi correnti** — Mostra il tipo di tecnologia integrata nei dischi (ad esempio, un disco SAS sicuro). Se è presente più di un tipo di disco, vengono visualizzate entrambe le tecnologie. • **Numero di serie** — indica il numero di serie dello shelf.

Scheda	Descrizione
IOM (ESM)	La scheda **IOM (ESM)** mostra lo stato del modulo di input/output (IOM), chiamato anche modulo di servizio ambientale (ESM). Monitora lo stato dei componenti in uno shelf di dischi e funge da punto di connessione tra il vassoio dell'unità e il controller. Lo stato può essere ottimale, non riuscito, ottimale (Miswire) o non certificato. Altre informazioni includono la versione del firmware e la versione delle impostazioni di configurazione. Selezionare **Mostra altre impostazioni** per visualizzare la velocità di trasferimento dati massima e corrente e lo stato della comunicazione della scheda (Sì o No). È anche possibile visualizzare questo stato selezionando l'icona IOM Accanto all'elenco a discesa Shelf.
Alimentatori	La scheda **alimentatori** mostra lo stato del contenitore dell'alimentatore e dell'alimentatore stesso. Lo stato può essere ottimale, non riuscito, rimosso o Sconosciuto. Mostra anche il codice dell'alimentatore. Per visualizzare questo stato, selezionare l'icona Power Supply (alimentatore) Accanto all'elenco a discesa Shelf.
Ventole	La scheda **ventole** mostra lo stato del filtro a carboni attivi e della ventola stessa. Lo stato può essere ottimale, non riuscito, rimosso o Sconosciuto. È possibile visualizzare questo stato anche selezionando l'icona ventola Accanto all'elenco a discesa Shelf.
Temperatura	La scheda **temperatura** mostra lo stato della temperatura dei componenti dello shelf, come i sensori, i controller e i contenitori di alimentazione/ventola. Lo stato può essere ottimale, temperatura nominale superata, temperatura massima superata o sconosciuta. È anche possibile visualizzare questo stato selezionando l'icona della temperatura Accanto all'elenco a discesa Shelf.
Batterie	La scheda **batterie** mostra lo stato delle batterie del controller. Lo stato può essere ottimale, non riuscito, rimosso o Sconosciuto. Altre informazioni includono l'età della batteria, i giorni prima della sostituzione, i cicli di apprendimento e le settimane tra i cicli di apprendimento. È possibile visualizzare questo stato anche selezionando l'icona delle batterie Accanto all'elenco a discesa Shelf.

Scheda	Descrizione
SFP	La scheda **SFP** mostra lo stato dei ricetrasmettitori SFP (Small Form-Factor Pluggable) sui controller. Lo stato può essere ottimale, non riuscito o Sconosciuto. Selezionare **Mostra altre impostazioni** per visualizzare il numero di parte, il numero di serie e il fornitore degli SFP. È possibile visualizzare questo stato anche selezionando l'icona SFP Accanto all'elenco a discesa Shelf.

3. Fare clic su **Chiudi**.

Aggiornare i cicli di apprendimento della batteria

Un ciclo di apprendimento è un ciclo automatico per la calibrazione dell'indicatore della batteria Smart. I cicli vengono pianificati per avviarsi automaticamente, nello stesso giorno e ora, a intervalli di 8 settimane (per controller). Se si desidera impostare un programma diverso, è possibile regolare i cicli di apprendimento.

A proposito di questa attività

L'aggiornamento dei cicli di apprendimento influisce su entrambe le batterie del controller.

Fasi

1. Selezionare **hardware**.
2. Selezionare l'elenco a discesa per lo shelf del controller, quindi selezionare **View settings** (Visualizza impostazioni).
3. Selezionare la scheda **batterie**.
4. Selezionare **Aggiorna cicli di apprendimento batteria**.

   Viene visualizzata la finestra di dialogo Update Battery Learn Cycles.

5. Dagli elenchi a discesa, selezionare un nuovo giorno e un'ora.
6. Fare clic su **Save** (Salva).

Gestire i controller

stati del controller

È possibile posizionare un controller in tre stati diversi: Online, offline e service mode.

Stato online

Lo stato online è il normale stato operativo del controller. Significa che il controller funziona normalmente ed è disponibile per le operazioni di i/O.

Quando si posiziona un controller online, lo stato viene impostato su ottimale.

Stato offline

Lo stato offline viene in genere utilizzato per preparare un controller per la sostituzione quando vi sono due controller nell'array di storage. Un controller può entrare nello stato offline in due modi: È possibile eseguire un comando esplicito o il controller potrebbe non funzionare. Un controller può uscire dallo stato offline solo emettendo un altro comando esplicito o sostituendo il controller guasto. È possibile posizionare un controller offline solo se sono presenti due controller nell'array di storage.

Quando un controller si trova nello stato offline, si verificano le seguenti condizioni:

- Il controller non è disponibile per i/O.
- Non è possibile gestire lo storage array attraverso tale controller.
- Tutti i volumi attualmente di proprietà di quel controller vengono spostati nell'altro controller.
- Il mirroring della cache viene disattivato e tutti i volumi vengono modificati in modalità di scrittura tramite cache.

Modalità di servizio

La modalità Service viene generalmente utilizzata solo dal supporto tecnico per spostare tutti i volumi di array di storage in un controller in modo che sia possibile eseguire la diagnosi dell'altro controller. Un controller deve essere inserito manualmente in modalità di servizio e deve essere riportato manualmente online una volta completata l'operazione di servizio.

Quando un controller è in modalità di servizio, sono soddisfatte le seguenti condizioni:

- Il controller non è disponibile per i/O.
- Il supporto tecnico può accedere al controller attraverso la porta seriale o la connessione di rete per analizzare i potenziali problemi.
- Tutti i volumi attualmente di proprietà di quel controller vengono spostati nell'altro controller.
- Il mirroring della cache viene disattivato e tutti i volumi vengono modificati in modalità di scrittura tramite cache.

Considerazioni per l'assegnazione degli indirizzi IP

Per impostazione predefinita, i controller vengono forniti con DHCP attivato su entrambe le porte di rete. È possibile assegnare indirizzi IP statici, utilizzare gli indirizzi IP statici predefiniti o utilizzare indirizzi IP assegnati da DHCP. È inoltre possibile utilizzare la configurazione automatica senza stato IPv6.

> IPv6 è disattivato per impostazione predefinita sui nuovi controller, ma è possibile configurare gli indirizzi IP delle porte di gestione utilizzando un metodo alternativo e quindi attivare IPv6 sulle porte di gestione utilizzando System Manager.

Quando la porta di rete si trova in uno stato di "collegamento inattivo", ovvero disconnesso da una LAN, il sistema riporta la configurazione come statica, visualizzando un indirizzo IP 0.0.0.0 (versioni precedenti) o DHCP abilitato senza alcun indirizzo IP riportato (versioni successive). Una volta che la porta di rete si trova in uno stato di "collegamento" (ovvero connesso a una LAN), tenta di ottenere un indirizzo IP tramite DHCP.

Se il controller non riesce a ottenere un indirizzo DHCP su una determinata porta di rete, ripristina un indirizzo IP predefinito, che potrebbe richiedere fino a 3 minuti. Gli indirizzi IP predefiniti sono i seguenti:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Quando si assegnano indirizzi IP:

- Riservare la porta 2 sui controller per l'utilizzo da parte del supporto clienti. Non modificare le impostazioni di rete predefinite (DHCP attivato).
- Per impostare gli indirizzi IP statici per i controller E2800 e E5700, utilizzare Gestione di sistema di SANtricity. Per impostare gli indirizzi IP statici per i controller E2700 e E5600, utilizzare Gestione storage SANtricity. Dopo aver configurato un indirizzo IP statico, questo rimane impostato attraverso tutti gli eventi link down/up.
- Per utilizzare DHCP per assegnare l'indirizzo IP del controller, collegare il controller a una rete in grado di elaborare le richieste DHCP. Utilizzare un lease DHCP permanente.

> Gli indirizzi predefiniti non sono persistenti tra gli eventi di collegamento inattivo. Quando una porta di rete su un controller è impostata per utilizzare DHCP, il controller tenta di ottenere un indirizzo DHCP per ogni evento di collegamento, inclusi inserimento dei cavi, riavvii e cicli di alimentazione. Ogni volta che un tentativo DHCP non riesce, viene utilizzato l'indirizzo IP statico predefinito per tale porta.

Configurare la porta di gestione

Il controller include una porta Ethernet utilizzata per la gestione del sistema. Se necessario, è possibile modificarne i parametri di trasmissione e gli indirizzi IP.

A proposito di questa attività

Durante questa procedura, selezionare la porta 1, quindi determinare la velocità e il metodo di indirizzamento della porta. La porta 1 si connette alla rete in cui il client di gestione può accedere al controller e a System Manager.

> Non utilizzare la porta 2 su entrambi i controller. La porta 2 è riservata al supporto tecnico.

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 di gestione che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configura porte di gestione**.

   Viene visualizzata la finestra di dialogo Configura porte di gestione.

5. Verificare che sia visualizzata la porta 1, quindi fare clic su **Avanti**.
6. Selezionare le impostazioni della porta di configurazione, quindi fare clic su **Avanti**.

   Dettagli del campo

Campo	Descrizione
Velocità e modalità duplex	Mantenere l'impostazione negoziazione automatica se si desidera che System Manager determini i parametri di trasmissione tra lo storage array e la rete; in alternativa, se si conosce la velocità e la modalità della rete, selezionare i parametri dall'elenco a discesa. Nell'elenco vengono visualizzate solo le combinazioni valide di velocità e duplex.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.

   Se si seleziona **Enable IPv4** (attiva IPv4), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv4. Se si seleziona **Enable IPv6** (attiva IPv6*), dopo aver fatto clic su **Next** (Avanti) viene visualizzata una finestra di dialogo per la selezione delle impostazioni IPv6. Se si selezionano 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 del campo

Campo	Descrizione
Ottenere automaticamente la configurazione dal server DHCP	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire l'indirizzo IP del controller. (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. Se si modifica la configurazione dell'indirizzo IP, si perde il percorso di gestione dello storage array. Se si utilizza Gestione unificata di SANtricity per gestire gli array in rete a livello globale, aprire l'interfaccia utente e accedere al **Gestisci › Scopri**. Se si utilizza Gestione storage SANtricity, è necessario rimuovere il dispositivo dalla finestra Gestione aziendale, aggiungerlo nuovamente all'EMW selezionando **Modifica › Aggiungi array storage**, quindi inserire il nuovo indirizzo IP.

8. Fare clic su **fine**.

Risultati

La configurazione della porta di gestione viene visualizzata nelle impostazioni del controller, scheda Management Ports (Porte di gestione).

Configurare gli indirizzi del server NTP

È possibile configurare una connessione al server NTP (Network Time Protocol) in modo che il controller interroga periodicamente il server NTP per aggiornare l'orologio interno dell'ora del giorno.

Prima di iniziare

- Nella rete deve essere installato e configurato un server NTP.
- È necessario conoscere l'indirizzo del server NTP primario e di un server NTP di backup opzionale. Questi indirizzi possono essere nomi di dominio completi, indirizzi IPv4 o indirizzi IPv6.

Se si inseriscono uno o più nomi di dominio per i server NTP, è necessario configurare anche un server DNS per risolvere l'indirizzo del server NTP. È necessario configurare il server DNS solo sui controller in cui è stato configurato NTP e fornito un nome di dominio.

A proposito di questa attività

NTP consente allo storage array di sincronizzare automaticamente i clock del controller con un host esterno utilizzando il protocollo SNTP (Simple Network Time Protocol). Il controller interroga periodicamente il server NTP configurato, quindi utilizza i risultati per aggiornare l'orologio interno dell'ora del giorno. Se solo un

controller ha attivato NTP, il controller alternativo sincronizza periodicamente il proprio clock con il controller che ha attivato NTP. Se nessuno dei due controller ha attivato NTP, i controller sincronizzano periodicamente i propri orologi.

> Non è necessario configurare NTP su entrambi i controller; tuttavia, in questo modo si migliora la capacità dello storage array di rimanere sincronizzato in caso di guasti hardware o di comunicazione.

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 che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configure NTP server** (Configura server NTP).

   Viene visualizzata la finestra di dialogo Configura server NTP (Network Time Protocol).

5. Selezionare **i want to enable NTP on Controller** (**A** or **B**).

   Nella finestra di dialogo vengono visualizzate ulteriori selezioni.

6. Selezionare una delle seguenti opzioni:
   - **Ottieni automaticamente gli indirizzi del server NTP dal server DHCP** — vengono visualizzati gli indirizzi del server NTP rilevati.

     > Se lo storage array è impostato per utilizzare un indirizzo NTP statico, non viene visualizzato alcun server NTP.

   - **Specificare manualmente gli indirizzi del server NTP** — inserire l'indirizzo del server NTP primario e un indirizzo del server NTP di backup. Il server di backup è opzionale. (Questi campi vengono visualizzati dopo aver selezionato il pulsante di opzione). L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
7. **Opzionale:** inserire le informazioni sul server e le credenziali di autenticazione per un server NTP di backup.
8. Fare clic su **Save** (Salva).

Risultati

La configurazione del server NTP viene visualizzata nella scheda delle impostazioni del controller, **DNS / NTP**.

Configurare gli indirizzi del server DNS

DNS (Domain Name System) viene utilizzato per risolvere i nomi di dominio completi per i controller e un server NTP (Network Time Protocol). Le porte di gestione dello storage array supportano contemporaneamente i protocolli IPv4 o IPv6.

Prima di iniziare

- Nella rete deve essere installato e configurato un server DNS.
- Si conosce l'indirizzo del server DNS primario e di un server DNS di backup opzionale. Questi indirizzi possono essere indirizzi IPv4 o IPv6.

A proposito di questa attività

Questa procedura descrive come specificare un indirizzo del server DNS primario e di backup. Il server DNS di backup può essere configurato in modo opzionale per l'utilizzo in caso di guasto di un server DNS primario.

> Se le porte di gestione dello storage array sono già state configurate con il protocollo DHCP (Dynamic host Configuration Protocol) e si dispone di uno o più server DNS o NTP associati alla configurazione DHCP, non è necessario configurare manualmente DNS o NTP. In questo caso, lo storage array avrebbe già ottenuto automaticamente gli indirizzi del server DNS/NTP. Tuttavia, seguire le istruzioni riportate di seguito per aprire la finestra di dialogo e assicurarsi che vengano rilevati gli indirizzi corretti.

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. Selezionare il controller da configurare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configura server DNS**.

   Viene visualizzata la finestra di dialogo Configura server DNS (Domain Name System).

5. Selezionare una delle seguenti opzioni:
   - **Ottieni automaticamente gli indirizzi del server DNS dal server DHCP** — vengono visualizzati gli indirizzi del server DNS rilevati.

     > Se lo storage array è impostato per utilizzare un indirizzo DNS statico, non viene visualizzato alcun server DNS.

   - **Specificare manualmente gli indirizzi del server DNS** — inserire un indirizzo del server DNS primario e un indirizzo del server DNS di backup. Il server di backup è opzionale. (Questi campi vengono visualizzati dopo aver selezionato il pulsante di opzione). Questi indirizzi possono essere indirizzi IPv4 o IPv6.
6. Fare clic su **Save** (Salva).
7. Ripetere questa procedura per l'altro controller.

Risultati

La configurazione DNS viene visualizzata nella scheda delle impostazioni del controller, **DNS / NTP**.

Visualizzare le impostazioni del controller

È possibile visualizzare informazioni su un controller, ad esempio lo stato delle interfacce host, delle interfacce disco e delle porte di gestione.

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. Per visualizzare le impostazioni del controller, eseguire una delle seguenti operazioni:
   - Fare clic sul controller per visualizzare il menu di scelta rapida, quindi selezionare **View settings** (Visualizza impostazioni).
   - Selezionare l'icona del controller (accanto all'elenco a discesa **Shelf**). Per le configurazioni duplex, selezionare **Controller A** o **Controller B** dalla finestra di dialogo, quindi fare clic su **Avanti**.

     Viene visualizzata la finestra di dialogo Controller Settings (Impostazioni controller).

4. Selezionare le schede per spostarsi tra le impostazioni delle proprietà.

   Alcune schede dispongono di un collegamento per **Mostra altre impostazioni** in alto a destra.

Dettagli del campo

Scheda	Descrizione
Base	Mostra lo stato del controller, il nome del modello, il codice ricambio, la versione corrente del firmware e la versione DELLA memoria ad accesso casuale statica non volatile (NVSRAM).
Cache	Mostra le impostazioni della cache del controller, che includono la cache dei dati, la cache del processore e la periferica di backup della cache. La periferica di backup della cache viene utilizzata per eseguire il backup dei dati nella cache in caso di perdita di alimentazione al controller. Lo stato può essere ottimale, non riuscito, rimosso, sconosciuto, protetto da scrittura, O incompatibile.
Interfacce host	Mostra le informazioni sull'interfaccia host e lo stato del collegamento di ciascuna porta. L'interfaccia host è la connessione tra il controller e l'host, ad esempio Fibre Channel o iSCSI. La posizione della scheda di interfaccia host (HIC) si trova nella scheda base o in uno slot (alloggiamento). "Baseboard" indica che le porte HIC sono integrate nel controller. Le porte "slot" si trovano sull'HIC opzionale.
Interfacce del disco	Mostra le informazioni sull'interfaccia del disco e lo stato del collegamento di ciascuna porta. L'interfaccia del disco è la connessione tra il controller e i dischi, ad esempio SAS.
Porte di gestione	Mostra i dettagli della porta di gestione, ad esempio il nome host utilizzato per accedere al controller e se è stato attivato un accesso remoto. La porta di gestione collega il controller e il client di gestione, che è il punto in cui viene installato un browser per l'accesso a System Manager.
DNS/NTP	Mostra il metodo di indirizzamento e gli indirizzi IP per il server DNS e il server NTP, se questi server sono stati configurati in System Manager. DNS (Domain Name System) è un sistema di denominazione per i dispositivi connessi a Internet o a una rete privata. Il server DNS mantiene una directory di nomi di dominio e li converte in indirizzi IP (Internet Protocol). Network Time Protocol (NTP) è un protocollo di rete per la sincronizzazione del clock tra sistemi di computer in reti di dati.

5. Fare clic su **Chiudi**.

Configurare l'accesso remoto (SSH)

Attivando l'accesso remoto, gli utenti esterni alla rete locale possono avviare una

sessione SSH e accedere alle impostazioni del controller.

Per SANtricity versione 11.74 e successive, è anche possibile configurare l'autorizzazione multifattore (MFA) richiedendo agli utenti di inserire una chiave SSH e/o una password SSH. Per le versioni 11.73 e precedenti di SANtricity, questa funzione *non* include un'opzione per l'autorizzazione a più fattori con chiavi SSH e password.

Rischi per la sicurezza — per motivi di sicurezza, solo il personale di supporto tecnico deve utilizzare la funzione di accesso remoto.

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 per il quale si desidera configurare l'accesso remoto.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Configura accesso remoto (SSH)**. (Per SANtricity versione 11.73 e precedenti, questa voce di menu è **Modifica accesso remoto**.)

   Viene visualizzata la finestra di dialogo per l'abilitazione dell'accesso remoto.

5. Selezionare la casella di controllo **Enable remote login** (attiva accesso remoto).

   Questa impostazione fornisce l'accesso remoto con tre opzioni per l'autorizzazione:

   - **Solo password**. Per questa opzione, fare clic su **Save** (Salva). Se si dispone di un sistema duplex, è possibile attivare l'accesso remoto sul secondo controller seguendo la procedura precedente.
   - **Chiave SSH o password**. Per questa opzione, passare alla fase successiva.
   - **Sia password che chiave SSH**. Per questa opzione, selezionare la casella di controllo **Richiedi chiave pubblica autorizzata e password per l'accesso remoto** e passare alla fase successiva.
6. Compilare il campo **Authorized public key** (chiave pubblica autorizzata). Questo campo contiene un elenco di chiavi pubbliche autorizzate, nel formato del file OpenSSH **authized_keys**.

   Durante la compilazione del campo **Authorized public key**, tenere presenti le seguenti linee guida:

   - Il campo **Authorized public key** (chiave pubblica autorizzata) si applica a entrambi i controller e deve essere configurato solo sul primo controller.
   - Il file **authized_keys** deve contenere una sola chiave per riga. Le righe che iniziano con n. e vuote vengono ignorate. Per ulteriori informazioni sul formato del file, vedere "Configurazione delle chiavi autorizzate per OpenSSH".
   - Un file **authized_keys** dovrebbe avere un aspetto simile al seguente esempio:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
j1tHymwtbdhPuipd2wIDAQAB
```

7. Al termine, fare clic su **Save** (Salva).
8. Per i sistemi duplex, è possibile attivare l'accesso remoto sul secondo controller seguendo la procedura descritta in precedenza. Se si sta configurando l'opzione sia per una password che per una chiave SSH, assicurarsi di selezionare nuovamente la casella di controllo **Richiedi chiave pubblica autorizzata e password per l'accesso remoto**.
9. Al termine della risoluzione dei problemi, è possibile disattivare l'accesso remoto tornando alla finestra di dialogo Configura accesso remoto e deselezionando la casella di controllo **attiva accesso remoto**. Se l'accesso remoto è attivato su un secondo controller, viene visualizzata una finestra di dialogo di conferma che consente di disattivare l'accesso remoto anche sul secondo controller.

   La disattivazione dell'accesso remoto termina tutte le sessioni SSH correnti e rifiuta le nuove richieste di accesso.

Posizionare il controller online

Se un controller è in stato offline o in modalità di servizio, è possibile ripristinarlo online.

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 su un controller in stato offline o in modalità di servizio.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Place online** (Esegui online) e confermare che si desidera eseguire l'operazione.

Risultati

Il rilevamento di un percorso preferito ripristinato da parte del driver multipath può richiedere fino a 10 minuti.

Tutti i volumi originariamente di proprietà di questo controller vengono automaticamente spostati di nuovo nel controller quando vengono ricevute richieste di i/o per ciascun volume. In alcuni casi, potrebbe essere necessario ridistribuire manualmente i volumi con il comando **redistribuisci volumi**.

Mettere il controller offline

Se viene richiesto di farlo, è possibile mettere un controller offline.

Prima di iniziare

- Lo storage array deve avere due controller. Il controller che non si sta mettendo offline deve essere in linea (nello stato ottimale).
- Assicurarsi che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un

driver multipath.

A proposito di questa attività

> Non mettere un controller offline a meno che non venga richiesto dal Recovery Guru o dal supporto tecnico.

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 che si desidera mettere offline.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Place offline** e confermare che si desidera eseguire l'operazione.

Risultati

System Manager potrebbe impiegare diversi minuti per aggiornare lo stato del controller su offline. Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

Impostare il controller in modalità di servizio

Se viene richiesto di farlo, è possibile impostare un controller in modalità di servizio.

Prima di iniziare

- Lo storage array deve avere due controller. Il controller che non si sta mettendo in modalità di servizio deve essere in linea (nello stato ottimale).
- Assicurarsi che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.

> Il posizionamento di un controller in modalità di servizio potrebbe ridurre significativamente le performance. Non impostare un controller in modalità di servizio a meno che non venga richiesto dal supporto tecnico.

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 che si desidera attivare in modalità di servizio.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **mettere in Service mode** e confermare che si desidera eseguire l'operazione.

Ripristinare (riavviare) il controller

Alcuni problemi richiedono un ripristino del controller (riavvio). È possibile ripristinare il controller anche se non si dispone dell'accesso fisico.

Prima di iniziare

- Lo storage array deve avere due controller. Il controller che non si sta reimpostando deve essere in linea (nello stato ottimale).
- Assicurarsi che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.

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 che si desidera ripristinare.

   Viene visualizzato il menu di scelta rapida del controller.

4. Selezionare **Reset** e confermare che si desidera eseguire l'operazione.

Gestire le porte iSCSI

Configurare le porte iSCSI

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

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).

> 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 del campo

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata (visualizzata solo per alcuni tipi di schede di interfaccia host)	Selezionare la velocità che corrisponde alla velocità del modulo SFP sulla porta.
Modalità FEC (Forward Error Correction) (visualizzata solo per alcuni tipi di schede di interfaccia host)	Se si desidera, selezionare una delle modalità FEC per la porta host specificata. La modalità Reed Solomon non supporta la velocità della porta di 25 Gbps.
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.
Porta TCP in ascolto (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

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

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 del 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 Impostazioni iSCSI, fare clic su **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 (Segreto CHAP iniziatore).

> 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**.

Risultati

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 la voce **Enable iSNS server**… 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 — "Vendor Specific Information". 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).

Risultati

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.

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 **Impostazioni › sistema**.
2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).

   Viene visualizzato un elenco delle sessioni iSCSI correnti.

3. **Opzionale:** per visualizzare ulteriori informazioni su una sessione iSCSI specifica, selezionare una sessione, quindi fare clic su **Visualizza dettagli**.

Dettagli del 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	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. **Opzionale:** per salvare il report in un file, fare clic su **Salva**.

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

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 **Impostazioni › sistema**.
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.

Configurare iSER su porte InfiniBand

Se il controller include una porta iSER su InfiniBand, è possibile configurare la connessione di rete all'host.

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.

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.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. Selezionare **Visualizza statistiche iSER su InfiniBand**.
3. Fare clic su una scheda per visualizzare i diversi set di statistiche.
4. **Opzionale:** per impostare la linea di base, fare clic su **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.

Gestire le porte NVMe

Panoramica di NVMe

Alcuni controller includono una porta per l'implementazione di NVMe (non-volatile Memory Express) su fabric. 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. Un host può accedere a un array di storage NVMe (chiamato *sottosistema*) utilizzando un fabric. 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.

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.

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.

> 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 Configura porte NVMe su InfiniBand.

5. Selezionare la porta HIC che si desidera configurare dall'elenco a discesa, quindi immettere l'indirizzo IP.

   Se si configura un array di storage EF600 con un HIC da 200 GB, questa finestra di dialogo visualizza due campi IP Address (Indirizzo IP), uno per una porta fisica (esterna) e uno per una porta virtuale (interna). È necessario assegnare un indirizzo IP univoco a entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e di ottenere le massime prestazioni dall'HIC. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

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.

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.

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

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

Dettagli del 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. Se si configura un array di storage EF600 con un HIC da 200 GB, questa finestra di dialogo visualizza due serie di campi per i parametri di rete, uno per una porta fisica (esterna) e uno per una porta virtuale (interna). È necessario assegnare parametri univoci per entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e di ottenere le massime prestazioni dall'HIC. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

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** — 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.
- **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. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics.

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 **Impostazioni › sistema**.
2. Selezionare **View NVMe over Fabrics Statistics** (Visualizza statistiche NVMe over Fabrics).
3. **Opzionale:** per impostare la linea di base, fare clic su **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.

Gestire i dischi

stati del disco

System Manager riporta diversi stati per i dischi.

stati di accessibilità

Stato	Definizione
Ignorato	Il disco è fisicamente presente, ma il controller non può comunicare con esso su entrambe le porte.
Incompatibile	Si verifica una delle seguenti condizioni: • Il disco non è certificato per l'utilizzo nello storage array. • Il disco ha dimensioni di settore diverse. • L'unità dispone di dati di configurazione inutilizzabili da una versione firmware precedente o più recente.
Rimosso	L'unità non è stata rimossa correttamente dall'array di storage.
Presente	Il controller può comunicare con il disco su entrambe le porte.
Non risponde	Il disco non risponde ai comandi.

stati dei ruoli

Stato	Definizione
Assegnato	Il disco è membro di un pool o di un gruppo di volumi.
Hot spare in uso	Il disco viene attualmente utilizzato come sostituto di un disco guasto. Le hot spare vengono utilizzate solo nei gruppi di volumi, non nei pool.
Hot spare in standby	Il disco è pronto per essere utilizzato come sostituto di un disco guasto. Le hot spare vengono utilizzate solo nei gruppi di volumi, non nei pool.
Non assegnato	Il disco non è membro di un pool o di un gruppo di volumi.

stati di disponibilità

Stato	Definizione
Non riuscito	Il disco non funziona. I dati sul disco non sono disponibili.

Stato	Definizione
Guasto imminente	È stato rilevato che il disco potrebbe guastarsi presto. I dati sul disco sono ancora disponibili.
Offline	L'unità non è disponibile per la memorizzazione dei dati, in genere perché fa parte di un gruppo di volumi in fase di esportazione o è in fase di aggiornamento del firmware.
Ottimale	Il disco funziona normalmente.

Dischi a stato solido (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.

Vantaggi degli SSD

I vantaggi degli SSD rispetto ai dischi rigidi includono:

- Avvio più rapido (senza spin up)
- Latenza inferiore
- IOPS (Higher i/o Operations per second)
- Maggiore affidabilità con meno parti in movimento
- Minore consumo di energia
- Meno calore prodotto e meno raffreddamento richiesto

Identificazione degli SSD

Dalla pagina hardware, è possibile individuare gli SSD nella vista dello shelf anteriore. Individuare gli alloggiamenti dei dischi che visualizzano l'icona di un fulmine che indica l'installazione di un SSD.

Gruppi di volumi

Tutti i dischi di un gruppo di volumi devono essere dello stesso tipo di supporto (tutti gli SSD o tutti i dischi rigidi). I gruppi di volumi non possono avere una combinazione di tipi di supporti o di tipi di interfaccia.

Caching

Il caching in scrittura del controller è sempre abilitato per gli SSD. Il caching in scrittura migliora le performance e prolunga la durata dell'SSD.

Oltre alla cache del controller, è possibile implementare la funzione cache SSD per migliorare le prestazioni generali del sistema. Nella cache SSD, i dati vengono copiati dai volumi e memorizzati su due volumi RAID interni (uno per controller).

Limitare la vista del disco

Se l'array di storage include dischi con diversi tipi di attributi fisici e logici, la pagina

hardware fornisce campi di filtro che consentono di limitare la visualizzazione del disco e individuare dischi specifici.

A proposito di questa attività

I filtri dei dischi possono limitare la visualizzazione solo a determinati tipi di dischi fisici (ad esempio, tutte le unità SAS), con determinati attributi di sicurezza (ad esempio, con funzionalità di protezione), in determinate posizioni logiche (ad esempio, Gruppo di volumi 1). È possibile utilizzare questi filtri insieme o separatamente.

> Se tutti i dischi condividono gli stessi attributi fisici, il campo di filtro **Mostra dischi che sono…** non viene visualizzato. Se tutti i dischi condividono gli stessi attributi logici, il campo **Anywhere in the storage array** filter non viene visualizzato.

Fasi

1. Selezionare **hardware**.
2. Nel primo campo del filtro (sotto **Mostra unità…**), fare clic sulla freccia a discesa per visualizzare i tipi di unità disponibili e gli attributi di sicurezza.

   I tipi di dischi possono includere:

   - Tipo di disco (SSD, HDD)
   - Tipo di interfaccia del disco
   - Capacità del disco (dal più alto al più basso)
   - Velocità del disco (dalla più alta alla più bassa) gli attributi di sicurezza possono includere:
   - Sicuro
   - Abilitato alla sicurezza
   - Compatibile CON DA (Data Assurance)
   - Conforme a FIPS
   - Conforme a FIPS (FIPS 140-2)
   - Conforme a FIPS (FIPS 140-3)

     Se uno di questi attributi è lo stesso per tutti i dischi, non viene visualizzato nell'elenco a discesa. Ad esempio, se lo storage array include tutti i dischi SSD con interfacce SAS e velocità di 15000 rpm, ma alcuni SSD hanno capacità diverse, l'elenco a discesa visualizza solo le capacità come scelta di filtraggio.

   Quando si seleziona un'opzione dal campo, le unità che non corrispondono ai criteri di filtro vengono visualizzate in grigio nella vista grafica.

3. Nella seconda casella di filtro, fare clic sulla freccia a discesa per visualizzare le posizioni logiche disponibili per i dischi.

   > Se è necessario cancellare i criteri di filtro, selezionare **Clear** (Cancella) all'estrema destra delle caselle di filtro.

   Le posizioni logiche possono includere:

   - Piscine
   - Gruppi di volumi

- Hot spare
- Cache SSD
- Non assegnato

  Quando si seleziona un'opzione dal campo, le unità che non corrispondono ai criteri di filtro vengono visualizzate in grigio nella vista grafica.

4. In alternativa, è possibile selezionare **accendere le luci di individuazione** all'estrema destra dei campi dei filtri per attivare le luci di individuazione dei dischi visualizzati.

   Questa azione consente di individuare fisicamente le unità nell'array di storage.

Accendere la spia di individuazione del disco

Dalla pagina hardware, è possibile accendere la spia di localizzazione per individuare la posizione fisica di un'unità nell'array di storage.

A proposito di questa attività

È possibile individuare singoli dischi o più dischi visualizzati nella pagina hardware.

Fasi

1. Selezionare **hardware**.
2. Per individuare una o più unità, effettuare una delle seguenti operazioni:
   - **Disco singolo** — dal grafico dello shelf, individuare il disco che si desidera individuare fisicamente nell'array. (Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**). Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **attiva indicatore di posizione**.

     La spia di localizzazione del disco si accende. Una volta individuato il disco, tornare alla finestra di dialogo e selezionare **Spegni**.

   - **Dischi multipli** — nei campi dei filtri, selezionare un tipo di disco fisico dall'elenco a discesa a sinistra e un tipo di disco logico dall'elenco a discesa a destra. Il numero di dischi che corrispondono ai criteri specificati viene visualizzato all'estrema destra dei campi. Quindi, è possibile fare clic su **accendere le luci di individuazione** o selezionare **individuare tutte le unità filtrate** dal menu di scelta rapida. Una volta individuati i dischi, tornare alla finestra di dialogo e selezionare **Spegni**.

Visualizzare lo stato e le impostazioni del disco

È possibile visualizzare lo stato e le impostazioni delle unità, ad esempio il tipo di supporto, il tipo di interfaccia e la capacità.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Selezionare l'unità per la quale si desidera visualizzare lo stato e le impostazioni.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Visualizza impostazioni**.

   Viene visualizzata la finestra di dialogo Drive Settings (Impostazioni disco).

5. Per visualizzare tutte le impostazioni, fare clic su **Mostra altre impostazioni** nella parte superiore destra della finestra di dialogo.

Dettagli del campo

Impostazioni	Descrizione
Stato	Visualizza gli errori ottimale, offline, non critico e non riuscito. Lo stato ottimale indica la condizione di lavoro desiderata.
Modalità	Visualizza assegnato, non assegnato, Standby hot spare o hot spare in uso.
Posizione	Mostra il numero dello shelf e dell'alloggiamento in cui si trova l'unità.
Assegnato/in grado di proteggere/proteggere	Se l'unità è assegnata a un pool, un gruppo di volumi o una cache SSD, in questo campo viene visualizzato "Assigned to" (assegnato a.). Il valore può essere un nome di pool, un nome di gruppo di volumi o un nome di cache SSD. Se l'unità è assegnata a un hot spare e la relativa modalità è Standby, in questo campo viene visualizzato il messaggio "è possibile proteggere per". Se l'hot spare è in grado di proteggere uno o più gruppi di volumi, vengono visualizzati i nomi dei gruppi di volumi. Se non è in grado di proteggere un gruppo di volumi, vengono visualizzati 0 gruppi di volumi. Se l'unità è assegnata a un hot spare e la relativa modalità è in uso, in questo campo viene visualizzato "Protecting" (protezione). Il valore corrisponde al nome del gruppo di volumi interessati. Se l'unità non è assegnata, questo campo non viene visualizzato.
Tipo di supporto	Visualizza il tipo di supporto di registrazione utilizzato dall'unità, che può essere un disco rigido (HDD) o un disco a stato solido (SSD).
Percentuale di durata utilizzata (mostrata solo se sono presenti dischi SSD)	La quantità di dati scritti sul disco fino ad oggi, divisa per il limite teorico di scrittura totale.
Tipo di interfaccia	Visualizza il tipo di interfaccia utilizzata dal disco, ad esempio SAS.
Ridondanza del percorso del disco	Indica se le connessioni tra il disco e il controller sono ridondanti (Sì) o meno (No).
Capacità (GiB)	Mostra la capacità utilizzabile (capacità totale configurata) del disco.
Velocità (giri/min)	Mostra la velocità in RPM (non viene visualizzata per gli SSD).
Data rate corrente	Mostra la velocità di trasferimento dei dati tra il disco e lo storage array.
Dimensione del settore logico (byte)	Mostra la dimensione del settore logico utilizzata dall'unità.

Impostazioni	Descrizione
Dimensione del settore fisico (byte)	Mostra la dimensione fisica del settore utilizzata dal disco. In genere, la dimensione fisica del settore è di 4096 byte per i dischi rigidi.
Versione del firmware del disco	Mostra il livello di revisione del firmware del disco.
World-wide identifier	Mostra l'identificatore esadecimale univoco del disco.
ID prodotto	Mostra l'identificativo del prodotto assegnato dal produttore.
Numero di serie	Mostra il numero di serie del disco.
Produttore	Mostra il vendor del disco.
Data di produzione	Mostra la data di creazione del disco. Non disponibile per i dischi NVMe.
Sicuro	Indica se il disco è compatibile con la protezione (Sì) o meno (No). I dischi con funzionalità di protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard) (livello 140-2 o 140-3), che crittografano i dati durante le operazioni di scrittura e decrittare i dati durante le operazioni di 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*.
Abilitato alla sicurezza	Indica se il disco è abilitato alla protezione (Sì) o meno (No). 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.
Accessibile in lettura/scrittura	Indica se l'unità è accessibile in lettura/scrittura (Sì) o meno (No).

Impostazioni	Descrizione
Identificatore della chiave di sicurezza del disco	Mostra la chiave di sicurezza per i dischi abilitati alla protezione. 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.
Supporto per Data Assurance (da)	Indica se la funzione Data Assurance (da) è attivata (Sì) o meno (No). Data Assurance (da) è una funzione che controlla e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Data Assurance può essere abilitato a livello di pool o gruppo di volumi, con host che utilizzano un'interfaccia i/o compatibile con da, ad esempio Fibre Channel.
Compatibile con DULBE	Indica se l'opzione Deallocated o Unwritten Logical Block Error (DULBE) è attivata (Sì) o meno (No). DULBE è un'opzione sui dischi NVMe che consente allo storage array EF300 o EF600 di supportare volumi con provisioning di risorse.

6. Fare clic su **Chiudi**.

Sostituire l'unità in modo logico

Se un disco si guasta o si desidera sostituirlo per qualsiasi altro motivo, è possibile sostituire logicamente il disco guasto con un disco non assegnato o un hot spare completamente integrato.

A proposito di questa attività

Quando si sostituisce logicamente un disco, questo viene assegnato e diventa un membro permanente del pool o gruppo di volumi associato.

Utilizzare l'opzione di sostituzione logica per sostituire i seguenti tipi di dischi:

- Dischi guasti
- Dischi mancanti
- Dischi SSD che il Recovery Guru ti ha notificato che stanno per finire il loro ciclo di vita
- Dischi rigidi che il Recovery Guru ha notificato che si è verificato un guasto imminente del disco
- Dischi assegnati (disponibili solo per i dischi di un gruppo di volumi, non in un pool)

Prima di iniziare

L'unità sostitutiva deve avere le seguenti caratteristiche:

- Nello stato ottimale

- Nello stato non assegnato
- Gli stessi attributi del disco da sostituire (tipo di supporto, tipo di interfaccia e così via)
- La stessa funzionalità FDE (consigliata, ma non richiesta)
- La stessa funzionalità da (consigliata, ma non richiesta)

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Fare clic sull'unità che si desidera sostituire logicamente.

   Viene visualizzato il menu di scelta rapida del disco.

4. Fare clic su **logicamente sostituire**.
5. **Opzionale:** selezionare la casella di controllo **disco guasto dopo la sostituzione** per eseguire il failover del disco originale dopo la sostituzione.

   Questa casella di controllo è attivata solo se l'unità assegnata originale non presenta guasti o è mancante.

6. Dalla tabella **Select a replacement drive** (selezionare un'unità sostitutiva), selezionare l'unità sostitutiva che si desidera utilizzare.

   La tabella elenca solo le unità compatibili con l'unità che si sta sostituendo. Se possibile, selezionare un'unità che mantenga la protezione contro la perdita di shelf e la protezione contro la perdita di cassetto.

7. Fare clic su **Sostituisci**.

   Se il disco originale è guasto o mancante, i dati vengono ricostruiti sul disco sostitutivo utilizzando le informazioni di parità. La ricostruzione inizia automaticamente. Gli indicatori luminosi di guasto del disco si spengono e gli indicatori luminosi di attività dei dischi nel pool o nel gruppo di volumi iniziano a lampeggiare.

   Se l'unità originale non presenta guasti o è mancante, i dati vengono copiati nell'unità sostitutiva. Questa operazione di copia viene avviata automaticamente. Una volta completata l'operazione di copia, il sistema passa allo stato non assegnato dell'unità originale o, se la casella di controllo è stata selezionata, allo stato non riuscito.

Ricostruire il disco manualmente

Normalmente, la ricostruzione del disco viene avviata automaticamente dopo la sostituzione di un disco. Se la ricostruzione del disco non viene avviata automaticamente, è possibile avviare la ricostruzione manualmente.

> Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

Il grafico cambia per mostrare i dischi al posto dei controller.

3. Fare clic sull'unità che si desidera ricostruire manualmente.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Reconstruct** (ricostruzione) e confermare che si desidera eseguire l'operazione.

Inizializzare (formattare) il disco

Se si spostano le unità assegnate da un array di storage a un altro, è necessario inizializzare (formattare) le unità prima di poterli utilizzare nel nuovo array di storage.

A proposito di questa attività

L'inizializzazione rimuove le informazioni di configurazione precedenti da un disco e le riporta allo stato non assegnato. L'unità è quindi disponibile per l'aggiunta a un nuovo pool o gruppo di volumi nel nuovo array di storage.

Utilizzare l'operazione di inizializzazione del disco quando si sposta un singolo disco. Non è necessario inizializzare le unità se si sposta un intero gruppo di volumi da un array di storage a un altro.

> **Possibile perdita di dati** — quando si inizializza un disco, tutti i dati sul disco vengono persi. Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Fare clic sull'unità che si desidera inizializzare.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Inizializza** e confermare che si desidera eseguire l'operazione.

Disco guasto

Se richiesto, è possibile eseguire il failover manuale di un disco.

A proposito di questa attività

System Manager monitora i dischi nell'array di storage. Quando rileva che un disco sta generando molti errori, il Recovery Guru ti notifica di un guasto imminente del disco. Se questo accade e si dispone di un disco sostitutivo, potrebbe essere necessario eseguire un'azione preventiva. Se non si dispone di un'unità sostitutiva, è possibile attendere il guasto dell'unità.

> **Possibile perdita dell'accesso ai dati** — questa operazione potrebbe causare la perdita dei dati o la perdita della ridondanza dei dati. Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

Fasi

1. Selezionare **hardware**.

2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Fare clic sull'unità che si desidera guastare.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Fail**.
5. Mantenere selezionata la casella di controllo **Copia contenuto disco prima di eseguire il guasto**.

   L'opzione di copia viene visualizzata solo per i dischi assegnati e per i gruppi di volumi non RAID 0.

   Prima di eseguire un guasto al disco, assicurarsi di copiare il contenuto del disco. A seconda della configurazione, è possibile perdere tutti i dati o la ridondanza dei dati sul pool o sul gruppo di volumi associato se non si copia prima il contenuto del disco.

   L'opzione di copia consente un ripristino più rapido del disco rispetto alla ricostruzione e riduce la possibilità di un errore del volume in caso di guasto di un altro disco durante l'operazione di copia.

6. Confermare che si desidera che il disco non sia in grado di funzionare correttamente.

   Una volta che il disco si è guastato, attendere almeno 30 secondi prima di rimuoverlo.

Cancellare i dischi

È possibile utilizzare l'opzione Erase (Cancella) per preparare un'unità non assegnata per la rimozione dal sistema. Questa procedura rimuove in modo permanente i dati, garantendo che non possano essere letti di nuovo.

Prima di iniziare

Il disco deve essere in uno stato non assegnato.

A proposito di questa attività

Utilizzare l'opzione Erase (Cancella) solo se si desidera rimuovere in modo permanente tutti i dati presenti su un disco. Se il disco è abilitato alla protezione, l'opzione Erase (Cancella) esegue una cancellazione crittografica e ripristina gli attributi di sicurezza del disco su Secure-capable (abilitato alla protezione).

> La funzione di cancellazione non supporta alcuni modelli di dischi meno recenti. Se si tenta di cancellare uno di questi modelli precedenti, viene visualizzato un messaggio di errore.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. In alternativa, è possibile utilizzare i campi di filtro per visualizzare tutti i dischi non assegnati nello shelf. Dall'elenco a discesa **Mostra unità che sono…**, selezionare **non assegnate**.

   La vista shelf mostra solo i dischi non assegnati; tutti gli altri sono disattivati.

4. Per aprire il menu di scelta rapida dell'unità, fare clic sull'unità che si desidera cancellare. Se si desidera selezionare più dischi, è possibile farlo nella finestra di dialogo Erase Drives (Cancella dischi).

> **Possibile perdita di dati** — l'operazione di cancellazione non può essere annullata. Assicurarsi di selezionare le unità corrette durante la procedura.

5. Dal menu di scelta rapida, selezionare **Erase** (Cancella).

   Viene visualizzata la finestra di dialogo Erase Drives (Cancella unità), che mostra tutte le unità idonee per un'operazione di cancellazione.

6. Se lo si desidera, selezionare altri dischi dalla tabella. Non è possibile selezionare *tutti* dischi; assicurarsi che un disco rimanga deselezionato.
7. Confermare l'operazione digitando `erase`, Quindi fare clic su **Erase** (Cancella).

> Continuare con questa operazione. Una volta fatto clic su Yes (Sì) nella finestra di dialogo successiva, l'operazione non può essere interrotta.

8. Nella finestra di dialogo Estimated Completion Time (tempo di completamento stimato), fare clic su **Yes** (Sì) per continuare con l'operazione di cancellazione.

Risultati

L'operazione di cancellazione potrebbe richiedere alcuni minuti o diverse ore. È possibile visualizzare lo stato nel **Home › Visualizza operazioni in corso**. Al termine dell'operazione di cancellazione, i dischi sono disponibili per l'utilizzo in un altro gruppo di volumi o pool di dischi o in un altro array di storage.

Al termine

Se si desidera utilizzare nuovamente il disco, è necessario inizializzarlo. A tale scopo, selezionare **Inizializza** dal menu di scelta rapida del disco.

Sbloccare o ripristinare i dischi NVMe o FIPS bloccati

Se si inseriscono una o più unità NVMe o FIPS bloccate in un array di storage, è possibile sbloccare i dati dell'unità aggiungendo il file della chiave di sicurezza associato alle unità. Se non si dispone di una chiave di sicurezza, è possibile eseguire un ripristino su ciascuna unità bloccata inserendo il proprio ID di sicurezza fisico (PSID) per ripristinare i propri attributi di sicurezza e cancellare i dati dell'unità.

Prima di iniziare

- Per l'opzione Unlock (Sblocca), assicurarsi che il file della chiave di sicurezza (con un'estensione di `.slk`) È disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). È inoltre necessario conoscere la password associata alla chiave.
- Per l'opzione Reset (Ripristina), è necessario trovare il PSID su ciascun disco che si desidera reimpostare. Per individuare il PSID, rimuovere fisicamente l'unità e individuare la stringa PSID (massimo 32 caratteri) sull'etichetta dell'unità, quindi reinstallare l'unità.

A proposito di questa attività

Questa attività descrive come sbloccare i dati nei dischi NVMe o FIPS importando un file di chiave di sicurezza nell'array di storage. Per le situazioni in cui la chiave di sicurezza non è disponibile, questa attività descrive anche come eseguire un ripristino su un disco bloccato.

> Se il disco è stato bloccato utilizzando un server di gestione delle chiavi esterno, selezionare **Impostazioni › sistema › Gestione delle chiavi di sicurezza** in System Manager per configurare la gestione delle chiavi esterne e sbloccare il disco.

È possibile accedere alla funzione di sblocco dalla pagina hardware o dal **Impostazioni › sistema › Gestione chiavi di sicurezza**. L'attività seguente fornisce istruzioni dalla pagina hardware.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Selezionare l'unità NVMe o FIPS che si desidera sbloccare o ripristinare.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Unlock** (sblocco) per applicare il file della chiave di sicurezza o **Reset** (Ripristino) se non si dispone di un file della chiave di sicurezza.

   Queste opzioni vengono visualizzate solo se si seleziona un disco NVMe o FIPS bloccato.

   > Durante un'operazione di ripristino, tutti i dati vengono cancellati. Eseguire un ripristino solo se non si dispone di una chiave di sicurezza. La reimpostazione di un disco bloccato rimuove in modo permanente tutti i dati presenti sul disco e ripristina i relativi attributi di sicurezza su "sicuro", ma non abilitato. **Questa operazione non è reversibile.**

5. Effettuare una delle seguenti operazioni:
   a. **Unlock**: Nella finestra di dialogo **Unlock Secure Drive**, fare clic su **Browse**, quindi selezionare il file della chiave di sicurezza corrispondente al disco che si desidera sbloccare. Quindi, immettere la password, quindi fare clic su **Unlock** (Sblocca).
   b. **Reset**: Nella finestra di dialogo **Reset Locked Drive**, immettere la stringa PSID nel campo, quindi digitare `RESET` per confermare. Fare clic su **Reset** (Ripristina).

      Per un'operazione di sblocco, è necessario eseguire questa operazione una sola volta per sbloccare tutti i dischi NVMe o FIPS. Per eseguire un'operazione di ripristino, è necessario selezionare singolarmente ogni disco che si desidera ripristinare.

Risultati

L'unità è ora disponibile per l'utilizzo in un altro gruppo di volumi o pool di dischi o in un altro array di storage.

Gestire le hot spare

Panoramica dei dischi hot spare

Le hot spare fungono da unità di standby in gruppi di volumi RAID 1, RAID 5 o RAID 6 per System Manager.

Si tratta di dischi completamente funzionanti che non contengono dati. Se un disco si guasta nel gruppo di volumi, il controller ricostruisce automaticamente i dati dal disco guasto a un disco assegnato come hot spare.

Le hot spare non sono dedicate a gruppi di volumi specifici. Possono essere utilizzati per qualsiasi disco guasto nell'array di storage, purché l'hot spare e l'unità condividano questi attributi:

- Capacità uguale (o maggiore capacità per l'hot spare)
- Stesso tipo di supporto (ad esempio HDD o SSD)
- Stesso tipo di interfaccia (ad esempio, SAS)

Come identificare le hot spare

È possibile assegnare hot spare tramite l'installazione guidata iniziale o dalla pagina hardware. Per determinare se sono assegnati hot spare, andare alla pagina hardware e cercare eventuali alloggiamenti per unità indicati in rosa.

Come funziona la copertura hot spare

La copertura hot spare funziona come segue:

- È possibile riservare un disco non assegnato come hot spare per i gruppi di volumi RAID 1, RAID 5 o RAID 6.

> Le hot spare non possono essere utilizzate per i pool che hanno un metodo diverso di protezione dei dati. Invece di riservare un disco aggiuntivo, i pool riservano la capacità di riserva (chiamata *capacità di conservazione*) all'interno di ogni disco del pool. Se un disco si guasta in un pool, il controller ricostruisce i dati in quella capacità di riserva.

- Se un disco all'interno di un gruppo di volumi RAID 1, RAID 5 o RAID 6 si guasta, il controller utilizza automaticamente i dati di ridondanza per ricostruire i dati dal disco guasto. Il disco hot spare viene sostituito automaticamente per il disco guasto senza richiedere uno swap fisico.
- Una volta sostituito fisicamente il disco guasto, viene eseguita un'operazione copyback dall'unità hot spare all'unità sostituita. Se l'unità hot spare è stata designata come membro permanente di un gruppo di volumi, l'operazione copyback non è necessaria.
- La disponibilità della protezione in caso di perdita dei vassoi e della protezione in caso di perdita dei cassetti per un gruppo di volumi dipende dalla posizione delle unità che compongono il gruppo di volumi. La protezione contro la perdita dei vassoi e la perdita dei cassetti potrebbe andare persa a causa di un disco guasto e della posizione dell'unità hot spare. Per assicurarsi che la protezione contro la perdita di vassoio e la protezione contro la perdita di cassetto non siano compromesse, è necessario sostituire un disco guasto per avviare il processo copyback.
- Il volume dell'array di storage rimane online e accessibile durante la sostituzione del disco guasto, poiché il disco hot spare viene sostituito automaticamente per il disco guasto.

Considerazioni sulla capacità del disco hot spare

Selezionare un'unità con una capacità uguale o superiore alla capacità totale dell'unità che si desidera proteggere. Ad esempio, se si dispone di un disco da 18 GB con capacità configurata di 8 GB, è possibile utilizzare un disco da 9 GB o superiore come hot spare. In genere, non assegnare un disco come hot spare a meno che la sua capacità non sia uguale o superiore alla capacità del disco più grande dell'array di storage.

> Se non sono disponibili hot spare con la stessa capacità fisica, è possibile utilizzare un disco con capacità inferiore come hot spare se la "capacità utilizzata" del disco è uguale o inferiore alla capacità del disco hot spare.

Considerazioni sui tipi di supporti e di interfaccia

L'unità utilizzata come hot spare deve condividere lo stesso tipo di supporto e tipo di interfaccia delle unità che proteggerà. Ad esempio, un'unità HDD non può fungere da hot spare per le unità SSD.

Considerazioni per dischi sicuri

Un disco sicuro, come FDE o FIPS, può fungere da hot spare per dischi con o senza funzionalità di sicurezza. Tuttavia, un disco non sicuro non può fungere da hot spare per dischi con funzionalità di sicurezza.

Quando si seleziona un'unità sicura da utilizzare per un hot spare, System Manager richiede di eseguire una cancellazione sicura prima di procedere. La cancellazione sicura ripristina gli attributi di sicurezza dell'unità su Secure-capable, ma non Secure-enabled.

> Quando si attiva la funzione Drive Security e si crea un pool o un gruppo di volumi da dischi sicuri, 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.

Numero consigliato di dischi hot spare

Se si è utilizzata l'installazione guidata iniziale per creare automaticamente hot spare, System Manager crea un hot spare ogni 30 dischi di un tipo di supporto e di interfaccia specifici. In caso contrario, è possibile creare manualmente dischi hot spare tra i gruppi di volumi nell'array di storage.

Assegnare hot spare

È possibile assegnare un hot spare come unità di standby per una protezione dei dati aggiuntiva nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Se un disco si guasta in uno di questi gruppi di volumi, il controller ricostruisce i dati dal disco guasto all'hot spare.

Prima di iniziare

- È necessario creare gruppi di volumi RAID 1, RAID 5 o RAID 6. (Non è possibile utilizzare hot spare per i pool. Un pool utilizza invece la capacità di riserva all'interno di ogni disco per la protezione dei dati.
- Deve essere disponibile un'unità che soddisfi i seguenti criteri:
  - Non assegnato, con stato ottimale.
  - Stesso tipo di supporto dei dischi nel gruppo di volumi (ad esempio, SSD).
  - Stesso tipo di interfaccia dei dischi nel gruppo di volumi (ad esempio, SAS).
  - Capacità uguale o superiore alla capacità utilizzata dei dischi nel gruppo di volumi.

A proposito di questa attività

Questa attività descrive come assegnare manualmente un hot spare dalla pagina hardware. La copertura consigliata è di due hot spare per set di dischi.

> È possibile assegnare hot spare anche dalla procedura guidata di installazione iniziale. È possibile determinare se le hot spare sono già assegnate cercando gli alloggiamenti per dischi indicati in rosa nella pagina hardware.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Selezionare un'unità non assegnata (visualizzata in grigio) che si desidera utilizzare come hot spare.

   Viene visualizzato il menu di scelta rapida del disco.

4. Selezionare **Assegna hot spare**.

   Se l'unità è abilitata per la cancellazione sicura, viene visualizzata la finestra di dialogo. Per utilizzare un disco abilitato alla protezione come hot spare, è necessario eseguire un'operazione di cancellazione sicura per rimuovere tutti i dati e reimpostare gli attributi di sicurezza.

   > **Possibile perdita di dati** — assicurarsi di aver selezionato il disco corretto. Una volta completata l'operazione di cancellazione sicura, non è possibile ripristinare i dati.

   Se il disco è abilitato **non** alla protezione, viene visualizzata la finestra di dialogo Confirm Assign Hot Spare Drive (Conferma assegnazione unità hot spare).

5. Esaminare il testo nella finestra di dialogo, quindi confermare l'operazione.

   Il disco viene visualizzato in rosa nella pagina hardware, che indica che si tratta di un disco hot spare.

Risultati

Se un disco all'interno di un gruppo di volumi RAID 1, RAID 5 o RAID 6 si guasta, il controller utilizza automaticamente i dati di ridondanza per ricostruire i dati dal disco guasto all'hot spare.

Annulla assegnazione hot spare

È possibile modificare un hot spare in un disco non assegnato.

Prima di iniziare

Lo hot spare deve essere in stato ottimale, Standby.

A proposito di questa attività

Non è possibile annullare l'assegnazione di un hot spare che sta assumendo il controllo di un disco guasto. Se lo hot spare non si trova in uno stato ottimale, seguire le procedure Recovery Guru per correggere eventuali problemi prima di tentare di annullare l'assegnazione del disco.

Fasi

1. Selezionare **hardware**.
2. Se la figura mostra i controller, fare clic su **Mostra parte anteriore dello shelf**.

   Il grafico cambia per mostrare i dischi al posto dei controller.

3. Selezionare l'unità hot spare (visualizzata in rosa) che si desidera annullare l'assegnazione.

   Se nell'alloggiamento rosa sono presenti linee diagonali, l'hot spare è attualmente in uso e non può essere disassegnato.

Viene visualizzato il menu di scelta rapida del disco.

4. Dall'elenco a discesa del disco, selezionare **Annulla assegnazione hot spare**.

   La finestra di dialogo mostra tutti i gruppi di volumi interessati dalla rimozione di questa hot spare e se altri hot spare li proteggono.

5. Confermare l'operazione di annullamento dell'assegnazione.

Risultati

Il disco viene riportato in Unassigned (non assegnato) (visualizzato in grigio).

FAQ sugli shelf

Che cos'è la protezione contro la perdita di shelf e la perdita di cassetto?

La protezione contro le perdite di shelf e la protezione contro le perdite di cassetto sono attributi di pool e gruppi di volumi che consentono di mantenere l'accesso ai dati in caso di guasto di un singolo shelf o cassetto.

Protezione contro la perdita di shelf

Uno shelf è l'enclosure che contiene i dischi o i dischi e il controller. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo shelf di dischi. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione dello shelf di dischi o il guasto di entrambi i moduli i/o (IOM).

> La protezione contro la perdita di shelf non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

I criteri per la protezione dalla perdita di shelf dipendono dal metodo di protezione, come descritto nella tabella seguente:

Livello	Criteri per la protezione contro la perdita di shelf	Numero minimo di shelf richiesti
Piscina	Il pool deve includere dischi di almeno cinque shelf e deve essere presente un numero uguale di dischi in ogni shelf. La protezione contro la perdita di shelf non è applicabile agli shelf ad alta capacità; se il sistema contiene shelf ad alta capacità, fare riferimento alla protezione contro la perdita di cassetto.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo shelf.	3

Livello	Criteri per la protezione contro la perdita di shelf	Numero minimo di shelf richiesti
RAID 3 o RAID 5	Ogni disco del gruppo di volumi si trova in uno shelf separato.	3
RAID 1	Ogni disco di una coppia RAID 1 deve essere collocato in uno shelf separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di shelf.	Non applicabile

Protezione in caso di perdita del cassetto

Un cassetto è uno dei compartimenti di uno shelf che si tira per accedere ai dischi. Solo gli scaffali ad alta capacità dispongono di cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo cassetto. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione del cassetto o il guasto di un componente interno del cassetto.

> La protezione contro la perdita di cassetto non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a un cassetto (e di conseguenza a un altro disco nel pool o nel gruppo di volumi) causa la perdita di dati.

I criteri per la protezione dalle perdite di cassetto dipendono dal metodo di protezione, come descritto nella tabella seguente:

Livello	Criteri per la protezione contro le perdite di cassetto	Numero minimo di cassetti richiesti
Piscina	I candidati al pool devono includere unità di tutti i cassetti e deve essere presente un numero uguale di unità in ciascun cassetto. Il pool deve includere dischi di almeno cinque cassetti e deve essere presente un numero uguale di dischi in ciascun cassetto. Uno shelf da 60 dischi può ottenere la protezione contro la perdita di cassetto quando il pool contiene 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 dischi. È possibile aggiungere incrementi in multipli di 5 al pool dopo la creazione iniziale.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo cassetto.	3

Livello	Criteri per la protezione contro le perdite di cassetto	Numero minimo di cassetti richiesti
RAID 3 o RAID 5	Ciascuna unità del gruppo di volumi si trova in un cassetto separato.	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione perdita cassetto.	Non applicabile

Quali sono i cicli di apprendimento della batteria?

Un ciclo di apprendimento è un ciclo automatico per la calibrazione dell'indicatore della batteria Smart.

Un ciclo di apprendimento è costituito da queste fasi:

- Scaricamento controllato della batteria
- Periodo di riposo
- Caricare

Le batterie vengono scaricate a una soglia prestabilita. Durante questa fase, l'indicatore della batteria viene calibrato.

Un ciclo di apprendimento richiede questi parametri:

- Batterie completamente cariche
- Nessuna batteria surriscaldata

I cicli di apprendimento per i sistemi di controller duplex si verificano contemporaneamente. Per i controller con alimentazione di backup da più di una batteria o un set di celle della batteria, i cicli di apprendimento si verificano in sequenza.

I cicli di apprendimento sono programmati per l'avvio automatico a intervalli regolari, alla stessa ora e nello stesso giorno della settimana. L'intervallo tra i cicli viene descritto in settimane.

> Il completamento di un ciclo di apprendimento potrebbe richiedere diverse ore.

FAQ sul controller

Che cos'è la negoziazione automatica?

La negoziazione automatica è la capacità di un'interfaccia di rete di coordinare automaticamente i propri parametri di connessione (velocità e duplex) con un'altra interfaccia di rete.

La negoziazione automatica è solitamente l'impostazione preferita per la configurazione delle porte di gestione; tuttavia, se la negoziazione non riesce, le impostazioni dell'interfaccia di rete non corrispondenti possono influire notevolmente sulle prestazioni della rete. Nei casi in cui tale condizione non sia accettabile, impostare manualmente le impostazioni dell'interfaccia di rete su una configurazione corretta. La negoziazione automatica viene eseguita dalle porte di gestione Ethernet del controller. La negoziazione automatica non viene eseguita dagli adattatori bus host iSCSI.

> Se la negoziazione automatica non riesce, il controller tenta di stabilire una connessione a 10BASE-T, half-duplex, che è il minimo comune denominatore.

Cos'è la configurazione automatica degli indirizzi IPv6 senza stato?

Con la configurazione automatica senza stato, gli host non ottengono indirizzi e altre informazioni di configurazione da un server.

La configurazione automatica stateless in IPv6 offre indirizzi link-local, multicasting e il protocollo Nighbor Discovery (ND). IPv6 può generare l'ID dell'interfaccia di un indirizzo dall'indirizzo del data link Layer sottostante.

La configurazione automatica stateless e la configurazione automatica stateful si integrano a vicenda. Ad esempio, l'host può utilizzare la configurazione automatica senza stato per configurare i propri indirizzi, ma utilizzare la configurazione automatica con stato per ottenere altre informazioni. La configurazione automatica con stato consente agli host di ottenere indirizzi e altre informazioni di configurazione da un server. Internet Protocol versione 6 (IPv6) definisce anche un metodo per rinumerare tutti gli indirizzi IP di una rete contemporaneamente. IPv6 definisce un metodo per i dispositivi in rete per configurare automaticamente il proprio indirizzo IP e altri parametri senza la necessità di un server.

I dispositivi eseguono questa procedura quando utilizzano la configurazione automatica stateless:

1. **Generare un indirizzo link-local** — il dispositivo genera un indirizzo link-local, che ha 10 bit, seguito da 54 zeri, e seguito dall'ID dell'interfaccia a 64 bit.
2. **Verificare l'univocità di un indirizzo link-local** — il nodo verifica per assicurarsi che l'indirizzo link-local generato non sia già in uso sulla rete locale. Il nodo invia un messaggio di sollecitazione vicino utilizzando il protocollo ND. In risposta, la rete locale ascolta un messaggio pubblicitario vicino, che indica che un altro dispositivo sta già utilizzando l'indirizzo link-local. In tal caso, è necessario generare un nuovo indirizzo link-local oppure la configurazione automatica non riesce e utilizzare un altro metodo.
3. **Assegnazione di un indirizzo link-local** — se il dispositivo supera il test di unicità, il dispositivo assegna l'indirizzo link-local alla propria interfaccia IP. L'indirizzo link-local può essere utilizzato per le comunicazioni sulla rete locale, ma non su Internet.
4. **Contattare il router** — il nodo tenta di contattare un router locale per ulteriori informazioni su come continuare la configurazione. Questo contatto viene eseguito ascoltando i messaggi pubblicitari del router inviati periodicamente dai router o inviando un messaggio di richiesta specifico del router per chiedere a un router informazioni sulle operazioni successive.
5. **Fornire la direzione al nodo** — il router fornisce la direzione al nodo su come procedere con la configurazione automatica. In alternativa, il router indica all'host come determinare l'indirizzo Internet globale.
6. **Configurare l'indirizzo globale** — l'host si configura con il suo indirizzo Internet univoco a livello globale. Questo indirizzo è generalmente formato da un prefisso di rete fornito all'host dal router.

Quale scegliere: DHCP o configurazione manuale?

Il metodo predefinito per la configurazione di rete è DHCP (Dynamic host Configuration Protocol). Utilizzare sempre questa opzione a meno che la rete non disponga di un server DHCP.

Che cos'è un server DHCP?

DHCP (Dynamic host Configuration Protocol) è un protocollo che automatizza l'assegnazione di un indirizzo IP (Internet Protocol).

A ciascuna periferica collegata a una rete TCP/IP deve essere assegnato un indirizzo IP univoco. Questi dispositivi includono i controller nell'array di storage.

Senza DHCP, un amministratore di rete inserisce questi indirizzi IP manualmente. Con DHCP, quando un client deve avviare le operazioni TCP/IP, il client trasmette una richiesta di informazioni sull'indirizzo. Il server DHCP riceve la richiesta, assegna un nuovo indirizzo per un periodo di tempo specificato chiamato periodo di lease e invia l'indirizzo al client. Con DHCP, una periferica può avere un indirizzo IP diverso ogni volta che si connette alla rete. In alcuni sistemi, l'indirizzo IP della periferica può cambiare anche quando la periferica è ancora connessa.

Come si configura il server DHCP?

È necessario configurare un server DHCP (Dynamic host Configuration Protocol) per utilizzare gli indirizzi IP (Internet Protocol) statici per i controller dell'array di storage.

Gli indirizzi IP assegnati dal server DHCP sono in genere dinamici e possono essere modificati in quanto il periodo di lease scade. Alcuni dispositivi, ad esempio server e router, devono utilizzare indirizzi statici. I controller dello storage array richiedono anche indirizzi IP statici.

Per informazioni su come assegnare indirizzi statici, consultare la documentazione relativa al server DHCP.

Perché è necessario modificare la configurazione di rete del controller?

Quando si utilizza la gestione fuori banda, è necessario impostare la configurazione di rete per ciascun controller (indirizzo IP (Internet Protocol), subnet mask (subnet mask) e gateway).

È possibile impostare la configurazione di rete utilizzando un server DHCP (Dynamic host Configuration Protocol). Se non si utilizza un server DHCP, è necessario immettere manualmente la configurazione di rete.

Dove è possibile ottenere la configurazione di rete?

È possibile ottenere l'indirizzo IP (Internet Protocol), la subnet mask (subnet mask) e le informazioni del gateway dall'amministratore di rete.

Queste informazioni sono necessarie quando si configurano le porte sui controller.

Quali sono le risposte PING di ICMP?

Internet Control message Protocol (ICMP) è uno dei protocolli della suite TCP/IP.

Il `ICMP echo request` e a.(`ICMP echo reply` i messaggi sono comunemente noti come `ping` messaggi. `Ping` è uno strumento per la risoluzione dei problemi utilizzato dagli amministratori di sistema per verificare manualmente la connettività tra i dispositivi di rete e per verificare il ritardo di rete e la perdita di pacchetti. Il `ping` il comando invia un `ICMP echo request` a un dispositivo in rete e il dispositivo risponde immediatamente con un(`ICMP echo reply`. A volte, la policy di sicurezza di rete di un'azienda richiede `ping` (`ICMP echo reply`) essere disattivati su tutti i dispositivi per renderli più difficili da rilevare da persone non autorizzate.

Quando è necessario aggiornare la configurazione della porta o il server iSNS dal server DHCP?

Aggiornare il server DHCP ogni volta che il server viene modificato o aggiornato e le informazioni DHCP relative all'array di storage corrente e all'array di storage che si desidera utilizzare sono cambiate.

In particolare, aggiornare la configurazione della porta o il server iSNS dal server DHCP quando si sa che il server DHCP assegnerà indirizzi diversi.

> L'aggiornamento della configurazione di una porta è distruttivo per tutte le connessioni iSCSI su tale porta.

Cosa devo fare dopo aver configurato le porte di gestione?

Se è stato modificato l'indirizzo IP per lo storage array, potrebbe essere necessario aggiornare la vista globale dell'array in Unified Manager.

Per aggiornare la vista array globale in Unified Manager, aprire l'interfaccia e accedere al **Manage › Discover**.

Se si utilizza ancora Gestione storage SANtricity, accedere alla finestra Gestione aziendale, dove è necessario rimuovere e aggiungere nuovamente il nuovo indirizzo IP.

Perché il sistema storage non è in modalità ottimale?

Un sistema storage in modalità non ottimale è dovuto a uno stato di configurazione del sistema non valido. Nonostante questo stato, il normale accesso i/o ai volumi esistenti è completamente supportato; tuttavia, System Manager proibirà alcune operazioni.

Un sistema storage potrebbe passare a una configurazione di sistema non valida per uno dei seguenti motivi:

- Il controller è fuori conformità, probabilmente perché ha un codice SMID (Submodel ID) errato o ha superato il limite delle funzionalità premium.
- È in corso un'operazione di servizio interna, ad esempio il download del firmware del disco.
- Il controller ha superato la soglia di errore di parità ed è entrato in blocco.
- Si è verificata una condizione generale di blocco.

Domande frequenti su iSCSI

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 su 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.

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).
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).

Quali altre operazioni è necessario eseguire per configurare o diagnosticare iSCSI?

Le sessioni iSCSI possono essere eseguite con host o array di storage remoti in una relazione di mirroring asincrona. Le seguenti tabelle elencano le funzioni di System Manager che è possibile utilizzare per configurare e gestire queste sessioni iSCSI.

> Le impostazioni iSCSI sono disponibili solo se lo storage array supporta iSCSI.

Configurare iSCSI

Azione	Posizione
Gestire le impostazioni iSCSI	1. Selezionare **Impostazioni › sistema**. 2. Scorrere verso il basso fino a **iSCSI settings** per visualizzare tutte le funzioni di gestione.
Configurare le porte iSCSI	1. Selezionare **hardware**. 2. Selezionare **Mostra retro dello shelf**. 3. Selezionare un controller. 4. Selezionare **Configure iSCSI ports** (Configura porte iSCSI).

Azione	Posizione
Impostare il segreto CHAP dell'host	1. Selezionare **Impostazioni › sistema**. 2. Scorrere fino a **iSCSI settings**, quindi selezionare **Configure Authentication** (Configura autenticazione). oppure 1. Selezionare **Storage › Hosts** (Storage[host]). 2. Selezionare un membro host. 3. Fare clic sul menu:scheda View/Edit Settings [host Ports] (Visualizza/Modifica impostazioni [Porte host]).

Eseguire la diagnosi di iSCSI

Azione	Posizione
Consente di visualizzare o terminare sessioni iSCSI	1. Selezionare **Impostazioni › sistema**. 2. Scorrere fino a **iSCSI settings**, quindi selezionare **View/End iSCSI sessions** (Visualizza/termina sessioni iSCSI). oppure 1. Selezionare **scheda Support › Support Center › Diagnostics**. 2. Selezionare **View/End iSCSI Sessions** (Visualizza/termina sessioni iSCSI).
Visualizzare le statistiche iSCSI	1. Selezionare **Impostazioni › sistema**. 2. Scorrere fino a **iSCSI Settings**, quindi selezionare **View iSCSI Statistics Packages** (Visualizza pacchetti di statistiche iSCSI). oppure 1. Selezionare **scheda Support › Support Center › Diagnostics**. 2. Selezionare **View iSCSI Statistics Packages** (Visualizza pacchetti di statistiche iSCSI).

Domande frequenti su NVMe

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 RDMA. 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. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics. 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.

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).
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.

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).

Perché sono presenti due indirizzi IP per una porta fisica?

Lo storage array EF600 può includere due HICS, uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. Ciascuna porta fisica a cui è possibile accedere dall'HIC esterno dispone di una porta virtuale associata dall'HIC interno.

Per ottenere prestazioni massime di 200 GB, è necessario assegnare un indirizzo IP univoco per le porte fisiche e virtuali in modo che l'host possa stabilire connessioni a ciascuna porta. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funziona a circa la metà della velocità.

Perché esistono due set di parametri per una porta fisica?

Lo storage array EF600 può includere due HICS, uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. Ciascuna porta fisica a cui è possibile accedere dall'HIC esterno dispone di una porta virtuale associata dall'HIC interno.

Per ottenere prestazioni massime di 200 GB, è necessario assegnare i parametri per le porte fisiche e virtuali in modo che l'host possa stabilire connessioni a ciascuna porta. Se non si assegnano parametri alla porta virtuale, l'HIC funziona a circa la metà della velocità.

FAQ sui dischi

Che cos'è un disco hot spare?

Le hot spare fungono da unità di standby nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Si tratta di dischi completamente funzionanti che non contengono dati. Se un disco si guasta nel gruppo di volumi, il controller ricostruisce automaticamente i dati dal disco guasto a un hot spare.

Se un disco si guasta nell'array di storage, il disco hot spare viene sostituito automaticamente per il disco guasto senza richiedere uno swap fisico. Se il disco hot spare è disponibile quando si verifica un guasto, il controller utilizza i dati di ridondanza per ricostruire i dati dal disco guasto al disco hot spare.

Un disco hot spare non è dedicato a un gruppo di volumi specifico. È invece possibile utilizzare un disco hot spare per qualsiasi disco guasto nell'array di storage con la stessa capacità o capacità inferiore. Un disco hot spare deve essere dello stesso tipo di supporto (HDD o SSD) dei dischi che protegge.

> I dischi hot spare non sono supportati con i pool. Invece dei dischi hot spare, i pool utilizzano la capacità di conservazione all'interno di ogni disco che comprende il pool.

Che cos'è la capacità di conservazione?

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata in un pool per supportare potenziali guasti del disco.

Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione in base al numero di dischi nel pool.

I pool utilizzano la capacità di conservazione durante la ricostruzione, mentre i gruppi di volumi utilizzano dischi hot spare per lo stesso scopo. Il metodo della capacità di conservazione è un miglioramento rispetto ai dischi hot spare perché consente una ricostruzione più rapida. La capacità di conservazione viene distribuita su un certo numero di dischi nel pool invece che su un disco nel caso di un disco hot spare, in modo da non essere limitati dalla velocità o dalla disponibilità di un disco.

Perché dovrei sostituire logicamente un disco?

Se un disco si guasta o si desidera sostituirlo per qualsiasi altro motivo e si dispone di un disco non assegnato nell'array di storage, è possibile sostituire logicamente il disco guasto con quello non assegnato. Se non si dispone di un disco non assegnato, è possibile sostituirlo fisicamente.

I dati dell'unità originale vengono copiati o ricostruiti sull'unità sostitutiva.

Dove è possibile visualizzare lo stato di un disco in fase di ricostruzione?

È possibile visualizzare lo stato di ricostruzione del disco dalla dashboard Operations in Progress (operazioni in corso).

Nella pagina iniziale, fare clic sul collegamento **View Operations in Progress** (Visualizza operazioni in corso) in alto a destra.

A seconda del disco, la ricostruzione completa potrebbe richiedere molto tempo. Se la proprietà di un volume è cambiata, potrebbe essere eseguita una ricostruzione completa invece della ricostruzione rapida.

Avvisi

Panoramica degli avvisi

È possibile configurare System Manager in modo che invii avvisi di array di storage tramite e-mail, trap SNMP e messaggi syslog.

Cosa sono gli avvisi?

Alerts notifica agli amministratori gli eventi importanti che si verificano sullo storage array. Gli eventi possono includere problemi come un guasto alla batteria, uno spostamento di un componente da ottimale a offline o errori di ridondanza nel controller. Tutti gli eventi critici sono considerati "allertabili", insieme ad alcuni eventi di avviso e informativi.

Scopri di più:

- "Come funzionano gli avvisi"
- "Terminologia degli avvisi"

Come si configurano gli avvisi?

È possibile configurare gli avvisi in modo che vengano inviati come messaggio a uno o più indirizzi e-mail, come trap SNMP a un server SNMP o come messaggio a un server syslog. La configurazione degli avvisi è disponibile dal **Impostazioni › Avvisi**.

Scopri di più:

- "Configurare il server di posta e i destinatari per gli avvisi"
- "Configurare il server syslog per gli avvisi"
- "Configurare gli avvisi SNMP"

Informazioni correlate

Scopri di più sui concetti relativi agli avvisi:

- "Panoramica del registro eventi"
- "Indicatori di data e ora incoerenti"

Concetti

Come funzionano gli avvisi

Gli avvisi informano gli amministratori degli eventi importanti che si verificano sullo storage array. Gli avvisi possono essere inviati tramite e-mail, trap SNMP e syslog.

Il processo di notifica funziona come segue:

1. Un amministratore configura uno o più dei seguenti metodi di avviso in System Manager:
    - **Email** — i messaggi vengono inviati agli indirizzi email.
    - **SNMP** — i trap SNMP vengono inviati a un server SNMP.

- **Syslog** — i messaggi vengono inviati a un server syslog.

2. Quando il monitor degli eventi dello storage array rileva un problema, scrive le informazioni relative a tale problema nel registro eventi (disponibile dal **Support › Event Log**). Ad esempio, i problemi possono includere eventi come un guasto alla batteria, un componente che passa da ottimale a offline o errori di ridondanza nel controller.
3. Se il monitor degli eventi determina che l'evento è "allertabile", invia una notifica utilizzando i metodi di avviso configurati (e-mail, SNMP e/o syslog). Tutti gli eventi critici sono considerati "allertabili", insieme ad alcuni eventi di avviso e informativi.

Configurazione degli avvisi

È possibile configurare gli avvisi dalla configurazione guidata iniziale (solo per gli avvisi e-mail) o dalla pagina Avvisi. Per verificare la configurazione corrente, accedere al **Impostazioni › Avvisi**.

Il riquadro Avvisi visualizza la configurazione degli avvisi, che può essere una delle seguenti:

- Non configurato.
- Configurato; è impostato almeno un metodo di avviso. Per determinare quali metodi di avviso sono configurati, puntare il cursore sul riquadro.

Informazioni sugli avvisi

Gli avvisi possono includere i seguenti tipi di informazioni:

- Nome dell'array di storage.
- Tipo di errore di evento correlato a una voce del registro eventi.
- Data e ora in cui si è verificato l'evento.
- Breve descrizione dell'evento.

Gli avvisi syslog seguono lo standard di messaggistica RFC 5424.

Terminologia degli avvisi

Scopri in che modo i termini degli avvisi si applicano al tuo array di storage.

Componente	Descrizione
Monitoraggio degli eventi	Il monitor degli eventi risiede nell'array di storage e viene eseguito come attività in background. Quando il monitor degli eventi rileva anomalie sull'array di storage, scrive informazioni sui problemi nel registro eventi. I problemi possono includere eventi come guasti alla batteria, spostamento di un componente da ottimale a offline o errori di ridondanza nel controller. Se il monitor degli eventi determina che l'evento è "allertabile", invia una notifica utilizzando i metodi di avviso configurati (e-mail, SNMP e/o syslog). Tutti gli eventi critici sono considerati "allertabili", insieme ad alcuni eventi di avviso e informativi.
Server di posta	Il server di posta viene utilizzato per inviare e ricevere avvisi e-mail. Il server utilizza il protocollo SMTP (Simple Mail Transfer Protocol).

Componente	Descrizione
SNMP	SNMP (Simple Network Management Protocol) è un protocollo standard Internet utilizzato per la gestione e la condivisione delle informazioni tra dispositivi su reti IP.
Trap SNMP	Un trap SNMP è una notifica inviata a un server SNMP. La trap contiene informazioni su problemi significativi con l'array di storage.
Destinazione trap SNMP	Una destinazione trap SNMP è un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
Nome di comunità	Un nome di comunità è una stringa che agisce come una password per i server di rete in un ambiente SNMP.
File MIB	Il file MIB (Management Information base) definisce i dati monitorati e gestiti nell'array di storage. Deve essere copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB è disponibile con il software System Manager sul sito del supporto.
Variabili MIB	Le variabili MIB (Management Information base) possono restituire valori come il nome dell'array di storage, la posizione dell'array e una persona di contatto in risposta a SNMP GetRequests.
Syslog	Syslog è un protocollo utilizzato dalle periferiche di rete per inviare messaggi di evento a un server di registrazione.
UDP	User Datagram Protocol (UDP) è un protocollo di livello di trasporto che specifica un numero di porta di origine e di destinazione nelle intestazioni dei pacchetti.

Gestire gli avvisi e-mail

Configurare il server di posta e i destinatari per gli avvisi

Per configurare gli avvisi e-mail, è necessario specificare un indirizzo del server di posta e gli indirizzi e-mail dei destinatari degli avvisi. Sono consentiti fino a 20 indirizzi e-mail.

Prima di iniziare

- L'indirizzo del server di posta deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6 o un nome di dominio completo.

> Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

- L'indirizzo e-mail da utilizzare come mittente dell'avviso deve essere disponibile. Indirizzo visualizzato nel campo "da" del messaggio di avviso. Nel protocollo SMTP è richiesto un indirizzo mittente; senza di esso, si verifica un errore.
- Gli indirizzi e-mail dei destinatari degli avvisi devono essere disponibili. Il destinatario è in genere un indirizzo per un amministratore di rete o di storage. È possibile inserire fino a 20 indirizzi e-mail.

A proposito di questa attività

Questa attività descrive come configurare il server di posta, inserire gli indirizzi e-mail per il mittente e i destinatari e verificare tutti gli indirizzi e-mail immessi nella pagina Avvisi.

> Gli avvisi e-mail possono essere configurati anche dalla procedura di installazione guidata iniziale.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.

   Se un server di posta elettronica non è ancora configurato, nella scheda e-mail viene visualizzato il messaggio "Configura server di posta".

3. Selezionare **Configura server di posta**.

   Viene visualizzata la finestra di dialogo Configura server di posta.

4. Immettere le informazioni sul server di posta, quindi fare clic su **Salva**.
   - **Indirizzo server di posta** — immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6 del server di posta.

     > Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

   - **Indirizzo email mittente** — Inserisci un indirizzo email valido da utilizzare come mittente del messaggio. Questo indirizzo viene visualizzato nel campo "da" del messaggio di posta elettronica.
   - **Encryption** — se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. In caso contrario, selezionare **Nessuno**.
   - **Nome utente e password** — se necessario, immettere un nome utente e una password per l'autenticazione con il mittente e il server di posta in uscita.
   - **Include contact information in email** — per includere le informazioni di contatto del mittente nel messaggio di avviso, selezionare questa opzione, quindi inserire un nome e un numero di telefono.

     Dopo aver fatto clic su **Salva**, gli indirizzi e-mail vengono visualizzati nella scheda e-mail della pagina Avvisi.

5. Selezionare **Aggiungi email**.

   Viene visualizzata la finestra di dialogo Aggiungi e-mail.

6. Inserire uno o più indirizzi e-mail per i destinatari degli avvisi, quindi fare clic su **Aggiungi**.

   Gli indirizzi e-mail vengono visualizzati nella pagina Avvisi.

7. Se si desidera assicurarsi che gli indirizzi e-mail siano validi, fare clic su **Test all emails** (verifica tutte le e-mail) per inviare i messaggi di prova ai destinatari.

Risultati

Dopo aver configurato gli avvisi e-mail, il monitor degli eventi invia messaggi e-mail ai destinatari specificati

ogni volta che si verifica un evento verificabile.

Modificare gli indirizzi e-mail per gli avvisi

È possibile modificare gli indirizzi e-mail dei destinatari che ricevono gli avvisi e-mail.

Prima di iniziare

L'indirizzo di posta elettronica che si desidera modificare deve essere definito nella scheda Email della pagina Alerts.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Nella tabella **Indirizzo email**, selezionare l'indirizzo che si desidera modificare, quindi fare clic sull'icona **Modifica** (matita) all'estrema destra.

   La riga diventa un campo modificabile.

4. Inserire un nuovo indirizzo, quindi fare clic sull'icona **Salva** (segno di spunta).

   Per annullare le modifiche, selezionare l'icona **Annulla** (X).

Risultati

La scheda Email della pagina Alerts (Avvisi) visualizza gli indirizzi e-mail aggiornati.

Aggiungere indirizzi e-mail per gli avvisi

È possibile aggiungere fino a 20 destinatari per gli avvisi e-mail.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Selezionare **Aggiungi email**.

   Viene visualizzata la finestra di dialogo Aggiungi e-mail.

4. Nel campo vuoto, immettere un nuovo indirizzo e-mail. Se si desidera aggiungere più indirizzi, selezionare **Aggiungi un'altra e-mail** per aprire un altro campo.
5. Fare clic su **Aggiungi**.

Risultati

Nella scheda Email della pagina Alerts (Avvisi) vengono visualizzati i nuovi indirizzi e-mail.

Eliminare gli indirizzi e-mail o i server di posta per gli avvisi

È possibile rimuovere il server di posta precedentemente definito in modo che gli avvisi non vengano più inviati agli indirizzi di posta elettronica oppure rimuovere singoli indirizzi di posta elettronica.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Dalla tabella, eseguire una delle seguenti operazioni:
   - Per rimuovere un server di posta in modo che gli avvisi non vengano più inviati agli indirizzi di posta elettronica, selezionare la riga del server di posta.
   - Per rimuovere un indirizzo e-mail in modo che gli avvisi non vengano più inviati a questo indirizzo, selezionare la riga dell'indirizzo e-mail che si desidera eliminare. Il pulsante **Delete** (Elimina) in alto a destra della tabella diventa disponibile per la selezione.
4. Fare clic su **Delete** (Elimina) e confermare l'operazione.

Modificare il server di posta per gli avvisi

È possibile modificare l'indirizzo del server e-mail e l'indirizzo del mittente utilizzati per gli avvisi e-mail.

Prima di iniziare

L'indirizzo del server di posta che si sta modificando deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6 o un nome di dominio completo.

> Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Email**.
3. Selezionare **Configura server di posta**.

   Viene visualizzata la finestra di dialogo Configura server di posta.

4. Modificare l'indirizzo del server di posta, le informazioni sul mittente e le informazioni di contatto.
   - **Indirizzo del server di posta** — consente di modificare il nome di dominio completo, l'indirizzo IPv4 o l'indirizzo IPv6 del server di posta.

     > Per utilizzare un nome di dominio completo, è necessario configurare un server DNS su entrambi i controller. È possibile configurare un server DNS dalla pagina hardware.

   - **Email sender address** — Modifica l'indirizzo email da utilizzare come mittente del messaggio. Questo indirizzo viene visualizzato nel campo "da" del messaggio di posta elettronica.
   - **Include contact information in email** — per modificare le informazioni di contatto del mittente, selezionare questa opzione, quindi modificare il nome e il numero di telefono.
5. Fare clic su **Save** (Salva).

Gestire gli avvisi SNMP

Configurare gli avvisi SNMP

Per configurare gli avvisi SNMP (Simple Network Management Protocol), è necessario identificare almeno un server in cui il monitor degli eventi dell'array di storage può inviare trap SNMP. La configurazione richiede un nome di comunità o un nome utente e un indirizzo IP per il server.

Prima di iniziare

- Un server di rete deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).
- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

  - Passare a. "Supporto NetApp".
  - Fare clic sulla scheda **Downloads**, quindi selezionare **Downloads**.
  - Fare clic su **Software controller OS SANtricity e-Series**.
  - Selezionare **Scarica ultima release**.
  - Effettuare l'accesso.
  - Accettare la dichiarazione di attenzione e il contratto di licenza.
  - Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come identificare il server SNMP per le destinazioni trap, quindi verificare la configurazione.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Al primo setup, nella scheda SNMP viene visualizzato "Configure Communities/Users" (Configura community/utenti).

3. Selezionare **Configura community/utenti**.

   Viene visualizzata la finestra di dialogo Select SNMP version (Seleziona versione SNMP).

4. Selezionare la versione SNMP per gli avvisi, **SNMPv2c** o **SNMPv3**.

   A seconda della selezione effettuata, viene visualizzata la finestra di dialogo Configura comunità o Configura utenti SNMPv3.

5. Seguire le istruzioni appropriate per SNMPv2c (community) o SNMPv3 (utenti):
   - **SNMPv2c (community)** — nella finestra di dialogo Configura community, immettere una o più stringhe di community per i server di rete. Un nome di comunità è una stringa che identifica un set noto di stazioni di gestione e viene in genere creato da un amministratore di rete. È costituito solo da caratteri

ASCII stampabili. Puoi aggiungere fino a 256 community. Al termine, fare clic su **Save** (Salva).

- **SNMPv3 (utenti)** — nella finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3), fare clic su **Add** (Aggiungi), quindi immettere le seguenti informazioni:
  - **Nome utente** — immettere un nome per identificare l'utente, che può contenere fino a 31 caratteri.
  - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
  - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
  - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri. Al termine, fare clic su **Aggiungi**, quindi su **Chiudi**.

6. Dalla pagina Avvisi con la scheda SNMP selezionata, fare clic su **Aggiungi destinazioni trap**.

   Viene visualizzata la finestra di dialogo Add Trap Destinations (Aggiungi destinazioni trap).

7. Immettere una o più destinazioni trap, selezionare i nomi di comunità o utenti associati, quindi fare clic su **Aggiungi**.
   - **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
   - **Nome di comunità o Nome utente** — dal menu a discesa, selezionare il nome di comunità (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne è stata definita una sola, il nome viene già visualizzato in questo campo).
   - **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, le destinazioni trap e i nomi associati vengono visualizzati nella scheda **SNMP** della pagina **Avvisi**.
8. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Aggiungere destinazioni trap per gli avvisi SNMP

È possibile aggiungere fino a 10 server per l'invio di trap SNMP.

Prima di iniziare

- Il server di rete che si desidera aggiungere deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), in modo che il monitor eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (sono consentiti fino a 10 server).
- Il file MIB (Management Information base) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito NetApp Support:

- Passare a. "Supporto NetApp".
- Fare clic su **Downloads**, quindi selezionare **Downloads**.
- Fare clic su **Software controller OS SANtricity e-Series**.
- Selezionare **Scarica ultima release**.
- Effettuare l'accesso.
- Accettare la dichiarazione di attenzione e il contratto di licenza.
- Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap attualmente definite vengono visualizzate nella tabella.

3. Selezionare **Add Trap Desinations** (Aggiungi Desination trap).

   Viene visualizzata la finestra di dialogo Add Trap Destinations (Aggiungi destinazioni trap).

4. Immettere una o più destinazioni trap, selezionare i nomi di comunità o utenti associati, quindi fare clic su **Aggiungi**.
   - **Destinazione trap** — immettere un indirizzo IPv4 o IPv6 del server che esegue un servizio SNMP.
   - **Nome di comunità o Nome utente** — dal menu a discesa, selezionare il nome di comunità (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne è stata definita una sola, il nome viene già visualizzato in questo campo).
   - **Send Authentication Failure Trap** — selezionare questa opzione (la casella di controllo) se si desidera avvisare la destinazione trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di comunità o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, nella tabella vengono visualizzate le destinazioni trap e i nomi di comunità o utenti associati.
5. Per assicurarsi che un trap sia valido, selezionare una destinazione trap dalla tabella, quindi fare clic su **Test Trap Destination** (destinazione trap test) per inviare un trap di test all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP ai server ogni volta che si verifica un evento verificabile.

Configurare le variabili SNMP MIB

Per gli avvisi SNMP, è possibile configurare facoltativamente le variabili MIB (Management Information base) che vengono visualizzate nei trap SNMP. Queste variabili possono restituire il nome dell'array di storage, la posizione dell'array e una persona di contatto.

Prima di iniziare

Il file MIB deve essere copiato e compilato sul server con l'applicazione di servizio SNMP.

Se non si dispone di un file MIB, è possibile ottenerlo come segue:

- Passare a. "Supporto NetApp".

- Fare clic su **Downloads**, quindi selezionare **Downloads**.
- Fare clic su **Software controller OS SANtricity e-Series**.
- Selezionare **Scarica ultima release**.
- Effettuare l'accesso.
- Accettare la dichiarazione di attenzione e il contratto di licenza.
- Scorrere verso il basso fino a visualizzare il file MIB per il tipo di controller in uso, quindi fare clic sul collegamento per scaricare il file.

A proposito di questa attività

Questa attività descrive come definire le variabili MIB per i trap SNMP. Queste variabili possono restituire i seguenti valori in risposta a SNMP GetRequests:

- `sysName` (nome dell'array di storage)
- `sysLocation` (posizione dello storage array)
- `sysContact` (nome di un amministratore)

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.
3. Selezionare **Configure SNMP MIB variables** (Configura variabili SNMP MIB).

   Viene visualizzata la finestra di dialogo Configura variabili MIB SNMP.

4. Immettere uno o più dei seguenti valori, quindi fare clic su **Save** (Salva).
   - **Name** — il valore per la variabile MIB `sysName`. Ad esempio, inserire un nome per l'array di storage.
   - **Location** — il valore della variabile MIB `sysLocation`. Ad esempio, inserire una posizione dell'array di storage.
   - **Contatto** — il valore della variabile MIB `sysContact`. Ad esempio, inserire un amministratore responsabile dello storage array.

Risultati

Questi valori vengono visualizzati nei messaggi trap SNMP per gli avvisi degli array di storage.

Modificare le community per le trap SNMPv2c

È possibile modificare i nomi di comunità per i trap SNMPv2c.

Prima di iniziare

È necessario creare un nome di comunità.

Fasi

1. Selezionare **impostazione › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Selezionare **Configura community**.
4. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**. I nomi di comunità possono essere costituiti solo da caratteri ASCII stampabili.

Risultati

La scheda SNMP della pagina Avvisi visualizza il nome di comunità aggiornato.

Modificare le impostazioni utente per i trap SNMPv3

È possibile modificare le definizioni utente per i trap SNMPv3.

Prima di iniziare

È necessario creare un utente per la trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella tabella.

3. Per modificare una definizione utente, selezionare l'utente nella tabella, quindi fare clic su **Configura utenti**.
4. Nella finestra di dialogo, fare clic su **Visualizza/Modifica impostazioni**.
5. Modificare le seguenti informazioni:
   - **Nome utente** — consente di modificare il nome che identifica l'utente, che può contenere fino a 31 caratteri.
   - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
   - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
   - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri.

Risultati

La scheda SNMP della pagina Avvisi visualizza le impostazioni aggiornate.

Aggiungere community per le trap SNMPv2c

È possibile aggiungere fino a 256 nomi di comunità per le trap SNMPv2c.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

Le destinazioni trap e i nomi di comunità vengono visualizzati nella tabella.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo Configura comunità.

4. Selezionare **Aggiungi un'altra community**.
5. Immettere il nuovo nome di comunità, quindi fare clic su **Salva**.

Risultati

Il nuovo nome di comunità viene visualizzato nella scheda SNMP della pagina Avvisi.

Aggiungere utenti per le trap SNMPv3

È possibile aggiungere fino a 256 utenti per i trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella tabella.

3. Selezionare **Configure Users** (Configura utenti).

   Viene visualizzata la finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3).

4. Selezionare **Aggiungi**.
5. Inserire le seguenti informazioni, quindi fare clic su **Aggiungi**.
   - **Nome utente** — immettere un nome per identificare l'utente, che può contenere fino a 31 caratteri.
   - **ID motore** — selezionare l'ID motore, utilizzato per generare chiavi di autenticazione e crittografia per i messaggi, che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, selezionare **locale**. Se si dispone di una configurazione non standard, selezionare **Custom**; viene visualizzato un altro campo in cui inserire l'ID del motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32 caratteri.
   - **Authentication credentials** — selezionare un protocollo di autenticazione che garantisca l'identità degli utenti. Quindi, inserire una password di autenticazione, necessaria quando si imposta o si modifica il protocollo di autenticazione. La password deve contenere da 8 a 128 caratteri.
   - **Privacy credentials** — selezionare un protocollo per la privacy utilizzato per crittografare il contenuto dei messaggi. Quindi, inserire una password per la privacy, necessaria quando il protocollo per la privacy viene impostato o modificato. La password deve contenere da 8 a 128 caratteri.

Rimuovere le community per le trap SNMPv2c

È possibile rimuovere un nome di comunità per i trap SNMPv2c.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi di comunità vengono visualizzati nella pagina **Avvisi**.

3. Selezionare **Configura community**.

   Viene visualizzata la finestra di dialogo Configura comunità.

4. Selezionare il nome della community che si desidera eliminare, quindi fare clic sull'icona **Rimuovi** (X) all'estrema destra.

   Se le destinazioni trap sono associate a questo nome di comunità, la finestra di dialogo Conferma rimozione comunità mostra gli indirizzi di destinazione trap interessati.

5. Confermare l'operazione, quindi fare clic su **Rimuovi**.

Risultati

Il nome di comunità e la destinazione trap associata vengono rimossi dalla pagina Avvisi.

Rimuovere gli utenti per i trap SNMPv3

È possibile rimuovere un utente per i trap SNMPv3.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Le destinazioni trap e i nomi utente vengono visualizzati nella pagina Avvisi.

3. Selezionare **Configure Users** (Configura utenti).

   Viene visualizzata la finestra di dialogo Configure SNMPv3 Users (Configura utenti SNMPv3).

4. Selezionare il nome utente che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
5. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Il nome utente e la destinazione trap associata vengono rimossi dalla pagina Avvisi.

Eliminare le destinazioni trap

È possibile eliminare un indirizzo di destinazione trap in modo che il monitor eventi dell'array di storage non invii più trap SNMP a tale indirizzo.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **SNMP**.

   Gli indirizzi di destinazione trap vengono visualizzati nella tabella.

3. Selezionare una destinazione trap, quindi fare clic su **Delete** (Elimina) in alto a destra nella pagina.
4. Confermare l'operazione, quindi fare clic su **Delete** (Elimina).

   L'indirizzo di destinazione non viene più visualizzato nella pagina Avvisi.

Risultati

La destinazione dei trap cancellati non riceve più trap SNMP dal monitor degli eventi dell'array di storage.

Gestire gli avvisi syslog

Configurare il server syslog per gli avvisi

Per configurare gli avvisi syslog, è necessario immettere un indirizzo del server syslog e una porta UDP. Sono consentiti fino a cinque server syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero della porta UDP del server syslog deve essere disponibile. Questa porta è generalmente 514.

A proposito di questa attività

Questa attività descrive come inserire l'indirizzo e la porta per il server syslog, quindi verificare l'indirizzo immesso.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.

   Se un server syslog non è ancora definito, nella pagina Avvisi viene visualizzato "Add Syslog Servers" (Aggiungi server Syslog).

3. Fare clic su **Aggiungi server Syslog**.

   Viene visualizzata la finestra di dialogo Add Syslog Server (Aggiungi server Syslog).

4. Inserire le informazioni relative a uno o più server syslog (massimo cinque), quindi fare clic su **Aggiungi**.
   - **Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **UDP Port** — in genere, la porta UDP per syslog è 514. Nella tabella vengono visualizzati i server syslog configurati.
5. Per inviare un avviso di test agli indirizzi del server, selezionare **Test All Syslog Servers** (verifica tutti i server Syslog).

Risultati

Il monitor degli eventi invia avvisi al server syslog ogni volta che si verifica un evento verificabile. Per configurare ulteriormente le impostazioni syslog per i registri di controllo, vedere "Configurare il server syslog per i registri di controllo".

Modificare i server syslog per gli avvisi

È possibile modificare l'indirizzo del server utilizzato per ricevere gli avvisi syslog.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.

3. Dalla tabella, selezionare un indirizzo server syslog, quindi fare clic sull'icona **Edit** (matita) a destra.

   La riga diventa un campo modificabile.

4. Modificare l'indirizzo del server e il numero della porta UDP, quindi fare clic sull'icona **Salva** (segno di spunta).

Risultati

L'indirizzo del server aggiornato viene visualizzato nella tabella.

Aggiungere server syslog per gli avvisi

È possibile aggiungere un massimo di cinque server per gli avvisi syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero della porta UDP del server syslog deve essere disponibile. Questa porta è generalmente 514.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.
3. Selezionare **Aggiungi server Syslog**.

   Viene visualizzata la finestra di dialogo Add Syslog Server (Aggiungi server Syslog).

4. Selezionare **Aggiungi un altro server syslog**.
5. Inserire le informazioni relative al server syslog, quindi fare clic su **Aggiungi**.
   - **Syslog Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **UDP Port** — in genere, la porta UDP per syslog è 514.

     È possibile configurare fino a cinque server syslog.

Risultati

Gli indirizzi del server syslog vengono visualizzati nella tabella.

Eliminare i server syslog per gli avvisi

È possibile eliminare un server syslog in modo che non riceva più avvisi.

Fasi

1. Selezionare **Impostazioni › Avvisi**.
2. Selezionare la scheda **Syslog**.
3. Selezionare un indirizzo del server syslog, quindi fare clic su **Remove** (Rimuovi) dall'alto a destra.

   Viene visualizzata la finestra di dialogo Conferma eliminazione server Syslog.

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

Risultati

Il server rimosso non riceve più avvisi dal monitor eventi.

FAQ

Cosa fare se gli avvisi sono disattivati?

Se si desidera che gli amministratori ricevano notifiche su eventi importanti che si verificano nell'array di storage, è necessario configurare un metodo di avviso.

Per gli array di storage gestiti con Gestore di sistema di SANtricity, è possibile configurare gli avvisi dalla pagina Avvisi. Le notifiche di avviso possono essere inviate tramite e-mail, trap SNMP o messaggi syslog. Inoltre, gli avvisi e-mail possono essere configurati dall'installazione guidata iniziale.

Come si configurano gli avvisi SNMP o syslog?

Oltre agli avvisi via email, è possibile configurare gli avvisi in modo che vengano inviati tramite trap SNMP (Simple Network Management Protocol) o messaggi syslog.

Per configurare gli avvisi SNMP o syslog, accedere al **Impostazioni › Avvisi**.

Perché i timestamp non sono coerenti tra l'array e gli avvisi?

Quando lo storage array invia avvisi, non corregge il fuso orario del server o dell'host di destinazione che riceve gli avvisi. Invece, l'array di storage utilizza l'ora locale (GMT) per creare l'indicazione dell'ora utilizzata per il record di avviso. Di conseguenza, potrebbero verificarsi delle incoerenze tra i timestamp per lo storage array e il server o l'host che riceve un avviso.

Poiché l'array di storage non corregge il fuso orario durante l'invio degli avvisi, l'indicazione dell'ora sugli avvisi è relativa al GMT, con un offset del fuso orario pari a zero. Per calcolare un indicatore data e ora appropriato al fuso orario locale, è necessario determinare l'offset dell'ora dal GMT, quindi aggiungere o sottrarre tale valore dai contrassegni data e ora.

Impostazioni dell'array

Panoramica delle impostazioni

È possibile configurare System Manager per alcune impostazioni generali degli array e funzionalità aggiuntive.

Quali impostazioni è possibile configurare?

Le impostazioni dell'array includono:

- "Performance e impostazioni della cache"
- "Bilanciamento automatico del carico"
- "Funzionalità add-on"

- "Sicurezza dei dischi"

Attività correlate

Scopri di più sulle attività correlate alle impostazioni di sistema:

- "Scaricare l'interfaccia a riga di comando (CLI)"
- "Creare una chiave di sicurezza interna"
- "Creare una chiave di sicurezza esterna"
- "Configurare le porte iSCSI"
- "Configurare NVME sulle porte IB"
- "Configurare NVMe sulle porte RoCE"

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**.

  - **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.

Configurare le impostazioni degli array

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).

Risultati

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 attiva indicatori Storage Array Locator e si accendono le spie di localizzazione dell'array di storage corrispondente.

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 System Manager).

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 dello storage array
   - Configurazione del volume
   - Configurazione dell'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 le "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 la configurazione dell'array di storage salvata in un altro array di storage, utilizzare l'interfaccia della riga di comando (SMcli) di SANtricity con `-f` per applicare `.cfg` file.

> È inoltre possibile caricare una configurazione di array di storage in altri array di storage utilizzando l'interfaccia di Unified Manager (selezionare **Manage › Import Settings**).

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

	Volume	Array di storage
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.

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.

Impostazione della cache	Descrizione
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 32 KiB. Il sistema consente la dimensione del blocco della cache di 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:
   - **Start demand cache wlushing** — scegliere una percentuale appropriata per l'i/o utilizzato nel proprio ambiente. Se si sceglie un valore inferiore al 80%, si potrebbe notare una riduzione delle performance.
   - **Dimensione blocco cache —** Scegli una dimensione adatta alle tue applicazioni.
4. Fare clic su **Save** (Salva).

Impostare il bilanciamento automatico del carico

La funzione di bilanciamento automatico del carico 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.

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.

A proposito di questa attività

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.

> Per il sistema storage EF600, questa funzione è disattivata per impostazione predefinita.

L'impostazione influisce sulle operazioni come segue:

- **On** (impostazione predefinita) — impostazione richiesta per la configurazione del mirroring con CLI e altri strumenti, come 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.

Configurare le funzionalità aggiuntive

Come funzionano le funzionalità aggiuntive

I componenti aggiuntivi sono funzionalità non incluse nella configurazione standard di System Manager e potrebbero richiedere 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 e il codice funzione per l'attivazione.
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.

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 per l'attivazione della funzione. Per i pacchetti di funzionalità, questo codice 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 a **licenze software** per il prodotto in uso.
   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 hardware inviando un'e-mail o un documento di testo al fornitore dello storage con le seguenti informazioni: Numero di serie dello chassis, identificativo di abilitazione e codice per l'attivazione 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 che descrivono la conversione e la preparazione per i nuovi attributi dello storage array. Per istruzioni sulla conversione del protocollo host, consultare la guida alla manutenzione dell'hardware del modello di controller in uso.
- 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. Tipo `change` sul 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.

Scaricare l'interfaccia a riga di comando (CLI)

Da System Manager, è possibile scaricare il pacchetto dell'interfaccia a riga di comando (CLI).

La CLI fornisce un metodo basato su testo per la configurazione e il monitoraggio degli array di storage. Comunica tramite https e utilizza la stessa sintassi della CLI disponibile nel pacchetto software di gestione installato esternamente. Non è richiesta alcuna chiave per scaricare la CLI.

Prima di iniziare

Sul sistema di gestione in cui si intende eseguire i comandi CLI deve essere disponibile Java Runtime Environment (JRE), versione 8 e successive.

Fasi

1. Selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **interfaccia riga di comando**.

   Il pacchetto ZIP viene scaricato nel browser.

3. Salvare il file ZIP nel sistema di gestione in cui si desidera eseguire i comandi CLI per l'array di storage, quindi estrarre il file.

   È ora possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:. Un riferimento al comando CLI è disponibile nel menu Help (Guida) in alto a destra dell'interfaccia utente di System Manager.

FAQ

Che cos'è il bilanciamento automatico del carico?

La funzione di bilanciamento automatico del carico fornisce un bilanciamento i/o automatizzato e garantisce che il traffico i/o in entrata dagli host sia gestito e bilanciato dinamicamente tra entrambi i controller.

La funzione di bilanciamento automatico del carico offre una migliore gestione delle risorse i/o, reagendo in modo dinamico alle variazioni di carico nel tempo e regolando automaticamente la proprietà dei controller di volume per correggere eventuali problemi di squilibrio 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.

> Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.

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 8, 16, 32 KiB. Tutti i volumi sul sistema storage condividono lo stesso spazio cache; pertanto, i volumi possono avere una sola dimensione del blocco cache.

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 32 KiB, ma è possibile impostare il valore su 8, 16, 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 (Sincronizza blocchi array di storage), 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.

Sicurezza dei dischi

Panoramica sulla sicurezza del disco

È possibile configurare Drive Security e la gestione delle chiavi dalla pagina Security Key Management.

Che cos'è Drive Security?

Drive Security è una funzione che impedisce l'accesso non autorizzato ai dati su dischi abilitati alla sicurezza quando vengono rimossi dallo storage array. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Quando i dischi FDE o FIPS vengono fisicamente rimossi dall'array, non possono funzionare fino a quando non vengono installati in un altro array. A questo punto, i dischi si trovano in uno stato di sicurezza bloccato fino a quando non viene fornita la chiave di sicurezza corretta. Una *chiave di sicurezza* è una stringa di caratteri condivisa tra questi tipi di dischi e i controller di un array di storage.

Scopri di più:

- "Funzionamento della funzione Drive Security"
- "Come funziona la gestione delle chiavi di sicurezza"
- "Promuovere la terminologia in materia di sicurezza"

Come si configura la gestione delle chiavi?

Per implementare Drive Security, è necessario che nell'array siano installati dischi FDE o FIPS. Per configurare la gestione delle chiavi per questi dischi, accedere al **Impostazioni › sistema › Gestione delle chiavi di sicurezza** dove è possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Infine, è possibile attivare Drive Security per pool e gruppi di volumi selezionando "Secure-capable" nelle impostazioni del volume.

Scopri di più:

- "Creare una chiave di sicurezza interna"
- "Creare una chiave di sicurezza esterna"
- "Creare il pool manualmente"
- "Creare gruppi di volumi"

Come faccio a sbloccare i dischi?

Se è stata configurata la gestione delle chiavi e successivamente sono state spostate le unità abilitate alla protezione da un array di storage a un altro, è necessario riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sui dischi.

Scopri di più:

- "Sbloccare i dischi quando si utilizza la gestione interna delle chiavi"

- "Sbloccare i dischi quando si utilizza la gestione esterna delle chiavi"

Informazioni correlate

Scopri di più sulle attività correlate alla gestione delle chiavi:

- "Utilizzare i certificati firmati CA per l'autenticazione con un server di gestione delle chiavi"
- "Eseguire il backup della chiave 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 mantenute e "nascoste" in una posizione non accessibile sulla 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 nascosta e 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. Ottenere un file di certificato client firmato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste KMIP.
   a. Innanzitutto, completare e scaricare una richiesta di firma del certificato (CSR) del client. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
   b. Successivamente, viene richiesto un certificato client firmato da una CA attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR.
   c. Una volta ottenuto un file di certificato client, copiarlo sull'host in cui si accede a System Manager.
4. Recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.
5. 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.
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.

Termine	Descrizione
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.

Configurare le chiavi di sicurezza

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 protezione. 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 protezione, viene visualizzata la finestra di dialogo Crea chiave di protezione.

3. Inserire le informazioni nei seguenti campi:

   - **Definire un identificatore della chiave di sicurezza** — è possibile 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, aggiunti a entrambe le estremità della stringa immessa. I caratteri generati garantiscono che l'identificatore sia univoco.

   - **Definire una passphrase/immettere nuovamente la 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**.

Risultati

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 protezione. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- Si dispone di un file di certificato client firmato per i controller dell'array di storage ed è stato copiato nell'host in cui si accede a System Manager. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

  > Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al 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 protezione esterna.

3. In **Connect to Key Server** (connessione al server chiavi), immettere le informazioni nei seguenti campi.
   - **Indirizzo del 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** — inserire il numero di porta utilizzato per le comunicazioni KMIP. Il numero di porta più comune utilizzato per le comunicazioni del server di gestione delle chiavi è 5696.

     Opzionale: se si desidera configurare un server chiavi di backup, fare clic su **Aggiungi server chiavi**,

quindi immettere le informazioni relative al server. Se non è possibile raggiungere il server principale delle chiavi, viene utilizzato il secondo server delle chiavi. Assicurarsi che ciascun server di chiavi abbia accesso allo stesso database di chiavi; in caso contrario, l'array eseguirà il post degli errori e non potrà utilizzare il server di backup.

> Viene utilizzato un solo server di chiavi alla volta. Se lo storage array non riesce a raggiungere il server principale delle chiavi, l'array contatterà il server delle chiavi di backup. Tenere presente che è necessario mantenere la parità su entrambi i server; in caso contrario, potrebbero verificarsi errori.

- **Select client certificate** — 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. È possibile scegliere un certificato root, intermedio o server per il server di gestione delle chiavi.

4. Fare clic su **Avanti**.
5. In **Create/Backup Key** (Crea/Backup chiave), è possibile creare una chiave di backup per motivi di sicurezza.
   - (Consigliato) per creare una chiave di backup, mantenere la casella di controllo selezionata, quindi immettere e confermare una 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'unità abilitata per la sicurezza dall'array di storage, è necessario conoscere la password per sbloccare i dati dell'unità.

+

   - Se non si desidera creare una chiave di backup, deselezionare la casella di controllo.

> Tenere presente che se si perde l'accesso al server delle chiavi esterno e non si dispone di una chiave di backup, l'accesso ai dati sui dischi viene perso se vengono migrati in un altro array di storage. Questa opzione è l'unico metodo per creare una chiave di backup in System Manager.

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.

Gestire le chiavi di sicurezza

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.

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 protezione).

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 la passphrase** — in ciascuno di questi campi, inserire la 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).
4. Per le chiavi di sicurezza esterne, se si desidera eliminare la vecchia chiave di sicurezza quando viene creata la nuova, selezionare "Delete current Security key…" (Elimina chiave di sicurezza corrente…). casella di controllo nella parte inferiore della finestra di dialogo.

> **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.

5. 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.

6. 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.

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 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.

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:
   - **Indirizzo del 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** — inserire il numero di porta utilizzato per le comunicazioni KMIP (Key Management Interoperability Protocol).

     Opzionale: è possibile includere un altro server chiavi facendo clic su **Aggiungi server chiavi**.

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.

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 Back Up Security Key (Esegui backup chiave di protezione).

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.

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 protezione).

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 quando si utilizza la gestione interna delle chiavi

Se è stata configurata la gestione interna delle chiavi e successivamente sono state spostate le unità abilitate alla protezione da un array di storage a un altro, è necessario riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sui dischi.

Prima di iniziare

- Nell'array di origine (l'array in cui si rimuovono i dischi), sono stati esportati gruppi di volumi e rimossi i dischi. Nell'array di destinazione, i dischi sono stati reinstallati.

  > La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite in "Knowledge base di NetApp". Seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo Impossibile creare la chiave di protezione. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- 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

Quando si utilizza la gestione interna delle chiavi, la chiave di sicurezza viene memorizzata localmente nell'array di storage. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dai dischi per l'accesso in lettura/scrittura. Quando i dischi vengono fisicamente rimossi dall'array e installati in un altro, non possono funzionare fino a quando non si fornisce la chiave di sicurezza corretta.

> È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando viene utilizzata la gestione delle chiavi *interne*. Se è stata utilizzata la gestione delle chiavi *external*, vedere "Sbloccare i dischi quando si utilizza la gestione esterna delle chiavi". Se si sta eseguendo un aggiornamento del controller e si stanno sostituendo tutti i controller con l'hardware più recente, è necessario seguire diversi passaggi come descritto nel centro di documentazione e-Series e SANtricity, in "Sbloccare i dischi".

Una volta reinstallati i dischi abilitati per la protezione in un altro array, questo rileva i dischi e visualizza una condizione di "attenzione necessaria" insieme allo stato "chiave di sicurezza necessaria". Per sbloccare i dati del disco, selezionare il file della chiave di sicurezza e immettere la password per la chiave. (Questa 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. **Opzionale:** posizionare 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.

Al termine

Nell'array di destinazione (l'array con i dischi appena installati), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite in "Knowledge base di NetApp".

Sbloccare i dischi quando si utilizza la gestione esterna delle chiavi

Se è stata configurata la gestione delle chiavi esterne e successivamente sono state spostate le unità abilitate alla protezione da un array di storage a un altro, è necessario riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sui dischi.

Prima di iniziare

- Nell'array di origine (l'array in cui si rimuovono i dischi), sono stati esportati gruppi di volumi e rimossi i dischi. Nell'array di destinazione, i dischi sono stati reinstallati.

  > La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite in "Knowledge base di NetApp". Seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- La funzione Drive Security deve essere attivata. In caso contrario, viene visualizzata la finestra di dialogo Impossibile creare la chiave di protezione. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
- È necessario conoscere l'indirizzo IP e il numero di porta del server di gestione delle chiavi.
- Si dispone di un file di certificato client firmato per i controller dell'array di storage ed è stato copiato nell'host in cui si accede a System Manager. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al server di gestione delle chiavi.

A proposito di questa attività

Quando si utilizza la gestione esterna delle chiavi, la chiave di sicurezza viene memorizzata esternamente su un server progettato per proteggere le chiavi di sicurezza. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dai dischi per l'accesso in lettura/scrittura. Quando i dischi vengono fisicamente rimossi dall'array e installati in un altro, non possono funzionare fino a quando non si fornisce la chiave di sicurezza corretta.

> È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando viene utilizzata la gestione delle chiavi *esterne*. Se è stata utilizzata la gestione delle chiavi *interna*, vedere "Sbloccare i dischi quando si utilizza la gestione interna delle chiavi". Se si sta eseguendo un aggiornamento del controller e si stanno sostituendo tutti i controller con l'hardware più recente, è necessario seguire diversi passaggi come descritto nel centro di documentazione e-Series e SANtricity, in "Sbloccare i dischi".

Una volta reinstallati i dischi abilitati per la protezione in un altro array, questo rileva i dischi e visualizza una condizione di "attenzione necessaria" insieme allo stato "chiave di sicurezza necessaria". Per sbloccare i dati del disco, importare il file della chiave di sicurezza e immettere la password per la chiave. (Questa password non corrisponde alla password Administrator dell'array di storage). Durante questo processo, l'array di storage viene configurato per l'utilizzo di un server di gestione delle chiavi esterno, quindi la chiave sicura sarà accessibile. È necessario fornire le informazioni di contatto del server per consentire all'array di storage di connettersi e recuperare la chiave di sicurezza.

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 **Create External Key** (Crea chiave esterna).
3. Completare la procedura guidata con le informazioni di connessione e i certificati richiesti.
4. Fare clic su **Test Communication** (verifica comunicazione) per garantire l'accesso al server di gestione delle chiavi esterno.
5. 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.

6. **Opzionale:** posizionare il mouse su un numero di disco per visualizzare la posizione dell'unità (numero di shelf e numero di alloggiamento).
7. 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.

8. Inserire la password associata al file delle chiavi.

   I caratteri immessi vengono mascherati.

9. 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.

Al termine

Nell'array di destinazione (l'array con i dischi appena installati), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia della riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite in "Knowledge base di NetApp".

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.

Gestione interna delle chiavi

Le chiavi interne vengono mantenute e "nascoste" in una posizione non accessibile sulla memoria persistente del controller. Prima di creare una chiave di sicurezza interna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

È quindi possibile creare una chiave di sicurezza interna, che implica la definizione di un identificatore e di una passphrase. L'identificatore è una stringa associata alla chiave di sicurezza e memorizzata sul controller e su tutti i dischi associati alla chiave. La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Al termine, la chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Gestione esterna delle chiavi

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol). Prima di creare una chiave di sicurezza esterna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.
3. Ottenere un file di certificato client firmato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste KMIP.
   a. Innanzitutto, completare e scaricare una richiesta di firma del certificato (CSR) del client. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
   b. Successivamente, viene richiesto un certificato client firmato da una CA attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
   c. Una volta ottenuto un file di certificato client, copiarlo sull'host in cui si accede a System Manager.
4. Recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

È quindi possibile creare una chiave esterna che preveda la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, vengono caricati anche i file dei certificati. Al termine, il sistema si connette al server di gestione delle chiavi con le credenziali immesse. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Perché è necessario definire una passphrase?

La password viene utilizzata per crittografare e decrittare il file della chiave di sicurezza memorizzato nel client di gestione locale. Senza la passphrase, la chiave di sicurezza non può essere decifrata e utilizzata per sbloccare i dati da un disco abilitato alla sicurezza se viene reinstallata in un altro array di storage.

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, è necessario importarne la chiave di sicurezza.

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

- Lo storage array deve già disporre di una chiave di sicurezza. I dischi migrati verranno ridimitati nell'array di storage di destinazione.
- Per i dischi che si stanno migrando, è necessario conoscere l'identificatore della chiave di sicurezza e la passphrase che corrisponde al file della chiave di sicurezza.
- Il file della chiave di sicurezza deve essere disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager).
- Se si sta reimpostando un disco NVMe bloccato, è necessario inserire l'ID di sicurezza del disco. Per individuare l'ID di sicurezza, rimuovere fisicamente l'unità e individuare la stringa PSID (massimo 32 caratteri) sull'etichetta dell'unità. Assicurarsi che il disco sia reinstallato prima di avviare l'operazione.

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

La finestra Drive Settings (Impostazioni disco) contiene informazioni sugli attributi Drive Security (protezione disco). "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).

Gestione degli accessi

Panoramica sulla gestione degli accessi

Access Management è un metodo per stabilire l'autenticazione dell'utente in System Manager.

Quali metodi di autenticazione sono disponibili?

I metodi di autenticazione includono RBAC (role-based access control), Directory Services e Security Assertion Markup Language (SAML):

- **RBAC/ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC applicate nell'array di storage. I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e i servizi di directory, ad esempio Active Directory di Microsoft.
- **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando SAML 2.0.

Scopri di più:

- "Come funziona Access Management"
- "Terminologia per la gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "Ruoli utente locali"
- "Servizi di directory"
- "SAML"

Come si configura l'autenticazione?

Lo storage array è preconfigurato per l'utilizzo di ruoli utente locali, un'implementazione delle funzionalità RBAC. Se si desidera configurare un metodo diverso, accedere al **Impostazioni › Gestione accessi**.

Scopri di più:

- "Aggiungere un server di directory LDAP"
- "Configurare SAML"

Informazioni correlate

Scopri di più sulle attività correlate alla gestione degli accessi:

- "Modificare le password"
- "Visualizzare l'attività del registro di audit"
- "Configurare il server syslog per i registri di controllo"

Concetti

Come funziona Access Management

Access Management è un metodo per stabilire l'autenticazione dell'utente in System Manager.

La configurazione e l'autenticazione dell'utente funzionano come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   > Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore accede a Access Management nell'interfaccia utente. Lo storage array è preconfigurato per l'utilizzo dei ruoli utente locali, ovvero un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
   - **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC applicate nell'array di storage. I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come singolo metodo di autenticazione o in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, ad eccezione dell'impostazione delle password per gli utenti.
   - **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft. Un amministratore si connette al server LDAP, quindi esegue il mapping degli utenti LDAP ai ruoli utente locali incorporati nell'array di storage.
   - **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando il linguaggio SAML (Security Assertion Markup Language) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi mappa gli utenti IdP ai ruoli utente locali integrati nell'array di storage.
4. L'amministratore fornisce agli utenti le credenziali di accesso per System Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali.

   > Se l'autenticazione viene gestita con SAML e SSO (Single Sign-on), il sistema potrebbe ignorare la finestra di dialogo di accesso di System Manager.

   Durante l'accesso, il sistema esegue le seguenti attività in background:

   - Autentica il nome utente e la password rispetto all'account utente.
   - Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
   - Fornisce all'utente l'accesso alle attività nell'interfaccia utente.

- Visualizza il nome utente nella parte superiore destra dell'interfaccia.

Attività disponibili in System Manager

L'accesso alle attività dipende dai ruoli assegnati a un utente, che includono:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Un'attività non disponibile viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente. Ad esempio, un utente con il ruolo Monitor può visualizzare tutte le informazioni sui volumi, ma non può accedere alle funzioni per la modifica di tale volume. Le schede relative a funzioni come **Copy Services** e **Add to workload** non saranno visualizzate; sono disponibili solo **View/Edit Settings**.

Limitazioni di Unified Manager e Storage Manager

Se SAML è configurato per un array di storage, gli utenti non possono rilevare o gestire lo storage per tale array da Unified Manager o dalle interfacce precedenti di Storage Manager.

Una volta configurati i ruoli utente locali e i servizi di directory, gli utenti devono immettere le credenziali prima di eseguire una delle seguenti funzioni:

- Ridenominazione dello storage array
- Aggiornamento del firmware del controller
- Caricamento della configurazione di uno storage array
- Esecuzione di uno script
- Tentativo di eseguire un'operazione attiva quando una sessione non utilizzata è scaduta

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management al tuo storage array.

Termine	Descrizione
Token di accesso	I token di accesso vengono utilizzati per autenticare con l'API REST o l'interfaccia della riga di comando (CLI) al posto di un nome utente e di una password. I token sono associati a un utente specifico (inclusi gli utenti LDAP) e includono un set di autorizzazioni e una scadenza.
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.

Termine	Descrizione
Binding	Le operazioni BIND vengono utilizzate per autenticare i client nel server di directory. Il binding in genere richiede credenziali di account e password, ma alcuni server consentono operazioni di binding anonime.
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
IDP	Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
LDAP	LDAP (Lightweight Directory Access Protocol) è un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi diversi di connettersi al server LDAP per la convalida degli utenti.
RBAC	RBAC (role-based access control) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. I controlli RBAC vengono applicati all'array di storage e includono ruoli predefiniti.
SAML	SAML (Security Assertion Markup Language) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata dello storage array è conforme a SAML2.0 per l'asserzione, l'autenticazione e l'autorizzazione dell'identità.
SP	Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) applicate all'array di storage includono profili utente predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni

per l'accesso alle attività in System Manager.

I profili utente e i ruoli mappati sono accessibili dal **Impostazioni › Gestione accessi › ruoli utente locali** nell'interfaccia utente di System Manager.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata attività, tale attività viene visualizzata in grigio o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate nell'array di storage. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati per lo storage array. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   > Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. Facoltativamente, l'amministratore assegna nuove password per ogni profilo utente.
4. Gli utenti accedono al sistema con le credenziali assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con servizi di directory

Per la gestione degli accessi, gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

Se nella rete vengono utilizzati un server LDAP e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il server LDAP. Le impostazioni includono il nome di dominio, l'URL e le informazioni sull'account di binding.
3. Se il server LDAP utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati CA (Certificate Authority) per l'autenticazione tra il server LDAP e lo storage array.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli dell'array di storage. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e lo storage array.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungere un server di directory.
- Modificare le impostazioni del server di directory.
- Associare gli utenti LDAP ai ruoli utente locali.
- Rimuovere un server di directory.

Gestione degli accessi con SAML

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità SAML (Security Assertion Markup Language) 2.0 integrate nell'array.

Workflow di configurazione

La configurazione SAML funziona come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni di amministratore della sicurezza.

   Il `admin` L'utente ha accesso completo a tutte le funzioni di System Manager.

2. L'amministratore accede alla scheda **SAML** in Gestione accessi.
3. Un amministratore configura le comunicazioni con il provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Per configurare le comunicazioni con lo storage array, l'amministratore scarica il file di metadati IdP dal sistema IdP, quindi utilizza System Manager per caricare il file nello storage array.
4. Un amministratore stabilisce una relazione di trust tra il service provider e l'IdP. Un service provider controlla l'autorizzazione dell'utente; in questo caso, il controller nell'array di storage agisce come service provider. Per configurare le comunicazioni, l'amministratore utilizza System Manager per esportare un file di metadati del service provider per ciascun controller. Dal sistema IdP, l'amministratore importa i file di metadati nell'IdP.

   Gli amministratori devono inoltre assicurarsi che IdP supporti la capacità di restituire un ID nome all'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi dell'utente definiti nell'IdP. A tale scopo, l'amministratore utilizza System Manager per creare le mappature.
6. L'amministratore verifica l'accesso SSO all'URL IdP. Questo test garantisce che lo storage array e IdP possano comunicare.

   Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

7. Da System Manager, l'amministratore abilita SAML per lo storage array.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare o creare nuove mappature dei ruoli
- Esportare i file del provider di servizi

Restrizioni di accesso

Quando SAML è attivato, gli utenti non possono rilevare o gestire lo storage per quell'array da Unified Manager o dall'interfaccia precedente di Storage Manager.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse degli array di storage:

- Finestra Enterprise Management (EMW)
- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Token di accesso

I token di accesso forniscono un metodo di autenticazione con l'API REST o l'interfaccia della riga di comando (CLI), senza esporre nomi utente e password. Un token è associato a un utente specifico (inclusi gli utenti LDAP) e include un set di autorizzazioni e una scadenza.

Accesso a token web SAML e JSON

Per impostazione predefinita, un sistema con SAML attivato non consente l'accesso ai tradizionali strumenti della riga di comando. L'API REST e la CLI diventano effettivamente inutilizzabili perché il flusso di lavoro MFA richiede un reindirizzamento a un server Identity Provider per l'autenticazione. Pertanto, è necessario generare token in System Manager, che richiede l'autenticazione di un utente tramite MFA.

> Non è necessario che SAML sia abilitato per utilizzare i token Web, ma SAML è consigliato per il massimo livello di sicurezza.

Workflow per la creazione e l'utilizzo dei token

1. Creare un token in System Manager e determinarne la scadenza.
2. Copiare il testo del token negli Appunti o scaricarlo in un file, quindi salvare il testo del token in una posizione sicura.
3. Utilizzare il token come segue:
   - **REST API**: Per utilizzare un token in una richiesta API REST, aggiungere un'intestazione HTTP alle richieste. Ad esempio:
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**: Per utilizzare un token nella CLI, aggiungere il valore del token nella riga di comando o utilizzare il percorso di un file contenente il valore del token. Ad esempio:
     - Valore del token sulla riga di comando: `-t access-token-value`
     - Percorso di un file contenente il valore del token: `-T access-token-file`

Scopri di più:

- "Creare token di accesso"
- "Modificare i token di accesso"
- "Revocare i token di accesso"

Utilizzare ruoli utente locali

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature dei profili utente ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nell'array di storage.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

I profili utente e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.

   I profili utente sono mostrati nella tabella:

   - **Root admin** (admin) — Super amministratore che ha accesso a tutte le funzioni del sistema. Questo profilo utente include tutti i ruoli.
   - **Storage admin** (storage) — l'amministratore responsabile di tutto il provisioning dello storage. Questo profilo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Security admin** (sicurezza) — l'utente responsabile della configurazione della sicurezza, inclusa la gestione degli accessi, la gestione dei certificati e le funzioni dei dischi abilitati alla sicurezza. Questo profilo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support admin** (support) — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo profilo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** (monitor) — utente con accesso in sola lettura al sistema. Questo profilo utente include solo il ruolo Monitor.

Modificare le password

È possibile modificare le password utente per ciascun profilo utente in Gestione accessi.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.
- È necessario conoscere la password dell'amministratore locale.

A proposito di questa attività

Quando si sceglie una password, tenere presenti le seguenti linee guida:

- Le nuove password utente locali devono soddisfare o superare l'impostazione corrente per una password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostati. Fare attenzione a includere spazi se inclusi nella password.
- Per una maggiore sicurezza, utilizzare almeno 15 caratteri alfanumerici e modificare la password frequentemente.

> La modifica della password in System Manager viene modificata anche nell'interfaccia della riga di comando (CLI). Inoltre, le modifiche apportate alla password causano l'interruzione della sessione attiva dell'utente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.

3. Selezionare un utente dalla tabella.

   Il pulsante Change Password (Modifica password) diventa disponibile.

4. Selezionare **Change Password** (Modifica password).

   Viene visualizzata la finestra di dialogo Change Password (Modifica password).

5. Se non è stata impostata alcuna lunghezza minima per le password utente locali, selezionare la casella per richiedere all'utente selezionato di immettere una password per accedere all'array di storage, quindi digitare la nuova password per l'utente selezionato.
6. Immettere la password dell'amministratore locale, quindi fare clic su **Change** (Modifica).

Risultati

Se l'utente è attualmente connesso, la modifica della password provoca l'interruzione della sessione attiva dell'utente.

Modificare le impostazioni della password utente locale

È possibile impostare la lunghezza minima richiesta per tutte le password utente locali nuove o aggiornate sull'array di storage. È inoltre possibile consentire agli utenti locali di accedere allo storage array senza inserire una password.

Prima di iniziare

Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.

A proposito di questa attività

Tenere presenti queste linee guida quando si imposta la lunghezza minima per le password utente locali:

- Le modifiche apportate non influiscono sulle password utente locali esistenti.
- La lunghezza minima richiesta per le password utente locali deve essere compresa tra 0 e 30 caratteri.
- Le nuove password utente locali devono soddisfare o superare l'impostazione di lunghezza minima corrente.
- Non impostare una lunghezza minima per la password se si desidera che gli utenti locali accedano allo storage array senza immettere una password.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare il pulsante **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Local User Password Settings (Impostazioni password utente locale).

4. Effettuare una delle seguenti operazioni:
   - Per consentire agli utenti locali di accedere allo storage array *senza* inserire una password, deselezionare la casella di controllo "Richiedi almeno tutte le password utente locali".
   - Per impostare una lunghezza minima della password per tutte le password utente locali, selezionare la casella di controllo "Richiedi almeno tutte le password utente locali", quindi utilizzare la casella di selezione per impostare la lunghezza minima richiesta per tutte le password utente locali.

Le nuove password utente locali devono soddisfare o superare l'impostazione corrente.

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

Utilizzare i servizi di directory

Aggiungere un server di directory LDAP

Per configurare l'autenticazione per la gestione degli accessi, è possibile stabilire comunicazioni tra lo storage array e un server LDAP, quindi mappare i gruppi di utenti LDAP ai ruoli predefiniti dell'array.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

A proposito di questa attività

L'aggiunta di un server di directory è un processo in due fasi. Immettere innanzitutto il nome di dominio e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per l'autenticazione se è firmato da un'autorità di firma non standard. Se si dispone delle credenziali per un account BIND, è anche possibile immettere il nome e la password dell'account utente. Quindi, mappare i gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

> Durante la procedura di aggiunta di un server LDAP, l'interfaccia di gestione legacy viene disattivata. L'interfaccia di gestione legacy (Symbol) è un metodo di comunicazione tra lo storage array e il client di gestione. Se disattivato, lo storage array e il client di gestione utilizzano un metodo di comunicazione più sicuro (REST API over https).

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda Directory Services (servizi directory), selezionare **Add Directory Server** (Aggiungi server directory).

   Viene visualizzata la finestra di dialogo Add Directory Server (Aggiungi server di directory).

3. Nella scheda Server Settings (Impostazioni server), immettere le credenziali per il server LDAP.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
Immettere il nome di dominio del server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente@dominio*) per specificare il server di directory da autenticare.	URL del server
Immettere l'URL per l'accesso al server LDAP nel formato `ldap[s]://host:*port*`.	Carica certificato (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato. Fare clic su **Browse** (Sfoglia) e selezionare un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati utilizzata per l'autenticazione del server LDAP.	Account BIND (opzionale)
Inserire un account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi. Immettere il nome dell'account in formato LDAP. Ad esempio, se l'utente bind è chiamato "bindacct", è possibile immettere un valore come "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Password bind (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato quando si immette un account BIND. Immettere la password per l'account BIND.	Verificare la connessione al server prima di aggiungerli
Selezionare questa casella di controllo per assicurarsi che lo storage array possa comunicare con la configurazione del server LDAP immessa. Il test si verifica dopo aver fatto clic su **Add** (Aggiungi) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=cpoc, DC=local`.
Attributo Username	Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i del gruppo	Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

4. Fare clic sulla scheda **mappatura ruolo**.
5. Assegnare i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare:[]{}()<>*+-=!?^	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli dell'array di storage da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestore di sistema di SANtricity. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol). • **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

6. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più

mappature gruppo-ruolo.

7. Al termine delle mappature, fare clic su **Aggiungi**.

   Il sistema esegue una convalida, assicurandosi che lo storage array e il server LDAP possano comunicare. Se viene visualizzato un messaggio di errore, selezionare le credenziali inserite nella finestra di dialogo e, se necessario, immettere nuovamente le informazioni.

Modificare le impostazioni del server di directory e le mappature dei ruoli

Se in precedenza è stato configurato un server di directory in Access Management, è possibile modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e i mapping gruppo-ruolo.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- È necessario definire un server di directory.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Directory Services**.
3. Se sono stati definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Directory Server Settings (Impostazioni server directory).

5. Nella scheda Server Settings (Impostazioni server), modificare le impostazioni desiderate.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
I nomi di dominio dei server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente@dominio*) per specificare il server di directory da autenticare.	URL del server
L'URL per l'accesso al server LDAP nel formato `ldap[s]://host:port`.	Account BIND (opzionale)
L'account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi.	Password bind (opzionale)
La password per l'account BIND. (Questo campo viene visualizzato quando viene inserito un account BIND).	Verificare la connessione al server prima di salvare

Impostazione	Descrizione
Verifica che lo storage array possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su **Save** (Salva) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=cpoc, DC=local`.
Attributo Username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

6. Nella scheda Role Mapping (mappatura ruolo), modificare la mappatura desiderata.

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare:[]{}()<>*+-=!?^	
Ruoli	Ruoli dell'array di storage da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestore di sistema di SANtricity. I ruoli dell'array di storage includono: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol). • **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

7. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
8. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la

sessione utente corrente.

Rimuovere il server di directory

Per interrompere la connessione tra un server di directory e lo storage array, è possibile rimuovere le informazioni sul server dalla pagina Access Management. È possibile eseguire questa attività se è stato configurato un nuovo server e si desidera rimuovere quello precedente.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Directory Services**.
3. Dall'elenco, selezionare il server di directory che si desidera eliminare.
4. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Remove Directory Server (Rimuovi server di directory).

5. Tipo `remove` Nel campo, quindi fare clic su **Rimuovi**.

   Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e i mapping dei ruoli vengono rimossi. Gli utenti non possono più accedere con le credenziali da questo server.

Utilizzare SAML

Configurare SAML

Per configurare l'autenticazione per Access Management, è possibile utilizzare le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un provider di identità e lo storage provider.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o il nome di dominio di ciascun controller dell'array di storage.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito che i clock del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni del clock del controller).

- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a System Manager.

A proposito di questa attività

Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP. Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità. Per stabilire una connessione tra IdP e lo storage array, è necessario condividere i file di metadati tra queste due entità. Quindi, mappare le entità utente IdP ai ruoli degli array di storage. Infine, prima di attivare SAML, è necessario verificare la connessione e gli accessi SSO.

SAML e Directory Services. Se si attiva SAML quando Directory Services è configurato come metodo di autenticazione, SAML sostituisce Directory Services in System Manager. Se si disattiva SAML in un secondo momento, la configurazione dei servizi di directory torna alla configurazione precedente.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

La configurazione dell'autenticazione SAML è una procedura multi-step.

Fase 1: Caricare il file di metadati IdP

Per fornire allo storage array le informazioni di connessione IdP, importare i metadati IdP in System Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute. È necessario caricare un solo file di metadati per l'array di storage, anche se sono presenti due controller.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.

   La pagina visualizza una panoramica delle fasi di configurazione.

3. Fare clic sul collegamento **Import Identity Provider (IdP) file**.

   Viene visualizzata la finestra di dialogo Importa file provider di identità.

4. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file di metadati IdP copiato nel sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'ID entità IdP.

5. Fare clic su **Importa**.

Fase 2: Esportare i file del provider di servizi

Per stabilire una relazione di trust tra IdP e l'array di storage, importare i metadati del service provider nell'IdP. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con i controller e per elaborare le richieste di autorizzazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP, in

modo che l'IdP possa comunicare con i service provider.

Fasi

1. Fare clic sul collegamento **Export Service Provider Files**.

   Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

2. Inserire l'indirizzo IP o il nome DNS del controller nel campo **Controller A**, quindi fare clic su **Export** per salvare il file di metadati nel sistema locale. Se lo storage array include due controller, ripetere questo passaggio per il secondo controller nel campo **Controller B**.

   Dopo aver fatto clic su **Esporta**, i metadati del provider di servizi vengono scaricati nel sistema locale. Prendere nota della posizione in cui è memorizzato il file.

3. Dal sistema locale, individuare i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

4. Dal server IdP, importare i file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare i file direttamente o inserire manualmente le informazioni del controller dai file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a System Manager, è necessario mappare gli attributi utente IdP e le appartenenze ai gruppi ai ruoli predefiniti dell'array di storage.

Prima di iniziare

- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Fare clic sul collegamento **mappatura dei ruoli di System Manager**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

2. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare:[]{}()<>*+-=!?^	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli dell'array di storage da mappare all'attributo. È necessario selezionare singolarmente ciascun ruolo da includere. Il ruolo Monitor è necessario in combinazione con gli altri ruoli per accedere a System Manager. Il ruolo Security Admin è richiesto anche per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol). • **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

3. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.

   I mapping dei ruoli possono essere modificati dopo l'attivazione di SAML.

4. Una volta completate le mappature, fare clic su **Save** (Salva).

Fase 4: Verifica dell'accesso SSO

Per garantire che il sistema IdP e lo storage array possano comunicare, è possibile eseguire un test di accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Selezionare il collegamento **Test SSO Login**.

   Viene visualizzata una finestra di dialogo per l'immissione delle credenziali SSO.

2. Immettere le credenziali di accesso per un utente con permessi di amministratore della sicurezza e di monitoraggio.

   Viene visualizzata una finestra di dialogo durante il test dell'accesso.

3. Cercare il messaggio Test Successful (Test riuscito). Se il test viene completato correttamente, passare alla fase successiva per l'abilitazione di SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

   - L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
   - I metadati caricati per il server IdP sono corretti.
   - Gli indirizzi del controller nei file di metadati SP sono corretti.

Fase 5: Abilitare SAML

Il passaggio finale consiste nel completare la configurazione SAML per l'autenticazione dell'utente. Durante questo processo, il sistema richiede anche di verificare un accesso SSO. Il processo di test di accesso SSO è descritto nel passaggio precedente.

Prima di iniziare

- Il file di metadati IdP viene importato in System Manager.
- Un file di metadati del service provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.
- È stata configurata almeno una mappatura dei ruoli Monitor e Security Admin.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

Fasi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML** (attiva SAML).

   Viene visualizzata la finestra di dialogo Conferma abilitazione SAML.

2. Tipo `enable`, Quindi fare clic su **Enable** (attiva).
3. Immettere le credenziali utente per un test di accesso SSO.

Risultati

Una volta attivato SAML, il sistema termina tutte le sessioni attive e inizia l'autenticazione degli utenti tramite SAML.

Modificare le mappature dei ruoli SAML

Se in precedenza è stato configurato SAML per Access Management, è possibile modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- SAML è configurato e abilitato.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **mappatura ruolo**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

4. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

   Prestare attenzione a non rimuovere le autorizzazioni mentre SAML è attivato, altrimenti si perde l'accesso a System Manager.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

5. Facoltativamente, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
6. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Esportare i file del provider di servizi SAML

Se necessario, è possibile esportare i metadati del service provider per lo storage array e reimportare i file nel sistema IdP (Identity Provider).

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- SAML è configurato e abilitato.

A proposito di questa attività

In questa attività, si esportano i metadati dai controller (un file per ciascun controller). L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con i controller ed elaborare le richieste di autenticazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP che IdP può utilizzare per l'invio delle richieste.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **Esporta**.

   Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

4. Per ciascun controller, fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

   > I campi dei nomi di dominio per ciascun controller sono di sola lettura.

   Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare i file di metadati del provider di servizi esportati.

   Per ciascun controller è disponibile un file in formato XML.

6. Dal server IdP, importare i file di metadati del provider di servizi. È possibile importare i file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

Utilizzare i token di accesso

Creare token di accesso

È possibile creare un token di accesso per l'autenticazione con l'API REST o l'interfaccia della riga di comando (CLI) al posto di un nome utente e di una password.

> I token non dispongono di password, pertanto è necessario gestirle con attenzione.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Access Token**.
3. Selezionare **View/Edit Access Token Settings** (Visualizza/Modifica impostazioni token di accesso). Nella finestra di dialogo, assicurarsi che la casella di controllo **Enable access token** (attiva token di accesso) sia selezionata. Fare clic su **Save** (Salva) per chiudere la finestra di dialogo.
4. Selezionare **Create Access Token** (Crea token di accesso).
5. Nella finestra di dialogo, selezionare la durata della validità del token.

   > Una volta scaduto il token, i tentativi di autenticazione dell'utente non avranno esito positivo.

6. Fare clic su **Crea.**
7. Nella finestra di dialogo, selezionare una delle seguenti opzioni:
   - **Copy** (Copia) per salvare il testo del token negli Appunti.
   - **Download** per salvare il testo del token in un file.

     > Assicurarsi di salvare il testo del token. Questa è l'unica opportunità per visualizzare il testo prima di chiudere la finestra di dialogo.

8. Fare clic su **Chiudi**.
9. Utilizzare il token come segue:
   - **REST API**: Per utilizzare un token in una richiesta API REST, aggiungere un'intestazione HTTP alle richieste. Ad esempio:
     `Authorization: Bearer <access-token-value>`

- **Secure CLI**: Per utilizzare un token nella CLI, aggiungere il valore del token nella riga di comando o utilizzare il percorso di un file contenente il valore del token. Ad esempio:
  - Valore del token sulla riga di comando: `-t access-token-value`
  - Percorso di un file contenente il valore del token: `-T access-token-file`

> Se non vengono specificati nome utente, password o token, l'interfaccia CLI richiede all'utente un valore del token di accesso sulla riga di comando.

Modificare le impostazioni del token di accesso

È possibile modificare le impostazioni per i token di accesso, che includono i tempi di scadenza e la possibilità di creare nuovi token.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Access Token**.
3. Selezionare **View/Edit Access Token Settings** (Visualizza/Modifica impostazioni token di accesso).
4. Nella finestra di dialogo, è possibile eseguire una o entrambe le seguenti operazioni:
   - Attiva o disattiva la creazione del token.
   - Modificare la scadenza dei token esistenti.

> Deselezionando l'impostazione **Enable access token**, si impedisce la creazione del token e l'autenticazione del token. Se successivamente riabiliti questa impostazione, i token non scaduti possono essere riutilizzati. Se si desidera revocare in modo permanente tutti i token esistenti, vedere "Revocare i token di accesso".

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

Revocare i token di accesso

È possibile revocare tutti i token di accesso se si determina che un token è stato compromesso o se si desidera eseguire una rotazione manuale della chiave per le chiavi crittografiche utilizzate per firmare e convalidare i token di accesso.

Questa operazione rigenera le chiavi utilizzate per firmare i token. Una volta ripristinate le chiavi, i token emessi da *all* vengono immediatamente invalidati. Poiché lo storage array non tiene traccia dei token, i singoli token non possono essere revocati.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Access Token**.
3. Selezionare **revoca tutti i token di accesso**.
4. Nella finestra di dialogo, fare clic su **Sì**.

Dopo aver revocato tutti i token, puoi creare nuovi token e utilizzarli immediatamente.

Gestire syslog

Visualizzare l’attività del registro di audit

Visualizzando i registri di controllo, gli utenti con autorizzazioni di amministratore della sicurezza possono monitorare le azioni degli utenti, gli errori di autenticazione, i tentativi di accesso non validi e la durata della sessione utente.

Prima di iniziare

È necessario effettuare l’accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro audit**.

   L’attività del registro di controllo viene visualizzata in formato tabulare, che include le seguenti colonne di informazioni:

   - **Data/ora** — Timestamp di quando lo storage array ha rilevato l’evento (in GMT).
   - **Username** — Nome utente associato all’evento. Per qualsiasi azione non autenticata sull’array di storage, viene visualizzato "N/A" come nome utente. Le azioni non autenticate potrebbero essere attivate dal proxy interno o da qualche altro meccanismo.
   - **Status Code** — Codice di stato HTTP dell’operazione (200, 400, ecc.) e testo descrittivo associato all’evento.
   - **URL a cui si accede** — URL completo (incluso host) e stringa di query.
   - **Client IP Address** — Indirizzo IP del client associato all’evento.
   - **Origine** — origine di registrazione associata all’evento, che può essere System Manager, CLI, Web Services o Support Shell.
   - **Descrizione** — ulteriori informazioni sull’evento, se applicabile.
3. Utilizzare le selezioni nella pagina Registro audit per visualizzare e gestire gli eventi.

Dettagli della selezione

Selezione	Descrizione
Mostra gli eventi del…	Limita gli eventi visualizzati in base all'intervallo di date (ultime 24 ore, ultimi 7 giorni, ultimi 30 giorni o un intervallo di date personalizzato).
Filtro	Limita gli eventi visualizzati dai caratteri immessi nel campo. Utilizzare le virgolette ("") per una corrispondenza esatta della parola, immettere `OR` per restituire una o più parole, oppure inserire un trattino (—) per omettere le parole.
Aggiornare	Selezionare **Refresh** (Aggiorna) per aggiornare la pagina agli eventi più recenti.
Visualizza/Modifica impostazioni	Selezionare **Visualizza/Modifica impostazioni** per aprire una finestra di dialogo che consente di specificare un criterio di log completo e il livello di azioni da registrare.
Eliminare gli eventi	Selezionare **Elimina** per aprire una finestra di dialogo che consente di rimuovere gli eventi precedenti dalla pagina.
Mostra/Nascondi colonne	Fare clic sull'icona della colonna **Mostra/Nascondi** per selezionare colonne aggiuntive da visualizzare nella tabella. Le colonne aggiuntive includono: • **Method** — il metodo HTTP (AD esempio, POST, GET, DELETE, ecc.). • **Comando CLI eseguito** — comando CLI (grammatica) eseguito per richieste CLI sicure. • **CLI Return Status** — un codice di stato CLI o una richiesta di file di input dal client. • **Symbol procedure** — procedura di simbolo eseguita. • **SSH Event Type** — tipo di eventi Secure Shell (SSH), come login, logout e login_fail. • **SSH Session PID** — numero ID del processo della sessione SSH. • **SSH Session Duration(s)** — il numero di secondi in cui l'utente ha effettuato l'accesso. • **Authentication Type** — i tipi possono includere Local user, LDAP, SAML e Access token. • **Authentication ID** — ID della sessione autenticata.
Attiva/disattiva filtri colonna	Fare clic sull'icona **Alterna** per aprire i campi di filtraggio per ciascuna colonna. Immettere i caratteri all'interno di un campo colonna per limitare gli eventi visualizzati da tali caratteri. Fare nuovamente clic sull'icona per chiudere i campi di filtraggio.

Selezione	Descrizione
Annulla le modifiche	Fare clic sull'icona **Annulla** per ripristinare la configurazione predefinita della tabella.
Esportare	Fare clic su **Export** (Esporta) per salvare i dati della tabella in un file CSV (comma Separated Value).

Definire i criteri del registro di controllo

È possibile modificare il criterio di sovrascrittura e i tipi di eventi registrati nel registro di controllo.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni del registro di controllo, che includono il criterio per la sovrascrittura degli eventi precedenti e il criterio per la registrazione dei tipi di evento.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Audit Log Settings (Impostazioni registro di controllo).

4. Modificare il criterio di sovrascrittura o i tipi di eventi registrati.

Dettagli del campo

Impostazione	Descrizione
Sovrascrivere il criterio	Determina il criterio per la sovrascrittura di eventi precedenti quando viene raggiunta la capacità massima: • **Consente di sovrascrivere gli eventi meno recenti nel registro di controllo quando il registro di controllo è pieno** — sovrascrive gli eventi precedenti quando il registro di controllo raggiunge 50,000 record. • **Richiedere l'eliminazione manuale degli eventi del registro di controllo** — specifica che gli eventi non verranno cancellati automaticamente; viene invece visualizzato un avviso di soglia in corrispondenza della percentuale impostata. Gli eventi devono essere cancellati manualmente. Se il criterio di sovrascrittura è disattivato e le voci del registro di controllo raggiungono il limite massimo, l'accesso a System Manager viene negato agli utenti senza autorizzazioni di amministratore della sicurezza. Per ripristinare l'accesso al sistema agli utenti senza autorizzazioni di amministratore della sicurezza, un utente assegnato al ruolo di amministratore della protezione deve eliminare i vecchi record di eventi. I criteri di sovrascrittura non si applicano se un server syslog è configurato per l'archiviazione dei registri di controllo.
Livello di azioni da registrare	Determina i tipi di eventi da registrare: • **Registra solo eventi di modifica** — Mostra solo gli eventi in cui un'azione dell'utente comporta la modifica del sistema. • **Registra tutti gli eventi di modifica e di sola lettura** — Mostra tutti gli eventi, inclusa un'azione dell'utente che comporta la lettura o il download delle informazioni.

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

Eliminare gli eventi dal registro di controllo

È possibile cancellare il registro di controllo degli eventi precedenti, rendendo più gestibile la ricerca tra gli eventi. È possibile salvare gli eventi precedenti in un file CSV (comma-Separated Values) al momento dell'eliminazione.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Audit Log.

4. Selezionare o immettere il numero di eventi meno recenti che si desidera eliminare.
5. Se si desidera esportare gli eventi cancellati in un file CSV (scelta consigliata), mantenere la casella di controllo selezionata. Quando si fa clic su **Delete** (Elimina) nella fase successiva, viene richiesto di inserire un nome e una posizione per il file. In caso contrario, se non si desidera salvare gli eventi in un file CSV, fare clic sulla casella di controllo per deselezionarla.
6. Fare clic su **Delete** (Elimina).

   Viene visualizzata una finestra di dialogo di conferma.

7. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

   Gli eventi meno recenti vengono rimossi dalla pagina Registro di controllo.

Configurare il server syslog per i registri di controllo

Se si desidera archiviare i registri di controllo su un server syslog esterno, è possibile configurare le comunicazioni tra tale server e lo storage array. Una volta stabilita la connessione, i registri di controllo vengono salvati automaticamente nel server syslog.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda Registro di controllo, selezionare **Configura server Syslog**.

   Viene visualizzata la finestra di dialogo Configura server Syslog.

3. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Add Syslog Server (Aggiungi server Syslog).

4. Inserire le informazioni relative al server, quindi fare clic su **Aggiungi**.
   - **Indirizzo server** — immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).

- **Carica certificato (opzionale)** — se è stato selezionato il protocollo TLS e non è stato ancora caricato un certificato CA firmato, fare clic su **Sfoglia** per caricare un file di certificato. I registri di controllo non vengono archiviati in un server syslog senza un certificato attendibile.

> Se il certificato diventa non valido in un secondo momento, l'handshake TLS avrà esito negativo. Di conseguenza, un messaggio di errore viene inviato al registro di controllo e i messaggi non vengono più inviati al server syslog. Per risolvere questo problema, è necessario correggere il certificato sul server syslog e accedere al **Impostazioni › Registro audit › Configura server Syslog › Test tutti**.

- **Port** — inserire il numero di porta del ricevitore syslog. Dopo aver fatto clic su **Add** (Aggiungi), viene visualizzata la finestra di dialogo Configure Syslog Servers (Configura server Syslog) e il server syslog configurato.

5. Per verificare la connessione del server con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti. Per configurare ulteriormente le impostazioni syslog per gli avvisi, vedere "Configurare il server syslog per gli avvisi".

Modificare le impostazioni del server syslog per i record del registro di controllo

È possibile modificare le impostazioni del server syslog utilizzato per l'archiviazione dei registri di controllo e caricare un nuovo certificato CA per il server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se si sta caricando un nuovo certificato CA, il certificato deve essere disponibile nel sistema locale.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda Registro di controllo, selezionare **Configura server Syslog**.

   I server syslog configurati vengono visualizzati nella pagina.

3. Per modificare le informazioni sul server, selezionare l'icona **Edit** (matita) a destra del nome del server, quindi apportare le modifiche desiderate nei seguenti campi:
   - **Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
   - **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
   - **Port** — inserire il numero di porta del ricevitore syslog.
4. Se il protocollo è stato modificato nel protocollo TLS sicuro (da UDP o TCP), fare clic su **Import Trusted Certificate** (Importa certificato attendibile) per caricare un certificato CA.
5. Per verificare la nuova connessione con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.

FAQ

Perché non riesco ad accedere?

Se si riceve un errore durante il tentativo di accesso a System Manager, esaminare queste possibili cause.

Gli errori di accesso a System Manager possono verificarsi per uno dei seguenti motivi:

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Il server di directory (se configurato) potrebbe non essere disponibile. In questo caso, provare ad accedere con un ruolo utente locale.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.
- È stata attivata una condizione di blocco e il registro di controllo potrebbe essere pieno. Accedere a Gestione accessi ed eliminare i vecchi eventi dal registro di controllo.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

Gli errori di accesso a un array di storage remoto per le attività di mirroring possono verificarsi per uno dei seguenti motivi:

- La password immessa non è corretta.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per effettuare nuovamente l'accesso.
- È stato raggiunto il numero massimo di connessioni client utilizzate sul controller. Verificare la presenza di più utenti o client.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, assicurarsi di soddisfare i seguenti requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

Cosa occorre sapere sulla mappatura dei ruoli degli array di storage?

Prima di mappare i gruppi ai ruoli, consultare le seguenti linee guida.

Le funzionalità RBAC (role-based access control) integrate dello storage array includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di

dischi), ma nessun accesso alla configurazione di sicurezza.

- **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol).
- **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Servizi di directory

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e servizi di directory, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Si conoscono i nomi di dominio del gruppo per i gruppi di utenti LDAP. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (`\`) se non fanno parte di un modello di espressione regolare:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

SAML

Se si utilizzano le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Conosci i nomi dei membri del gruppo.
- Si conosce il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (`\`) se non fanno parte di un modello di espressione regolare:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

Quali strumenti di gestione esterni potrebbero essere interessati da questa modifica?

Quando si apportano alcune modifiche in System Manager, ad esempio la commutazione dell'interfaccia di gestione o l'utilizzo di SAML per un metodo di autenticazione, l'utilizzo di alcuni strumenti e funzionalità esterni potrebbe essere limitato.

Interfaccia di gestione

Gli strumenti che comunicano direttamente con l'interfaccia di gestione legacy (Symbol), come il provider SMI-S SANtricity o OnCommand Insight (OCI), non funzionano se non è attivata l'impostazione dell'interfaccia di gestione legacy. Inoltre, non è possibile utilizzare i comandi CLI legacy o eseguire operazioni di mirroring se questa impostazione è disattivata.

Per ulteriori informazioni, contatta il supporto tecnico.

Autenticazione SAML

Quando SAML è attivato, i seguenti client non possono accedere ai servizi e alle risorse dell'array di storage:

- Finestra Enterprise Management (EMW)
- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Per ulteriori informazioni, contatta il supporto tecnico.

Cosa occorre sapere prima di configurare e abilitare SAML?

Prima di configurare e attivare le funzionalità SAML (Security Assertion Markup Language) per l'autenticazione, assicurarsi di soddisfare i seguenti requisiti e comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurarsi che:

- Nella rete è configurato un provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi e i gruppi utente nel sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito che i clock del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e disponibile sul sistema locale utilizzato per accedere a System Manager.
- Si conosce l'indirizzo IP o il nome di dominio di ciascun controller dell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza. Si consiglia di testare gli accessi SSO prima di attivare SAML nella fase finale di

configurazione. (Il sistema esegue anche un test di accesso SSO prima di attivare SAML).

- Se si disattiva SAML in futuro, il sistema ripristina automaticamente la configurazione precedente (ruoli utente locali e/o servizi di directory).
- Se i servizi di directory sono attualmente configurati per l'autenticazione dell'utente, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse degli array di storage:
  - Finestra Enterprise Management (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client Software Developer Kit (SDK)
  - Client in-band
  - Client REST API per l'autenticazione di base HTTP
  - Effettuare l'accesso utilizzando l'endpoint REST API standard

Quali tipi di eventi vengono registrati nel registro di controllo?

Il registro di controllo può registrare gli eventi di modifica o gli eventi di modifica e di sola lettura.

A seconda delle impostazioni del criterio, vengono visualizzati i seguenti tipi di eventi:

- **Eventi di modifica** — azioni dell'utente da System Manager che comportano modifiche al sistema, come il provisioning dello storage.
- **Eventi di modifica e sola lettura** — azioni dell'utente che comportano modifiche al sistema, nonché eventi che comportano la visualizzazione o il download di informazioni, come la visualizzazione delle assegnazioni dei volumi.

Cosa occorre sapere prima di configurare un server syslog?

È possibile archiviare i registri di controllo su un server syslog esterno.

Prima di configurare un server syslog, tenere presenti le seguenti linee guida.

- Assicurarsi di conoscere l'indirizzo del server, il protocollo e il numero della porta. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.
- Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.
- Le impostazioni dei criteri di sovrascrittura (disponibili in **View/Edit Settings**) non influiscono sulla gestione dei registri con una configurazione del server syslog.
- I registri di controllo seguono il formato di messaggistica RFC 5424.

Il server syslog non riceve più registri di controllo. Cosa devo fare?

Se è stato configurato un server syslog con un protocollo TLS, il server non può ricevere messaggi se il certificato non è valido per qualsiasi motivo. Nel registro di controllo viene

visualizzato un messaggio di errore relativo al certificato non valido.

Per risolvere questo problema, è necessario innanzitutto correggere il certificato per il server syslog. Una volta stabilita una catena di certificati valida, accedere al **Impostazioni › Registro audit › Configura server Syslog › Test tutti**.

Certificati

Panoramica dei certificati

È possibile utilizzare System Manager per creare CSR (Certificate Signing Request), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Esistono due tipi di certificati: Un *certificato firmato* viene validato da un'autorità di certificazione (CA) e un *certificato autofirmato* viene validato dal proprietario dell'entità anziché da una terza parte.

Scopri di più:

- "Come funzionano i certificati"
- "Terminologia del certificato"

Come si configurano i certificati firmati?

Si genera prima una richiesta di firma da System Manager, quindi si invia il file a una CA. Una volta che la CA restituisce i file di certificato, è possibile importarli utilizzando System Manager.

Scopri di più:

- "USA certificati firmati CA per i controller"
- "Utilizzare i certificati firmati CA per l'autenticazione con un server di gestione delle chiavi"

Informazioni correlate

Scopri di più sulle attività correlate ai certificati:

- "Visualizzare le informazioni sul certificato importato"
- "Attiva il controllo della revoca del certificato"

Concetti

Come funzionano i certificati

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet.

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con System Manager è possibile gestire i certificati tra il browser di un sistema di gestione host (che funge da client) e i controller di un sistema storage (che funge da

server).

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

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

Certificati firmati

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

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

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

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

Certificati autofirmati

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

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

Certificati utilizzati per il server di gestione delle chiavi

Se si utilizza un server di gestione delle chiavi esterno con la funzione Drive Security, è anche possibile gestire i certificati per l'autenticazione tra il server e i controller.

Terminologia del certificato

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per il rilascio di un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
Catena di certificati	Gerarchia di file che aggiunge un livello di protezione ai certificati. In genere, la catena include un certificato root nella parte superiore della gerarchia, uno o più certificati intermedi e i certificati server che identificano le entità.
Certificato del client	Per la gestione delle chiavi di sicurezza, un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa fidarsi dei propri indirizzi IP.
Certificato intermedio	Uno o più certificati intermedi si diramano dalla directory principale nella catena di certificati. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
Certificato del server di gestione delle chiavi	Per la gestione delle chiavi di sicurezza, un certificato del server di gestione delle chiavi convalida il server, in modo che lo storage array possa fidarsi del proprio indirizzo IP.
Archivio chiavi	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle chiavi pubbliche e ai certificati corrispondenti. Queste chiavi e certificati identificano le proprie entità, ad esempio i controller.
Server OCSP	Il server OCSP (Online Certificate Status Protocol) determina se l'autorità di certificazione (CA) ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un server se il certificato viene revocato.

Termine	Descrizione
Certificato root	Il certificato root si trova nella parte superiore della gerarchia nella catena del certificato e contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
Certificato firmato	Certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include i dettagli relativi al proprietario dell'entità (in genere, un server o un sito Web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di trust e quindi viene utilizzato più spesso negli ambienti di produzione. Definito anche "certificato firmato da CA" o "certificato di gestione".
Certificato autofirmato	Un certificato autofirmato viene validato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA e, di conseguenza, viene spesso utilizzato negli ambienti di test. Detto anche certificato "preinstallato".
Certificato del server	Il certificato del server si trova nella parte inferiore della catena di certificati. Identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di un sistema storage richiede un certificato server separato.

Utilizzare i certificati

USA certificati firmati CA per i controller

È possibile ottenere certificati con firma CA per comunicazioni sicure tra i controller e il browser utilizzato per l'accesso a System Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o i nomi DNS di ciascun controller.

A proposito di questa attività

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

Fase 1: Completare gli CSR per i controller

È necessario innanzitutto generare un file CSR (Certificate Signing Request) per ciascun controller dell'array di storage.

A proposito di questa attività

Questa attività descrive come generare un file CSR da System Manager. La CSR fornisce informazioni sull'organizzazione e sull'indirizzo IP o il nome DNS del controller. Durante questa attività, viene generato un file CSR se l'array di storage ha un controller e due file CSR se ha due controller.

> In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare i file CSR.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Array Management (Gestione array), selezionare **complete CSR** (completa CSR).

   > Se viene visualizzata una finestra di dialogo che richiede di accettare un certificato autofirmato per il secondo controller, fare clic su **Accetta certificato autofirmato** per continuare.

3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città in cui si trova il tuo storage array o il tuo business.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova lo storage array o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.

   > Alcuni campi potrebbero essere precompilati con le informazioni appropriate, ad esempio l'indirizzo IP del controller. Non modificare i valori prepopolati a meno che non si sia certi che siano errati. Ad esempio, se non è stata ancora completata una CSR, l'indirizzo IP del controller viene impostato su "localhost". In questo caso, è necessario modificare "localhost" con il nome DNS o l'indirizzo IP del controller.

4. Verificare o inserire le seguenti informazioni sul controller A nell'array di storage:
   - **Controller A common name** — per impostazione predefinita viene visualizzato l'indirizzo IP o il nome DNS del controller A. Assicurarsi che l'indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere a System Manager nel browser. Il nome DNS non può iniziare con un carattere jolly.
   - **Controller A alternate IP addresses** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il controller A. Per più voci, utilizzare un formato delimitato da virgole.
   - **Controller A alternate DNS Names** — se il nome comune è un nome DNS, inserire eventuali nomi DNS aggiuntivi per il controller A. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Il nome DNS non può iniziare con un carattere jolly. Se lo storage array dispone di un solo controller, il pulsante **Finish** è disponibile.

     Se lo storage array ha due controller, il pulsante **Next** (Avanti) è disponibile.

> Non fare clic sul collegamento **Ignora questo passaggio** quando si crea una richiesta CSR. Questo collegamento viene fornito in situazioni di ripristino degli errori. In rari casi, una richiesta CSR potrebbe non riuscire su un controller, ma non sull'altro. Questo collegamento consente di saltare la fase per la creazione di una richiesta CSR sul controller A, se già definita, e passare alla fase successiva per la creazione di una richiesta CSR sul controller B.

5. Se è presente un solo controller, fare clic su **fine**. Se sono presenti due controller, fare clic su **Avanti** per immettere le informazioni relative al controller B (come sopra), quindi fare clic su **fine**.

   Per un singolo controller, un file CSR viene scaricato nel sistema locale. Per i controller doppi, vengono scaricati due file CSR. La posizione della cartella del download dipende dal browser in uso.

6. Passare a. Fase 2: Inviare i file CSR.

Fase 2: Inviare i file CSR

Dopo aver creato i file CSR (Certificate Signing Request), inviare i file a un'autorità di certificazione (CA). I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: pem, .crt, .cer o .key.

Fasi

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

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

3. Quando la CA restituisce i certificati firmati, passare a. Fase 3: Importazione dei certificati firmati per i controller.

Fase 3: Importazione dei certificati firmati per i controller

Una volta ricevuti i certificati firmati dall'autorità di certificazione (CA), importare i file per i controller.

Prima di iniziare

- La CA ha restituito file di certificato firmati. Questi file includono il certificato root, uno o più certificati intermedi e i certificati del server.
- Se la CA ha fornito un file di certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: Il certificato root, uno o più certificati intermedi e i certificati del server che identificano i controller. È possibile utilizzare Windows `certmgr` Utility per disimballare i file (fare clic con il pulsante destro del mouse e selezionare **All Tasks › Export**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- I file dei certificati sono stati copiati nel sistema host in cui si accede a System Manager.

Fasi

1. Selezionare il **Impostazioni › certificati**
2. Dalla scheda Array Management (Gestione array), selezionare **Import** (Importa).

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

3. Fare clic sui pulsanti **Browse** per selezionare prima i file dei certificati principali e intermedi, quindi selezionare ciascun certificato server per i controller. I file root e intermedi sono gli stessi per entrambi i controller. Solo i certificati server sono univoci per ciascun controller. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

   I file vengono caricati e validati.

Risultato

La sessione viene terminata automaticamente. Per rendere effettive le certificazioni, è necessario effettuare nuovamente l'accesso. Quando si effettua nuovamente l'accesso, vengono utilizzati i nuovi certificati firmati dalla CA per la sessione.

Reimpostare i certificati di gestione

È possibile ripristinare i certificati sui controller dall'utilizzo dei certificati firmati dalla CA ai certificati autofirmati impostati in fabbrica.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati con FIRMA CA devono essere importati in precedenza.

A proposito di questa attività

La funzione Reset elimina i file di certificato firmati dalla CA corrente da ciascun controller. I controller torneranno quindi a utilizzare certificati autofirmati.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Array Management (Gestione array), selezionare **Reset** (Ripristina).

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

3. Tipo `reset` Nel campo, quindi fare clic su **Reset**.

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

Risultati

I controller tornano a utilizzare certificati autofirmati. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Visualizzare le informazioni sul certificato importato

Dalla pagina certificati, è possibile visualizzare il tipo di certificato, l'autorità di emissione e l'intervallo di date valido dei certificati per l'array di storage.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare una delle schede per visualizzare le informazioni relative ai certificati.

Scheda	Descrizione
Gestione degli array	Visualizzare le informazioni sui certificati firmati dalla CA importati per ciascun controller, inclusi il file root, i file intermedi e i file server.
Affidabile	Visualizza le informazioni su tutti gli altri tipi di certificati importati per i controller. Utilizzare il campo del filtro sotto **Mostra certificati…** per visualizzare i certificati installati dall'utente o preinstallati. • **Installato dall'utente** — certificati caricati da un utente nell'array di storage, che possono includere certificati attendibili quando il controller agisce come client (anziché come server), certificati LDAPS e certificati Identity Federation. • **Preinstallati** — certificati autofirmati inclusi con lo storage array.
Gestione delle chiavi	Consente di visualizzare informazioni sui certificati firmati dalla CA importati per un server di gestione delle chiavi esterno.

Importare i certificati per i controller quando agiscono come client

Se il controller rifiuta una connessione perché non è in grado di convalidare la catena di trust per un server di rete, è possibile importare un certificato dalla scheda Trusted che consente al controller (che agisce come client) di accettare le comunicazioni da quel server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I file dei certificati vengono installati nel sistema locale.

A proposito di questa attività

Se si desidera consentire a un altro server di contattare i controller (ad esempio, un server LDAP o un server syslog che utilizza TLS), potrebbe essere necessario importare i certificati dalla scheda Trusted.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Trusted (attendibile), selezionare **Import** (Importa).

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

3. Fare clic su **Browse** (Sfoglia) per selezionare i file di certificato per i controller.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultati

I file vengono caricati e validati.

Attiva il controllo della revoca del certificato

È possibile attivare i controlli automatici dei certificati revocati, in modo che un server OCSP (Online Certificate Status Protocol) blocchi gli utenti da connessioni non sicure.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Su entrambi i controller viene configurato un server DNS, che consente di utilizzare un nome di dominio completo per il server OCSP. Questa attività è disponibile nella pagina hardware.
- Se si desidera specificare il proprio server OCSP, è necessario conoscere l'URL di tale server.

A proposito di questa attività

Il controllo automatico della revoca è utile nei casi in cui la CA ha emesso un certificato in modo errato o una chiave privata è compromessa.

Durante questa attività, è possibile configurare un server OCSP o utilizzare il server specificato nel file del certificato. Il server OCSP determina se la CA ha revocato i certificati prima della data di scadenza pianificata, quindi impedisce all'utente di accedere a un sito se il certificato viene revocato.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   È inoltre possibile attivare il controllo delle revoche dalla scheda **Gestione chiavi**.

3. Fare clic su **attività non comuni**, quindi selezionare **attiva verifica revoca** dal menu a discesa.
4. Selezionare **i want to enable revocation checking**, in modo che nella casella di controllo venga visualizzato un segno di spunta e che nella finestra di dialogo vengano visualizzati altri campi.
5. Nel campo **OCSP responder address** (Indirizzo responder OCSP), è possibile inserire un URL per un server responder OCSP. Se non si immette un indirizzo, il sistema utilizza l'URL del server OCSP dal file del certificato.
6. Fare clic su **Test Address** per verificare che il sistema possa stabilire una connessione all'URL specificato.
7. Fare clic su **Save** (Salva).

Risultati

Se lo storage array tenta di connettersi a un server con un certificato revocato, la connessione viene negata e viene registrato un evento.

Eliminare i certificati attendibili

È possibile eliminare i certificati installati dall'utente precedentemente importati dalla scheda Trusted.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Se si sta aggiornando un certificato attendibile con una nuova versione, il certificato aggiornato deve essere importato prima di eliminare il vecchio certificato.

> Prima di importare un certificato sostitutivo, si potrebbe perdere l'accesso a un sistema se si elimina un certificato utilizzato per autenticare i controller e un altro server, ad esempio un server LDAP.

A proposito di questa attività

Questa attività descrive come eliminare i certificati installati dall'utente. I certificati autofirmati preinstallati non possono essere cancellati.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Trusted**.

   La tabella mostra i certificati attendibili dell'array di storage.

3. Nella tabella, selezionare il certificato che si desidera rimuovere.
4. Fare clic sul **attività non comuni › Elimina**.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

5. Tipo `delete` Nel campo, quindi fare clic su **Delete** (Elimina).

Utilizzare i certificati firmati CA per l'autenticazione con un server di gestione delle chiavi

Per comunicazioni sicure tra un server di gestione delle chiavi e i controller degli array di storage, è necessario configurare i set di certificati appropriati.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

L'autenticazione tra i controller e un server di gestione delle chiavi è una procedura in due fasi.

Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi

È necessario innanzitutto generare un file CSR (Certificate Signing Request), quindi utilizzare la CSR per richiedere un certificato client firmato a un'autorità di certificazione (CA) attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Key Management (Gestione chiavi), selezionare **complete CSR** (completa CSR).
3. Inserire le seguenti informazioni:
   - **Nome comune** — un nome che identifica questa CSR, ad esempio il nome dell'array di storage, che verrà visualizzato nei file di certificato.
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città o la località in cui si trova l'organizzazione.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova l'organizzazione.
   - **Codice ISO Paese** — Codice ISO (International Organization for Standardization) a due cifre, ad esempio USA, in cui si trova l'organizzazione.
4. Fare clic su **Download**.

   Un file CSR viene salvato nel sistema locale.
5. Richiedere un certificato client firmato a una CA attendibile dal server di gestione delle chiavi.
6. Se si dispone di un certificato client, visitare il sito Web all'indirizzo Fase 2: Importazione dei certificati per il server di gestione delle chiavi.

Fase 2: Importazione dei certificati per il server di gestione delle chiavi

Come fase successiva, importare i certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi. Esistono due tipi di certificati: Il certificato client convalida i controller dello storage array, mentre il certificato del server di gestione delle chiavi convalida il server. È necessario caricare sia il file di certificato del client per i controller che il file di certificato del server per il server di gestione delle chiavi.

Prima di iniziare

- Si dispone di un file di certificato client firmato (vedere Fase 1: Completare e inviare la CSR per l'autenticazione con un server di gestione delle chiavi) Ed è stato copiato sull'host in cui si accede a System Manager. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

Per ulteriori informazioni sul certificato del server, consultare la documentazione relativa al server di gestione delle chiavi.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Dalla scheda Key Management (Gestione chiavi), selezionare **Import** (Importa).

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

3. Accanto a **Select client certificate** (Seleziona certificato client), fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato client per i controller dell'array di storage.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Accanto a **Select key management server's server certificate**, fare clic sul pulsante **Browse** (Sfoglia) per selezionare il file di certificato del server per il server di gestione delle chiavi. È possibile scegliere un certificato root, intermedio o server per il server di gestione delle chiavi.

   Il nome del file viene visualizzato nella finestra di dialogo.

5. Fare clic su **Importa**.

   I file vengono caricati e validati.

Esportare i certificati del server di gestione delle chiavi

È possibile salvare un certificato per un server di gestione delle chiavi nel computer locale.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- I certificati devono essere importati in precedenza.

Fasi

1. Selezionare il **Impostazioni › certificati**.
2. Selezionare la scheda **Key Management** (Gestione chiavi).
3. Dalla tabella, selezionare il certificato che si desidera esportare, quindi fare clic su **Esporta**.

   Viene visualizzata la finestra di dialogo Save (Salva).

4. Inserire un nome file e fare clic su **Save** (Salva).

FAQ

Perché viene visualizzata la finestra di dialogo Impossibile accedere ad altri controller?

Quando si eseguono determinate operazioni relative ai certificati CA (ad esempio, l'importazione di un certificato), potrebbe essere visualizzata una finestra di dialogo che

richiede di accettare un certificato autofirmato per il secondo controller.

Negli array di storage con due controller (configurazioni duplex), questa finestra di dialogo viene talvolta visualizzata se Gestione sistema SANtricity non riesce a comunicare con il secondo controller o se il browser non può accettare il certificato durante un determinato momento di un'operazione.

Se viene visualizzata questa finestra di dialogo, fare clic su **Accetta certificato autofirmato** per continuare. Se viene richiesta una password da un'altra finestra di dialogo, immettere la password dell'amministratore utilizzata per accedere a System Manager.

Se questa finestra di dialogo viene visualizzata di nuovo e non è possibile completare un'attività di certificazione, provare una delle seguenti procedure:

- Utilizzare un tipo di browser diverso per accedere a questo controller, accettare il certificato e continuare.
- Accedere al secondo controller con System Manager, accettare il certificato autofirmato, quindi tornare al primo controller e continuare.

Come è possibile sapere quali certificati devono essere caricati in System Manager per la gestione esterna delle chiavi?

Per la gestione esterna delle chiavi, vengono importati due tipi di certificati per l'autenticazione tra lo storage array e il server di gestione delle chiavi in modo che le due entità possano fidarsi l'una dell'altra.

Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste del protocollo KMIP (Key Management Interoperability Protocol). Per ottenere un certificato client, utilizzare System Manager per completare una CSR per lo storage array. È quindi possibile caricare la CSR su un server di gestione delle chiavi e generare un certificato client da tale server. Una volta ottenuto un certificato client, copiare il file sull'host in cui si accede a System Manager.

Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. Recuperare il file di certificato del server dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager.

Cosa devo sapere sulla verifica della revoca dei certificati?

System Manager consente di controllare i certificati revocati utilizzando un server OCSP (Online Certificate Status Protocol), invece di caricare gli elenchi di revoca dei certificati (CRL).

I certificati revocati non devono più essere attendibili. Un certificato potrebbe essere revocato per diversi motivi; ad esempio, se l'autorità di certificazione (CA) ha emesso il certificato in modo errato, una chiave privata è stata compromessa o l'entità identificata non è conforme ai requisiti dei criteri.

Dopo aver stabilito una connessione a un server OCSP in Gestione sistema, lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog. Lo storage array tenta di validare i certificati di questi server per assicurarsi che non siano stati revocati. Il server restituisce quindi il valore "buono", "revocato" o "sconosciuto" per il certificato. Se il certificato viene revocato o l'array non riesce a contattare il server OCSP, la connessione viene rifiutata.

Se si specifica un indirizzo del responder OCSP in System Manager o nell'interfaccia della riga di comando (CLI), l'indirizzo OCSP trovato nel file del certificato viene sovrascritta.

Per quali tipi di server verrà attivato il controllo delle revoche?

Lo storage array esegue il controllo delle revoche ogni volta che si connette a un server AutoSupport, a un server EKMS (External Key Management Server), a un server LDAPS (Lightweight Directory Access Protocol over SSL) o a un server Syslog.

Supporto

Panoramica del supporto

La pagina Support (Assistenza) fornisce l'accesso alle risorse di supporto tecnico.

Quali attività di supporto sono disponibili?

In Assistenza, è possibile visualizzare i contatti del supporto tecnico, eseguire la diagnostica, configurare AutoSupport, visualizzare il registro eventi ed eseguire gli aggiornamenti del software.

Scopri di più:

- "Panoramica delle funzionalità di AutoSupport"
- "Panoramica del registro eventi"
- "Panoramica di Upgrade Center"

Come posso contattare il supporto tecnico?

Dalla pagina principale, fare clic su **Support › Support Center › scheda Support Resources**. Le informazioni di contatto del supporto tecnico sono elencate nella parte superiore destra dell'interfaccia.

Visualizzare informazioni e diagnostiche

Visualizza il profilo dello storage array

Il profilo dello storage array fornisce una descrizione di tutti i componenti e le proprietà dello storage array.

A proposito di questa attività

È possibile utilizzare il profilo dello storage array come ausilio durante il ripristino o come panoramica della configurazione corrente dello storage array. È possibile salvare una copia del profilo dello storage array sul client di gestione e conservare una copia cartacea del profilo dello storage array con lo storage array. Creare una nuova copia del profilo dello storage array se la configurazione cambia.

Fasi

1. Selezionare **scheda Support › Support Center › Support Resources**.
2. Scorrere fino a **Launch Detailed storage array information**, quindi selezionare **Storage Array Profile**.

   Il report viene visualizzato sullo schermo.

Dettagli del campo

Sezione	Descrizione
Array di storage	Mostra tutte le opzioni che è possibile configurare e le opzioni statiche di sistema per lo storage array. Queste opzioni includono il numero di controller, shelf di dischi, dischi, pool di dischi, gruppi di volumi, Volumi e dischi hot spare; il numero massimo di shelf di dischi, dischi a stato solido (SSD) e volumi consentiti; il numero di gruppi di snapshot, immagini snapshot, volumi di snapshot e gruppi di coerenza; informazioni sulle funzionalità; informazioni sulle versioni del firmware; informazioni sul numero di serie dello chassis; informazioni sullo stato AutoSupport e sulla pianificazione AutoSupport; Le impostazioni per la raccolta automatica dei dati di supporto e la raccolta pianificata dei dati di supporto, l'ID WWID (World-Wide Identifier) dell'array di storage e le impostazioni di cache e scansione dei supporti.
Storage	Mostra un elenco di tutti i dispositivi di storage nell'array di storage. A seconda della configurazione dell'array di storage, la sezione Storage (archiviazione) potrebbe visualizzare queste sottosezioni. • **Disk Pools** — Mostra un elenco di tutti i pool di dischi nell'array di storage. • **Volume Groups** — Mostra un elenco di tutti i gruppi di volumi nell'array di storage. I volumi e la capacità libera sono elencati nell'ordine in cui sono stati creati. • **Volumes** — Mostra un elenco di tutti i volumi nell'array di storage. Le informazioni elencate includono il nome del volume, lo stato del volume, la capacità, il livello RAID, il gruppo di volumi o il pool di dischi, il tipo di disco e ulteriori dettagli. • **Volumi mancanti** — Mostra un elenco di tutti i volumi nell'array di storage che attualmente hanno uno stato mancante. Le informazioni elencate includono il WWID (World Wide Identifier) per ciascun volume mancante.

Sezione	Descrizione
Servizi di copia	Mostra un elenco di tutti i servizi di copia utilizzati per l'array di storage. A seconda della configurazione dello storage array, la sezione Copy Services (servizi di copia) potrebbe visualizzare le seguenti sottosezioni: • **Volume Copies** — Mostra un elenco di tutte le coppie di copie nell'array di storage. Le informazioni elencate includono il numero di copie, i nomi delle coppie di copie, lo stato, l'indicatore data e ora di inizio e ulteriori dettagli. • **Snapshot Groups** — Mostra un elenco di tutti i gruppi di snapshot nell'array di storage. • **Snapshot Images** — Mostra un elenco di tutti gli snapshot nell'array di storage. • **Snapshot Volumes** — Mostra un elenco di tutti i volumi di snapshot nell'array di storage. • **Consistency Groups** — Mostra un elenco di tutti i gruppi di coerenza nell'array di storage. • **Member Volumes** — Mostra un elenco di tutti i volumi membri del gruppo di coerenza nell'array di storage. • **Mirror Groups** — Mostra un elenco di tutti i volumi mirrorati. • **Reserved Capacity** — Mostra un elenco di tutti i volumi di capacità riservati nell'array di storage.
Assegnazioni host	Mostra un elenco delle assegnazioni degli host nell'array di storage. Le informazioni elencate includono il nome del volume, il numero di unità logica (LUN), l'ID del controller, il nome host o il nome del cluster host e lo stato del volume. Le informazioni aggiuntive elencate includono le definizioni della topologia e dei tipi di host.

Sezione	Descrizione
Hardware	Mostra un elenco di tutto l'hardware dell'array di storage. A seconda della configurazione dello storage array, la sezione hardware potrebbe visualizzare queste sottosezioni. • **Controller** — Mostra un elenco di tutti i controller nell'array di storage e include la posizione, lo stato e la configurazione del controller. Inoltre, include informazioni sul canale del disco, informazioni sul canale host e informazioni sulla porta Ethernet. • **Drives** — Mostra un elenco di tutti i dischi dell'array di storage. I dischi sono elencati in ordine di ID shelf, ID cassetto e ID slot. Le informazioni elencate includono l'ID dello shelf, l'ID del cassetto, l'ID dello slot, lo stato, la capacità raw, Il tipo di supporto, il tipo di interfaccia, la velocità di trasferimento dati corrente, l'ID del prodotto e la versione del firmware per ciascun disco. La sezione Drive include anche informazioni sul canale dei dischi, informazioni sulla copertura hot spare e informazioni sulla durata dell'utilizzo (solo per i dischi SSD). Le informazioni sulla durata includono la durata percentuale utilizzata, ovvero la quantità di dati scritti finora sui dischi SSD, divisa per il limite teorico di scrittura totale per i dischi. • **Drive Channels** — Mostra le informazioni per tutti i canali del disco nello storage array. Le informazioni elencate includono lo stato del canale, lo stato del collegamento (se applicabile), il numero di dischi e il numero di errori cumulativi. • **Shelves** — Mostra le informazioni per tutti gli shelf dell'array di storage. Le informazioni elencate includono i tipi di unità e le informazioni di stato per ciascun componente dello shelf. I componenti dello shelf possono includere batterie, ricetrasmettitori SFP (Small Form-Factor Pluggable), contenitori per ventole di alimentazione o contenitori per moduli di input/output (IOM). La sezione hardware mostra anche l'identificatore della chiave di sicurezza se viene utilizzata una chiave di sicurezza dall'array di storage.
Caratteristiche	Mostra un elenco dei Feature Pack installati e il numero massimo consentito di gruppi di snapshot, snapshot (legacy) e volumi per host o cluster host. Le informazioni contenute nella sezione caratteristiche includono anche Drive Security, vale a dire se lo storage array è abilitato alla sicurezza o disattivato.

3. Per cercare il profilo dello storage array, digitare un termine di ricerca nella casella di testo **Find**, quindi fare clic su **Find**.

   Vengono evidenziati tutti i termini corrispondenti. Per scorrere tutti i risultati uno alla volta, continuare a fare clic su **Find** (trova).

4. Per salvare il profilo dello storage array, fare clic su **Save** (Salva).

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

Visualizza l'inventario di software e firmware

L'inventario di software e firmware elenca le versioni del firmware per ciascun componente dell'array di storage.

A proposito di questa attività

Uno storage array è costituito da molti componenti, che possono includere controller, dischi, cassetti e moduli di input/output (IOM). Ciascuno di questi componenti contiene firmware. Alcune versioni del firmware dipendono da altre versioni del firmware. Per acquisire informazioni su tutte le versioni del firmware dell'array di storage, visualizzare l'inventario di software e firmware. Il supporto tecnico può analizzare l'inventario del software e del firmware per rilevare eventuali errori di corrispondenza del firmware.

Fasi

1. Selezionare **scheda Support › Support Center › Support Resources**.
2. Scorrere fino a **Launch Detailed storage array information**, quindi selezionare **Software and firmware Inventory**.

   Sullo schermo viene visualizzato il report Software and firmware Inventory (inventario software e firmware).

3. Per salvare l'inventario di software e firmware, fare clic su **Save** (Salva).

   Il file viene salvato nella cartella Download del browser con il nome file `firmware-inventory.txt`.

4. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Raccogliere i dati diagnostici

Raccogliere i dati di supporto manualmente

È possibile raccogliere diversi tipi di dati di inventario, stato e performance relativi all'array di storage in un singolo file. Il supporto tecnico può utilizzare il file per la risoluzione dei problemi e ulteriori analisi.

A proposito di questa attività

> Se la funzione AutoSupport è attivata, è anche possibile raccogliere questi dati accedendo alla scheda **AutoSupport** e selezionando **Send AutoSupport spedizione**.

È possibile eseguire una sola operazione di raccolta alla volta. Se si tenta di avviare un'altra operazione, viene visualizzato un messaggio di errore.

> Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Collect Support Data**.
3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome `support-data.7z`. Se lo shelf

contiene cassetti, i dati diagnostici per lo shelf vengono archiviati in un file separato con zip denominato `tray-component-state-capture.7z`.

4. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Raccogliere i dati di configurazione

È possibile salvare i dati di configurazione RAID dal controller, che include tutti i dati per gruppi di volumi e pool di dischi. A questo punto, è possibile contattare il supporto tecnico per ottenere assistenza per il ripristino dei dati.

A proposito di questa attività

Questa attività descrive come salvare lo stato corrente del database di configurazione RAID. Questi dati vengono recuperati dalla posizione di memoria RPA del controller.

> La funzione Collect Configuration Data salva le stesse informazioni del comando CLI per `save storageArray dbmDatabase`.

Questa attività deve essere eseguita solo se richiesto da un'operazione Recovery Guru o dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
3. Nella finestra di dialogo, fare clic su **Collect** (Raccogli).

   Il file, `configurationData-<arrayName>-<dateTime>.7z`, Viene salvato nella cartella Download del browser.

4. Per ulteriori informazioni sull'invio del file e sul caricamento dei dati nel sistema, contattare il supporto tecnico.

Recuperare i file di supporto per il ripristino

Il supporto tecnico può utilizzare i file di supporto per il ripristino per risolvere i problemi. System Manager salva automaticamente questi file.

Prima di iniziare

Il supporto tecnico ha richiesto l'invio di file aggiuntivi per la risoluzione dei problemi.

A proposito di questa attività

I file di supporto per il ripristino includono i seguenti tipi di file:

- Supporto dei file di dati
- Storia di AutoSupport
- Log di AutoSupport
- File di diagnostica SAS/RLS
- Dati del profilo di recovery
- File di acquisizione del database

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Recupera file di supporto ripristino**.

   Una finestra di dialogo elenca tutti i file di supporto per il ripristino raccolti dall'array di storage. Per trovare file specifici, è possibile ordinare qualsiasi colonna o digitare caratteri nella casella **Filter**.

3. Selezionare un file, quindi fare clic su **Download**.

   Il file viene salvato nella cartella Download del browser.

4. Se si desidera salvare altri file, ripetere il passaggio precedente.
5. Fare clic su **Chiudi**.
6. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Recuperare i buffer di traccia

È possibile recuperare i buffer di traccia dai controller e inviare il file al supporto tecnico per l'analisi.

A proposito di questa attività

Il firmware utilizza i buffer di traccia per registrare l'elaborazione, in particolare le condizioni di eccezione, che potrebbero essere utili per il debug. È possibile recuperare i buffer di traccia senza interrompere il funzionamento dello storage array e con un effetto minimo sulle performance.

> Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Recupera buffer traccia**.
3. Selezionare la casella di controllo accanto a ciascun controller per il quale si desidera recuperare i buffer di traccia.

   È possibile selezionare uno o entrambi i controller. Se il messaggio di stato del controller a destra di una casella di controllo è Failed (guasto) o Disabled (Disattivato), la casella di controllo è disattivata.

4. Fare clic su **Sì**.

   Il file viene salvato nella cartella Download del browser con il nome file `trace-buffers.7z`.

5. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Raccogliere le statistiche del percorso di i/O.

È possibile salvare il file delle statistiche del percorso i/o e inviarlo al supporto tecnico per l'analisi.

A proposito di questa attività

Il supporto tecnico utilizza le statistiche del percorso i/o per diagnosticare i problemi di performance. I problemi di performance delle applicazioni possono essere causati dall'utilizzo della memoria, dall'utilizzo della CPU,

dalla latenza di rete, dalla latenza di i/o o o da altri problemi. Le statistiche del percorso i/o vengono raccolte automaticamente durante la raccolta dei dati di supporto oppure è possibile raccoglierle manualmente. Inoltre, se AutoSupport è attivato, le statistiche del percorso i/o vengono raccolte automaticamente e inviate al supporto tecnico.

I contatori delle statistiche del percorso i/o vengono ripristinati dopo aver confermato che si desidera raccogliere le statistiche del percorso i/O. I contatori vengono azzerati anche se successivamente si annulla l'operazione. I contatori vengono ripristinati anche quando il controller viene reimpostato (riavviato).

Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Collect i/o Path Statistics** (raccolta statistiche percorso i/o).
3. Confermare che si desidera eseguire l'operazione digitando `collect`, Quindi fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome file `io-path-statistics.7z`.

4. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Recuperare l'immagine di integrità

È possibile rivedere un'immagine dello stato di salute del controller. Un'immagine di integrità è un dump di dati raw della memoria del processore del controller che il supporto tecnico può utilizzare per diagnosticare un problema con un controller.

A proposito di questa attività

Il firmware genera automaticamente un'immagine dello stato di salute quando rileva determinati errori. Una volta generata un'immagine di integrità, il controller che ha generato l'errore si riavvia e un evento viene registrato nel registro eventi.

Se AutoSupport è attivato, l'immagine dello stato di salute viene inviata automaticamente al supporto tecnico. Se AutoSupport non è attivato, è necessario contattare il supporto tecnico per istruzioni su come recuperare l'immagine sanitaria e inviarla per l'analisi.

Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Recupera immagine salute**.

   Prima di scaricare il file, consultare la sezione dei dettagli per visualizzare le dimensioni dell'immagine sanitaria.

3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome `health-image.7z`.

4. Seguire le istruzioni fornite dal supporto tecnico per inviare il file.

Intraprendere azioni di recovery

Visualizza log dei settori illeggibili

È possibile salvare il registro dei settori illeggibili e inviare il file al supporto tecnico per l'analisi.

A proposito di questa attività

Il log dei settori illeggibili contiene record dettagliati di settori illeggibili causati da dischi che segnalano errori irrecuperabili dei supporti. I settori illeggibili vengono rilevati durante le normali operazioni di i/o e durante le operazioni di modifica, come le ricostruzioni. Quando vengono rilevati settori illeggibili su un array di storage, viene visualizzato un avviso di attenzione per l'array di storage. Il Recovery Guru distingue quale condizione di settore illeggibile richiede attenzione. I dati contenuti in un settore illeggibile non possono essere recuperati e devono essere considerati perduti.

Il registro dei settori illeggibili può memorizzare fino a 1,000 settori illeggibili. Quando il registro dei settori illeggibili raggiunge 1,000 voci, si applicano le seguenti condizioni:

- Se vengono rilevati nuovi settori illeggibili durante la ricostruzione, la ricostruzione non riesce e non viene registrata alcuna voce.
- Per i nuovi settori illeggibili rilevati durante l'i/o, l'i/o non funziona e non viene registrata alcuna voce.

> Queste azioni includono le scritture RAID 5 e RAID 6 che avrebbero avuto successo prima dell'overflow.

> **Possibile perdita di dati** — il ripristino da settori illeggibili è una procedura complicata che può coinvolgere diversi metodi. Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Visualizza/Cancella settori illeggibili**.
3. Per salvare il log dei settori illeggibili:

   a. Nella prima colonna della tabella, è possibile selezionare singoli volumi per i quali si desidera salvare il registro dei settori illeggibili (fare clic sulla casella di controllo accanto a ciascun volume) oppure selezionare tutti i volumi (selezionare la casella di controllo nell'intestazione della tabella).

      Per trovare volumi particolari, è possibile ordinare qualsiasi colonna o digitare caratteri nella casella **Filter**.

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

   Il file viene salvato nella cartella Download del browser con il nome `unreadable-sectors.txt`.

4. Se il supporto tecnico richiede di cancellare il registro dei settori illeggibili, attenersi alla seguente procedura:

   a. Nella prima colonna della tabella, è possibile selezionare singoli volumi per i quali si desidera cancellare il registro dei settori illeggibili (fare clic sulla casella di controllo accanto a ciascun volume) oppure selezionare tutti i volumi (selezionare la casella di controllo nell'intestazione della tabella).

   b. Fare clic su **Clear** e confermare che si desidera eseguire l'operazione.

Riattivare le porte delle unità

È possibile indicare al controller che è stata intrapresa un'azione correttiva per il ripristino da una condizione di errato cablaggio.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.
2. Selezionare **Riabilitare Drive Ports** e confermare che si desidera eseguire l'operazione.

   Questa opzione viene visualizzata solo quando le porte dei dischi sono disattivate per lo storage array.

   Il controller riattiva le porte SAS disabilitate quando viene rilevato un errore di cablaggio.

Cancellare la modalità di recovery

Dopo aver ripristinato la configurazione di un array di storage, utilizzare l'operazione Clear Recovery Mode per ripristinare l'i/o sullo storage array e ripristinare le normali operazioni.

Prima di iniziare

- Se si desidera ripristinare una configurazione precedente dello storage array, è necessario ripristinare la configurazione dal backup prima di cancellare la modalità di ripristino.
- Per assicurarsi che il ripristino sia stato eseguito correttamente, è necessario eseguire controlli di convalida o rivolgersi al supporto tecnico. Una volta stabilito che il ripristino è stato eseguito correttamente, è possibile cancellare la modalità di ripristino.

A proposito di questa attività

L'array di storage contiene un database di configurazione che include un record della relativa configurazione logica (pool, gruppi di volumi, volumi e così via). Se si cancella intenzionalmente la configurazione dello storage array o se il database di configurazione viene danneggiato, lo storage array entra in modalità di recovery. La modalità Recovery (Recovery) interrompe l'i/o e blocca il database di configurazione, consentendo di eseguire una delle seguenti operazioni:

- Ripristinare la configurazione dal backup automatico memorizzato nei dispositivi flash del controller. A tale scopo, è necessario contattare il supporto tecnico.
- Ripristinare la configurazione da un'operazione precedente di salvataggio del database di configurazione. Le operazioni di salvataggio del database di configurazione vengono eseguite tramite l'interfaccia a riga di comando (CLI).
- Riconfigurare lo storage array da zero.

Dopo aver ripristinato o ridefinito la configurazione dello storage array e aver verificato che tutto sia in buone buone modi, è necessario cancellare manualmente la modalità di recovery.

> Non è possibile annullare l'operazione Clear Recovery Mode dopo l'avvio. La cancellazione della modalità di ripristino può richiedere molto tempo. Eseguire questa operazione solo se richiesto dal supporto tecnico.

Fasi

1. Selezionare **scheda Support › Support Center › Diagnostics**.

2. Selezionare **Clear Recovery Mode** (Cancella modalità di ripristino) e confermare che si desidera eseguire questa operazione.

   Questa opzione viene visualizzata solo se lo storage array è in modalità di ripristino.

Gestire AutoSupport

Panoramica delle funzionalità di AutoSupport

La funzione AutoSupport monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.

Il supporto tecnico utilizza i dati AutoSupport in modo proattivo per accelerare la diagnosi e la risoluzione dei problemi dei clienti e per rilevare ed evitare potenziali problemi.

I dati AutoSupport includono informazioni sulla configurazione, lo stato, le performance e gli eventi di sistema di uno storage array. I dati AutoSupport non contengono dati utente. Le spedizioni possono essere inviate immediatamente o in base a una pianificazione (giornaliera e settimanale).

Vantaggi principali

Alcuni dei vantaggi principali della funzione AutoSupport includono:

- Tempi di risoluzione dei casi più rapidi
- Monitoraggio sofisticato per una gestione più rapida degli incidenti
- Creazione automatica di report in base a una pianificazione e generazione automatica di report sugli eventi critici
- Richieste automatizzate di sostituzione dell'hardware per componenti selezionati, ad esempio dischi
- Avvisi non intrusivi per notificare un problema e fornire informazioni al supporto tecnico per intraprendere azioni correttive
- Strumenti di analisi AutoSupport che monitorano le spedizioni per problemi di configurazione noti

Funzionalità di Individual AutoSupport

La funzione AutoSupport è composta da tre funzioni individuali che vengono attivate separatamente.

- **Basic AutoSupport** — consente allo storage array di raccogliere e inviare automaticamente i dati al supporto tecnico.
- **AutoSupport OnDemand** — consente al supporto tecnico di richiedere la ritrasmissione di un precedente dispatch AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
- **Diagnostica remota** — consente al supporto tecnico di richiedere una nuova spedizione AutoSupport aggiornata quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti nuove richieste in sospeso e risponde di conseguenza.

Differenza tra AutoSupport e Collect dati di supporto

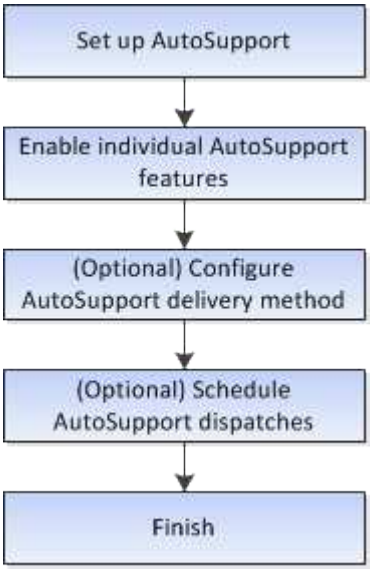
Nello storage array esistono due metodi per raccogliere i dati di supporto:

- **Funzione AutoSupport** — i dati vengono raccolti automaticamente.
- **Opzione Collect Support Data** — i dati devono essere raccolti e inviati manualmente.

La funzione AutoSupport è più semplice da utilizzare perché i dati vengono raccolti e inviati automaticamente. I dati AutoSupport possono essere utilizzati in modo proattivo per prevenire i problemi prima che si verifichino. La funzione AutoSupport accelera la risoluzione dei problemi perché il supporto tecnico ha già accesso ai dati. Per questi motivi, la funzionalità AutoSupport è il metodo di raccolta dati preferito da utilizzare.

Flusso di lavoro per la funzione AutoSupport

In Gestore di sistema, configurare la funzione AutoSupport seguendo questa procedura.



Attivare o disattivare le funzioni AutoSupport

È possibile attivare la funzione AutoSupport e le singole funzioni AutoSupport durante la configurazione iniziale oppure attivarle o disattivarle in un secondo momento.

Prima di iniziare

Se si desidera attivare AutoSupport OnDemand o Diagnostica remota, il metodo di erogazione AutoSupport deve essere impostato su HTTPS.

A proposito di questa attività

È possibile disattivare la funzione AutoSupport in qualsiasi momento, ma si consiglia di lasciarla attivata. L'attivazione della funzione AutoSupport può accelerare significativamente la determinazione e la risoluzione dei problemi in caso di problemi sullo storage array.

La funzione AutoSupport è composta da tre funzioni individuali che vengono attivate separatamente.

- **Basic AutoSupport** — consente allo storage array di raccogliere e inviare automaticamente i dati al supporto tecnico.
- **AutoSupport OnDemand** — consente al supporto tecnico di richiedere la ritrasmissione di un precedente dispatch AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono

avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.

- **Diagnostica remota** — consente al supporto tecnico di richiedere una nuova spedizione AutoSupport aggiornata quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti nuove richieste in sospeso e risponde di conseguenza.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **attiva/Disattiva funzionalità AutoSupport**.
3. Selezionare le caselle di controllo accanto alle funzioni AutoSupport che si desidera attivare.

   Le funzioni dipendono l'una dall'altra, come indicato dal rientro degli elementi nella finestra di dialogo. Ad esempio, è necessario attivare AutoSupport OnDemand prima di poter attivare la diagnostica remota.

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

   Se si disattiva AutoSupport, viene visualizzata una notifica nella pagina iniziale. Per chiudere la notifica, fare clic su **Ignora**.

Configurare il metodo di erogazione AutoSupport

La funzione AutoSupport supporta i protocolli HTTPS, HTTP e SMTP per l'invio delle spedizioni al supporto tecnico.

Prima di iniziare

- La funzione AutoSupport deve essere attivata. Puoi vedere se è attivato nella pagina AutoSupport.
- Nella rete deve essere installato e configurato un server DNS. L'indirizzo del server DNS deve essere configurato in System Manager (questa attività è disponibile nella pagina hardware).

A proposito di questa attività

Esaminare i diversi protocolli:

- **HTTPS** — consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTPS. Se si desidera attivare AutoSupport OnDemand o Diagnostica remota, il metodo di erogazione AutoSupport deve essere impostato su HTTPS.
- **HTTP** — consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTP.
- **E-mail** — consente di utilizzare un server e-mail come metodo di recapito per l'invio di messaggi AutoSupport.

> **Differenze tra i metodi HTTPS/HTTP ed e-mail**. Il metodo di recapito della posta elettronica, che utilizza SMTP, presenta alcune importanti differenze rispetto ai metodi di recapito HTTPS e HTTP. Innanzitutto, le dimensioni delle spedizioni per il metodo e-mail sono limitate a 5 MB, il che significa che alcune raccolte di dati ASUP non verranno inviate. In secondo luogo, la funzione AutoSupport OnDemand è disponibile solo sui metodi HTPP e HTTPS.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Configura metodo di erogazione AutoSupport**.

   Viene visualizzata una finestra di dialogo in cui sono elencati i metodi di consegna dell'invio.

3. Selezionare il metodo di erogazione desiderato, quindi selezionare i parametri per il metodo di erogazione. Effettuare una delle seguenti operazioni:
   - Se si seleziona HTTPS o HTTP, selezionare uno dei seguenti parametri di erogazione:
     - **Direttamente** — questo parametro di erogazione è la selezione predefinita. Questa opzione consente di connettersi direttamente al sistema di supporto tecnico di destinazione utilizzando il protocollo HTTPS o HTTP.
     - **Via Proxy server** — questa opzione consente di specificare i dettagli del server proxy HTTP necessari per stabilire la connessione con il sistema di supporto tecnico di destinazione. Specificare l'indirizzo host e il numero di porta. Tuttavia, è necessario immettere solo i dettagli di autenticazione dell'host (nome utente e password), se necessario.
     - **Tramite PAC (Proxy Auto-Configuration script)** — specificare la posizione di un file PAC (Proxy Auto-Configuration) script. Un file PAC consente al sistema di scegliere automaticamente il server proxy appropriato per stabilire una connessione con il sistema di supporto tecnico di destinazione.
   - Se è stata selezionata l'opzione e-mail, immettere le seguenti informazioni:
     - Indirizzo del server di posta come nome di dominio completo, indirizzo IPv4 o indirizzo IPv6.
     - L'indirizzo e-mail visualizzato nel campo da del messaggio e-mail di spedizione AutoSupport.
     - **Opzionale; se si desidera eseguire un test di configurazione**: L'indirizzo e-mail a cui viene inviata una conferma quando il sistema AutoSupport riceve l'invio del test.
     - Se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. In caso contrario, selezionare **Nessuno**.
     - Se necessario, immettere un nome utente e una password per l'autenticazione con il mittente e il server di posta in uscita.
4. Se si dispone di un firewall che blocca l'erogazione di questi dispatches ASUP, aggiungere il seguente URL alla whitelist: `https://support.netapp.com/put/AsupPut/`
5. Fare clic su **Test Configuration** (verifica configurazione) per verificare la connessione al server del supporto tecnico utilizzando i parametri di consegna specificati. Se è stata attivata la funzione AutoSupport on-Demand, il sistema verificherà anche la connessione per l'erogazione del dispatch AutoSupport on-Demand.

   Se il test di configurazione non riesce, controllare le impostazioni di configurazione ed eseguire nuovamente il test. Se il test continua a non riuscire, contattare il supporto tecnico.

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

Pianifica le spedizioni AutoSupport

System Manager crea automaticamente una pianificazione predefinita per le spedizioni AutoSupport. Se preferisci, puoi specificare la tua pianificazione.

Prima di iniziare

La funzione AutoSupport deve essere attivata. Puoi vedere se è attivato nella pagina AutoSupport.

A proposito di questa attività

- **Daily Time** — le spedizioni giornaliere vengono raccolte e inviate ogni giorno durante l'intervallo di tempo specificato. System Manager seleziona un tempo casuale durante l'intervallo. Tutti gli orari sono in UTC (Coordinated Universal Time), che potrebbe essere diverso dall'ora locale dello storage array. È necessario convertire l'ora locale dell'array di storage in UTC.
- **Giorno settimanale** — le spedizioni settimanali vengono raccolte e inviate una volta alla settimana. System Manager seleziona un giorno casuale tra i giorni specificati. Deselezionare tutti i giorni in cui non si desidera consentire l'invio settimanale. System Manager seleziona un giorno casuale tra i giorni consentiti.
- **Weekly Time** — le spedizioni settimanali vengono raccolte e inviate una volta alla settimana durante l'intervallo di tempo specificato. System Manager seleziona un tempo casuale durante l'intervallo. Tutti gli orari sono in UTC (Coordinated Universal Time), che potrebbe essere diverso dall'ora locale dello storage array. È necessario convertire l'ora locale dell'array di storage in UTC.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Schedule AutoSupport Dispatches**.

   Viene visualizzata la procedura guidata Schedule AutoSupport Dispatches.

3. Seguire i passaggi della procedura guidata.

Inviare le spedizioni AutoSupport

System Manager consente di inviare le spedizioni AutoSupport al supporto tecnico, senza attendere un invio pianificato.

Prima di iniziare

La funzione AutoSupport deve essere attivata. Puoi vedere se è attivato nella pagina AutoSupport.

A proposito di questa attività

Questa operazione raccoglie i dati di supporto e li invia automaticamente al supporto tecnico, in modo che possano risolvere i problemi.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Invia AutoSupport spedizione**.

   Viene visualizzata la finestra di dialogo Invia AutoSupport di spedizione.

3. Confermare l'operazione selezionando **Invia**.

Visualizzare lo stato di AutoSupport

La pagina AutoSupport mostra se la funzione AutoSupport e le singole funzioni AutoSupport sono attualmente attivate.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Osservare il lato destro della pagina sotto le schede per verificare se la funzione AutoSupport di base è attivata.

3. Posizionare il cursore del mouse sul punto interrogativo per verificare se le singole funzioni AutoSupport sono attivate.

Visualizza il registro AutoSupport

Il registro AutoSupport fornisce informazioni sullo stato, la cronologia delle spedizioni e gli errori riscontrati durante la consegna delle spedizioni AutoSupport.

A proposito di questa attività

Possono esistere più file di log. Quando il file di log corrente raggiunge i 200 KB, viene archiviato e creato un nuovo file di log. Il nome del file di log archiviato è `ASUPMessages.n`, dove *n* è un numero intero compreso tra 1 e 9. Se esistono più file di log, è possibile scegliere di visualizzare il log più recente o un log precedente.

- **Current log** — Mostra un elenco degli ultimi eventi acquisiti.
- **Archived log** — Mostra un elenco di eventi precedenti.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Visualizza log AutoSupport**.

   Viene visualizzata una finestra di dialogo che elenca il registro AutoSupport corrente.

3. Se si desidera visualizzare i registri AutoSupport precedenti, selezionare il pulsante di opzione **Archived**, quindi selezionare un registro dall'elenco a discesa **Select AutoSupport log**.

   L'opzione Archived (Archiviato) viene visualizzata solo se i registri archiviati sono presenti nell'array di storage.

   Il log AutoSupport selezionato viene visualizzato nella finestra di dialogo.

4. **Opzionale:** per cercare nel registro AutoSupport, digitare un termine nella casella **trova** e fare clic su **trova**.

   Fare nuovamente clic su **Find** (trova) per cercare altre occorrenze del termine.

Attiva la finestra di manutenzione AutoSupport

Attivare la finestra di manutenzione di AutoSupport per eliminare la creazione automatica di ticket in caso di eventi di errore. In modalità operativa normale, lo storage array utilizza AutoSupport per aprire un caso con il supporto in caso di problemi.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **attiva finestra manutenzione AutoSupport**.
3. Inserire l'indirizzo e-mail per ricevere una conferma dell'elaborazione della richiesta della finestra di manutenzione.

   A seconda della configurazione, è possibile immettere fino a cinque indirizzi e-mail. Se si desidera aggiungere più indirizzi, selezionare **Aggiungi un'altra e-mail** per aprire un altro campo.

4. Specificare la durata (in ore) per attivare la finestra di manutenzione.

   La durata massima supportata è di 72 ore.

5. Fare clic su **Sì**.

   La creazione automatica del ticket AutoSupport in caso di eventi di errore viene temporaneamente soppressa per la finestra di durata specificata.

Al termine

La finestra di manutenzione non inizia fino a quando la richiesta dello storage array non viene elaborata dai server AutoSupport. Attendere che venga ricevuta un'e-mail di conferma prima di eseguire qualsiasi attività di manutenzione sullo storage array.

Disattiva la finestra di manutenzione di AutoSupport

Disattivare la finestra di manutenzione di AutoSupport per consentire la creazione automatica del ticket in caso di eventi di errore. Quando la finestra di manutenzione di AutoSupport è disattivata, lo storage array utilizza AutoSupport per aprire un caso con il supporto in caso di problemi.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Disattiva finestra manutenzione AutoSupport**.
3. Inserire l'indirizzo e-mail per ricevere una conferma dell'elaborazione della richiesta di disattivazione della finestra di manutenzione.

   A seconda della configurazione, è possibile immettere fino a cinque indirizzi e-mail. Se si desidera aggiungere più indirizzi, selezionare **Aggiungi un'altra e-mail** per aprire un altro campo.

4. Fare clic su **Sì**.

   La creazione automatica del ticket AutoSupport in caso di eventi di errore è attivata.

Al termine

La finestra di manutenzione non terminerà fino a quando la richiesta dello storage array non sarà stata elaborata dai server AutoSupport. Prima di procedere, attendere la ricezione di un'e-mail di conferma.

Visualizzare gli eventi

Panoramica del registro eventi

Il registro eventi fornisce una cronologia degli eventi che si sono verificati sull'array di storage, che aiuta il supporto tecnico nella risoluzione dei problemi relativi agli eventi che hanno causato guasti.

È possibile utilizzare il registro eventi come strumento diagnostico supplementare per il Recovery Guru per il tracciamento degli eventi degli array di storage. Fare sempre riferimento al Recovery Guru prima di tutto quando si tenta di eseguire il ripristino a seguito di guasti dei componenti nell'array di storage.

Categorie di eventi

Gli eventi nel registro eventi sono classificati con stati diversi. Gli eventi sui quali è necessario intervenire hanno i seguenti stati:

- Critico
- Attenzione

Gli eventi che sono informativi e non richiedono alcuna azione immediata sono i seguenti:

- Informativo

Eventi critici

Gli eventi critici indicano un problema con lo storage array. Se si risolve immediatamente l'evento critico, si potrebbe evitare la perdita di accesso ai dati.

Quando si verifica un evento critico, questo viene registrato nel registro eventi. Tutti gli eventi critici vengono inviati alla console di gestione SNMP o al destinatario dell'e-mail configurato per la ricezione delle notifiche di avviso. Se l'ID dello shelf non è noto al momento dell'evento, l'ID dello shelf viene elencato come "Shelf unknown".

Quando si riceve un evento critico, fare riferimento alla procedura Recovery Guru per una descrizione dettagliata dell'evento critico. Completare la procedura Recovery Guru per correggere l'evento critico. Per correggere alcuni eventi critici, potrebbe essere necessario contattare il supporto tecnico.

Visualizzare gli eventi utilizzando il registro eventi

È possibile visualizzare il registro eventi, che fornisce un record storico degli eventi che si sono verificati sullo storage array.

Fasi

1. Selezionare **Support › Event Log** (supporto[Registro eventi]).

   Viene visualizzata la pagina Registro eventi.

Dettagli della pagina

Elemento	Descrizione
Campo View All (Visualizza tutto)	Consente di alternare tra tutti gli eventi e solo quelli critici e di avviso.
Campo del filtro	Filtra gli eventi. Utile per visualizzare solo gli eventi correlati a un componente specifico, a un evento specifico e così via
Selezionare l'icona delle colonne.	Consente di selezionare altre colonne da visualizzare. Altre colonne forniscono informazioni aggiuntive sull'evento.
Caselle di controllo	Consente di selezionare gli eventi da salvare. La casella di controllo nell'intestazione della tabella seleziona tutti gli eventi.
Colonna Data/ora	La data e l'ora dell'evento, in base all'orologio del controller. Il registro eventi ordina inizialmente gli eventi in base al numero di sequenza. Di solito, questa sequenza corrisponde alla data e all'ora. Tuttavia, i due clock dei controller nell'array di storage potrebbero non essere sincronizzati. In questo caso, alcune incongruenze percepite potrebbero apparire nel registro eventi in relazione agli eventi e alla data e all'ora visualizzate.
Colonna Priority (priorità)	Questi valori di priorità esistono: • **Critico** — si è verificato un problema con lo storage array. Tuttavia, se si esegue un'azione immediata, si potrebbe impedire la perdita di accesso ai dati. Gli eventi critici vengono utilizzati per le notifiche degli avvisi. Tutti gli eventi critici vengono inviati a qualsiasi client di gestione della rete (tramite trap SNMP) o al destinatario di posta elettronica configurato. • **Attenzione** — si è verificato un errore che ha degradato le prestazioni e la capacità dello storage array di ripristinare da un altro errore. • **Informazionale** — informazioni non critiche relative allo storage array.
Colonna Component Type (tipo di componente)	Il componente interessato dall'evento. Il componente potrebbe essere hardware, ad esempio un disco o un controller, oppure software, ad esempio il firmware del controller.
Colonna Component Location (posizione componente)	La posizione fisica del componente nell'array di storage.

Elemento	Descrizione
Colonna Description (Descrizione)	Una descrizione dell'evento. **Esempio** — `Drive write failure - retries exhausted`
Colonna Sequence Number	Un numero a 64 bit che identifica in modo univoco una voce di log specifica per un array di storage. Questo numero aumenta di uno ad ogni nuova voce del registro eventi. Per visualizzare queste informazioni, fare clic sull'icona **Select columns** (Seleziona colonne).
Colonna tipo di evento	Un numero di 4 cifre che identifica ciascun tipo di evento registrato. Per visualizzare queste informazioni, fare clic sull'icona **Select columns** (Seleziona colonne).
Colonna codici specifici evento	Queste informazioni vengono utilizzate dal supporto tecnico. Per visualizzare queste informazioni, fare clic sull'icona **Select columns** (Seleziona colonne).
Colonna Categoria evento	• **Guasto** – Un componente dell'array di storage si è guastato, ad esempio un guasto al disco o alla batteria. • **Modifica di stato**: Un elemento dell'array di storage che ha cambiato stato; ad esempio, un volume è passato allo stato ottimale o un controller è passato allo stato offline. • **Interno** – operazioni interne del controller che non richiedono un'azione da parte dell'utente; ad esempio, il controller ha completato l'inizio della giornata. • **Comando** – un comando che è stato inviato all'array di storage; ad esempio, è stato assegnato un hot spare. • **Errore** – è stata rilevata una condizione di errore sull'array di storage; ad esempio, un controller non è in grado di sincronizzare e svuotare la cache oppure viene rilevato un errore di ridondanza sull'array di storage. • **Generale** – qualsiasi evento che non si adatti bene ad altre categorie. Per visualizzare queste informazioni, fare clic sull'icona **Seleziona colonne**.
Registrato per colonna	Il nome del controller che ha registrato l'evento. Per visualizzare queste informazioni, fare clic sull'icona **Seleziona colonne**.

2. Per recuperare nuovi eventi dallo storage array, fare clic su **Refresh**.

   La registrazione e la visualizzazione di un evento nella pagina Registro eventi possono richiedere alcuni minuti.

3. Per salvare il registro eventi in un file:

   a. Selezionare la casella di controllo accanto a ciascun evento che si desidera salvare.

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

   Il file viene salvato nella cartella Download del browser con il nome `major-event-log-timestamp.log`.

4. Per cancellare gli eventi dal registro eventi:

   Il registro eventi memorizza circa 8,000 eventi prima di sostituire un evento con un nuovo evento. Se si desidera conservare gli eventi, è possibile salvarli e cancellarli dal registro eventi.

   a. Innanzitutto, salvare il registro eventi.
   b. Fare clic su **Clear All** (Cancella tutto) e confermare che si desidera eseguire l'operazione.

Gestire gli aggiornamenti

Panoramica di Upgrade Center

Utilizzare il Centro di aggiornamento per scaricare il software e il firmware più recenti e per aggiornare i controller e le unità.

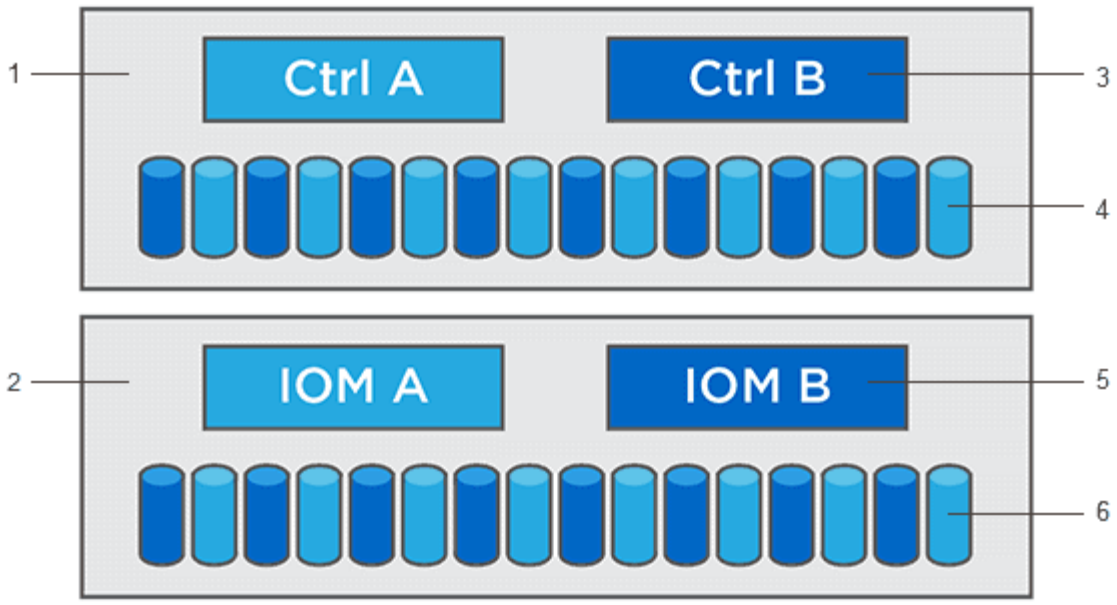
Panoramica sull'aggiornamento del controller

È possibile aggiornare il software e il firmware dello storage array per ottenere le ultime funzionalità e correzioni di bug.

Componenti inclusi nell'aggiornamento del controller del sistema operativo

Diversi componenti dello storage array contengono software o hardware che è possibile aggiornare occasionalmente.

- **Software di gestione** — System Manager è il software che gestisce lo storage array.
- **Controller firmware** — il firmware del controller gestisce l'i/o tra host e volumi.
- **Controller NVSRAM** — Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller.
- **IOM firmware** — il firmware del modulo i/o (IOM) gestisce la connessione tra un controller e uno shelf di dischi. Inoltre, monitora lo stato dei componenti.
- **Software di supervisore** — il software di supervisore è la macchina virtuale su un controller in cui viene eseguito il software.



[1] shelf del controller; [2] shelf del disco; [3] Software, firmware del controller, NVSRAM del controller, Software del supervisore; [4] firmware del disco; [5] firmware IOM; [6] firmware del disco

È possibile visualizzare le versioni software e firmware correnti nella finestra di dialogo Software and firmware Inventory (inventario software e firmware). Accedere al **Support › Upgrade Center**, quindi fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware).

Come parte del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover e/o HBA dell'host in modo che l'host possa interagire correttamente con i controller. Per determinare se questo è il caso, consultare la "Tool di matrice di interoperabilità NetApp".

Quando interrompere i/O.

Se lo storage array contiene due controller e si dispone di un driver multipath installato, lo storage array può continuare l'elaborazione dell'i/o durante l'aggiornamento. Durante l'aggiornamento, il controller A esegue il failover di tutti i volumi nel controller B, esegue l'upgrade, recupera i volumi e tutti i volumi del controller B, quindi aggiorna il controller B.

Verifica dello stato di salute prima dell'aggiornamento

Durante il processo di aggiornamento viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa continuare. Le seguenti condizioni potrebbero impedire l'aggiornamento:

- Dischi assegnati non riusciti
- Hot spare in uso
- Gruppi di volumi incompleti
- Operazioni esclusive in esecuzione
- Volumi mancanti
- Controller in stato non ottimale
- Numero eccessivo di eventi del registro eventi

- Errore di convalida del database di configurazione
- Dischi con versioni precedenti di DACstore

È inoltre possibile eseguire il controllo dello stato di salute pre-aggiornamento separatamente senza eseguire un aggiornamento.

Panoramica sull'aggiornamento del disco

Il firmware del disco controlla le caratteristiche operative di basso livello di un disco. Periodicamente, i produttori di dischi rilasciano aggiornamenti al firmware del disco per aggiungere nuove funzionalità, migliorare le prestazioni e correggere i difetti.

Aggiornamenti del firmware del disco online e offline

Esistono due tipi di metodi di aggiornamento del firmware del disco: Online e offline.

Online

Durante un aggiornamento online, i dischi vengono aggiornati in sequenza, uno alla volta. Lo storage array continua l'elaborazione dell'i/o durante l'aggiornamento. Non è necessario interrompere l'i/O. Se un disco è in grado di eseguire un aggiornamento online, il metodo online viene utilizzato automaticamente.

I dischi che possono eseguire un aggiornamento online includono:

- Dischi in un pool ottimale
- Dischi in un gruppo ottimale di volumi ridondanti (RAID 1, RAID 5 e RAID 6)
- Dischi non assegnati
- Dischi hot spare in standby

L'aggiornamento del firmware di un disco online può richiedere diverse ore per esporre l'array di storage a potenziali errori di volume. In questi casi si potrebbero verificare errori di volume:

- In un gruppo di volumi RAID 1 o RAID 5, un disco si guasta mentre viene aggiornato un altro disco del gruppo di volumi.
- In un pool o gruppo di volumi RAID 6, due dischi si guastano mentre viene aggiornato un altro disco del pool o gruppo di volumi.

Offline (parallelo)

Durante un aggiornamento offline, tutti i dischi dello stesso tipo di disco vengono aggiornati contemporaneamente. Questo metodo richiede l'interruzione dell'attività di i/o nei volumi associati ai dischi selezionati. Poiché è possibile aggiornare più dischi contemporaneamente (in parallelo), il downtime complessivo è notevolmente ridotto. Se un disco può eseguire solo un aggiornamento offline, il metodo offline viene utilizzato automaticamente.

I seguenti dischi DEVONO utilizzare il metodo offline:

- Dischi in un gruppo di volumi non ridondante (RAID 0)
- Dischi in un pool o un gruppo di volumi non ottimali
- Dischi nella cache SSD

Compatibilità

Ciascun file del firmware del disco contiene informazioni sul tipo di disco su cui viene eseguito il firmware. È possibile scaricare il file del firmware specificato solo su un'unità compatibile. System Manager verifica automaticamente la compatibilità durante il processo di aggiornamento.

Aggiornare il software e il firmware del controller

È possibile aggiornare il software dello storage array e, facoltativamente, il firmware IOM e la memoria ad accesso casuale statica non volatile (NVSRAM) per assicurarsi di disporre di tutte le funzionalità più recenti e delle correzioni dei bug.

Prima di iniziare

- Si sa se si desidera aggiornare il firmware IOM.

  Di norma, è necessario aggiornare tutti i componenti contemporaneamente. Tuttavia, è possibile decidere di non aggiornare il firmware IOM se non si desidera aggiornarlo come parte dell'aggiornamento del software del sistema operativo SANtricity o se il supporto tecnico ha richiesto di eseguire il downgrade del firmware IOM (è possibile eseguire il downgrade del firmware solo utilizzando l'interfaccia della riga di comando).

- Si sa se si desidera aggiornare il file NVSRAM del controller.

  Di norma, è necessario aggiornare tutti i componenti contemporaneamente. Tuttavia, si potrebbe decidere di non aggiornare il file NVSRAM del controller se il file è stato patchato o è una versione personalizzata e non si desidera sovrascriverlo.

- Si sa se si desidera attivare l'aggiornamento del sistema operativo ora o in una versione successiva.

  I motivi per l'attivazione successiva potrebbero includere:

  - **Ora del giorno** — l'attivazione del software e del firmware può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. Il failover dei controller durante l'attivazione potrebbe risultare inferiore al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.
- Si sa se si desidera passare da dischi non protetti o da dischi protetti internamente per utilizzare un server di gestione delle chiavi esterno (KMS) per la sicurezza dei dischi.
- Si sa se si desidera utilizzare il controllo degli accessi basato sui ruoli nel proprio array di storage.

A proposito di questa attività

Puoi scegliere di aggiornare solo il file del software del sistema operativo o solo il file Controller NVSRAM oppure puoi scegliere di aggiornare entrambi i file.

Eseguire questa operazione solo se richiesto dal supporto tecnico.

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

Fasi

1. Se l'array di storage contiene un solo controller o non si dispone di un driver multipath installato, interrompere l'attività i/o dell'array di storage per evitare errori dell'applicazione. Se lo storage array

dispone di due controller e si dispone di un driver multipath installato, non è necessario interrompere l'attività di i/O.

2. Selezionare **Support › Upgrade Center**.
3. Scaricare il nuovo file dal sito Support sul client di gestione.
   a. Fare clic su **NetApp Support** per avviare il sito Web Support.
   b. Nel sito Web del supporto tecnico, fare clic sulla scheda **Downloads**, quindi selezionare **Downloads**.
   c. Selezionare **Software del controller del sistema operativo SANtricity e-Series**.
   d. Seguire le istruzioni rimanenti.

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

4. Se NON si desidera aggiornare il firmware IOM, fare clic su **Sospendi sincronizzazione automatica IOM**.

   Se si dispone di uno storage array con un singolo controller, il firmware IOM non viene aggiornato.

5. Nella sezione aggiornamento software SANtricity OS, fare clic su **Avvia aggiornamento**.

   Viene visualizzata la finestra di dialogo Aggiorna software SANtricity OS.

6. Selezionare uno o più file per avviare il processo di aggiornamento:
   a. Selezionare il file del software SANtricity OS facendo clic su **Sfoglia** e selezionando il file del software del sistema operativo scaricato dal sito Web del supporto.
   b. Selezionare il file NVSRAM del controller facendo clic su **Browse** (Sfoglia) e selezionando il file NVSRAM scaricato dal sito di supporto. I file NVSRAM del controller hanno un nome file simile a. `N2800-830000-000.dlp`.

      Si verificano queste azioni:

      - Per impostazione predefinita, vengono visualizzati solo i file compatibili con la configurazione corrente dell'array di storage.
      - Quando si seleziona un file per l'aggiornamento, vengono visualizzati il nome e le dimensioni del file.
7. **Opzionale:** se è stato selezionato un file del software SANtricity OS da aggiornare, è possibile trasferire i file sul controller senza attivarli selezionando la casella di controllo **Trasferisci file ora, ma non eseguire l'aggiornamento (attiva l'aggiornamento in seguito)**.
8. Fare clic su **Start** e confermare che si desidera eseguire l'operazione.

   È possibile annullare l'operazione durante il controllo dello stato di salute prima dell'aggiornamento, ma non durante il trasferimento o l'attivazione.

9. **Opzionale:** per visualizzare un elenco degli aggiornamenti, fare clic su **Salva registro**.

   Il file viene salvato nella cartella Download del browser con il nome `drive_upgrade_log-timestamp.txt`.

Al termine

- Verificare che tutti i componenti siano visualizzati nella pagina hardware.

- Verificare le nuove versioni software e firmware selezionando la finestra di dialogo Software and firmware Inventory (selezionare **Support › Upgrade Center**, quindi fare clic sul collegamento **Software and firmware Inventory**).
- Se IL controller NVSRAM è stato aggiornato, tutte le impostazioni personalizzate applicate all'NVSRAM esistente andranno perse durante il processo di attivazione. Al termine del processo di attivazione, è necessario applicare nuovamente le impostazioni personalizzate A NVSRAM.

Attivare il software e il firmware del controller

È possibile scegliere di attivare i file di aggiornamento immediatamente o attendere fino a un momento più comodo.

A proposito di questa attività

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

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

Se il software o il firmware è stato trasferito ma non attivato, viene visualizzata una notifica nell'area Notifiche della home page di System Manager e nella pagina Upgrade Center.

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

Fasi

1. Selezionare **Support › Upgrade Center**.
2. Nell'area aggiornamento del software del controller del sistema operativo SANtricity, fare clic su **attiva** e confermare che si desidera eseguire l'operazione.

   È possibile annullare l'operazione durante il controllo dello stato di salute prima dell'aggiornamento, ma non durante l'attivazione.

   Viene avviato il controllo dello stato di salute prima dell'aggiornamento. Se il controllo dello stato di salute prima dell'aggiornamento viene superato, il processo di aggiornamento procede all'attivazione dei file. Se il controllo dello stato di salute prima dell'aggiornamento non riesce, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Per alcuni tipi di condizioni, il supporto tecnico potrebbe consigliare di continuare con l'aggiornamento nonostante gli errori selezionando la casella di controllo **Allow Upgrade** (Consenti aggiornamento).

   Una volta completato correttamente il controllo dello stato di salute prima dell'aggiornamento, si verifica l'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dello storage array e dai componenti che si stanno attivando.

3. **Opzionale:** per visualizzare un elenco degli aggiornamenti, fare clic su **Salva registro**.

   Il file viene salvato nella cartella Download del browser con il nome `drive_upgrade_log-timestamp.txt`.

Al termine

- Verificare che tutti i componenti siano visualizzati nella pagina hardware.
- Verificare le nuove versioni software e firmware selezionando la finestra di dialogo Software and firmware Inventory (selezionare **Support › Upgrade Center**, quindi fare clic sul collegamento **Software and firmware Inventory**).
- Se IL controller NVSRAM è stato aggiornato, tutte le impostazioni personalizzate applicate all'NVSRAM esistente andranno perse durante il processo di attivazione. Al termine del processo di attivazione, è necessario applicare nuovamente le impostazioni personalizzate A NVSRAM.

Aggiornare il firmware del disco

È possibile aggiornare il firmware dei dischi per assicurarsi di disporre delle funzionalità più recenti e delle correzioni dei bug.

Prima di iniziare

- È stato eseguito il backup dei dati utilizzando il backup disk-to-disk, la copia del volume (su un gruppo di volumi non interessato dall'aggiornamento del firmware pianificato) o un mirror remoto.
- Lo stato dello storage array è ottimale.
- Tutti i dischi hanno uno stato ottimale.
- Non sono in esecuzione modifiche di configurazione sullo storage array.
- Se i dischi sono in grado di eseguire solo un aggiornamento offline, l'attività di i/o su tutti i volumi associati ai dischi viene interrotta.

Fasi

1. Selezionare **Support › Upgrade Center**.
2. Scaricare i nuovi file dal sito Support sul client di gestione.
   a. In aggiornamento del firmware del disco, fare clic su **NetApp Support**.
   b. Sul sito Web del supporto NetApp, fare clic sulla scheda **Downloads**.
   c. Selezionare **Disk Drive & firmware Matrix** (matrice disco e firmware).
   d. Seguire le istruzioni rimanenti.
3. In aggiornamento del firmware del disco, fare clic su **Avvia aggiornamento**.

   Viene visualizzata una finestra di dialogo che elenca i file del firmware del disco attualmente in uso.

4. Estrarre (decomprimere) i file scaricati dal sito del supporto.
5. Fare clic su **Browse** (Sfoglia) e selezionare i nuovi file del firmware del disco scaricati dal sito di supporto.

   I file del firmware del disco hanno un nome file simile a. `D_HUC101212CSS600_30602291_MS01_2800_0002` con l'estensione di `.dlp`.

   È possibile selezionare fino a quattro file del firmware del disco, uno alla volta. Se più di un file del firmware del disco è compatibile con lo stesso disco, viene visualizzato un errore di conflitto del file. Decidere quale file del firmware del disco utilizzare per l'aggiornamento e rimuovere l'altro.

6. Fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Select Drives** (Seleziona unità), che elenca le unità che è possibile

aggiornare con i file selezionati.

Vengono visualizzati solo i dischi compatibili.

Il firmware selezionato per il disco viene visualizzato nell'area Proposed firmware information (informazioni firmware proposte). Se è necessario modificare il firmware, fare clic su **Indietro** per tornare alla finestra di dialogo precedente.

7. Selezionare il tipo di aggiornamento che si desidera eseguire:
   - **Online (impostazione predefinita)** — Mostra i dischi in grado di supportare il download del firmware _mentre lo storage array sta elaborando i/O. Quando si seleziona questo metodo di aggiornamento, non è necessario interrompere l'i/o dei volumi associati utilizzando questi dischi. Questi dischi vengono aggiornati uno alla volta mentre lo storage array sta elaborando i/o su tali dischi.
   - **Offline (Parallel)** — Mostra i dischi che possono supportare il download del firmware *solo quando l'attività di i/o viene interrotta* su qualsiasi volume che utilizza i dischi. Quando si seleziona questo metodo di aggiornamento, è necessario interrompere tutte le attività di i/o su tutti i volumi che utilizzano i dischi che si stanno aggiornando. I dischi che non hanno ridondanza devono essere elaborati come operazioni offline. Questo requisito include qualsiasi disco associato alla cache SSD, un gruppo di volumi RAID 0 o qualsiasi pool o gruppo di volumi degradati. L'aggiornamento offline (parallelo) è in genere più rapido rispetto al metodo online (predefinito).
8. Nella prima colonna della tabella, selezionare il disco o i dischi che si desidera aggiornare.
9. Fare clic su **Start** e confermare che si desidera eseguire l'operazione.

   Per interrompere l'aggiornamento, fare clic su **Stop**. Tutti i download del firmware attualmente in corso sono stati completati. Tutti i download del firmware non avviati vengono annullati.

   > L'interruzione dell'aggiornamento del firmware del disco potrebbe causare la perdita di dati o la mancata disponibilità dei dischi.

10. **Opzionale:** per visualizzare un elenco degli aggiornamenti, fare clic su **Salva registro**.

    Il file viene salvato nella cartella Download del browser con il nome `drive_upgrade_log-timestamp.txt`.

11. Se durante la procedura di aggiornamento si verifica uno dei seguenti errori, eseguire l'azione consigliata appropriata.

Errori e azioni consigliate

Se si verifica questo errore di download del firmware…	Quindi procedere come segue…
Dischi assegnati non riusciti	Un motivo del guasto potrebbe essere che il disco non dispone della firma appropriata. Assicurarsi che il disco interessato sia un disco autorizzato. Per ulteriori informazioni, contatta il supporto tecnico. Quando si sostituisce un'unità, assicurarsi che la capacità dell'unità sostitutiva sia uguale o superiore a quella dell'unità che si sta sostituendo. È possibile sostituire il disco guasto mentre lo storage array riceve i/O.
Controllare l'array di storage	• Assicurarsi che a ciascun controller sia stato assegnato un indirizzo IP. • Assicurarsi che tutti i cavi collegati al controller non siano danneggiati. • Assicurarsi che tutti i cavi siano collegati saldamente.
Dischi hot spare integrati	Questa condizione di errore deve essere corretta prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Gruppi di volumi incompleti	Se uno o più gruppi di volumi o pool di dischi sono incompleti, è necessario correggere questa condizione di errore prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Operazioni esclusive (diverse dai supporti in background/scansione di parità) attualmente in esecuzione su qualsiasi gruppo di volumi	Se sono in corso una o più operazioni esclusive, queste devono essere completate prima di poter aggiornare il firmware. Utilizzare System Manager per monitorare l'avanzamento delle operazioni.
Volumi mancanti	È necessario correggere la condizione del volume mancante prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Controller in uno stato diverso da quello ottimale	Uno dei controller degli array di storage richiede attenzione. Questa condizione deve essere corretta prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Informazioni sulla partizione dello storage non corrispondenti tra i grafici a oggetti del controller	Si è verificato un errore durante la convalida dei dati sui controller. Contattare il supporto tecnico per risolvere il problema.

Se si verifica questo errore di download del firmware…	Quindi procedere come segue…
Controllo SPM Verify Database Controller non riuscito	Si è verificato un errore nel database di mappatura delle partizioni di storage su un controller. Contattare il supporto tecnico per risolvere il problema.
Convalida del database di configurazione (se supportata dalla versione del controller dell'array di storage)	Si è verificato un errore del database di configurazione su un controller. Contattare il supporto tecnico per risolvere il problema.
Controlli correlati A MEL	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 10 eventi DDE Informational o Critical MEL	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi critici MEL di pagina 2C	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici su Drive Channel degradati	Contattare il supporto tecnico per risolvere il problema.
Più di 4 voci MEL critiche negli ultimi 7 giorni	Contattare il supporto tecnico per risolvere il problema.

Al termine

L'aggiornamento del firmware del disco è stato completato. È possibile riprendere le normali operazioni.

Esaminare i possibili errori di aggiornamento del software e del firmware

Possono verificarsi errori durante l'aggiornamento del software del controller o del firmware del disco.

Errore di download del firmware	Descrizione	Azione consigliata
Dischi assegnati non riusciti	Impossibile aggiornare un disco assegnato nell'array di storage.	Un motivo del guasto potrebbe essere che il disco non dispone della firma appropriata. Assicurarsi che il disco interessato sia un disco autorizzato. Per ulteriori informazioni, contatta il supporto tecnico. Quando si sostituisce un'unità, assicurarsi che la capacità dell'unità sostitutiva sia uguale o superiore a quella dell'unità che si sta sostituendo. È possibile sostituire il disco guasto mentre lo storage array riceve i/O.
Dischi hot spare integrati	Se l'unità è contrassegnata come hot spare ed è in uso per un gruppo di volumi, il processo di aggiornamento del firmware non riesce.	Questa condizione di errore deve essere corretta prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Gruppi di volumi incompleti	Se un disco che fa parte di un gruppo di volumi viene ignorato, rimosso o non risponde, viene considerato un gruppo di volumi incompleto. Un gruppo di volumi incompleto impedisce gli aggiornamenti del firmware.	Se uno o più gruppi di volumi o pool di dischi sono incompleti, è necessario correggere questa condizione di errore prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Operazioni esclusive (diverse dai supporti in background/scansione di parità) attualmente in esecuzione su qualsiasi gruppo di volumi	Impossibile aggiornare il firmware se sono in corso operazioni esclusive su un volume.	Se sono in corso una o più operazioni esclusive, queste devono essere completate prima di poter aggiornare il firmware. Utilizzare System Manager per monitorare l'avanzamento delle operazioni.
Volumi mancanti	Impossibile aggiornare il firmware se manca un volume.	È necessario correggere la condizione del volume mancante prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.
Controller in uno stato diverso da quello ottimale	Impossibile aggiornare il firmware se uno dei controller si trova in uno stato diverso da quello ottimale.	Uno dei controller degli array di storage richiede attenzione. Questa condizione deve essere corretta prima di poter aggiornare il firmware. Avviare System Manager e utilizzare Recovery Guru per risolvere il problema.

Errore di download del firmware	Descrizione	Azione consigliata
Controllo SPM Verify Database Controller non riuscito	Impossibile aggiornare il firmware perché il database dei mapping delle partizioni di storage è corrotto.	Si è verificato un errore nel database di mappatura delle partizioni di storage su un controller. Contattare il supporto tecnico per risolvere il problema.
Configuration Database Validation (convalida del database di configurazione) (se supportata dalla versione del controller dell'array di storage)	Impossibile aggiornare il firmware perché il database di configurazione è corrotto.	Si è verificato un errore del database di configurazione su un controller. Contattare il supporto tecnico per risolvere il problema.
Controlli correlati A MEL	Impossibile aggiornare il firmware perché il registro eventi contiene errori.	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 10 eventi DDE Informational o Critical MEL	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono stati segnalati più di 10 eventi DDE informativi o MEL critici.	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi critici MEL di pagina 2C	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono stati segnalati più di due eventi MEL critici 2C di pagina.	Contattare il supporto tecnico per risolvere il problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici su Drive Channel degradati	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono stati segnalati più di due eventi MEL critici del canale del disco degradati.	Contattare il supporto tecnico per risolvere il problema.
Più di 4 voci MEL critiche negli ultimi 7 giorni	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono state segnalate più di quattro voci del registro eventi critici.	Contattare il supporto tecnico per risolvere il problema.
È richiesto un indirizzo IP di gestione valido.	Per eseguire questa operazione, è necessario un indirizzo IP del controller valido.	Contattare il supporto tecnico per risolvere il problema.
Il comando richiede un indirizzo IP di gestione attivo per ciascun controller da fornire.	Per eseguire questa operazione, è necessario un indirizzo IP del controller per ciascun controller associato all'array di storage.	Contattare il supporto tecnico per risolvere il problema.
Tipo di file di download non gestito restituito.	Il file di download specificato non è supportato.	Contattare il supporto tecnico per risolvere il problema.

Errore di download del firmware	Descrizione	Azione consigliata
Si è verificato un errore durante la procedura di caricamento del download del firmware.	Il download del firmware non è riuscito perché il controller non è in grado di elaborare la richiesta. Verificare che lo storage array sia ottimale e riprovare l'operazione.	Se l'errore si verifica nuovamente dopo aver verificato che lo storage array è ottimale, contattare il supporto tecnico per risolvere il problema.
Si è verificato un errore durante la procedura di attivazione del firmware.	L'attivazione del firmware non è riuscita perché il controller non è in grado di elaborare la richiesta. Verificare che lo storage array sia ottimale e riprovare l'operazione.	Se l'errore si verifica nuovamente dopo aver verificato che lo storage array è ottimale, contattare il supporto tecnico per risolvere il problema.
È stato raggiunto un timeout durante l'attesa del riavvio del controller{0}.	Il software di gestione non riesce a riconnettersi al controller{0} dopo un riavvio. Verificare la presenza di un percorso di connessione operativa all'array di storage e riprovare l'operazione se non è stata completata correttamente.	Se l'errore si verifica nuovamente dopo aver verificato che lo storage array è ottimale, contattare il supporto tecnico per risolvere il problema.

È possibile correggere alcune di queste condizioni utilizzando Recovery Guru in System Manager. Tuttavia, per alcune delle condizioni, potrebbe essere necessario contattare il supporto tecnico. Le informazioni sul download del firmware del controller più recente sono disponibili sullo storage array. Queste informazioni aiutano il supporto tecnico a comprendere le condizioni di errore che hanno impedito l'aggiornamento e il download del firmware.

FAQ

Quali dati vengono raccolti?

La funzionalità AutoSupport e la raccolta manuale dei dati di supporto consentono di raccogliere i dati in un pacchetto di assistenza clienti per la risoluzione dei problemi e l'analisi dei problemi in remoto da parte del supporto tecnico.

Il bundle di assistenza clienti raccoglie tutti i tipi di informazioni sull'array di storage in un singolo file compresso. Le informazioni raccolte comprendono la configurazione fisica, la configurazione logica, le informazioni sulla versione, gli eventi, i file di log, e dati sulle performance. Le informazioni vengono utilizzate solo dal supporto tecnico per risolvere i problemi relativi allo storage array.

Cosa mostrano i dati dei settori illeggibili?

È possibile visualizzare dati dettagliati sui settori illeggibili rilevati sui dischi dello storage array.

Il registro dei settori illeggibili mostra prima il settore illeggibile più recente. Il registro contiene le seguenti informazioni sui volumi che contengono i settori illeggibili. I campi sono ordinabili.

Campo	Descrizione
Volume interessato	Mostra l'etichetta del volume. Se un volume mancante contiene settori illeggibili, viene visualizzato il World Wide Identifier per il volume mancante.
LUN (Logical Unit Number)	Mostra il LUN del volume. Se il volume non dispone di un LUN, nella finestra di dialogo viene visualizzato NA.
Assegnato a.	Mostra gli host o i cluster di host che hanno accesso al volume. Se il volume non è accessibile da un host, da un cluster host o anche da un cluster predefinito, la finestra di dialogo mostra NA.

Per visualizzare ulteriori informazioni sui settori illeggibili, fare clic sul segno più (+) accanto a un volume.

Campo	Descrizione
Data/ora	Mostra la data e l'ora in cui è stato rilevato il settore illeggibile.
Volume Logical Block Address (Indirizzo blocco logico volume)	Mostra l'indirizzo logico del blocco (LBA) del volume.
Posizione del disco	Mostra lo shelf del disco, il cassetto (se lo shelf del disco dispone di cassetti) e la posizione dell'alloggiamento.
Drive Logical Block Address (Indirizzo blocco logico unità)	Mostra l'LBA del disco.
Tipo di guasto	Mostra uno dei seguenti tipi di errore: • **Fisico** — errore del supporto fisico. • **Logico** — un errore di lettura in un'altra parte dello stripe che causa dati illeggibili. Ad esempio, un settore illeggibile a causa di errori dei supporti in altre parti del volume. • **Incoerente** — dati di ridondanza incoerenti. • **Data Assurance** — errore di Data Assurance.

Che cos'è un'immagine sanitaria?

Un'immagine di integrità è un dump di dati raw della memoria del processore del controller che il supporto tecnico può utilizzare per diagnosticare un problema con un controller.

Il firmware genera automaticamente un'immagine dello stato di salute quando rileva determinati errori. In alcuni scenari di risoluzione dei problemi, il supporto tecnico potrebbe richiedere il recupero del file di immagine di integrità e l'invio.

Quali sono le funzioni di AutoSupport?

La funzione AutoSupport è composta da tre funzioni individuali che vengono attivate separatamente.

- **Basic AutoSupport** — consente allo storage array di raccogliere e inviare automaticamente i dati al supporto tecnico.
- **AutoSupport OnDemand** — consente al supporto tecnico di richiedere la ritrasmissione di un precedente dispatch AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
- **Diagnostica remota** — consente al supporto tecnico di richiedere una nuova spedizione AutoSupport aggiornata quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti nuove richieste in sospeso e risponde di conseguenza.

Che tipo di dati vengono raccolti tramite la funzione AutoSupport?

La funzione AutoSupport contiene tre tipi di spedizione standard: Spedizioni di eventi, spedizioni pianificate e spedizioni di diagnostica on-demand e remote.

I dati AutoSupport non contengono dati utente.

- **Dispatch evento**

  Quando si verificano eventi nel sistema che richiedono una notifica proattiva al supporto tecnico, la funzione AutoSupport invia automaticamente un dispatch attivato dagli eventi.

  - Inviato quando si verifica un evento di supporto sull'array di storage gestito.
  - Include un'istantanea completa di ciò che stava accadendo con lo storage array al momento dell'evento.
- **Spedizioni pianificate**

  La funzione AutoSupport invia automaticamente diverse spedizioni in base a una pianificazione regolare.

  - **Daily Dispatches** — inviato una volta al giorno durante un intervallo di tempo configurabile dall'utente. Include i registri degli eventi di sistema correnti e i dati sulle prestazioni.
  - **Spedizioni settimanali** — inviate una volta alla settimana durante un giorno e un intervallo di tempo configurabili dall'utente. Include informazioni sulla configurazione e sullo stato del sistema.
- **Dispatches di AutoSupport OnDemand e diagnostica remota**
  - **AutoSupport OnDemand** — consente al supporto tecnico di richiedere la ritrasmissione di un precedente dispatch AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in con il server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
  - **Diagnostica remota** — consente al supporto tecnico di richiedere una nuova spedizione AutoSupport aggiornata quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dallo storage array, non dal server AutoSupport. Lo storage array esegue periodicamente il check-in

con il server AutoSupport per determinare se sono presenti nuove richieste in sospeso e risponde di conseguenza.

Come si configura il metodo di consegna per la funzione AutoSupport?

La funzione AutoSupport supporta i protocolli HTTPS, HTTP e SMTP per l'invio di AutoSupport al supporto tecnico.

Prima di iniziare

- La funzione AutoSupport deve essere attivata. Puoi vedere se è attivato nella pagina AutoSupport.
- Nella rete deve essere installato e configurato un server DNS. L'indirizzo del server DNS deve essere configurato in System Manager (questa attività è disponibile nella pagina hardware).

A proposito di questa attività

Esaminare i diversi protocolli:

- **HTTPS** — consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTPS. Se si desidera attivare AutoSupport OnDemand o Diagnostica remota, il metodo di erogazione AutoSupport deve essere impostato su HTTPS.
- **HTTP** — consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTP.
- **E-mail** — consente di utilizzare un server e-mail come metodo di recapito per l'invio di messaggi AutoSupport.

> **Differenze tra i metodi HTTPS/HTTP ed e-mail**. Il metodo di recapito della posta elettronica, che utilizza SMTP, presenta alcune importanti differenze rispetto ai metodi di recapito HTTPS e HTTP. Innanzitutto, le dimensioni delle spedizioni per il metodo e-mail sono limitate a 5 MB, il che significa che alcune raccolte di dati ASUP non verranno inviate. In secondo luogo, la funzione AutoSupport OnDemand è disponibile solo sui metodi HTPP e HTTPS.

Fasi

1. Selezionare **scheda supporto › Centro di supporto › AutoSupport**.
2. Selezionare **Configura metodo di erogazione AutoSupport**.

   Viene visualizzata una finestra di dialogo in cui sono elencati i metodi di consegna dell'invio.

3. Selezionare il metodo di erogazione desiderato, quindi selezionare i parametri per il metodo di erogazione. Effettuare una delle seguenti operazioni:
   - Se si seleziona HTTPS o HTTP, selezionare uno dei seguenti parametri di erogazione:
     - **Direttamente** — questo parametro di erogazione è la selezione predefinita. Questa opzione consente di connettersi direttamente al sistema di supporto tecnico di destinazione utilizzando il protocollo HTTPS o HTTP.
     - **Via Proxy server** — questa opzione consente di specificare i dettagli del server proxy HTTP necessari per stabilire la connessione con il sistema di supporto tecnico di destinazione. Specificare l'indirizzo host e il numero di porta. Tuttavia, è necessario immettere solo i dettagli di autenticazione dell'host (nome utente e password), se necessario.
     - **Tramite PAC (Proxy Auto-Configuration script)** — specificare la posizione di un file PAC (Proxy Auto-Configuration) script. Un file PAC consente al sistema di scegliere automaticamente il server proxy appropriato per stabilire una connessione con il sistema di supporto tecnico di destinazione.

- Se è stata selezionata l'opzione e-mail, immettere le seguenti informazioni:
  - Indirizzo del server di posta come nome di dominio completo, indirizzo IPv4 o indirizzo IPv6.
  - L'indirizzo e-mail visualizzato nel campo da del messaggio e-mail di spedizione AutoSupport.
  - **Opzionale; se si desidera eseguire un test di configurazione.** l'indirizzo e-mail a cui viene inviata una conferma quando il sistema AutoSupport riceve l'invio del test.
  - Se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. In caso contrario, selezionare **Nessuno**.
  - Se necessario, immettere un nome utente e una password per l'autenticazione con il mittente e il server di posta in uscita.

4. Fare clic su **Test Configuration** (verifica configurazione) per verificare la connessione al server del supporto tecnico utilizzando i parametri di consegna specificati. Se è stata attivata la funzione AutoSupport on-Demand, il sistema verificherà anche la connessione per l'erogazione del dispatch AutoSupport on-Demand.

   Se il test di configurazione non riesce, controllare le impostazioni di configurazione ed eseguire nuovamente il test. Se il test continua a non riuscire, contattare il supporto tecnico.

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

Che cosa sono i dati di configurazione?

Quando si seleziona Collect Configuration Data (Raccogli dati di configurazione), il sistema salva lo stato corrente del database di configurazione RAID.

Il database di configurazione RAID include tutti i dati relativi ai gruppi di volumi e ai pool di dischi sul controller. La funzione Collect Configuration Data salva le stesse informazioni del comando CLI per `save storageArray dbmDatabase`.

Cosa occorre sapere prima di aggiornare il software SANtricity OS?

Prima di aggiornare il software e il firmware del controller, tenere presente questi elementi.

- Hai letto il documento e il `readme.txt` e hanno determinato che si desidera eseguire l'aggiornamento.
- Si sa se si desidera aggiornare il firmware IOM.

  Di norma, è necessario aggiornare tutti i componenti contemporaneamente. Tuttavia, è possibile decidere di non aggiornare il firmware IOM se non si desidera aggiornarlo come parte dell'aggiornamento del software del controller del sistema operativo SANtricity o se il supporto tecnico ha richiesto di eseguire il downgrade del firmware IOM (è possibile eseguire il downgrade del firmware solo utilizzando l'interfaccia della riga di comando).

- Si sa se si desidera aggiornare il file NVSRAM del controller.

  Di norma, è necessario aggiornare tutti i componenti contemporaneamente. Tuttavia, si potrebbe decidere di non aggiornare il file NVSRAM del controller se il file è stato patchato o è una versione personalizzata e non si desidera sovrascriverlo.

- Si sa se si desidera attivare ora o in un secondo momento.

I motivi per l'attivazione successiva potrebbero includere:

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

Questi componenti fanno parte dell'aggiornamento del software del controller del sistema operativo SANtricity:

- **Software di gestione** — System Manager è il software che gestisce lo storage array.
- **Controller firmware** — il firmware del controller gestisce l'i/o tra host e volumi.
- **Controller NVSRAM** — Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller.
- **IOM firmware** — il firmware del modulo i/o (IOM) gestisce la connessione tra un controller e uno shelf di dischi. Inoltre, monitora lo stato dei componenti.
- **Software di supervisore** — il software di supervisore è la macchina virtuale su un controller in cui viene eseguito il software.

Come parte del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover e/o HBA dell'host in modo che l'host possa interagire correttamente con i controller.

Per determinare se questo è il caso, consultare la "Tool di matrice di interoperabilità NetApp".

Se l'array di storage contiene un solo controller o non si dispone di un driver multipath installato, interrompere l'attività i/o dell'array di storage per evitare errori dell'applicazione. Se lo storage array dispone di due controller e si dispone di un driver multipath installato, non è necessario interrompere l'attività di i/O.

Non apportare modifiche allo storage array durante l'aggiornamento.

Cosa occorre sapere prima di sospendere la sincronizzazione automatica IOM?

La sospensione della sincronizzazione automatica IOM impedisce l'aggiornamento del firmware IOM al successivo aggiornamento del software del controller del sistema operativo SANtricity.

Normalmente, il software del controller e il firmware IOM vengono aggiornati come bundle. È possibile sospendere la sincronizzazione automatica IOM se si dispone di una speciale build del firmware IOM che si desidera conservare nell'enclosure. In caso contrario, al successivo aggiornamento del software del controller verrà ripristinato il firmware IOM in dotazione con il software del controller.

Perché l'aggiornamento del firmware procede così lentamente?

L'avanzamento dell'aggiornamento del firmware dipende dal carico complessivo del sistema.

Durante un aggiornamento online del firmware del disco, se si verifica un trasferimento di volume durante il processo di ricostruzione rapida, il sistema avvia una ricostruzione completa sul volume trasferito. Questa operazione potrebbe richiedere molto tempo. Il tempo effettivo di ricostruzione completa dipende da diversi fattori, tra cui la quantità di attività i/o che si verifica durante l'operazione di ricostruzione, il numero di dischi nel

gruppo di volumi, l'impostazione della priorità di ricostruzione e le prestazioni del disco.

Cosa occorre sapere prima di aggiornare il firmware del disco?

Prima di aggiornare il firmware del disco, tenere presente questi elementi.

- Per precauzione, eseguire il backup dei dati utilizzando il backup disk-to-disk, la copia del volume (su un gruppo di volumi non interessato dall'aggiornamento del firmware pianificato) o un mirror remoto.
- Potrebbe essere necessario aggiornare solo alcune unità per verificare il funzionamento del nuovo firmware e verificare che funzioni correttamente. Se il nuovo firmware funziona correttamente, aggiornare i dischi rimanenti.
- In caso di dischi guasti, correggerli prima di avviare l'aggiornamento del firmware.
- Se i dischi sono in grado di eseguire un aggiornamento offline, interrompere l'attività di i/o in tutti i volumi associati ai dischi. Quando l'attività di i/o viene interrotta, non possono verificarsi operazioni di configurazione associate a tali volumi.
- Non rimuovere alcun disco durante l'aggiornamento del firmware del disco.
- Non apportare modifiche alla configurazione dello storage array durante l'aggiornamento del firmware del disco.

Come si sceglie il tipo di aggiornamento da eseguire?

È possibile scegliere il tipo di aggiornamento da eseguire sul disco in base allo stato del pool o del gruppo di volumi.

- **Online**

  Se il pool o il gruppo di volumi supporta la ridondanza ed è ottimale, è possibile utilizzare il metodo online per aggiornare il firmware del disco. Il metodo Online scarica il firmware *mentre lo storage array sta elaborando i/o* nei volumi associati utilizzando questi dischi. Non è necessario interrompere l'i/o dei volumi associati utilizzando questi dischi. Questi dischi vengono aggiornati uno alla volta ai volumi associati ai dischi. Se l'unità non è assegnata a un pool o a un gruppo di volumi, il relativo firmware può essere aggiornato con il metodo Online o Offline. Le prestazioni del sistema potrebbero risentire dell'utilizzo del metodo online per l'aggiornamento del firmware del disco.

- **Non in linea**

  Se il pool o il gruppo di volumi non supporta la ridondanza (RAID 0) o è degradato, è necessario utilizzare il metodo offline per aggiornare il firmware del disco. Il metodo offline aggiornerà il firmware *solo quando l'attività di i/o viene interrotta* ai volumi associati che utilizzano questi dischi. È necessario arrestare tutti i i/o per tutti i volumi associati che utilizzano questi dischi. Se l'unità non è assegnata a un pool o a un gruppo di volumi, il relativo firmware potrebbe essere aggiornato con il metodo Online o Offline.

Gestione di array multipli con Unified Manager 6

Interfaccia principale

Panoramica dell'interfaccia di Unified Manager

Unified Manager è un'interfaccia basata su web che consente di gestire più array di storage in una singola vista.

Pagina principale

Quando si accede a Unified Manager, la pagina principale si apre su **Gestisci - tutto**. Da questa pagina è possibile scorrere un elenco degli array di storage rilevati nella rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Barra laterale di navigazione

È possibile accedere alle funzioni e alle funzioni di Unified Manager dalla barra laterale di navigazione.

Area	Descrizione
Gestire	Scopri gli array di storage nella tua rete, avvia Gestore di sistema SANtricity per un array, importa le impostazioni da un array a più array e gestisci i gruppi di array. Selezionare le caselle di controllo accanto ai nomi degli array per eseguire operazioni su di essi, ad esempio l'importazione delle impostazioni e la creazione di gruppi di array. I puntini di sospensione alla fine di ogni riga forniscono un menu in linea per le operazioni su un singolo array, ad esempio la ridenominazione.
Operazioni	Visualizzare l'avanzamento delle operazioni batch, ad esempio l'importazione delle impostazioni da un array all'altro. Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.
Gestione dei certificati	Gestire i certificati per l'autenticazione tra browser e client.
Gestione degli accessi	Stabilire l'autenticazione dell'utente per l'interfaccia di Unified Manager.
Supporto	Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

Impostazioni dell'interfaccia e guida

Nella parte superiore destra dell'interfaccia, è possibile accedere alla Guida e ad altra documentazione. È inoltre possibile accedere alle opzioni di amministrazione, disponibili dal menu a discesa accanto al proprio nome di accesso.

Login e password degli utenti

L'utente corrente che ha effettuato l'accesso al sistema viene visualizzato nella parte superiore destra dell'interfaccia.

Per ulteriori informazioni su utenti e password, consulta:

- "Impostare la protezione della password amministratore"
- "Modificare la password admin"
- "Modificare le password per i profili utente locali"

Browser supportati

È possibile accedere a Unified Manager da diversi tipi di browser.

Sono supportati i seguenti browser e versioni.

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

Il proxy dei servizi Web deve essere installato e disponibile nel browser.

Impostare la protezione della password amministratore

È necessario configurare Unified Manager con una password di amministratore per proteggerla da accessi non autorizzati.

Password amministratore e profili utente

Quando si avvia Unified Manager per la prima volta, viene richiesto di impostare una password di amministratore. Qualsiasi utente che dispone della password di amministratore può apportare modifiche alla configurazione degli array di storage.

Oltre alla password di amministratore, l'interfaccia di Unified Manager include profili utente preconfigurati con uno o più ruoli mappati. Per ulteriori informazioni, vedere "Come funziona Access Management".

Gli utenti e le mappature non possono essere modificati. È possibile modificare solo le password. Per modificare le password, vedere:

- "Modificare la password admin"
- "Modificare le password per i profili utente locali"

Timeout della sessione

Il software richiede la password una sola volta durante una singola sessione di gestione. Per impostazione predefinita, una sessione scade dopo 30 minuti di inattività. A questo punto, è necessario immettere nuovamente la password. Se un altro utente accede al software da un altro client di gestione e modifica la password mentre la sessione è in corso, viene richiesta una password la volta successiva che si tenta di eseguire un'operazione di configurazione o un'operazione di visualizzazione.

Per motivi di sicurezza, è possibile tentare di inserire una password solo cinque volte prima che il software entri in uno stato di "blocco". In questo stato, il software rifiuta i successivi tentativi di immissione della password. Attendere 10 minuti per ripristinare lo stato "normale" prima di inserire nuovamente la password.

È possibile regolare i timeout della sessione o disattivarli del tutto. Per ulteriori informazioni, vedere "Gestire i timeout delle sessioni".

Modificare la password admin

È possibile modificare la password admin utilizzata per accedere a Unified Manager.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.
- È necessario conoscere la password admin corrente.

A proposito di questa attività

Quando si sceglie una password, tenere presenti le seguenti linee guida:

- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostati. Fare attenzione a includere spazi se inclusi nella password.
- Per una maggiore sicurezza, utilizzare almeno 15 caratteri alfanumerici e modificare la password frequentemente.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare l'utente **admin** dalla tabella.

   Il pulsante Change Password (Modifica password) diventa disponibile.

4. Selezionare **Change Password** (Modifica password).

   Viene visualizzata la finestra di dialogo Change Password (Modifica password).

5. Se non è stata impostata alcuna lunghezza minima per le password utente locali, selezionare la casella di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Immettere la nuova password nei due campi.
7. Immettere la password dell'amministratore locale per confermare l'operazione, quindi fare clic su **Change** (Modifica).

Gestire i timeout delle sessioni

È possibile configurare i timeout per Unified Manager, 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 di Unified 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. Dalla barra dei menu, selezionare la freccia a discesa accanto al nome di accesso utente.
2. Selezionare **Enable/Disable session timeout** (attiva/Disattiva timeout sessione).

   Viene visualizzata la finestra di dialogo attiva/Disattiva timeout sessione.

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

   Il timeout minimo che è possibile impostare è di 15 minuti.

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

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

Storage array

Panoramica del rilevamento

Per gestire le risorse di storage, è necessario prima rilevare gli array di storage nella rete.

Come si rilevano gli array?

Utilizzare la pagina Add/Discover per trovare e aggiungere gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare più array o un singolo array. A tale scopo, immettere gli indirizzi IP di rete, quindi Unified Manager tenta di stabilire singole connessioni a ciascun indirizzo IP dell'intervallo.

Scopri di più:

- "Considerazioni per il rilevamento degli array"
- "Scopri più array di storage"
- "Scopri un singolo array"

Come si gestiscono gli array?

Dopo aver individuato gli array, accedere alla pagina **Gestisci - tutto**. Da questa pagina è possibile scorrere

un elenco degli array di storage rilevati nella rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Se si desidera gestire un singolo array, selezionarlo e aprire System Manager.

Scopri di più:

- "Considerazioni sull'accesso a System Manager"
- "Gestire un singolo array di storage"
- "Visualizzare lo stato degli array di storage"

Concetti

Considerazioni per il rilevamento degli array

Prima di poter visualizzare e gestire le risorse di storage, Unified Manager deve rilevare gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare più array o un singolo array.

Rilevamento di più array di storage

Se si sceglie di rilevare più array, immettere un intervallo di indirizzi IP di rete e Unified Manager tenta di stabilire connessioni individuali a ciascun indirizzo IP dell'intervallo. Qualsiasi array di storage raggiunto correttamente viene visualizzato nella pagina Discover e può essere aggiunto al dominio di gestione.

Rilevamento di un singolo storage array

Se si sceglie di rilevare un singolo array, inserire il singolo indirizzo IP per uno dei controller nell'array di storage e quindi aggiungere il singolo array di storage.

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

Credenziali dell'utente

Nell'ambito del processo di rilevamento, è necessario fornire la password di amministratore per ciascun array di storage che si desidera aggiungere.

Certificati di servizi Web

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

- **Certificati attendibili**

  Per gli array rilevati da Unified Manager, potrebbe essere necessario installare certificati attendibili aggiuntivi forniti dall'autorità di certificazione.

  Utilizzare il pulsante **Importa** per importare questi certificati. Se si è connessi a questo array in

precedenza, uno o entrambi i certificati controller sono scaduti, revocati o mancano un certificato root o un certificato intermedio nella relativa catena di certificati. È necessario sostituire il certificato scaduto o revocato o aggiungere il certificato root o intermedio mancante prima di gestire lo storage array.

- **Certificati autofirmati**

  È possibile utilizzare anche certificati autofirmati. Se l'amministratore tenta di rilevare gli array senza importare certificati firmati, Unified Manager visualizza una finestra di dialogo di errore che consente all'amministratore di accettare il certificato autofirmato. Il certificato autofirmato dell'array di storage viene contrassegnato come attendibile e l'array di storage viene aggiunto a Unified Manager.

  Se le connessioni all'array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza dell'array di storage prima di aggiungere l'array di storage a Unified Manager.

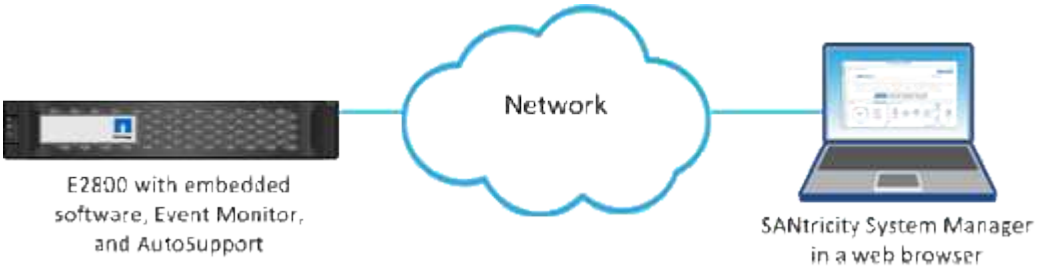
Considerazioni sull'accesso a System Manager

È possibile selezionare uno o più array di storage e utilizzare l'opzione Launch per aprire System Manager quando si desidera configurare e gestire gli array di storage.

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

Per accedere a System Manager, è necessario disporre di:

- Uno dei modelli di array elencati di seguito: "Panoramica dell'hardware e-Series"
- Connessione out-of-band a un client di gestione della rete con un browser Web.



Scopri gli array

Scopri più array di storage

Vengono rilevati più array per rilevare tutti gli array di storage nella subnet in cui risiede il server di gestione e aggiungere automaticamente gli array rilevati al dominio di gestione.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore della sicurezza.
- Lo storage array deve essere configurato e configurato correttamente.
- Le password degli array di storage devono essere impostate utilizzando il riquadro Access Management di System Manager.
- Per risolvere i certificati non attendibili, è necessario disporre di file di certificati attendibili provenienti da un'autorità di certificazione (CA) e che i file di certificati siano disponibili nel sistema locale.

Il rilevamento degli array è una procedura multi-step.

Fase 1: Inserire l'indirizzo di rete

Immettere un intervallo di indirizzi di rete per la ricerca nella sottorete locale. Qualsiasi array di storage raggiunto correttamente viene visualizzato nella pagina Discover e potrebbe essere aggiunto al dominio di gestione.

Per interrompere l'operazione di rilevamento per qualsiasi motivo, fare clic su **Stop Discovery** (Interrompi rilevamento).

Fasi

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

   Viene visualizzata la finestra di dialogo Add/Discover (Aggiungi/rileva).

2. Selezionare il pulsante di opzione **Scopri tutti gli array di storage all'interno di un intervallo di rete**.
3. Inserire l'indirizzo di rete iniziale e quello finale per la ricerca nella sottorete locale, quindi fare clic su **Avvia rilevamento**.

   Viene avviato il processo di rilevamento. Il completamento di questo processo di rilevamento può richiedere alcuni minuti. La tabella nella pagina Discover viene popolata durante il rilevamento degli array di storage.

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

4. Esaminare l'elenco degli array di storage rilevati.
5. Selezionare la casella di controllo accanto a un array di storage che si desidera aggiungere al dominio di gestione, quindi fare clic su **Avanti**.

   Unified Manager esegue un controllo delle credenziali su ciascun array che si sta aggiungendo al dominio di gestione. Potrebbe essere necessario risolvere eventuali certificati autofirmati e non attendibili associati a tale array.

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

Fase 2: Risoluzione dei certificati autofirmati durante il rilevamento

Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage stiano utilizzando certificati da un'origine attendibile.

Fasi

1. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, passare alla scheda successiva della procedura guidata. I certificati autofirmati verranno contrassegnati come attendibili e gli array di storage verranno aggiunti a Unified Manager.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una a Unified Manager.

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

Fase 3: Risoluzione dei certificati non attendibili durante il rilevamento

I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Durante il processo di rilevamento dell'array, è possibile risolvere i certificati non attendibili importando un certificato CA (Certificate Authority) (o certificato firmato da CA) emesso da una terza parte attendibile.

Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

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

Fasi

1. Selezionare la casella di controllo accanto a qualsiasi array di storage per cui si desidera risolvere i certificati non attendibili, quindi selezionare il pulsante **Importa**.

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

2. Fare clic su **Browse** (Sfoglia) per selezionare i file di certificato per gli array di storage.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

3. Fare clic su **Importa**.

   I file vengono caricati e validati.

   > Qualsiasi array di storage con problemi di certificato non attendibili che non sono stati risolti non verrà aggiunto a Unified Manager.

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

Fase 4: Fornire le password

È necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

Fasi

1. Inserire la password per ciascun array di storage che si desidera aggiungere a Unified Manager.
2. **Opzionale:** Associa gli array di storage a un gruppo: Dall'elenco a discesa, seleziona il gruppo desiderato da associare agli array di storage selezionati.
3. Fare clic su **fine**.

Al termine

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

> La connessione di Unified Manager agli array di storage specificati può richiedere alcuni minuti.

Scopri un singolo array

Utilizzare l'opzione Add/Discover Single Storage Array (Aggiungi/rileva singolo array di storage) per rilevare e aggiungere manualmente un singolo array di storage alla rete aziendale.

Prima di iniziare

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

Fasi

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

   Viene visualizzata la finestra di dialogo Add/Discover (Aggiungi/rileva).

2. Selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage).
3. Inserire l'indirizzo IP di uno dei controller nell'array di storage, quindi fare clic su **Avvia rilevamento**.

   La connessione di Unified Manager all'array di storage specificato può richiedere alcuni minuti.

   > Il messaggio Storage Array Not Accessible (Storage Array non accessibile) viene visualizzato quando la connessione all'indirizzo IP del controller specificato non riesce.

4. Se richiesto, risolvere eventuali certificati autofirmati.

   Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage rilevati stiano utilizzando certificati da un'origine attendibile. Se non riesce a individuare un certificato digitale per un array di storage, richiede di risolvere il certificato non firmato da un'autorità di certificazione (CA) riconosciuta aggiungendo un'eccezione di protezione.

5. Se richiesto, risolvere eventuali certificati non attendibili.

   I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Risolvi i certificati non attendibili importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

6. Fare clic su **Avanti**.
7. **Opzionale:** associare lo storage array rilevato a un gruppo: Dall'elenco a discesa, selezionare il gruppo desiderato da associare allo storage array.

   Il gruppo "tutti" è selezionato per impostazione predefinita.

8. Inserire la password dell'amministratore per lo storage array che si desidera aggiungere al dominio di gestione, quindi fare clic su **OK**.

Al termine

L'array di storage viene aggiunto a Unified Manager e, se specificato, viene aggiunto anche al gruppo selezionato.

Se è attivata la raccolta automatica dei dati di supporto, i dati di supporto vengono raccolti automaticamente per un array di storage aggiunto.

Gestire gli array

Visualizzare lo stato degli array di storage

Unified Manager visualizza lo stato di ciascun array di storage rilevato.

Accedere alla pagina **Gestisci - tutto**. Da questa pagina è possibile visualizzare lo stato della connessione tra il proxy dei servizi Web e l'array di storage.

Gli indicatori di stato sono descritti nella seguente tabella.

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

Gestire un singolo array di storage

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

Fasi

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

   Il sistema apre una nuova finestra e visualizza la pagina di accesso di System Manager.

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

Modificare le password degli array di storage

È possibile aggiornare le password utilizzate per visualizzare e accedere agli array di storage in Unified Manager.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore dello storage.
- È necessario conoscere la password corrente per lo storage array, impostata in System Manager.

A proposito di questa attività

In questa attività, immettere la password corrente per uno storage array in modo da potervi accedere in Unified Manager. Questo potrebbe essere necessario se la password dell'array è stata modificata in System Manager e ora deve essere modificata anche in Unified Manager.

Fasi

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

Rimuovere gli array di storage da Gestione unificata di SANtricity

È possibile rimuovere uno o più array di storage se non si desidera più gestirli da Unified Manager.

A proposito di questa attività

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

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

Fasi

1. Selezionare la pagina **Gestisci**.
2. Selezionare uno o più array di storage che si desidera rimuovere.
3. Selezionare **Uncommon Tasks › Remove storage array**.

   Lo storage array viene rimosso da tutte le viste in Gestione unificata di SANtricity.

Importazione delle impostazioni

Panoramica dell'importazione delle impostazioni

La funzione Import Settings (Impostazioni importazione) consente di eseguire un'operazione batch per importare le impostazioni da un array a più array. Questa funzione consente di risparmiare tempo quando è necessario configurare più array nella rete.

Quali impostazioni è possibile importare?

È possibile importare metodi di avviso, configurazioni AutoSupport, configurazioni dei servizi directory, configurazioni dello storage (come gruppi di volumi e pool) e impostazioni di sistema (come il bilanciamento automatico del carico).

Scopri di più:

- "Come funziona Import Settings (Impostazioni di importazione)"
- "Requisiti per la replica delle configurazioni di storage"

Come si esegue un'importazione in batch?

Su uno storage array da utilizzare come origine, aprire System Manager e configurare le impostazioni desiderate. Quindi, da Unified Manager, accedere alla pagina Manage (Gestione) e importare le impostazioni in uno o più array.

Scopri di più:

- "Importare le impostazioni degli avvisi"
- "Importa impostazioni AutoSupport"
- "Importare le impostazioni dei servizi di directory"
- "Importare le impostazioni di configurazione dello storage"
- "Importare le impostazioni di sistema"

Concetti

Come funziona Import Settings (Impostazioni di importazione)

È possibile utilizzare Unified Manager per importare le impostazioni da un array di storage a più array di storage. La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che consente di risparmiare tempo quando è necessario configurare più array nella rete.

Impostazioni disponibili per l'importazione

È possibile importare le seguenti configurazioni in più array:

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

- **Impostazioni di sistema** — configurazioni relative a:
  - Impostazioni di scansione dei supporti per un volume
  - Impostazioni SSD
  - Bilanciamento automatico del carico (non include il reporting sulla connettività host)

Workflow di configurazione

Per importare le impostazioni, seguire questo flusso di lavoro:

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

Requisiti per la replica delle configurazioni di storage

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

Shelf

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

Controller

- Il tipo di controller può essere diverso tra gli array di origine e di destinazione (ad esempio, l'importazione da E2800 a E5700), ma il tipo di enclosure RBOD deve essere identico.
- L'HICS, incluse le funzionalità da dell'host, deve essere identico tra gli array di origine e di destinazione.
- L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
- Le impostazioni FDE non sono incluse nel processo di importazione.

Stato

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

Storage

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

destinazioni.

- I volumi thin non sono inclusi nel processo di importazione.

Utilizzare le importazioni in batch

Importare le impostazioni degli avvisi

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

Prima di iniziare

- Gli avvisi sono configurati in System Manager per lo storage array che si desidera utilizzare come origine (**Impostazioni › Avvisi**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Per l'operazione di importazione, è possibile selezionare avvisi e-mail, SNMP o syslog. Le impostazioni importate includono:

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

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

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

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

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

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

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

5. Fare clic su **fine**.

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

Risultati

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

Importa impostazioni AutoSupport

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

Prima di iniziare

- AutoSupport è configurato in Gestione sistema per lo storage array che si desidera utilizzare come origine (**supporto › Centro di supporto**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

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

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

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

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

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

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

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

5. Fare clic su **fine**.

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

Risultati

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

Importare le impostazioni dei servizi di directory

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

Prima di iniziare

- I servizi di directory sono configurati in System Manager per lo storage array che si desidera utilizzare come origine (**Impostazioni › Gestione accessi**).
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

Le impostazioni importate includono il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

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

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

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

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

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

5. Fare clic su **fine**.

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

Risultati

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

Importare le impostazioni di sistema

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

Prima di iniziare

- Le impostazioni di sistema sono configurate in System Manager per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

A proposito di questa attività

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

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

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

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

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

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

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

5. Fare clic su **fine**.

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

Risultati

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

Importare le impostazioni di configurazione dello storage

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

Prima di iniziare

- Lo storage viene configurato in Gestore di sistema di SANtricity per l'array di storage che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).

- Gli array di origine e di destinazione devono soddisfare i seguenti requisiti:
  - Gli shelf in cui risiedono i controller devono essere identici.
  - Gli ID degli shelf devono essere identici.
  - Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità.
  - Il tipo di enclosure RBOD deve essere identico.
  - L'HICS, incluse le funzionalità di Data Assurance dell'host, deve essere identico.
  - Gli array di destinazione devono essere nello stato ottimale.
  - La capacità del volume sull'array di destinazione è maggiore della capacità dell'array di origine.
- Hai compreso le seguenti restrizioni:
  - L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
  - Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.
  - I volumi thin non sono inclusi nel processo di importazione.

A proposito di questa attività

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

Fasi

1. Nella pagina Manage (Gestione), fare clic su **Import Settings** (Impostazioni importazione).

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

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

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

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

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

5. Fare clic su **fine**.

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

Risultati

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

FAQ

Quali impostazioni verranno importate?

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che carica le configurazioni da un array di storage a più array di storage. Le impostazioni importate durante questa operazione dipendono dalla configurazione dell'array di storage di origine in System Manager.

È possibile importare le seguenti impostazioni in più array di storage:

- **Avvisi via email** — le impostazioni includono un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — le impostazioni includono un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — le impostazioni includono un nome di comunità e un indirizzo IP per il server SNMP.
- **AutoSupport** — le impostazioni includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.
- **Directory Services** — la configurazione include il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.
- **Configurazione dello storage** — le configurazioni includono volumi (solo volumi thick e non repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.
- **Impostazioni di sistema** — le configurazioni includono le impostazioni di scansione dei supporti per un volume, la cache SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Perché non vengono visualizzati tutti gli array di storage?

Durante l'operazione Import Settings (Impostazioni di importazione), alcuni storage array potrebbero non essere disponibili nella finestra di dialogo di selezione della destinazione.

Gli array di storage potrebbero non essere visualizzati per i seguenti motivi:

- La versione del firmware è inferiore alla 8.50.
- Lo storage array non è in linea.
- Il sistema non è in grado di comunicare con tale array (ad esempio, l'array presenta problemi di certificato, password o rete).

Gruppi di array

Panoramica dei gruppi

Dalla pagina Manage Groups (Gestisci gruppi), è possibile creare un set di gruppi di array di storage per una gestione più semplice.

Cosa sono i gruppi di array?

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

Esistono due tipi di gruppi:

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

Come si configurano i gruppi?

Dalla pagina Manage Groups (Gestisci gruppi), è possibile creare un gruppo e quindi aggiungere array a tale gruppo.

Scopri di più:

- "Configurare il gruppo di array di storage"

Configurare il gruppo di array di storage

È possibile creare gruppi di storage e quindi aggiungere array di storage ai gruppi.

La configurazione dei gruppi è una procedura in due fasi.

Fase 1: Creare un gruppo

Si crea prima un gruppo. Il gruppo di storage definisce quali dischi forniscono lo storage che costituisce il volume.

Fasi

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

Fase 2: Aggiungere un array di storage al gruppo

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

Fasi

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

4. Fare clic su **Aggiungi.**

Rimuovere gli array di storage dal gruppo

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

A proposito di questa attività

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

Fasi

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

Eliminare il gruppo di array di storage

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

A proposito di questa attività

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

Fasi

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

Rinominare il gruppo di array di storage

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

A proposito di questa attività

Tenere presenti queste linee guida.

- Un nome può essere composto da lettere, numeri e caratteri speciali come sottolineatura (_), trattino (-) e cancelletto (n.). Se si sceglie un altro carattere, viene visualizzato un messaggio di errore. Viene richiesto di scegliere un altro nome.
- Limitare il nome a 30 caratteri. Gli spazi iniziali e finali del nome vengono cancellati.
- Utilizzare un nome univoco e significativo, facile da comprendere e ricordare.
- Evitare nomi o nomi arbitrari che perderebbero rapidamente il loro significato in futuro.

Fasi

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

Aggiornamenti

Panoramica di Upgrade Center

Dal Centro aggiornamenti, è possibile gestire il software SANtricity OS e gli aggiornamenti DI NVSRAM per più array di storage.

Come funzionano gli aggiornamenti?

È possibile scaricare il software del sistema operativo più recente e aggiornare uno o più array.

Workflow di upgrade

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

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

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

Upgrade immediato o a fasi

È possibile attivare l'aggiornamento immediatamente o eseguirlo in un secondo momento. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

- **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. A seconda del carico di i/o e delle dimensioni della cache, il completamento di un aggiornamento del controller può richiedere da 15 a 25 minuti. I controller si riavviano e si eseguono il failover durante l'attivazione, pertanto le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.

Per attivare il software in fasi, andare al **supporto › Centro di aggiornamento** e fare clic su **attiva** nell'area denominata aggiornamento del software del controller del sistema operativo SANtricity.

Controllo dello stato di salute

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare (andare al **Upgrade Center › Pre-Upgrade Health Check**).

Il controllo dello stato di salute valuta tutti i componenti del sistema di storage per assicurarsi che l'aggiornamento possa continuare. Le seguenti condizioni potrebbero impedire l'aggiornamento:

- Dischi assegnati non riusciti
- Hot spare in uso
- Gruppi di volumi incompleti
- Operazioni esclusive in esecuzione
- Volumi mancanti
- Controller in stato non ottimale
- Numero eccessivo di eventi del registro eventi
- Errore di convalida del database di configurazione
- Dischi con versioni precedenti di DACstore

Cosa devo sapere prima di eseguire l'aggiornamento?

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

Versioni correnti

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

Altri componenti che richiedono l'aggiornamento

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare il driver multipath/failover dell'host o il driver HBA in modo che l'host possa interagire correttamente con i controller.

Per informazioni sulla compatibilità, fare riferimento a. "Matrice di interoperabilità NetApp". Inoltre, consultare le procedure riportate nelle Express Guide del sistema operativo in uso. Le guide rapide sono disponibili sul sito "Documentazione e-Series e SANtricity".

Controller doppi

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

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

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

Aggiornare software e firmware

Eseguire un controllo dello stato di salute prima dell'aggiornamento

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

Fasi

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

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

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

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

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

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

Aggiornare il sistema operativo SANtricity

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

Prima di iniziare

- I file più recenti del sistema operativo SANtricity sono disponibili sul sistema host in cui sono in esecuzione il proxy dei servizi Web SANtricity e il gestore unificato.
- Si sa se si desidera attivare l'aggiornamento software ora o in una versione successiva.

  È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

  - **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. Il failover dei controller durante l'attivazione potrebbe risultare inferiore al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — si consiglia di testare il nuovo software del sistema operativo su un array di storage prima di aggiornare i file su altri array di storage.

> Per eseguire l'aggiornamento alla versione 11.80.x o successiva, i sistemi devono disporre di SANtricity OS 11.70.5.

A proposito di questa attività

> Rischio di perdita di dati o di danneggiamento dello storage array: Non apportare modifiche allo storage array durante l'aggiornamento. Mantenere l'alimentazione dello storage array.

Fasi

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

   Viene visualizzata la pagina aggiornamento del software SANtricity OS.

4. Scarica il pacchetto software SANtricity OS più recente dal sito di supporto NetApp sul computer locale.

   a. Fare clic su **Aggiungi nuovo file al repository software**.
   b. Fare clic sul collegamento per trovare gli ultimi download del sistema operativo SANtricity*.
   c. Fare clic sul collegamento **Download Latest Release** (Scarica ultima versione).
   d. Seguire le istruzioni rimanenti per scaricare il file del sistema operativo SANtricity e IL file NVSRAM sul computer locale.

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

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

aggiornare i controller:

a. Dall'elenco a discesa **selezionare un file del software SANtricity OS**, selezionare il file del sistema operativo scaricato sul computer locale.

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

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

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

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

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

     Per attivare il software trasferito, selezionare **Upgrade Center › Activate Staged OS Software**.

   - Digitare **UPGRADE** per confermare che si desidera trasferire e attivare le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Upgrade**.

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

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

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

10. **Opzionale:** una volta completato l'aggiornamento, è possibile visualizzare un elenco degli aggiornamenti per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

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

Attivare il software del sistema operativo in fasi

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

A proposito di questa attività

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

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

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

Fasi

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

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

    - Nell'ambito del processo di attivazione viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'attivazione possa continuare.
    - Se un controllo dello stato di salute non riesce per un array di storage, l'attivazione si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'attivazione.
    - È possibile annullare l'operazione di attivazione dopo il controllo dello stato di salute pre-aggiornamento. Una volta completato correttamente il controllo dello stato di salute prima dell'aggiornamento, si verifica l'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dello storage array e dai componenti che si stanno attivando.
3. **Opzionale:** una volta completata l'attivazione, è possibile visualizzare un elenco degli elementi attivati per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

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

Gestire il repository software

Il repository software elenca tutti i file software associati al proxy dei servizi Web.

Se il file che si desidera utilizzare non viene visualizzato, utilizzare l'opzione Gestisci repository software per importare uno o più file SANtricity OS nel sistema host in cui sono in esecuzione il proxy dei servizi Web e Unified Manager. Puoi anche scegliere di eliminare uno o più file SANtricity OS disponibili nel repository software.

Prima di iniziare

Se si stanno aggiungendo file SANtricity OS, assicurarsi che i file del sistema operativo siano disponibili sul sistema locale.

Fasi

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

   Viene visualizzata la finestra di dialogo Manage Software Repository (Gestisci repository software).

2. Eseguire una delle seguenti operazioni:

Opzione	Eseguire questa operazione
Importa	a. Fare clic su **Importa.** b. Fare clic su **Browse** (Sfoglia), quindi individuare il percorso in cui si trovano i file del sistema operativo che si desidera aggiungere. I file del sistema operativo hanno un nome file simile a. `N2800-830000-000.dlp`. c. Selezionare uno o più file del sistema operativo da aggiungere, quindi fare clic su **Importa**.
Eliminare	a. Selezionare uno o più file del sistema operativo che si desidera rimuovere dal repository software. b. Fare clic su **Delete** (Elimina).

Risultati

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

Software per sistemi operativi chiari e staged

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

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Upgrade Center › Cancella software**

sistema operativo in fasi.

Viene visualizzata la finestra di dialogo Clear Staged OS Software (Cancella software per sistemi operativi in fasi) che elenca tutti i sistemi storage rilevati con software o NVSRAM in sospeso.

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

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

Mirroring

Panoramica del mirroring

Utilizza le funzionalità di mirroring per replicare i dati tra uno storage array locale e uno storage array remoto, in modo asincrono o sincrono.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Che cos'è il mirroring?

Le applicazioni SANtricity includono due tipi di mirroring: Asincrono e sincrono. Il mirroring asincrono copia i volumi di dati su richiesta o in base a una pianificazione, riducendo al minimo o evitando i downtime che potrebbero derivare da danneggiamento o perdita dei dati. Il mirroring sincrono replica i volumi di dati in tempo reale per garantire una disponibilità continua.

Scopri di più:

- "Come funziona il mirroring"
- "Terminologia mirrorata"

Come si configura il mirroring?

È possibile configurare il mirroring asincrono o sincrono in Unified Manager, quindi utilizzare System Manager per gestire le sincronizzazioni.

Scopri di più:

- "Flusso di lavoro di configurazione del mirroring"
- "Requisiti per l'utilizzo del mirroring"
- "Creare una coppia asincrona con mirroring"
- "Creare una coppia sincrona con mirroring"

Concetti

Come funziona il mirroring

Unified Manager include opzioni di configurazione per le funzionalità di mirroring di SANtricity, che consentono agli amministratori di replicare i dati tra due array di storage per la protezione dei dati.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Tipi di mirroring

Le applicazioni SANtricity includono due tipi di mirroring: Asincrono e sincrono.

Il mirroring asincrono copia i volumi di dati su richiesta o in base a una pianificazione, riducendo al minimo o evitando i downtime che potrebbero derivare da danneggiamento o perdita dei dati. Il mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati modificati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato in base alla larghezza di banda. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, man mano che le risorse di rete diventano disponibili. Questo tipo di mirroring è ideale per processi periodici come backup e archiviazione.

Il mirroring sincrono replica i volumi di dati in tempo reale per garantire una disponibilità continua. Lo scopo è quello di raggiungere un obiettivo RPO (Recovery Point Objective) di zero dati persi, grazie alla disponibilità di una copia dei dati importanti in caso di disastro su uno dei due storage array. La copia è identica ai dati di produzione in ogni momento perché ogni volta che viene eseguita una scrittura nel volume primario, viene eseguita una scrittura nel volume secondario. L'host non riceve una conferma che la scrittura è riuscita fino a quando il volume secondario non viene aggiornato con le modifiche apportate sul volume primario. Questo tipo di mirroring è ideale per scopi di business continuity come il disaster recovery.

Differenze tra i tipi di mirroring

La seguente tabella descrive le principali differenze tra i due tipi di mirroring.

Attributo	Asincrono	Sincrono
Metodo di replica	Point-in-time — il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente.	Continuo — il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura host.
Distanza	Supporta lunghe distanze tra gli array. In genere, la distanza è limitata solo dalle funzionalità della rete e dalla tecnologia di estensione del canale.	Limitato a distanze più brevi tra gli array. In genere, la distanza deve essere entro circa 10 km (6.2 miglia) dallo storage array locale per soddisfare i requisiti di latenza e performance applicativa.
Metodo di comunicazione	Una rete IP o Fibre Channel standard.	Solo rete Fibre Channel.
Tipi di volume	Standard o sottile.	Solo standard.

Flusso di lavoro di configurazione del mirroring

È possibile configurare il mirroring asincrono o sincrono in Unified Manager, quindi utilizzare System Manager per gestire le sincronizzazioni.

Workflow di mirroring asincrono

Il mirroring asincrono coinvolge il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare lo storage array locale come origine per il trasferimento dei dati.
   b. Creare o selezionare un gruppo di coerenza mirror esistente, che è un contenitore per il volume primario sull'array locale e il volume secondario sull'array remoto. I volumi primario e secondario sono denominati "coppia mirrorata". Se si crea il gruppo di coerenza mirror per la prima volta, specificare se si desidera eseguire sincronizzazioni manuali o pianificate.
   c. Selezionare un volume primario dall'array di storage locale, quindi determinarne la capacità riservata. La capacità riservata è la capacità fisica allocata da utilizzare per l'operazione di copia.
   d. Selezionare un array di storage remoto come destinazione del trasferimento, un volume secondario, quindi determinarne la capacità riservata.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.
2. Verificare l'avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avviare System Manager per l'array locale.
   b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale".
3. In alternativa, è possibile riprogrammare o eseguire manualmente i trasferimenti di dati successivi in System Manager. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.

> Poiché la replica asincrona è periodica, il sistema può consolidare i blocchi modificati e conservare la larghezza di banda della rete. L'impatto sul throughput di scrittura e sulla latenza di scrittura è minimo.

Workflow di mirroring sincrono

Il mirroring sincrono include il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare un array di storage locale come origine per il trasferimento dei dati.
   b. Selezionare un volume primario dall'array di storage locale.
   c. Selezionare un array di storage remoto come destinazione per il trasferimento dei dati, quindi selezionare un volume secondario.
   d. Selezionare le priorità di sincronizzazione e risincronizzazione.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, il trasferimento iniziale potrebbe richiedere diverse ore.
2. Verificare l'avanzamento della sincronizzazione iniziale:

a. In Unified Manager, avviare System Manager per l'array locale.

b. In System Manager, visualizzare lo stato dell'operazione di mirroring. Una volta completato il mirroring, lo stato della coppia mirrorata è "ottimale". I due array tentano di rimanere sincronizzati con le normali operazioni. Solo i blocchi nuovi e modificati vengono trasferiti dal volume primario al volume secondario.

3. In alternativa, è possibile modificare le impostazioni di sincronizzazione in System Manager.

> Poiché la replica sincrona è continua, il collegamento di replica tra i due siti deve fornire funzionalità di larghezza di banda sufficienti.

Terminologia mirrorata

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

Termine	Descrizione
Storage array locale	L'array di storage locale è l'array di storage su cui si sta agendo.
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un contenitore per una o più coppie mirrorate. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror. Tutte le coppie mirrorate in un gruppo vengono risincronizzate simultaneamente, preservando così un punto di ripristino coerente. Il mirroring sincrono non utilizza gruppi di coerenza mirror.
Coppia mirrorata	Una coppia mirrorata è composta da due volumi, un volume primario e un volume secondario. Nel mirroring asincrono, una coppia mirrorata appartiene sempre a un gruppo di coerenza mirror. Le operazioni di scrittura vengono eseguite prima nel volume primario e poi replicate nel volume secondario. Ogni coppia mirrorata in un gruppo di coerenza mirror condivide le stesse impostazioni di sincronizzazione.
Volume primario	Il volume principale di una coppia mirrorata è il volume di origine da mirrorare.
Storage array remoto	L'array di storage remoto è generalmente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione del servizio di copia e oggetto di storage. Non è direttamente leggibile dall'host. Questi volumi sono necessari per consentire al controller di salvare in modo persistente le informazioni necessarie per mantenere il mirroring in uno stato operativo. Contengono informazioni come i delta log e i dati copy-on-write.
Volume secondario	Il volume secondario di una coppia mirrorata si trova in genere in un sito secondario e contiene una replica dei dati.

Termine	Descrizione
Sincronizzazione	La sincronizzazione avviene alla sincronizzazione iniziale tra lo storage array locale e lo storage array remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario non vengono sincronizzati dopo un'interruzione della comunicazione. Quando il collegamento di comunicazione funziona di nuovo, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Requisiti per l'utilizzo del mirroring

Se si prevede di configurare il mirroring, tenere presenti i seguenti requisiti.

Unified Manager

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Storage array

> Il mirroring sincrono non è disponibile sull'array di storage EF600 o EF300.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

Requisiti di connettività

Il mirroring tramite un'interfaccia FC (asincrona o sincrona) richiede quanto segue:

- Ogni controller dello storage array dedica la porta host FC con il numero più alto alle operazioni di mirroring.
- Se il controller dispone di porte FC di base e porte FC HIC (host Interface Card), la porta con il numero più alto si trova su un HIC. Tutti gli host connessi alla porta dedicata vengono disconnessi e non vengono accettate richieste di accesso all'host. Le richieste di i/o su questa porta vengono accettate solo dai controller che partecipano alle operazioni di mirroring.

- Le porte di mirroring dedicate devono essere collegate a un ambiente fabric FC che supporti le interfacce del servizio di directory e del servizio di nomi. In particolare, FC-al e point-to-point non sono supportati come opzioni di connettività tra i controller che partecipano a relazioni mirror.

Il mirroring tramite un'interfaccia iSCSI (solo asincrona) richiede quanto segue:

- A differenza di FC, iSCSI non richiede una porta dedicata. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare alcuna delle porte iSCSI front-end dello storage array per l'utilizzo con il mirroring asincrono; tali porte sono condivise sia per il traffico mirror asincrono che per le connessioni i/o host-to-array.
- Il controller mantiene un elenco di sistemi storage remoti con i quali l'iSCSI Initiator tenta di stabilire una sessione. La prima porta che stabilisce correttamente una connessione iSCSI viene utilizzata per tutte le comunicazioni successive con l'array di storage remoto. Se la comunicazione non riesce, viene tentata una nuova sessione utilizzando tutte le porte disponibili.
- Le porte iSCSI sono configurate a livello di array porta per porta. La comunicazione tra controller per la messaggistica di configurazione e il trasferimento dei dati utilizza le impostazioni globali, incluse le impostazioni per:
  - VLAN: Per comunicare, i sistemi locali e remoti devono avere la stessa impostazione VLAN
  - Porta di ascolto iSCSI
  - Frame jumbo
  - Priorità Ethernet

> La comunicazione tra controller iSCSI deve utilizzare una porta di connessione host e non la porta Ethernet di gestione.

Volumi mirrorati candidati

- Il livello RAID, i parametri di caching e le dimensioni dei segmenti possono essere diversi sui volumi primari e secondari di una coppia mirrorata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

- Il volume secondario deve essere grande almeno quanto il volume primario.
- Un volume può partecipare a una sola relazione di mirroring.
- Per una coppia sincrona con mirroring, i volumi primario e secondario devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring sincrono, esistono limiti al numero di volumi supportati su un determinato array di storage. Assicurarsi che il numero di volumi configurati sull'array di storage sia inferiore al limite supportato. Quando il mirroring sincrono è attivo, i due volumi di capacità riservata creati vengono conteggiati rispetto al limite di volume.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità di Drive Security.
  - Se il volume primario è in grado di supportare FIPS, il volume secondario deve essere in grado di supportare FIPS.
  - Se il volume primario è compatibile con FDE, il volume secondario deve essere compatibile con FDE.

- Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Capacità riservata

Mirroring asincrono:

- Un volume a capacità riservata è necessario per un volume primario e per un volume secondario in una coppia mirrorata per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono ulteriore capacità riservata, è necessario assicurarsi di disporre di capacità libera su entrambi gli array di storage nella relazione mirror.

Mirroring sincrono:

- La capacità riservata è necessaria per un volume primario e per un volume secondario per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.
- I volumi di capacità riservati vengono creati automaticamente quando viene attivato il mirroring sincrono. Poiché sia il volume primario che il volume secondario di una coppia mirrorata richiedono capacità riservata, è necessario assicurarsi di disporre di una capacità libera sufficiente su entrambi gli array di storage che partecipano alla relazione di mirroring sincrono.

Funzione di protezione del disco

- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono disporre di impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizzano dischi sicuri, il volume primario e il volume secondario devono utilizzare lo stesso tipo di disco. Questa restrizione non viene applicata; pertanto, è necessario verificarla da soli.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

Configurare il mirroring

Creare una coppia asincrona con mirroring

Per configurare il mirroring asincrono, si crea una coppia mirrorata che include un volume primario sull'array locale e un volume secondario sull'array remoto.

Prima di iniziare

Prima di creare una coppia mirrorata, soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array e i volumi di storage:

- Ogni array di storage deve avere due controller.

- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.
- Sono stati creati i volumi primario e secondario che si desidera utilizzare nella relazione di mirroring asincrono.
- Il volume secondario deve essere grande almeno quanto il volume primario.

A proposito di questa attività

Il processo per creare una coppia asincrona con mirroring è una procedura multi-step.

Fase 1: Creare o selezionare un gruppo di coerenza mirror

In questo passaggio, creare un nuovo gruppo di coerenza mirror o selezionarne uno esistente. Un gruppo di coerenza mirror è un contenitore per i volumi primario e secondario (la coppia mirrorata) e specifica il metodo di risincronizzazione desiderato (manuale o automatico) per tutte le coppie del gruppo.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage locale che si desidera utilizzare per l'origine.
2. Selezionare **azioni › Crea coppia di mirroring asincrono**.

   Viene visualizzata la procedura guidata Create Asynchronous Mirrored Pair.

3. Selezionare un gruppo di coerenza mirror esistente o crearne uno nuovo.

   Per selezionare un gruppo esistente, assicurarsi che sia selezionato **un gruppo di coerenza mirror esistente**, quindi selezionare il gruppo dalla tabella. Un gruppo di coerenza può includere più coppie mirrorate.

   Per creare un nuovo gruppo, procedere come segue:

   a. Selezionare **Un nuovo gruppo di coerenza mirror**, quindi fare clic su **Avanti**.
   b. Immettere un nome univoco che descriva meglio i dati sui volumi che verranno mirrorati tra i due array di storage. Un nome può essere composto solo da lettere, numeri e caratteri speciali di sottolineatura (_), trattino (-) e il segno hash (n.). Un nome non può superare i 30 caratteri e non può contenere spazi.
   c. Selezionare l'array di storage remoto su cui si desidera stabilire una relazione mirror con l'array di storage locale.

      Se lo storage array remoto è protetto da password, il sistema richiede una password.

   d. Scegliere se sincronizzare le coppie mirrorate manualmente o automaticamente:
      - **Manuale** — selezionare questa opzione per avviare manualmente la sincronizzazione per tutte le coppie mirrorate all'interno di questo gruppo. Tenere presente che per eseguire una

risincronizzazione in un secondo momento, è necessario avviare System Manager per l'array di storage primario, quindi andare al **Storage › Asynchronous Mirroring**, selezionare il gruppo dalla scheda **Mirror Consistency Groups**, quindi selezionare **More › Manually resincronize**.

- **Automatico** — selezionare l'intervallo desiderato in **minuti**, **ore** o **giorni**, dall'inizio dell'aggiornamento precedente all'inizio dell'aggiornamento successivo. Ad esempio, se l'intervallo di sincronizzazione è impostato su 30 minuti e il processo di sincronizzazione inizia alle 16:00, il processo successivo inizia alle 16:30

e. Selezionare le impostazioni di avviso desiderate:

- Per le sincronizzazioni manuali, specificare la soglia (definita dalla percentuale della capacità rimanente) per la ricezione degli avvisi.
- Per le sincronizzazioni automatiche, è possibile impostare tre metodi di avviso: quando la sincronizzazione non è stata completata in un determinato periodo di tempo, quando i dati del punto di ripristino sull'array remoto sono più vecchi di un limite di tempo specifico e quando la capacità riservata si avvicina a una soglia specifica (definita dalla percentuale della capacità rimanente).

4. Selezionare **Avanti** e passare a. Fase 2: Selezionare il volume principale.

   Se è stato definito un nuovo gruppo di coerenza mirror, Unified Manager crea prima il gruppo di coerenza mirror sull'array di storage locale, quindi crea il gruppo di coerenza mirror sull'array di storage remoto. È possibile visualizzare e gestire il gruppo di coerenza mirror avviando System Manager per ciascun array.

> Se Unified Manager crea correttamente il gruppo di coerenza mirror sull'array di storage locale, ma non lo crea sull'array di storage remoto, elimina automaticamente il gruppo di coerenza mirror dall'array di storage locale. Se si verifica un errore mentre Unified Manager sta tentando di eliminare il gruppo di coerenza mirror, è necessario eliminarlo manualmente.

Fase 2: Selezionare il volume principale

In questa fase, selezionare il volume primario da utilizzare nella relazione di mirroring e allocare la capacità riservata. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco.

Tutti i volumi aggiunti al gruppo di coerenza mirror sull'array di storage locale avranno il ruolo principale nella relazione mirror.

Fasi

1. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume primario, quindi fare clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, selezionare la capacità riservata per il volume primario.

   Tenere presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume di base, e di solito questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Aggiorna candidati**.
   - La capacità richiesta varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume primario e al tempo necessario per mantenere la capacità.
   - In generale, scegliere una capacità più elevata per la capacità riservata se si verifica una o entrambe le seguenti condizioni:
     - Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.

    - Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.

3. Selezionare **Avanti** e passare a. Fase 3: Selezionare il volume secondario.

Fase 3: Selezionare il volume secondario

In questa fase, selezionare il volume secondario da utilizzare nella relazione di mirroring e allocare la capacità riservata. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco.

Tutti i volumi aggiunti al gruppo di coerenza mirror sull'array di storage remoto avranno il ruolo secondario nella relazione mirror.

Fasi

1. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume secondario nella coppia mirrorata, quindi fare clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, selezionare la capacità riservata per il volume secondario.

   Tenere presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume di base, e di solito questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Aggiorna candidati**.
   - La capacità richiesta varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume primario e al tempo necessario per mantenere la capacità.
   - In generale, scegliere una capacità più elevata per la capacità riservata se si verifica una o entrambe le seguenti condizioni:
     - Si intende mantenere la coppia mirrorata per un lungo periodo di tempo.
     - Una grande percentuale di blocchi di dati cambierà sul volume primario a causa dell'intensa attività di i/O. Utilizzare dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume primario.
3. Selezionare **fine** per completare la sequenza di mirroring asincrono.

Risultati

Unified Manager esegue le seguenti operazioni:

- Avvia la sincronizzazione iniziale tra lo storage array locale e lo storage array remoto.
- Crea la capacità riservata per la coppia mirrorata sull'array di storage locale e sull'array di storage remoto.

> Se il volume sottoposto a mirroring è un volume sottile, solo i blocchi sottoposti a provisioning (capacità allocata anziché capacità riportata) vengono trasferiti al volume secondario durante la sincronizzazione iniziale. In questo modo si riduce la quantità di dati da trasferire per completare la sincronizzazione iniziale.

Creare una coppia sincrona con mirroring

Per configurare il mirroring sincrono, creare una coppia mirrorata che includa un volume primario sull'array locale e un volume secondario sull'array remoto.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Prima di iniziare

Prima di creare una coppia mirrorata, soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array e i volumi di storage:

- I due storage array che si intende utilizzare per il mirroring vengono rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel.
- Sono stati creati i volumi primario e secondario che si desidera utilizzare nella relazione di mirroring sincrono.
- Il volume primario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere grande almeno quanto il volume primario.

A proposito di questa attività

Il processo per creare coppie sincrone mirrorate è una procedura multi-step.

Fase 1: Selezionare il volume principale

In questa fase, selezionare il volume primario da utilizzare nella relazione di mirroring sincrono. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. Il volume selezionato contiene il ruolo principale nella relazione mirror.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage locale che si desidera utilizzare per l'origine.
2. Selezionare **azioni › Crea coppia sincrona con mirroring**.

   Viene visualizzata la procedura guidata Create Synchronous Mirrored Pair.

3. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume principale nel mirror.

4. Selezionare **Avanti** e passare a. Fase 2: Selezionare il volume secondario.

Fase 2: Selezionare il volume secondario

In questa fase, selezionare il volume secondario da utilizzare nella relazione di mirroring. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per la coppia mirrorata. I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. Il volume selezionato avrà il ruolo secondario nella relazione mirror.

Fasi

1. Selezionare l'array di storage remoto su cui si desidera stabilire una relazione mirror con l'array di storage locale.

   > Se lo storage array remoto è protetto da password, il sistema richiede una password.

   - Gli array di storage sono elencati in base al nome dell'array di storage. Se non si è nominato un array di storage, questo verrà elencato come "senza nome".
   - Se lo storage array che si desidera utilizzare non è presente nell'elenco, assicurarsi che sia stato rilevato in Unified Manager.
2. Dall'elenco dei volumi idonei, selezionare un volume che si desidera utilizzare come volume secondario nel mirror.

   > Se si sceglie un volume secondario con una capacità superiore a quella del volume primario, la capacità utilizzabile viene limitata alle dimensioni del volume primario.

3. Fare clic su **Avanti** e passare a. Fase 3: Selezionare le impostazioni di sincronizzazione.

Fase 3: Selezionare le impostazioni di sincronizzazione

In questa fase, selezionare le impostazioni che determinano la modalità di sincronizzazione dei dati dopo un'interruzione della comunicazione. È possibile impostare la priorità con cui il proprietario del controller del volume primario sincronizza i dati con il volume secondario dopo un'interruzione della comunicazione. È inoltre necessario selezionare il criterio di risincronizzazione, manuale o automatico.

Fasi

1. Utilizzare la barra di scorrimento per impostare la priorità di sincronizzazione.

   La priorità di sincronizzazione determina la quantità di risorse di sistema utilizzate per completare la sincronizzazione iniziale e l'operazione di risincronizzazione dopo un'interruzione della comunicazione rispetto alle richieste di i/o del servizio.

   La priorità impostata in questa finestra di dialogo si applica sia al volume primario che al volume secondario. È possibile modificare la velocità sul volume primario in un secondo momento accedendo a System Manager e selezionando il **Storage › Synchronous Mirroring › More › Edit Settings** (Storage[mirroring sincrono > Altro > Modifica impostazioni).

   Sono disponibili cinque tassi di priorità di sincronizzazione:

   - Più basso
   - Basso
   - Medio

- Alto
- Massimo

  Se la priorità di sincronizzazione è impostata sul tasso più basso, l'attività di i/o ha la priorità e l'operazione di risincronizzazione richiede più tempo. Se la priorità di sincronizzazione è impostata sulla velocità massima, l'operazione di risincronizzazione viene assegnata alla priorità, ma l'attività di i/o per l'array di storage potrebbe risentirne.

2. Scegliere se risincronizzare le coppie mirrorate sull'array di storage remoto manualmente o automaticamente.
   - **Manuale** (opzione consigliata) — selezionare questa opzione per richiedere la ripresa manuale della sincronizzazione dopo il ripristino della comunicazione su una coppia mirrorata. Questa opzione offre la migliore opportunità per il ripristino dei dati.
   - **Automatico** — selezionare questa opzione per avviare la risincronizzazione automaticamente dopo il ripristino della comunicazione su una coppia mirrorata.

     Per riprendere manualmente la sincronizzazione, accedere a System Manager e selezionare **Storage › Synchronous Mirroring**, evidenziare la coppia mirrorata nella tabella e selezionare **Resume** sotto **More**.

3. Fare clic su **fine** per completare la sequenza di mirroring sincrono.

Risultati

Una volta attivato il mirroring, il sistema esegue le seguenti operazioni:

- Avvia la sincronizzazione iniziale tra lo storage array locale e lo storage array remoto.
- Imposta la priorità di sincronizzazione e il criterio di risincronizzazione.
- Riserva la porta con il numero più alto dell'HIC del controller per la trasmissione dei dati mirror.

  Le richieste di i/o ricevute su questa porta vengono accettate solo dal proprietario del controller preferito remoto del volume secondario nella coppia mirrorata. (Sono consentite prenotazioni sul volume primario).

- Crea due volumi di capacità riservata, uno per ciascun controller, che vengono utilizzati per la registrazione delle informazioni di scrittura per il ripristino da ripristini del controller e altre interruzioni temporanee.

  La capacità di ciascun volume è di 128 MiB. Tuttavia, se i volumi sono collocati in un pool, 4 GiB saranno riservati per ogni volume.

Al termine

Accedere a System Manager e selezionare **Home › View Operations in Progress** (Visualizza operazioni in corso) per visualizzare l'avanzamento dell'operazione di mirroring sincrono. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

FAQ

Cosa è necessario sapere prima di creare un gruppo di coerenza mirror?

Seguire queste linee guida prima di creare un gruppo di coerenza mirror.

Soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sull'host locale tramite una connessione HTTPS.
- Unified Manager deve mostrare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare il proprio certificato di sicurezza utilizzando Unified Manager e accedere al **Certificate › Certificate Management** (Gestione certificati).

Assicurarsi inoltre di soddisfare i seguenti requisiti per gli array di storage:

- I due storage array devono essere rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- Gli array di storage locali e remoti sono collegati tramite un fabric Fibre Channel o un'interfaccia iSCSI.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Cosa occorre sapere prima di creare una coppia mirrorata?

Prima di creare una coppia mirrorata, seguire queste linee guida.

- È necessario disporre di due array di storage.
- Ogni array di storage deve avere due controller.
- I due storage array devono essere rilevati in Unified Manager.
- Ciascun controller dell'array primario e secondario deve disporre di una porta di gestione Ethernet configurata e deve essere collegato alla rete.
- Gli array di storage dispongono di una versione firmware minima di 7.84. (Ciascuno di essi può eseguire diverse versioni del sistema operativo).
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera eseguire il mirroring.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

> Il mirroring sincrono non è disponibile sul sistema storage EF600 o EF300.

Perché dovrei modificare questa percentuale?

La capacità riservata corrisponde in genere al 20% del volume di base per le operazioni di mirroring asincrono. Di solito questa capacità è sufficiente.

La capacità necessaria varia in base alla frequenza e alle dimensioni delle scritture i/o nel volume di base e alla durata dell'utilizzo del servizio di copia dell'oggetto di storage. In generale, scegliere una percentuale maggiore per la capacità riservata se sussistono una o entrambe le seguenti condizioni:

- Se la durata di un'operazione di copia del servizio di un oggetto di storage specifico sarà molto lunga.
- Se una grande percentuale di blocchi di dati cambia sul volume di base a causa di un'intensa attività di i/O. Utilizza dati storici sulle performance o altre utility del sistema operativo per determinare l'attività i/o tipica del volume di base.

Perché vengono visualizzati più candidati con capacità riservata?

Se in un pool o gruppo di volumi sono presenti più volumi che soddisfano la percentuale di capacità selezionata per l'oggetto di storage, verranno visualizzati più volumi candidati.

È possibile aggiornare l'elenco dei candidati consigliati modificando la percentuale di spazio su disco fisico che si desidera riservare sul volume di base per le operazioni del servizio di copia. I candidati migliori vengono visualizzati in base alla selezione effettuata.

Perché non vengono visualizzati tutti i volumi?

Quando si seleziona un volume primario per una coppia mirrorata, un elenco mostra tutti i volumi idonei.

I volumi non idonei all'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Per il mirroring sincrono, i volumi primario e secondario di una coppia mirrorata devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring asincrono, i thin volumi devono avere l'espansione automatica abilitata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona con mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie mirrorate asincrone non idonee non vengono visualizzate nell'elenco dei volumi disponibili.

Perché non vengono visualizzati tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario nell'array di storage remoto, un elenco mostra tutti i volumi idonei per la coppia mirrorata.

I volumi non idonei per l'utilizzo non vengono visualizzati nell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è un volume standard, ad esempio un volume snapshot.
- Il volume non è ottimale.
- Il volume sta già partecipando a una relazione di mirroring.
- Per il mirroring asincrono, gli attributi del thin volume tra il volume primario e il volume secondario non corrispondono.
- Se si utilizza Data Assurance (da), il volume primario e il volume secondario devono avere le stesse impostazioni da.

    - Se il volume primario è abilitato da, il volume secondario deve essere abilitato da.
    - Se il volume primario non è abilitato da, il volume secondario non deve essere abilitato da.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità di Drive Security.
    - Se il volume primario è in grado di supportare FIPS, il volume secondario deve essere in grado di supportare FIPS.
    - Se il volume primario è compatibile con FDE, il volume secondario deve essere compatibile con FDE.
    - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Qual è l'impatto della priorità di sincronizzazione sulle velocità di sincronizzazione?

La priorità di sincronizzazione definisce il tempo di elaborazione allocato per le attività di sincronizzazione in relazione alle prestazioni del sistema.

Il proprietario del controller del volume primario esegue questa operazione in background. Allo stesso tempo, il proprietario del controller elabora le scritture i/o locali nel volume primario e le scritture remote associate nel volume secondario. Poiché la risincronizzazione distoglie le risorse di elaborazione del controller dall'attività di i/o, la risincronizzazione può avere un impatto sulle prestazioni dell'applicazione host.

Tenere presenti queste linee guida per determinare il tempo necessario per una priorità di sincronizzazione e il modo in cui le priorità di sincronizzazione possono influire sulle prestazioni del sistema.

Sono disponibili i seguenti tassi di priorità:

- Più basso
- Basso
- Medio
- Alto
- Massimo

Il tasso di priorità più basso supporta le prestazioni del sistema, ma la risincronizzazione richiede più tempo. Il tasso di priorità più elevato supporta la risincronizzazione, ma le prestazioni del sistema potrebbero essere compromesse.

Queste linee guida approssimano le differenze tra le priorità.

Tasso di priorità per la sincronizzazione completa	Tempo trascorso rispetto alla massima velocità di sincronizzazione
Più basso	Circa otto volte più a lungo rispetto al tasso di priorità più elevato.
Basso	Circa sei volte più a lungo rispetto al tasso di priorità più elevato.
Medio	Circa tre volte e mezzo fino al tasso di priorità più elevato.

Tasso di priorità per la sincronizzazione completa	Tempo trascorso rispetto alla massima velocità di sincronizzazione
Alto	Circa il doppio rispetto al tasso di priorità più elevato.

Le dimensioni del volume e i carichi della velocità di i/o dell'host influiscono sui confronti dei tempi di sincronizzazione.

Perché si consiglia di utilizzare una policy di sincronizzazione manuale?

La risincronizzazione manuale è consigliata perché consente di gestire il processo di risincronizzazione in modo da offrire la migliore opportunità di recupero dei dati.

Se si utilizza un criterio di risincronizzazione automatica e si verificano problemi di comunicazione intermittente durante la risincronizzazione, i dati sul volume secondario potrebbero essere temporaneamente danneggiati. Una volta completata la risincronizzazione, i dati vengono corretti.

Certificati

Panoramica dei certificati

Gestione certificati consente di creare richieste di firma del certificato (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Esistono due tipi di certificati: Un *certificato firmato* viene validato da un'autorità di certificazione (CA) e un *certificato autofirmato* viene validato dal proprietario dell'entità anziché da una terza parte.

Scopri di più:

- "Come funzionano i certificati"
- "Terminologia del certificato"

Come si configurano i certificati?

Da Certificate Management, è possibile configurare i certificati per la stazione di gestione che ospita Unified Manager e importare i certificati per i controller negli array.

Scopri di più:

- "Utilizzare i certificati firmati dalla CA per il sistema di gestione"
- "Importare certificati per gli array"

Concetti

Come funzionano i certificati

I certificati sono file digitali che identificano entità online, come siti Web e server, per

comunicazioni sicure su Internet.

Certificati firmati

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Con Unified Manager, è possibile gestire i certificati per il browser su un sistema di gestione host e i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

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

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

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

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

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

Certificati autofirmati

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

I certificati autofirmati non sono "trusted" dai browser. Ogni volta che si tenta di connettersi a un sito Web che

contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

Certificati per Unified Manager

L'interfaccia di Unified Manager viene installata con il proxy dei servizi Web su un sistema host. Quando si apre un browser e si tenta di connettersi a Unified Manager, il browser tenta di verificare che l'host sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA per il server, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. In alternativa, è possibile ottenere certificati digitali firmati da una CA in modo da non visualizzare più il messaggio di avviso.

Certificati per i controller

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

Terminologia del certificato

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per il rilascio di un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
Catena di certificati	Gerarchia di file che aggiunge un livello di protezione ai certificati. In genere, la catena include un certificato root nella parte superiore della gerarchia, uno o più certificati intermedi e i certificati server che identificano le entità.
Certificato intermedio	Uno o più certificati intermedi si diramano dalla directory principale nella catena di certificati. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
Archivio chiavi	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle chiavi pubbliche e ai certificati corrispondenti. Queste chiavi e certificati identificano le proprie entità, ad esempio i controller.

Termine	Descrizione
Certificato root	Il certificato root si trova nella parte superiore della gerarchia nella catena del certificato e contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
Certificato firmato	Certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include i dettagli relativi al proprietario dell'entità (in genere, un server o un sito Web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di trust e quindi viene utilizzato più spesso negli ambienti di produzione. Definito anche "certificato firmato da CA" o "certificato di gestione".
Certificato autofirmato	Un certificato autofirmato viene validato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di attendibilità di un certificato firmato dalla CA e, di conseguenza, viene spesso utilizzato negli ambienti di test. Detto anche certificato "preinstallato".
Certificato del server	Il certificato del server si trova nella parte inferiore della catena di certificati. Identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di un sistema storage richiede un certificato server separato.
Truststore	Un truststore è un repository che contiene certificati di terze parti attendibili, ad esempio CA.

Utilizzare i certificati firmati dalla CA per il sistema di gestione

È possibile ottenere e importare certificati firmati dalla CA per un accesso sicuro al sistema di gestione che ospita Unified Manager.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

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

Fase 1: Completare un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui sono installati Web Services Proxy e Unified Manager.

In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare il file CSR.

Fasi

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

Fase 2: Inviare il file CSR

Dopo aver creato un file di richiesta di firma del certificato (CSR), lo si invia a un'autorità di certificazione (CA) per ricevere certificati di gestione firmati per il sistema che ospita Unified Manager e Web Services Proxy.

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

Fasi

1. Individuare il file CSR scaricato.

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

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

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

3. Quando la CA restituisce i certificati firmati, passare a. Fase 3: Importazione dei certificati di gestione.

Fase 3: Importazione dei certificati di gestione

Dopo aver ricevuto i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui sono installati Web Services Proxy e l'interfaccia di Unified Manager.

Prima di iniziare

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

Fasi

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

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

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

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultati

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

Reimpostare i certificati di gestione

È possibile ripristinare lo stato originale autofirmato del certificato di gestione.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

A proposito di questa attività

Questa attività elimina il certificato di gestione corrente dal sistema host in cui sono installati Web Services Proxy e Unified Manager. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

Fasi

1. Selezionare **Impostazioni > certificati**.
2. Selezionare la scheda **Array Management**, quindi selezionare **Reset**.

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

3. Tipo `reset` Nel campo, quindi fare clic su **Reset**.

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

Risultati

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

Utilizzare certificati array

Importare certificati per gli array

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

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.
- Se si importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

Fasi

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

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

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

   Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

   Il certificato viene caricato e validato.

Eliminare i certificati attendibili

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

Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.

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

Fasi

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

   > La funzione **Delete** non è disponibile per i certificati preinstallati.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

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

   Il certificato viene rimosso dalla tabella.

Risolvi i certificati non attendibili

I certificati non attendibili si verificano quando uno storage array tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura.

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

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore della sicurezza.
- Se si intende importare un certificato firmato dalla CA:
  - È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
  - La CA ha restituito file di certificato attendibili.
  - I file dei certificati sono disponibili nel sistema locale.

A proposito di questa attività

Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti.

- Uno o entrambi i certificati vengono revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

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

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

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

   Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

   Il certificato viene caricato e validato.

Gestire i certificati

Visualizzare i certificati

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

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni del certificato non vengono visualizzate.

Fasi

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

Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

Prima di iniziare

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

Fasi

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

Gestione degli accessi

Panoramica sulla gestione degli accessi

Access Management è un metodo per configurare l'autenticazione dell'utente in Unified Manager.

Quali metodi di autenticazione sono disponibili?

Sono disponibili i seguenti metodi di autenticazione:

- **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC (role-based access control). I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.
- **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando SAML 2.0.

Scopri di più:

- "Come funziona Access Management"
- "Terminologia per la gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "SAML"

Come si configura Access Management?

Il software SANtricity è preconfigurato per l'utilizzo dei ruoli utente locali. Se si desidera utilizzare LDAP, è possibile configurarlo nella pagina Gestione accessi.

Scopri di più:

- "Gestione degli accessi con ruoli utente locali"
- "Gestione degli accessi con servizi di directory"
- "Configurare SAML"

Concetti

Come funziona Access Management

Utilizzare Access Management per stabilire l'autenticazione dell'utente in Unified Manager.

Workflow di configurazione

La configurazione di Access Management funziona come segue:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

   > Per il primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema. La password deve essere impostata al primo accesso.

2. L'amministratore accede a Access Management nell'interfaccia utente, che include ruoli utente locali preconfigurati. Questi ruoli sono un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
   - **Ruoli utente locali** — l'autenticazione viene gestita tramite funzionalità RBAC. I ruoli utente locali includono utenti predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come singolo metodo di autenticazione o in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, ad eccezione dell'impostazione delle password per gli utenti.
   - **Servizi di directory** — l'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft. Un amministratore si connette al server LDAP, quindi associa gli utenti LDAP ai ruoli utente locali.
   - **SAML** — l'autenticazione viene gestita tramite un provider di identità (IdP) utilizzando il linguaggio SAML (Security Assertion Markup Language) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi mappa gli utenti IdP ai ruoli utente locali integrati nell'array di storage.
4. L'amministratore fornisce agli utenti le credenziali di accesso per Unified Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali. Durante l'accesso, il sistema esegue le seguenti attività in background:
   - Autentica il nome utente e la password rispetto all'account utente.
   - Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
   - Fornisce all'utente l'accesso alle funzioni dell'interfaccia utente.
   - Visualizza il nome utente nel banner superiore.

Funzioni disponibili in Unified Manager

L'accesso alle funzioni dipende dai ruoli assegnati a un utente, che includono:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.

- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Una funzione non disponibile è disattivata o non viene visualizzata nell'interfaccia utente.

Terminologia per la gestione degli accessi

Scopri come si applicano i termini di Access Management a Unified Manager.

Termine	Descrizione
Active Directory	Active Directory (ad) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Binding	Le operazioni BIND vengono utilizzate per autenticare i client nel server di directory. Il binding in genere richiede credenziali di account e password, ma alcuni server consentono operazioni di binding anonime.
CIRCA	Un'autorità di certificazione (CA) è un'entità attendibile che emette documenti elettronici, denominati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti Web, consentendo connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli autori degli attacchi di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e l'identità dell'entità attendibile che certifica (firma) queste informazioni.
LDAP	LDAP (Lightweight Directory Access Protocol) è un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi diversi di connettersi al server LDAP per la convalida degli utenti.
RBAC	RBAC (role-based access control) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. Unified Manager include ruoli predefiniti.
SAML	SAML (Security Assertion Markup Language) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata dello storage array è conforme a SAML2.0 per l'asserzione, l'autenticazione e l'autorizzazione dell'identità.
SSO	SSO (Single Sign-on) è un servizio di autenticazione che consente a un set di credenziali di accesso di accedere a più applicazioni.

Termine	Descrizione
Proxy dei servizi Web	Il proxy dei servizi Web, che fornisce l'accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia di Unified Manager è disponibile con Web Services Proxy.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (role-based access control) includono utenti predefiniti con uno o più ruoli mappati. Ogni ruolo include le autorizzazioni per l'accesso alle attività in Unified Manager.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata funzione, tale funzione non è disponibile per la selezione o non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali

Gli amministratori possono utilizzare le funzionalità RBAC (role-based access control) applicate in Unified Manager. Queste funzionalità sono denominate "ruoli utente locali".

Workflow di configurazione

I ruoli utente locali sono preconfigurati nel sistema. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

   Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente predefiniti e non modificabili.
3. Facoltativamente, l'amministratore assegna nuove password per ogni profilo utente.
4. Gli utenti accedono al sistema con le credenziali assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con servizi di directory

Gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.

Workflow di configurazione

Se nella rete vengono utilizzati un server LDAP e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni di amministratore di sicurezza.

   > Il `admin` l'utente ha accesso completo a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il server LDAP. Le impostazioni includono il nome di dominio, l'URL e le informazioni sull'account di binding.
3. Se il server LDAP utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati CA (Certificate Authority) per l'autenticazione tra il server LDAP e il sistema host in cui è installato il proxy dei servizi Web.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli utente locali. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il server LDAP e il proxy dei servizi Web.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungere un server di directory.
- Modificare le impostazioni del server di directory.
- Associare gli utenti LDAP ai ruoli utente locali.
- Rimuovere un server di directory.
- Modificare le password.
- Impostare una lunghezza minima per le password.
- Consentire agli utenti di effettuare l'accesso senza password.

Gestione degli accessi con SAML

Per la gestione degli accessi, gli amministratori possono utilizzare le funzionalità SAML (Security Assertion Markup Language) 2.0 integrate nell'array.

Workflow di configurazione

La configurazione SAML funziona come segue:

1. Un amministratore effettua l'accesso a Unified Manager con un profilo utente che include le autorizzazioni Security Admin.

   > Il `admin` L'utente ha accesso completo a tutte le funzioni di System Manager.

2. L'amministratore accede alla scheda **SAML** in Gestione accessi.
3. Un amministratore configura le comunicazioni con il provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Per configurare le comunicazioni con lo storage array, l'amministratore scarica il file di metadati IdP dal sistema IdP, quindi utilizza Unified Manager per caricare il file nello storage array.
4. Un amministratore stabilisce una relazione di trust tra il service provider e l'IdP. Un service provider controlla l'autorizzazione dell'utente; in questo caso, il controller nell'array di storage agisce come service provider. Per configurare le comunicazioni, l'amministratore utilizza Unified Manager per esportare un file di metadati del provider di servizi per il controller. Dal sistema IdP, l'amministratore importa il file di metadati nell'IdP.

   > Gli amministratori devono inoltre assicurarsi che IdP supporti la capacità di restituire un ID nome all'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi dell'utente definiti nell'IdP. A tale scopo, l'amministratore utilizza Unified Manager per creare le mappature.
6. L'amministratore verifica l'accesso SSO all'URL IdP. Questo test garantisce che lo storage array e IdP possano comunicare.

   > Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

7. Da Unified Manager, l'amministratore abilita SAML per lo storage array.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modificare o creare nuove mappature dei ruoli
- Esportare i file del provider di servizi

Restrizioni di accesso

Quando SAML è attivato, gli utenti non possono rilevare o gestire lo storage per quell'array dall'interfaccia precedente di Storage Manager.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse degli array di storage:

- Finestra Enterprise Management (EMW)

- Interfaccia a riga di comando (CLI)
- Client Software Developer Kit (SDK)
- Client in-band
- Client REST API per l'autenticazione di base HTTP
- Effettuare l'accesso utilizzando l'endpoint REST API standard

Utilizzare ruoli utente locali

Visualizzare i ruoli utente locali

Dalla scheda Local User Roles (ruoli utente locali), è possibile visualizzare le mappature degli utenti ai ruoli predefiniti. Questi mapping fanno parte del RBAC (role-based access control) applicato nel proxy dei servizi Web per Unified Manager.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Gli utenti e le mappature non possono essere modificati. È possibile modificare solo le password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.

   Gli utenti sono mostrati nella tabella:

   - **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli.
   - **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor.
   - **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor.
   - **Ro** (sola lettura) — questo utente include solo il ruolo Monitor.

Modificare le password per i profili utente locali

È possibile modificare le password utente per ciascun utente in Gestione accessi.

Prima di iniziare

- Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.
- È necessario conoscere la password dell'amministratore locale.

A proposito di questa attività

Quando si sceglie una password, tenere presenti le seguenti linee guida:

- Le nuove password utente locali devono soddisfare o superare l'impostazione corrente per una password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostati. Fare attenzione a includere spazi se inclusi nella password.
- Per una maggiore sicurezza, utilizzare almeno 15 caratteri alfanumerici e modificare la password frequentemente.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare un utente dalla tabella.

   Il pulsante Change Password (Modifica password) diventa disponibile.

4. Selezionare **Change Password** (Modifica password).

   Viene visualizzata la finestra di dialogo Change Password (Modifica password).

5. Se non è stata impostata alcuna lunghezza minima per le password utente locali, selezionare la casella di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Immettere la nuova password per l'utente selezionato nei due campi.
7. Immettere la password dell'amministratore locale per confermare l'operazione, quindi fare clic su **Change** (Modifica).

Risultati

Se l'utente è attualmente connesso, la modifica della password provoca l'interruzione della sessione attiva dell'utente.

Modificare le impostazioni della password utente locale

È possibile impostare la lunghezza minima richiesta per tutte le password utente locali nuove o aggiornate. È inoltre possibile consentire agli utenti locali di accedere al sistema senza inserire una password.

Prima di iniziare

Devi essere connesso come amministratore locale, che include le autorizzazioni di amministratore root.

A proposito di questa attività

Tenere presenti queste linee guida quando si imposta la lunghezza minima per le password utente locali:

- Le modifiche apportate non influiscono sulle password utente locali esistenti.
- La lunghezza minima richiesta per le password utente locali deve essere compresa tra 0 e 30 caratteri.
- Le nuove password utente locali devono soddisfare o superare l'impostazione di lunghezza minima corrente.

- Non impostare una lunghezza minima per la password se si desidera che gli utenti locali accedano al sistema senza immettere una password.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **ruoli utente locali**.
3. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Local User Password Settings (Impostazioni password utente locale).

4. Effettuare una delle seguenti operazioni:
   - Per consentire agli utenti locali di accedere al sistema *senza* inserire una password, deselezionare la casella di controllo "Richiedi almeno tutte le password utente locali".
   - Per impostare una lunghezza minima della password per tutte le password utente locali, selezionare la casella di controllo "Richiedi almeno tutte le password utente locali", quindi utilizzare la casella di selezione per impostare la lunghezza minima richiesta per tutte le password utente locali.

     Le nuove password utente locali devono soddisfare o superare l'impostazione corrente.

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

Utilizzare i servizi di directory

Aggiungere il server di directory

Per configurare l'autenticazione per la gestione degli accessi, è necessario stabilire le comunicazioni tra un server LDAP e l'host che esegue il proxy dei servizi Web per Unified Manager. Quindi, associare i gruppi di utenti LDAP ai ruoli utente locali.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

A proposito di questa attività

L'aggiunta di un server di directory è un processo in due fasi. Immettere innanzitutto il nome di dominio e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per l'autenticazione se è firmato da un'autorità di firma non standard. Se si dispone delle credenziali per un account BIND, è anche possibile immettere il nome e la password dell'account utente. Quindi, mappare i gruppi di utenti del server LDAP ai ruoli utente locali.

Fasi

1. Selezionare **Access Management**.
2. Dalla scheda **Directory Services**, selezionare **Add Directory Server** (Aggiungi server di directory).

Viene visualizzata la finestra di dialogo Add Directory Server (Aggiungi server di directory).

3. Nella scheda **Server Settings** (Impostazioni server), immettere le credenziali per il server LDAP.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
Immettere il nome di dominio del server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente@dominio*) per specificare il server di directory da autenticare.	URL del server
Immettere l'URL per l'accesso al server LDAP nel formato `ldap[s]://host:*port*`.	Carica certificato (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato solo se è stato specificato un protocollo LDAPS nel campo URL server sopra riportato. Fare clic su **Browse** (Sfoglia) e selezionare un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati utilizzata per l'autenticazione del server LDAP.	Account BIND (opzionale)
Inserire un account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi. Immettere il nome dell'account in formato LDAP. Ad esempio, se l'utente bindacct è chiamato "bindacct", è possibile immettere un valore come `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Password bind (opzionale)

Impostazione	Descrizione
Questo campo viene visualizzato quando si immette un account BIND. Immettere la password per l'account BIND.	Verificare la connessione al server prima di aggiungerli
Selezionare questa casella di controllo per assicurarsi che il sistema possa comunicare con la configurazione del server LDAP immessa. Il test si verifica dopo aver fatto clic su **Add** (Aggiungi) nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Immettere il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=cpoc, DC=local`.
Attributo Username	Inserire l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Inserire un elenco di attributi di gruppo nell'utente, che viene utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

4. Fare clic sulla scheda **mappatura ruolo**.
5. Assegnare i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
Specificare il nome distinto del gruppo (DN) per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata ({}) se non fanno parte di un modello di espressione regolare:[]()<>*+-=!?^	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli utente locali da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management. • **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

6. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
7. Al termine delle mappature, fare clic su **Aggiungi**.

   Il sistema esegue una convalida, assicurandosi che lo storage array e il server LDAP possano comunicare. Se viene visualizzato un messaggio di errore, selezionare le credenziali inserite nella finestra di dialogo e,

se necessario, immettere nuovamente le informazioni.

Modificare le impostazioni del server di directory e le mappature dei ruoli

Se in precedenza è stato configurato un server di directory in Access Management, è possibile modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e i mapping gruppo-ruolo.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- È necessario definire un server di directory.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **Directory Services**.
3. Se sono stati definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Directory Server Settings (Impostazioni server directory).

5. Nella scheda **Server Settings** (Impostazioni server), modificare le impostazioni desiderate.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio/i
I nomi di dominio dei server LDAP. Per più domini, inserire i domini in un elenco separato da virgole. Il nome di dominio viene utilizzato nel login (*nome utente@dominio*) per specificare il server di directory da autenticare.	URL del server
L'URL per l'accesso al server LDAP nel formato `ldap[s]://host:port`.	Account BIND (opzionale)
L'account utente di sola lettura per le query di ricerca sul server LDAP e per la ricerca all'interno dei gruppi.	Password bind (opzionale)
La password per l'account BIND. (Questo campo viene visualizzato quando viene inserito un account BIND).	Verificare la connessione al server prima di salvare

Impostazione	Descrizione
Verifica che il sistema possa comunicare con la configurazione del server LDAP. Il test si verifica dopo aver fatto clic su **Save** (Salva). Se questa casella di controllo è selezionata e il test non riesce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per ignorare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
Ricerca DN base	Il contesto LDAP per la ricerca degli utenti, in genere sotto forma di `CN=Users, DC=cpoc, DC=local`.
Attributo Username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per il mapping gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

6. Nella scheda **role Mapping**, modificare la mappatura desiderata.

Dettagli del campo

Impostazione	Descrizione
Mapping	DN gruppo
Il nome di dominio del gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata () se non fanno parte di un modello di espressione regolare: []{}()<>*+-=!?^	
Ruoli	I ruoli da mappare al DN del gruppo. È necessario selezionare singolarmente ciascun ruolo che si desidera includere per questo gruppo. Il ruolo di monitoraggio è necessario in combinazione con gli altri ruoli per accedere a Gestione unificata di SANtricity. I ruoli includono: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management. • **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore.

7. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
8. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Rimuovere il server di directory

Per interrompere la connessione tra un server di directory e il proxy dei servizi Web, è possibile rimuovere le informazioni sul server dalla pagina Gestione accessi. È possibile eseguire questa attività se è stato configurato un nuovo server e si desidera rimuovere quello precedente.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Fasi

1. Selezionare **Access Management**.
2. Selezionare la scheda **Directory Services**.
3. Dall'elenco, selezionare il server di directory che si desidera eliminare.
4. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Remove Directory Server (Rimuovi server di directory).

5. Tipo `remove` Nel campo, quindi fare clic su **Rimuovi**.

   Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e i mapping dei ruoli vengono rimossi. Gli utenti non possono più accedere con le credenziali da questo server.

Utilizzare SAML

Configurare SAML

Per configurare l'autenticazione per Access Management, è possibile utilizzare le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un provider di identità e lo storage provider.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o il nome di dominio del controller nell'array di storage.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito la sincronizzazione del clock del controller e del server IdP (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a Unified Manager.

A proposito di questa attività

Un provider di identità (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se tale utente è autenticato correttamente. È possibile configurare IdP in modo da fornire l'autenticazione a più fattori e utilizzare qualsiasi database utente, ad esempio Active Directory. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP. Un service provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, lo storage array agisce come service provider per richiedere l'autenticazione al provider di identità. Per stabilire una connessione tra IdP e lo storage array, è necessario condividere i file di metadati tra queste due entità. Quindi, mappare le entità utente IdP ai ruoli degli array di storage. Infine, prima di attivare SAML, è necessario verificare la connessione e gli accessi SSO.

SAML e Directory Services. Se si attiva SAML quando Directory Services è configurato come metodo di autenticazione, SAML sostituisce Directory Services in Unified Manager. Se si disattiva SAML in un secondo momento, la configurazione dei servizi di directory torna alla configurazione precedente.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

La configurazione dell'autenticazione SAML è una procedura multi-step.

Fase 1: Caricare il file di metadati IdP

Per fornire allo storage array le informazioni di connessione IdP, importare i metadati IdP in Unified Manager. Il sistema IdP ha bisogno di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per validare le risposte ricevute.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.

   La pagina visualizza una panoramica delle fasi di configurazione.

3. Fare clic sul collegamento **Import Identity Provider (IdP) file**.

   Viene visualizzata la finestra di dialogo Importa file provider di identità.

4. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file di metadati IdP copiato nel sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'ID entità IdP.

5. Fare clic su **Importa**.

Fase 2: Esportare i file del provider di servizi

Per stabilire una relazione di trust tra IdP e l'array di storage, importare i metadati del service provider nell'IdP. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il controller ed elaborare le richieste di autorizzazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP, in modo che l'IdP possa comunicare con i service provider.

Fasi

1. Fare clic sul collegamento **Export Service Provider Files**.

Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

2. Inserire l'indirizzo IP o il nome DNS del controller nel campo **Controller A**, quindi fare clic su **Export** per salvare il file di metadati nel sistema locale.

   Dopo aver fatto clic su **Esporta**, i metadati del provider di servizi vengono scaricati nel sistema locale. Prendere nota della posizione in cui è memorizzato il file.

3. Dal sistema locale, individuare il file di metadati del Service Provider in formato XML esportato.
4. Dal server IdP, importare il file di metadati del provider di servizi per stabilire la relazione di trust. È possibile importare il file direttamente o inserire manualmente le informazioni del controller dal file.

Fase 3: Mappare i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a Unified Manager, è necessario mappare gli attributi utente IdP e le appartenenze ai gruppi ai ruoli predefiniti dell'array di storage.

Prima di iniziare

- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Fare clic sul collegamento **mapping dei ruoli di Unified Manager**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

2. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (\) se non fanno parte di un modello di espressione regolare:[]{}()<>*+-=!?^	
Ruoli	Fare clic nel campo e selezionare uno dei ruoli dell'array di storage da mappare all'attributo. È necessario selezionare singolarmente ciascun ruolo da includere. Per accedere a Unified Manager, è necessario il ruolo di monitoraggio in combinazione con gli altri ruoli. Il ruolo Security Admin è richiesto anche per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **Storage admin** — accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Security admin** — accesso alla configurazione della sicurezza in Access Management, gestione dei certificati, gestione dei registri di controllo e possibilità di attivare o disattivare l'interfaccia di gestione legacy (Symbol). • **Support admin** — accesso a tutte le risorse hardware dello storage array, dati di guasto, eventi MEL e aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

3. Se lo si desidera, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.

   I mapping dei ruoli possono essere modificati dopo l'attivazione di SAML.

4. Una volta completate le mappature, fare clic su **Save** (Salva).

Fase 4: Verifica dell'accesso SSO

Per garantire che il sistema IdP e lo storage array possano comunicare, è possibile eseguire un test di accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.

Fasi

1. Selezionare il collegamento **Test SSO Login**.

   Viene visualizzata una finestra di dialogo per l'immissione delle credenziali SSO.

2. Immettere le credenziali di accesso per un utente con permessi di amministratore della sicurezza e di monitoraggio.

   Viene visualizzata una finestra di dialogo durante il test dell'accesso.

3. Cercare il messaggio Test Successful (Test riuscito). Se il test viene completato correttamente, passare alla fase successiva per l'abilitazione di SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

   - L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
   - I metadati caricati per il server IdP sono corretti.
   - L'indirizzo del controller nei file di metadati SP è corretto.

Fase 5: Abilitare SAML

Il passaggio finale consiste nel completare la configurazione SAML per l'autenticazione dell'utente. Durante questo processo, il sistema richiede anche di verificare un accesso SSO. Il processo di test di accesso SSO è descritto nel passaggio precedente.

Prima di iniziare

- Il file di metadati IdP viene importato in Unified Manager.
- Un file di metadati del service provider per il controller viene importato nel sistema IdP per la relazione di trust.
- È stata configurata almeno una mappatura dei ruoli Monitor e Security Admin.

Modifica e disattivazione. una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza.

Fasi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML** (attiva SAML).

   Viene visualizzata la finestra di dialogo Conferma abilitazione SAML.

2. Tipo `enable`, Quindi fare clic su **Enable** (attiva).
3. Immettere le credenziali utente per un test di accesso SSO.

Risultati

Una volta attivato SAML, il sistema termina tutte le sessioni attive e inizia l'autenticazione degli utenti tramite SAML.

Modificare le mappature dei ruoli SAML

Se in precedenza è stato configurato SAML per Access Management, è possibile modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- Un amministratore IdP ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- SAML è configurato e abilitato.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **mappatura ruolo**.

   Viene visualizzata la finestra di dialogo mappatura ruoli.

4. Assegnare gli attributi e i gruppi degli utenti IdP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

   Prestare attenzione a non rimuovere le autorizzazioni mentre SAML è attivato, altrimenti si perde l'accesso a Unified Manager.

Dettagli del campo

Impostazione	Descrizione
Mapping	Attributo dell'utente
Specificare l'attributo (ad esempio, "membro di") per il gruppo SAML da mappare.	Valore dell'attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

> Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

5. Facoltativamente, fare clic su **Add another mapping** (Aggiungi un'altra mappatura) per immettere più mappature gruppo-ruolo.
6. Fare clic su **Save** (Salva).

Risultati

Una volta completata questa attività, tutte le sessioni utente attive vengono terminate. Viene conservata solo la sessione utente corrente.

Esportare i file del provider di servizi SAML

Se necessario, è possibile esportare i metadati del service provider per l'array di storage e reimportare il file nel sistema IdP (Identity Provider).

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- SAML è configurato e abilitato.

A proposito di questa attività

In questa attività, si esportano i metadati dal controller. L'IdP ha bisogno di questi metadati per stabilire una relazione di trust con il controller ed elaborare le richieste di autenticazione. Il file include informazioni come il nome di dominio del controller o l'indirizzo IP che IdP può utilizzare per l'invio delle richieste.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **SAML**.
3. Selezionare **Esporta**.

   Viene visualizzata la finestra di dialogo Esporta file provider di servizi.

4. Fare clic su **Export** (Esporta) per salvare il file di metadati nel sistema locale.

   Il campo del nome di dominio è di sola lettura.

   Prendere nota della posizione in cui è memorizzato il file.

5. Dal sistema locale, individuare il file di metadati del Service Provider in formato XML esportato.
6. Dal server IdP, importare il file di metadati del provider di servizi. È possibile importare il file direttamente o inserire manualmente le informazioni del controller.
7. Fare clic su **Chiudi**.

FAQ

Perché non riesco ad accedere?

Se si riceve un errore durante il tentativo di accesso, esaminare queste possibili cause.

Gli errori di accesso possono verificarsi per uno dei seguenti motivi:

- Il nome utente o la password immessi non sono corretti.
- Privilegi insufficienti.
- Si è tentato di accedere più volte senza successo, attivando la modalità di blocco. Attendere 10 minuti per eseguire nuovamente l'accesso.
- L'autenticazione SAML è attivata. Aggiornare il browser per accedere.

Cosa occorre sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, è necessario soddisfare determinati requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali del server LDAP devono essere disponibili, inclusi il nome di dominio, l'URL del server e, facoltativamente, il nome utente e la password dell'account BIND.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del server LDAP deve essere installata sul computer locale.

Cosa occorre sapere sulla mappatura dei ruoli degli array di storage?

Prima di mappare i gruppi ai ruoli, rivedere le linee guida.

Le funzionalità RBAC (role-based access control) includono i seguenti ruoli:

- **Storage admin** — accesso completo in lettura/scrittura agli oggetti storage sugli array, ma nessun accesso alla configurazione di sicurezza.
- **Security admin** — accesso alla configurazione di sicurezza in Access Management e Certificate Management.
- **Support admin** — accesso a tutte le risorse hardware su storage array, dati di guasto ed eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.

- **Monitor** — accesso in sola lettura a tutti gli oggetti di storage, ma nessun accesso alla configurazione di sicurezza.

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

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e servizi di directory, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Si conoscono i nomi di dominio del gruppo per i gruppi di utenti LDAP.

SAML

Se si utilizzano le funzionalità SAML (Security Assertion Markup Language) integrate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza al gruppo nel sistema IdP.
- Conosci i nomi dei membri del gruppo.
- Si conosce il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali di espressione regolare devono essere escapati con una barra rovesciata (`\`) se non fanno parte di un modello di espressione regolare:

  ```
  \.[]{}()<>*+-=!?^$|
  ```

- Il ruolo Monitor è necessario per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo di monitoraggio presente.

Cosa occorre sapere prima di configurare e abilitare SAML?

Prima di configurare e attivare le funzionalità SAML (Security Assertion Markup Language) per l'autenticazione, assicurarsi di soddisfare i seguenti requisiti e comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurarsi che:

- Nella rete è configurato un provider di identità (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è autenticato correttamente. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi e i gruppi utente nel sistema IdP.
- Un amministratore IdP ha garantito che IdP supporti la capacità di restituire un ID nome all'autenticazione.
- Un amministratore ha garantito la sincronizzazione del clock del controller e del server IdP (tramite un server NTP o regolando le impostazioni del clock del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e disponibile sul sistema locale utilizzato per accedere a Unified Manager.
- Si conosce l'indirizzo IP o il nome di dominio del controller nell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disattivarlo tramite l'interfaccia utente, né modificare le impostazioni IdP. Se è necessario disattivare o modificare la configurazione SAML, contattare il supporto tecnico per assistenza. Si consiglia di testare gli accessi SSO prima di attivare SAML nella fase finale di configurazione. (Il sistema esegue anche un test di accesso SSO prima di attivare SAML).
- Se si disattiva SAML in futuro, il sistema ripristina automaticamente la configurazione precedente (ruoli utente locali e/o servizi di directory).
- Se i servizi di directory sono attualmente configurati per l'autenticazione dell'utente, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse degli array di storage:
  - Finestra Enterprise Management (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client Software Developer Kit (SDK)
  - Client in-band
  - Client REST API per l'autenticazione di base HTTP
  - Effettuare l'accesso utilizzando l'endpoint REST API standard

Quali sono gli utenti locali?

Gli utenti locali sono predefiniti nel sistema e includono autorizzazioni specifiche.

Gli utenti locali includono:

- **Admin** — Amministratore eccellente che ha accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli. La password deve essere impostata al primo accesso.
- **Storage** — l'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Security** — l'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Support** — l'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Monitor** — un utente con accesso in sola lettura al sistema. Questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **rw** (lettura/scrittura) — questo utente include i seguenti ruoli: Amministratore dello storage, amministratore del supporto e monitor. Questo account viene disattivato fino a quando non viene impostata una password.
- **Ro** (sola lettura) — questo utente include solo il ruolo Monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Versioni precedenti

Consultare i collegamenti riportati di seguito per accedere alla documentazione relativa alle versioni precedenti dell'hardware e-Series e del software SANtricity. I collegamenti consentono di accedere a un altro sito di documentazione.

Documentazione hardware per le release precedenti

- "Installare i vassoi dei dischi controller E2712, E2724, E5612, E5624 e i vassoi dei dischi di espansione DE1600 e DE5600"
- "Installare i vassoi dei dischi controller E2760 e E5660 e i vassoi dei dischi di espansione DE6600"
- "Installare gli array flash EF560 e i vassoi di espansione flash DE5600"
- "Installare sistemi meno recenti"
- "Manutenzione di sistemi meno recenti"
- "Aggiunta di un secondo controller a E2600 ed E2700"
- "Modificare o aggiungere protocolli host"
- "Conversione da alimentazione CA a CC"

Documentazione software per le release precedenti

SANtricity versione 11.7

- "Guida di System Manager"
- "Guida di Unified Manager"

SANtricity versione 11.6

- "Guida di System Manager"
- "Guida di Unified Manager"

SANtricity versione 11.5

- "Guida di System Manager"

SANtricity versione 11.4

- "AMW (E2700, E5600/EF560)"
- "GUIDA DI EMW (E2700, E5600/EF560)"

Note legali

Le note legali forniscono l’accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all’indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per i sistemi operativi SANtricity e-Series/EF-Series"