Documentazione sui sistemi e-Series

E-Series Systems

NetApp
March 22, 2024

Sommario

Documentazione sui sistemi e-Series

Note di rilascio

Novità di SANtricity OS

La seguente tabella descrive le nuove funzionalità di SANtricity OS 11.8 per la gestione integrata dei controller EF300, EF600, E2800/EF280 e E5700/EF570.

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.
Cache di lettura SSD aumentata massima	Cache di lettura SSD massima aumentata da 5TB GB a 8TB TB.
Assegna la cache in lettura all-flash a un singolo volume in configurazioni duplex	È ora possibile assegnare tutta la cache in lettura SSD allo stesso volume sui sistemi duplex ogni volta che un singolo volume utilizza l'intera cache SSD.
Numero di serie dell'unità aggiunto alla tabella riepilogativa del profilo dell'array di storage	Il numero di serie dell'unità è stato aggiunto alla tabella di riepilogo dell'unità nel profilo Storage Array.
Aggiunti dom0-misc-log all'ASUP giornaliero	I registri dom0-misc per i controller A e B sono stati aggiunti agli ASP giornalieri.
La porta 443 viene ora utilizzata per impostazione predefinita per la comunicazione tra applicazioni e servizi Web incorporati	La porta 443 viene ora utilizzata per impostazione predefinita quando si comunica con il server Web incorporato. Il `-useLegacyTransferPort` Il comando CLI è stato aggiunto per coloro che invece desiderano utilizzare la porta di trasferimento legacy 8443. Per ulteriori informazioni sul nuovo comando CLI -useLegacyTransferPort, vedere la "Novità di SANtricity CLI".
Capacità di avanzamento della parità del volume di scansione	I seguenti comandi CLI sono stati implementati per supportare operazioni di scansione della parità di volume basate su processi: • Avvia controllo parità volume • Errori del processo di controllo parità del volume di salvataggio • Interrompere il processo di verifica della parità del volume • Mostra processi di controllo parità volume Per ulteriori informazioni sui nuovi comandi CLI di scansione della parità del volume basati sui processi, consultare la "Novità di SANtricity CLI".
Supporto MFA per Unified Manager	Il supporto dell'autenticazione a più fattori (MFA) è ora supportato in Unified Manager.

Nuova funzionalità	Descrizione
Icona di attivazione/disattivazione per la vista hardware anteriore-posteriore	Nella vista hardware di System Manager/Unified Manager, sono ora disponibili le due schede seguenti per controllare la vista anteriore e posteriore: • Scheda Drives (unità) • Scheda Controller e componenti
Plug-in vCenter Storage	Il plug-in vCenter Storage è stato aggiornato per verificarne la compatibilità con la release e-Series 11,80.
Proxy dei servizi Web 6,0	Web Services Proxy è stato aggiornato alla versione 6,0 per la compatibilità con la versione 11,80 di e-Series.
Flag di creazione dei casi ASUP rimosso per gli eventi di superamento della temperatura nominale e massima di e-Series	Il flag di creazione del caso è ora disabilitato per gli eventi di superamento della temperatura nominale e massima che non richiedono alcuna azione.
Flag di creazione priorità caso attivato per l'evento 0x1209 Mel	Viene ora creato un contrassegno di creazione del caso per `MEL_EV_DEGRADE_CHANNEL 0x1209` Evento MEL.

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

Cosa include questo sito

Questo sito contiene informazioni su release, modelli e componenti specifici di e-Series.

Che cosa è incluso	Cosa *non* è incluso
Questo sito contiene informazioni relative alle seguenti release e tipi di componenti: • **Software SANtricity** — versione 11.50 e successive. • **Firmware del controller** — versione 8.50 e successive. • **Tipi di controller** — tutti i modelli E2800, EF280, EF300, E5700, EF570, E EF600. • **Tipi di interfaccia** — Fibre Channel, iSCSI, iSER, SAS e NVMe. • **Sistemi operativi installati sugli host** — Linux, VMware e Windows. Potrebbero essere supportate interfacce e sistemi operativi aggiuntivi. Per ulteriori informazioni, contatta il supporto tecnico.	Questo sito *non* contiene informazioni relative alle release _precedenti alla versione software 11.50 o alla versione firmware 8.50. Per le versioni precedenti, visitare il "E-Series e risorse di documentazione SANtricity" pagina. Per informazioni sui requisiti di preparazione del sito, visitare il sito Web all'indirizzo "NetApp Hardware Universe".

Scopri di più sui sistemi e-Series

Terminologia e-Series

Scopri di più sui termini utilizzati in e-Series.

Termine	Descrizione
controller	Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni.
configurazioni duplex/simplex	Il duplex è una configurazione a due moduli controller all'interno dello storage array. Simplex è una configurazione a modulo controller singolo.
DISCO RIGIDO	I dischi rigidi (HDD) sono dispositivi di storage dei dati che utilizzano dischi metallici rotanti con rivestimento magnetico.

Termine	Descrizione
HIC	Una scheda di interfaccia host (HIC) collega l'array all'host. Può essere installato in via opzionale all'interno di un contenitore del controller.
IB	InfiniBand (IB) è uno standard di comunicazione per la trasmissione dei dati tra server e sistemi storage dalle performance elevate.
IOPS	Gli IOPS sono operazioni di input/output al secondo.
mirroring	Il mirroring è la replica dei volumi di dati su storage array separati per garantire la disponibilità continua.
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.
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.
Unità rack (U)	Un'unità rack (abbreviata U) è un'unità di misura definita come 44.50 millimetri (1.75 pollici).
SAS	Serial Attached SCSI (SAS) è un protocollo seriale point-to-point che collega i controller direttamente ai dischi.
ROCE	RDMA over Converged Ethernet (RoCE) è un protocollo di rete che consente l'accesso remoto diretto alla memoria (RDMA) su una rete Ethernet.
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.
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.

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.
array di storage	Uno storage array include shelf, controller, dischi, software e firmware.
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.
carico di lavoro	Un workload è un oggetto storage che supporta un'applicazione. Per alcune applicazioni, System Manager 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.

Panoramica dell'hardware e-Series

Gli storage array e-Series sono disponibili in diverse configurazioni e modelli.

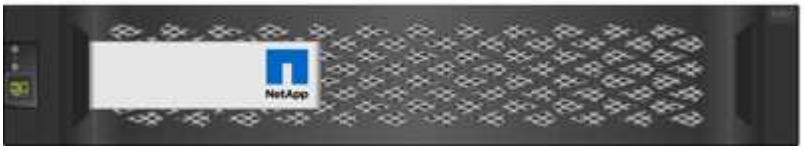
Uno storage array include shelf, controller, dischi, software e firmware. L'array può essere installato in un rack o cabinet, con hardware personalizzabile per uno o due controller, in uno shelf da 12, 24 o 60 dischi. È possibile collegare lo storage array a UNA SAN da diversi tipi di interfaccia e a diversi sistemi operativi host.

Gli array e-Series sono disponibili nei seguenti modelli:

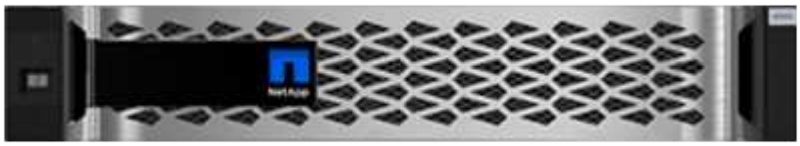
- Serie E2800 — ibrido entry-level
- Serie EF280 — all flash entry-level
- Serie EF300 — all flash entry-level, all NVMe
- Serie E5700 — ibrido midrange
- Serie EF570 — all flash midrange
- Serie EF600 — midrange all flash, all NVMe

> Per SANtricity OS 11,80GA e versioni successive, tutte le porte USB sono disattivate su E2800, EF280, E5700, EF570, EF600, e EF300.

Modelli E2800

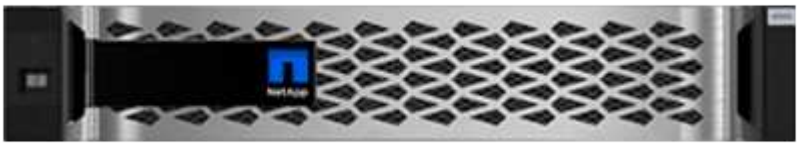
Componente	Specifica
Dimensioni rack:	• 2U12 (2 unità rack; 12 unità) • 2U24 (2 unità rack; 24 unità)  • 4U60 (4 unità rack; 60 unità) 
Dischi:	Supporta i seguenti tipi di dischi: • NL-SAS da 3.5" (fino a 180) • SSD SAS da 2.5" (fino a 120) • HDD SAS da 2.5" (fino a 180)
Interfacce:	Disponibile con le seguenti interfacce: • SAS 12 GB • ISCSI da 10 GB o 25 GB • Fibre Channel da 16 GB o 32 GB

Modelli EF280

Componente	Specifica
Dimensioni rack:	2U24 (2 unità rack; 24 unità) 
Dischi:	Supporta fino a 96 unità SSD da 2.5"

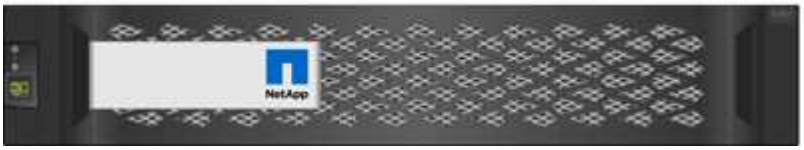
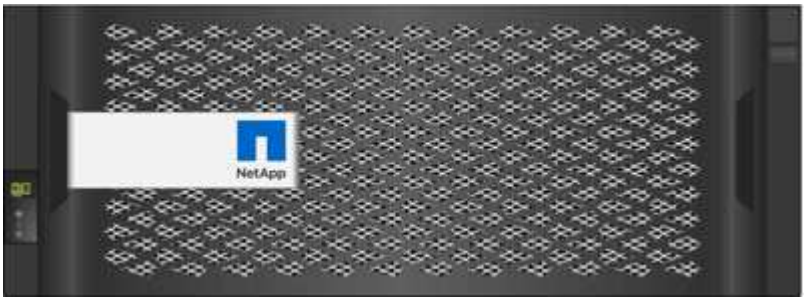
Componente	Specifica
Interfacce:	Disponibile con le seguenti interfacce: • SAS 12 GB • ISCSI da 10 GB o 25 GB • Fibre Channel da 16 GB o 32 GB

Modelli EF300

Componente	Specifica
Dimensioni rack:	2U24 (2 unità rack; 24 unità) 
Dischi e HICS:	Supporta i seguenti dischi con una singola scheda di interfaccia host (HIC) per controller: • Unità SSD NVMe: Fino a 24 unità SSD NVMe nello shelf del controller. • Unità NL-SAS con shelf di espansione: Qualsiasi combinazione di shelf DE212C e DE460C non deve superare un totale di 240 slot per unità NL-SAS e 4 shelf di espansione, a meno che non si utilizzino solo shelf DE212C, sono consentiti 8 shelf DE212C. Ad esempio, 4 shelf DE460C o 8 shelf DE212C o 2 shelf DE460C più 2 shelf DE212. • Unità SSD SAS con shelf di espansione: Qualsiasi combinazione di shelf DE212C, DE224C e DE460C non deve superare un totale di 96 slot per unità SSD SAS e 4 shelf di espansione, a meno che non vengano utilizzati solo shelf DE212C, sono consentiti 8 shelf DE212C. Ad esempio, 1 shelf DE460C più 1 shelf DE224C più 1 shelf DE212C o 4 shelf DE224C o 8 shelf DE212C. Per SANtricity OS 11,80GA e versioni successive, EF300 supporta le configurazioni di shelf di espansione senza dischi nello slot di base Quando si utilizza questa configurazione, assicurarsi che le unità siano inserite nello shelf di espansione e collegate correttamente al vassoio di base prima di accendere il sistema.

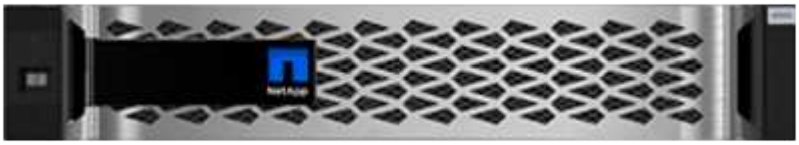
Componente	Specifica
Interfacce:	Disponibile con le seguenti interfacce: • 25 GB iSCSI • 32 GB NVMe/Fibre Channel • SCSI/Fibre Channel da 32 GB • ISER/IB da 100 GB • 100 GB SRP/IB • 100 GB NVMe/IB • 100 GB NVMe/RoCE

Modelli E5700

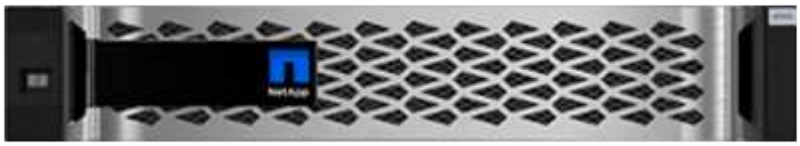
Componente	Specifica
Dimensioni rack:	• 2U24 (2 unità rack; 24 unità)  • 4U60 (4 unità rack; 60 unità) 
Dischi:	Supporta fino a 480 dei seguenti tipi di dischi: • Dischi NL-SAS da 3.5" • Unità SSD SAS da 2.5" • Unità HDD SAS da 2.5"

Componente	Specifica
Interfacce:	Disponibile con le seguenti interfacce: • SAS 12 GB • ISCSI da 10 GB o 25 GB • Fibre Channel da 16 GB o 32 GB • 32 GB NVMe/Fibre Channel • ISER/IB da 100 GB • 100 GB SRP/IB • 100 GB NVMe/IB • 100 GB NVMe/RoCE

Modelli EF570

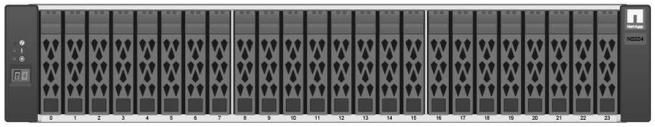
Componente	Specifica
Dimensioni rack:	2U24 (2 unità rack; 24 unità) 
Dischi:	Supporta fino a 120 unità SSD da 2.5"
Interfacce:	Disponibile con le seguenti interfacce: • SAS 12 GB • ISCSI da 10 GB o 25 GB • Fibre Channel da 16 GB o 32 GB • 32 GB NVMe/Fibre Channel • ISER/IB da 100 GB • 100 GB SRP/IB • 100 GB NVMe/IB • 100 GB NVMe/RoCE

Modelli EF600

Componente	Specifica
Dimensioni rack:	2U24 (2 unità rack; 24 unità) 
Dischi e HICS:	Supporta i seguenti dischi con una singola scheda di interfaccia host (HIC) per controller: • Unità SSD NVMe: Fino a 24 unità SSD NVMe nello shelf del controller. • Unità NL-SAS con shelf di espansione: Qualsiasi combinazione di shelf DE212C e DE460C non deve superare un totale di 420 slot per unità NL-SAS e 7 shelf di espansione, a meno che non si utilizzino solo shelf DE212C, sono consentiti 8 shelf DE212C. Ad esempio, 7 shelf DE460C o 8 shelf DE212C o 5 shelf DE460C più 2 shelf DE212. • Unità SSD SAS con shelf di espansione: Qualsiasi combinazione di shelf DE212C, DE224C e DE460C non deve superare un totale di 96 slot per unità SSD SAS e 7 shelf di espansione, a meno che non vengano utilizzati solo shelf DE212C, sono consentiti 8 shelf DE212C. Ad esempio, 1 shelf DE460C più 1 shelf DE224C più 1 shelf DE212C o 4 shelf DE224C o 8 shelf DE212C Per SANtricity OS 11,80GA e versioni successive, EF600 supporta le configurazioni di shelf di espansione senza dischi nello slot di base Quando si utilizza questa configurazione, assicurarsi che le unità siano inserite nello shelf di espansione e collegate correttamente al vassoio di base prima di accendere il sistema.
Interfacce:	Disponibile con le seguenti interfacce: • 25 GB iSCSI • 32 GB NVMe/Fibre Channel • SCSI/Fibre Channel da 32 GB • ISER/IB da 100 GB • 100 GB SRP/IB • 100 GB NVMe/IB • 100 GB NVMe/RoCE • ISER/IB da 200 GB • 200 GB NVMe/IB • 200 GB NVMe/RoCE

Tipi di shelf e-Series

I sistemi e-Series sono disponibili in una vasta gamma di formati di shelf.

Tipo di shelf	Illustrazione
• DE212C:* • 2u12 (2 unità rack; 12 unità) • HDD da 3.5" e/o SSD da 2.5" (con adattatore) • Solo controller E2800	
• DE224C:* • 2u24 (2 unità rack; 24 unità) • HDD da 2.5" e/o SSD da 2.5" • Controller E2800, EF280, E5700 e EF570	
• DE460C:* • 4u60 (4 unità rack; 60 unità) • Dischi da 3.5" e 2.5" (NL-SAS, SAS e SSD) • Controller E2800 ed E5700	
• NE224:* • 2u24 (2 unità rack; 24 unità) • Unità SSD NVMe da 2.5" • Controller EF300 e EF600	

Panoramica del software SANtricity

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

Il software SANtricity è costituito da queste interfacce di gestione:

- System Manager — interfaccia basata su web utilizzata per gestire un controller in un array di storage.
- Unified Manager: Interfaccia basata su web utilizzata per visualizzare e gestire tutti gli array di storage della rete.
- Proxy dei servizi Web - API REST utilizzata per visualizzare e gestire tutti gli array di storage nella rete.
- Command line Interface (CLI) - un’applicazione software per la configurazione e il monitoraggio degli array di storage.

> Gli storage array EF600 e EF300 non supportano funzionalità di mirroring, thin volumi o SSD cache.

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.

Proxy dei servizi web SANtricity

Web Services Proxy è un server API RESTful in grado di gestire centinaia di array e-Series nuovi e legacy. Il proxy viene installato separatamente su un server Windows o Linux.

I servizi Web includono la documentazione API che consente di interagire direttamente con L'API REST. Per accedere alla documentazione API dei servizi Web, aprire un browser e immettere l'URL che punta al server in cui è installato il proxy dei servizi Web.

Interfaccia a riga di comando (CLI)

L'interfaccia a riga di comando (CLI) è un'applicazione software che consente di configurare e monitorare gli array di storage. Utilizzando la CLI, è possibile eseguire i comandi da un prompt del sistema operativo, ad esempio il prompt di DOS C:, un percorso del sistema operativo Linux o un percorso del sistema operativo Solaris.

Video e-Series

Accedi alle demo video per saperne di più sui sistemi e-Series.

E-Series: Storage rapido, semplice e affidabile

Questo video evidenzia i vantaggi principali derivanti dall'utilizzo dei sistemi NetApp e-Series rispetto all'utilizzo di server commodity per lo storage.

"Video NetApp: Vantaggi principali derivanti dall'utilizzo dei sistemi NetApp e-Series rispetto all'utilizzo di server commodity per lo storage"

System Manager: Installazione e configurazione semplificate

Questa demo tecnica mostra come l'interfaccia di gestione del sistema SANtricity basata su web consente una facile configurazione e configurazione di NetApp E2800.

"Video NetApp: Gestore di sistema SANtricity: Configurazione e installazione semplici"

Guida rapida per e-Series

Per essere operativi con i sistemi e-Series, è necessario installare componenti hardware, configurare i sistemi host e configurare lo storage.

1 **Installare l'hardware**

Per installare l'hardware e-Series, accedere alle istruzioni di installazione e configurazione per lo storage array e il tipo di shelf:

- "Serie EF600 o EF300 con shelf da 24 dischi"
- "Serie E2800/EF280 o E5700/EF570 con shelf da 12 o 24 dischi"
- "Serie E2800 o E5700 con shelf da 60 dischi"

2 Configurare l'armadietto

Se si sta configurando un nuovo cabinet per lo storage array, è necessario spostare il cabinet nella posizione permanente, installare l'hardware e collegarlo a una fonte di alimentazione. Per configurare il cabinet, accedere alle seguenti istruzioni:

- "Installare il cabinet 3040 40U"

3 Installare le guide

Al momento della spedizione, ogni shelf include hardware per il montaggio in rack. Per istruzioni dettagliate sull'installazione delle guide, selezionare i tipi di guide:

- "Installare le guide di supporto regolabili"
- "Installare l'enclosure 2U in un rack a quattro montanti"
- "Installare lo shelf DE224C in un rack a due montanti"
- "Installazione di SuperRail in un rack a quattro montanti (shelf DE224C/DE460C)"

4 Collegare i cavi

Le istruzioni di installazione e configurazione (fase 1) includono istruzioni per il collegamento dei cavi. Tuttavia, se sono necessari elenchi di cavi e ricetrasmettitori supportati, Best practice per il cablaggio e informazioni dettagliate sulle porte host del controller, accedere alle seguenti istruzioni:

- "Hardware Cable e-Series"

5 Configurare gli host

Per rendere lo storage disponibile a un host, selezionare una guida per il tipo di sistema operativo dell'host:

- "Configurazione di Linux Express"
- "Configurazione di VMware Express"
- "Configurazione di Windows Express"

6 Configurare lo storage

Per configurare lo storage, è possibile accedere all'interfaccia basata su Web, System Manager, puntando un browser all'indirizzo IP del controller. L'installazione guidata consente di iniziare a configurare il sistema. In alternativa, è possibile utilizzare anche l'interfaccia della riga di comando (CLI).

Selezionare l’interfaccia che si desidera utilizzare:

- "Guida in linea di Gestore di sistema SANtricity per 11.8x"
- "Guida in linea di Gestione sistemi SANtricity per 11.7x"
- "Guida in linea di Gestione sistemi SANtricity per 11,6x"

Installare l’hardware

EF300 ed EF600

Installare e configurare i sistemi storage EF300 e EF600

Scopri come installare e configurare il sistema storage EF300 o EF600.

È possibile scegliere uno dei seguenti formati per l’installazione e la configurazione del nuovo sistema di storage.

- **PDF**

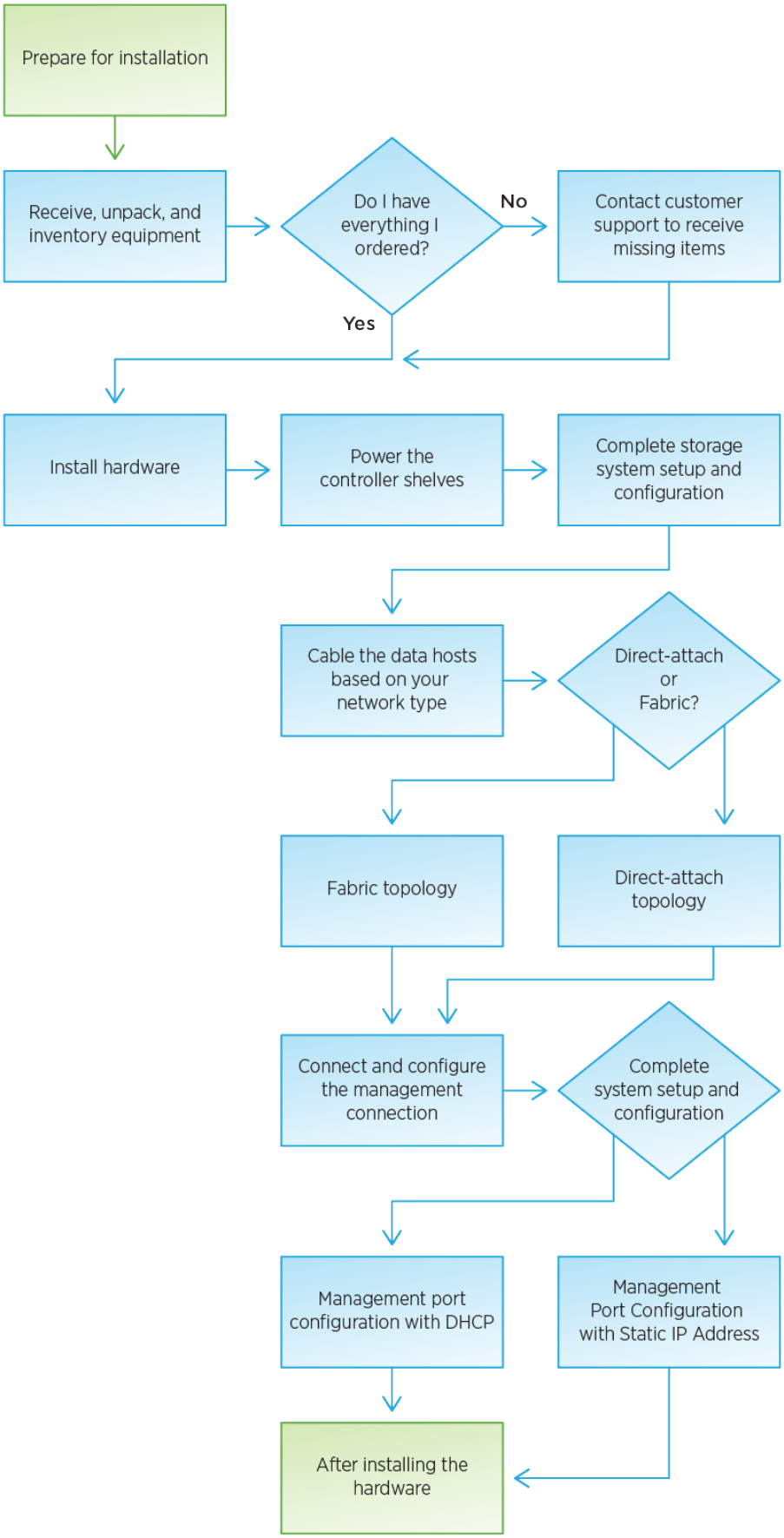
  Questo è un "Poster in formato PDF" di istruzioni passo-passo con collegamenti in tempo reale a contenuti aggiuntivi.

- **Istruzioni online**

  Di seguito sono riportate le istruzioni di installazione online descritte in questo sito. Inizia con Preparazione per l’installazione per iniziare.

Processo di installazione

Prima di installare e configurare il nuovo sistema storage, acquisire familiarità con il processo di installazione:


Prepare for installation
Receive, unpack, and inventory equipment
Do I have everything I ordered?
No
Contact customer support to receive missing items
Yes
Install hardware
Power the controller shelves
Complete storage system setup and configuration
Cable the data hosts based on your network type
Direct-attach or Fabric?
Fabric topology
Direct-attach topology
Connect and configure the management connection
Complete system setup and configuration
Management port configuration with DHCP
Management Port Configuration with Static IP Address
After installing the hardware

Preparazione per l'installazione

Scopri come prepararti per l'installazione del tuo sistema storage EF300 o EF600.

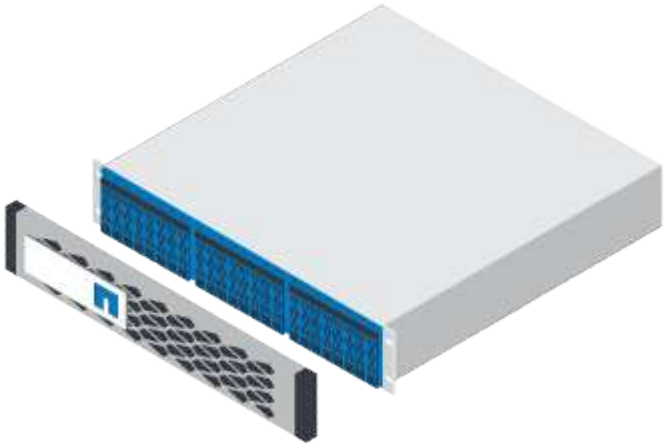
Prima di iniziare

Se si sta cablando EF300 per l'espansione SAS, consultare le seguenti informazioni:

- "Aggiungere schede di espansione SAS" Per l'installazione della scheda di espansione SAS.
- "Panoramica dei cavi" Per il cablaggio di espansione SAS.

Fasi

1. Creare un account e registrare l'hardware all'indirizzo "Supporto NetApp".
2. Assicurarsi che nella confezione ricevuta siano presenti i seguenti elementi.


Shelf con dischi installati (pannello e cappucci terminali confezionati separatamente)

Hardware per il montaggio in rack

La seguente tabella identifica i tipi di cavi che potrebbero essere ricevuti. Se si riceve un cavo non elencato nella tabella, vedere "Hardware Universe" individuare il cavo e identificarne l'utilizzo.

Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi Ethernet RJ-45 (se ordinati)	Connessione di gestione

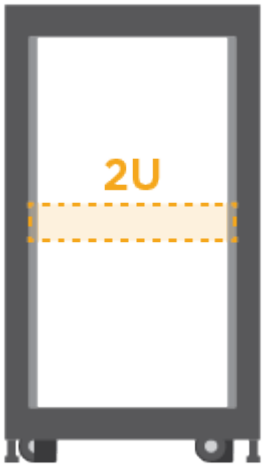
Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi i/o (se ordinati)	Cablaggio degli host di dati
	Cavi di alimentazione (se ordinati)	Accensione del sistema storage

3. Assicurarsi di fornire i seguenti elementi.


Cacciavite Phillips n. 2

Torcia

Braccialetto ESD



Spazio rack 2U: Uno standard da 19" Rack da 48.30 cm per rack 2U delle seguenti dimensioni.

Profondità: 19.0" (48.3 cm)

Larghezza: 17.6" (44.7 cm)

Altezza: 3.34" (8.48 cm)

Shelf: 24 dischi

Peso massimo: 27.4 kg (60.5 lb)

L'utilizzo di cabinet di terze parti potrebbe causare la limitazione dell'accesso al controller da parte dei cavi di alimentazione.

Un browser supportato per il software di gestione:

- Google Chrome (versione 89 e successive)
- Microsoft Edge (90 e versioni successive)
- Mozilla Firefox (versione 80 e successive)
- Safari (versione 14 e successive)

Installare l’hardware

È possibile installare un sistema storage EF300 o EF600 in un rack a due montanti o in un cabinet di sistema NetApp.

Prima di iniziare

Assicurarsi di eseguire le seguenti operazioni:

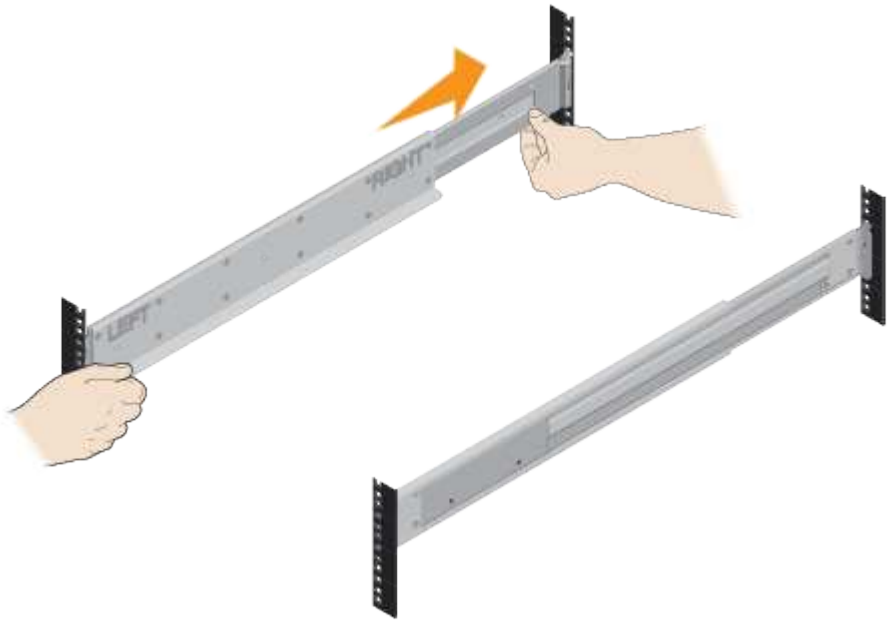
- Registrare l’hardware all’indirizzo "Supporto NetApp".
- Preparare un’area di lavoro piana e priva di elettricità statica.
- Adottare precauzioni antistatiche.

Fasi

1. Disimballare l’hardware.
   a. Disimballare il contenuto e inventariare l’hardware contenuto in base alla distinta di imballaggio.
   b. Prima di procedere, leggere tutte le istruzioni.
2. Montare le guide.

   Per evitare che l’apparecchiatura si rovescii, installare l’hardware dal fondo del rack o dell’armadietto fino alla parte superiore.

   Se le istruzioni sono state fornite con l’hardware per il montaggio in rack, fare riferimento a tali istruzioni per informazioni su come installare le guide. Per ulteriori istruzioni sul montaggio in rack, vedere "Hardware per il montaggio in rack".

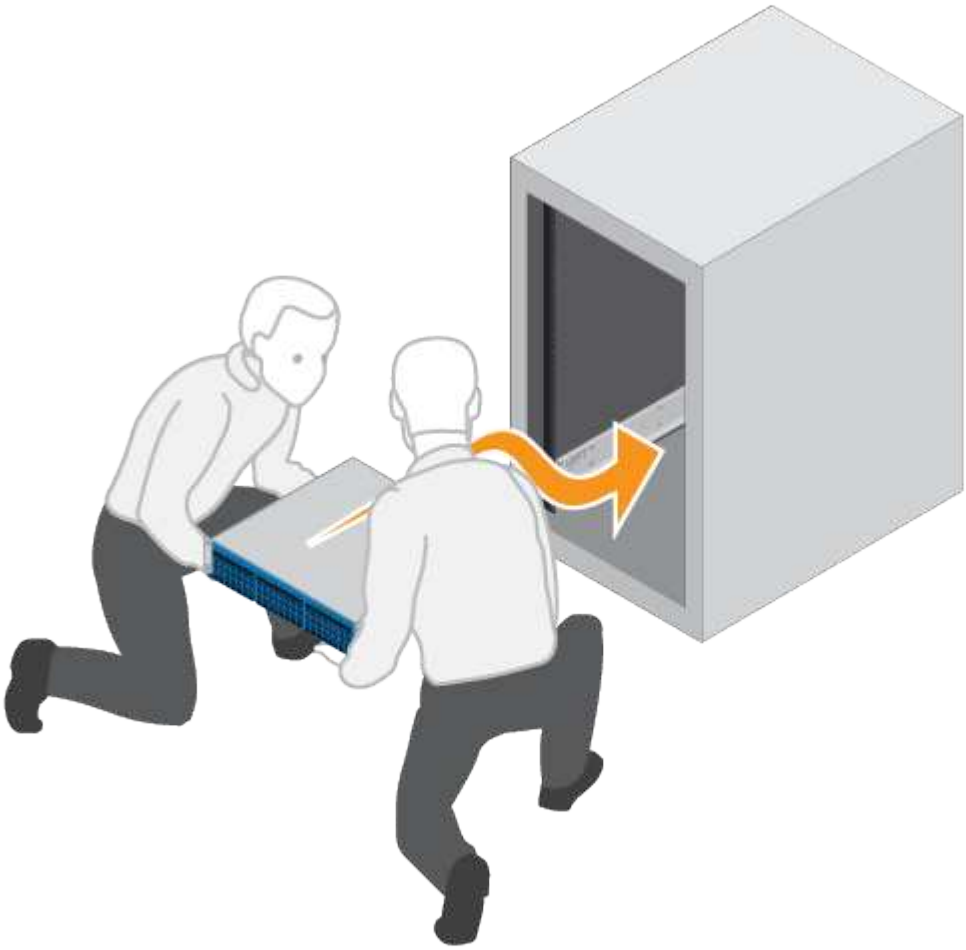
   

3. Installare lo shelf.

a. Se si installano più shelf, iniziare l'installazione dal basso verso la parte superiore del cabinet. Posizionare il retro del ripiano sulle guide.

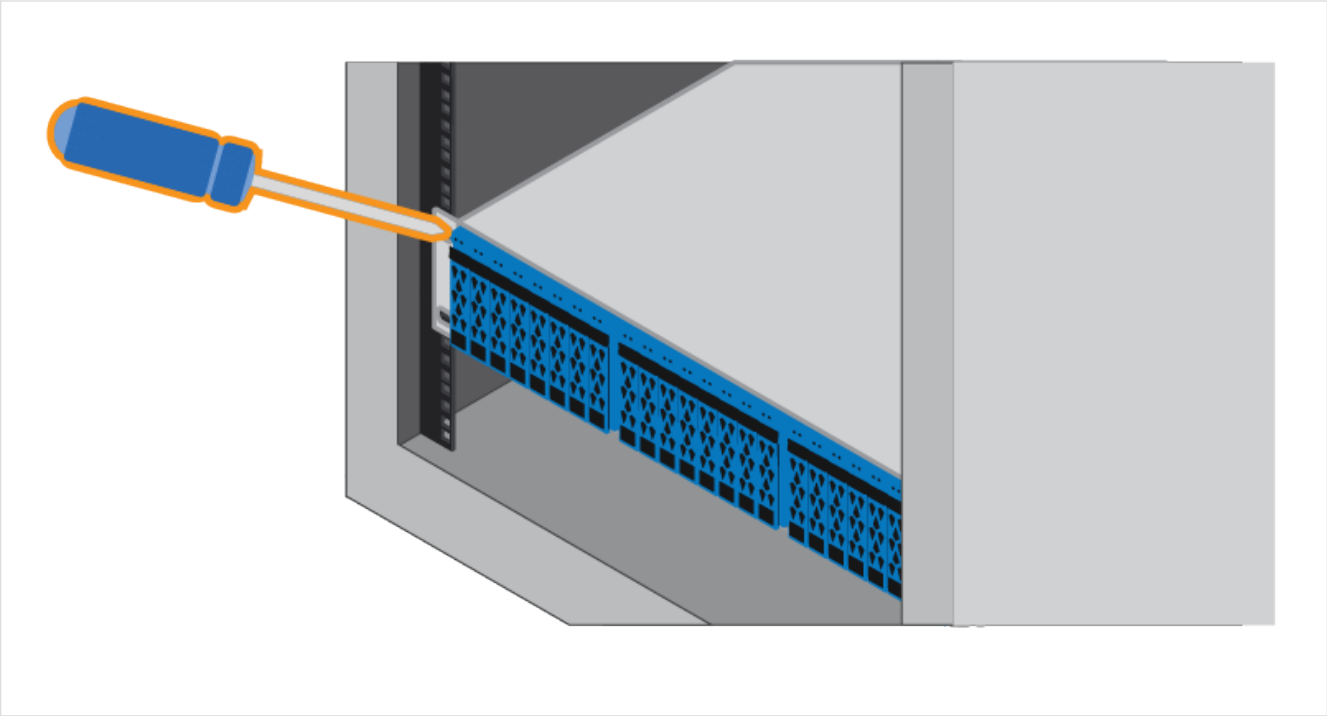
> Quando si installa lo shelf, utilizzare un team-lift con due persone.

b. Sostenendo lo shelf dal basso, farlo scorrere nel cabinet.



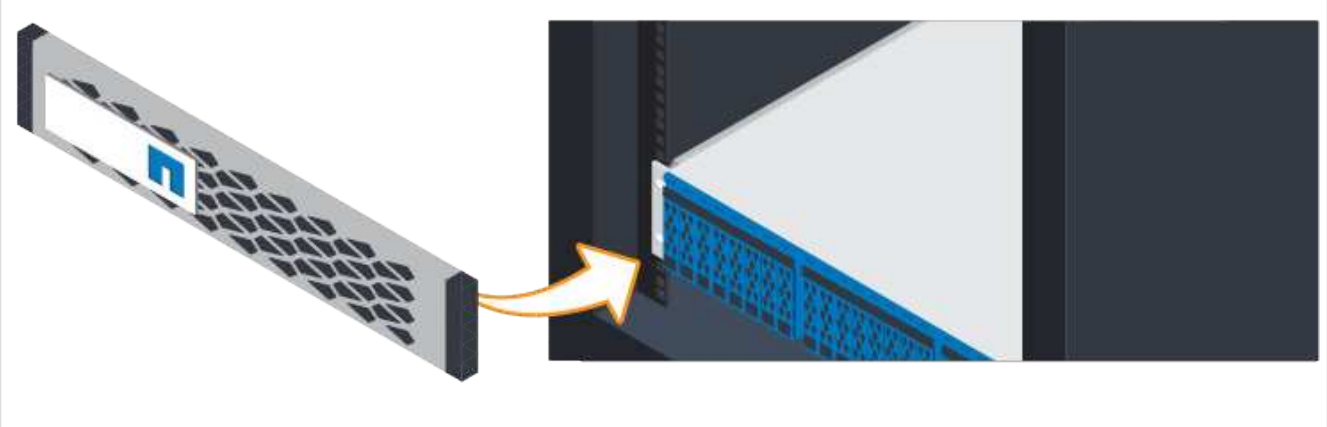
4. Fissare lo shelf.

Per ulteriori informazioni, vedere "Hardware per il montaggio in rack".



5. Installare la mascherina.

   a. Allineare la piastra anteriore allo scaffale e farla scattare in posizione.



Alimentare gli shelf dei controller

Scopri come collegare i cavi di alimentazione e alimentare gli shelf di dischi.

Prima di iniziare

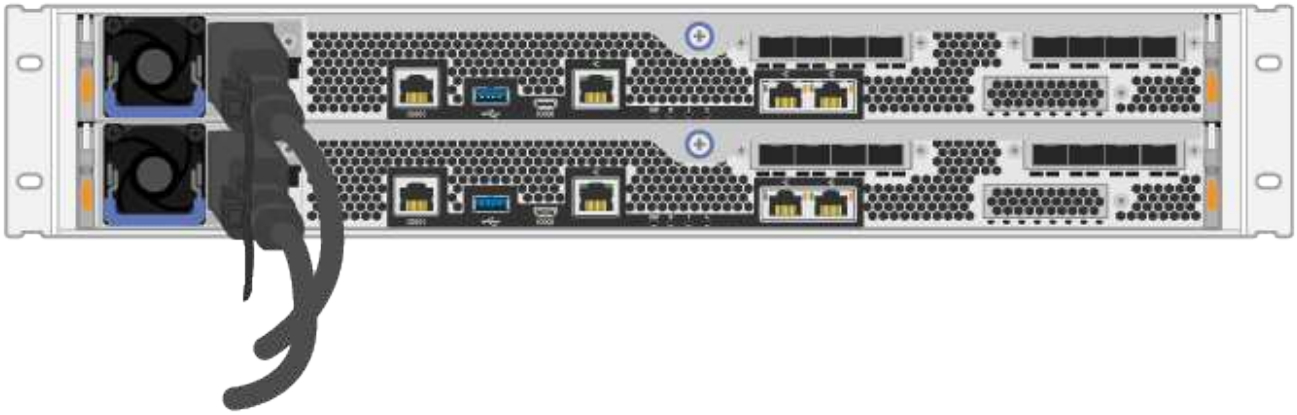
Assicurarsi di effettuare le seguenti operazioni:

- Installare l'hardware.
- Adottare precauzioni antistatiche.

Fasi

1. Collegare i cavi di alimentazione, uno a ciascun controller (EF600 mostrato di seguito).

Cavi di alimentazione



2. Collegare i due cavi di alimentazione, uno per ciascun controller, a due unità di distribuzione dell'alimentazione (PDU) separate nell'armadio o nel rack.

> L'accesso a un contenitore di controller EF300 o EF600 dallo shelf può essere bloccato da PDU di terze parti. Non utilizzare prese di corrente direttamente dietro il contenitore del controller.

3. Attendere cinque minuti per avviare il controller prima di completare la configurazione e la configurazione del sistema di storage.

Risultato

Il controller si avvia automaticamente. I LED lampeggiano e le ventole iniziano a indicare che il controller è in fase di accensione.

> Le ventole sono molto rumorose quando si accende per la prima volta.

Configurazione e configurazione complete del sistema storage

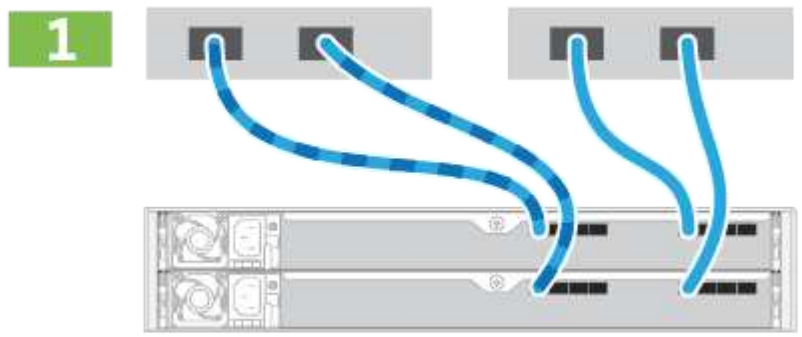
Informazioni su come collegare i cavi del controller alla rete, quindi completare l'installazione e la configurazione.

Fase 1: Collegare via cavo gli host dati

Collegare il sistema storage in base alla topologia di rete.

Opzione 1: Topologia a collegamento diretto

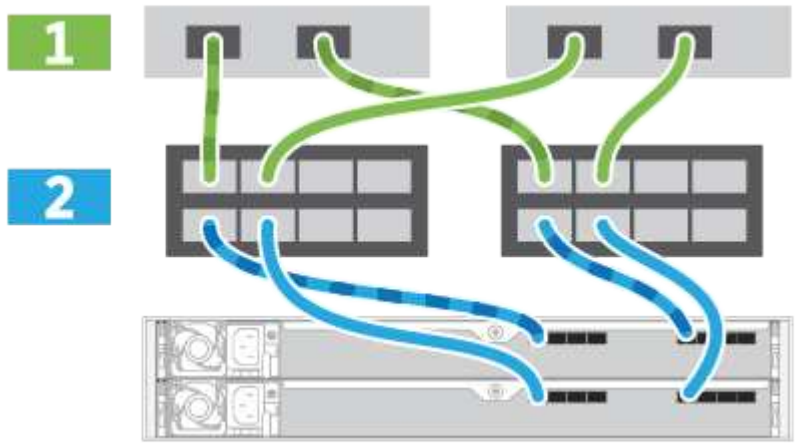
Nell'esempio seguente viene illustrato il collegamento dei cavi agli host di dati utilizzando una topologia a collegamento diretto.



1. Collegare ciascun adattatore host direttamente alle porte host dei controller.

Opzione 2: Topologia del fabric

Nell'esempio seguente viene illustrato il collegamento degli host di dati mediante una topologia fabric.



1. Collegare ciascun adattatore host direttamente allo switch.
2. Collegare ogni switch direttamente alle porte host dei controller.

Fase 2: Connessione e configurazione della connessione di gestione

È possibile configurare le porte di gestione del controller utilizzando un server DHCP o un indirizzo IP statico.

Opzione 1: Server DHCP

Scopri come configurare le porte di gestione con un server DHCP.

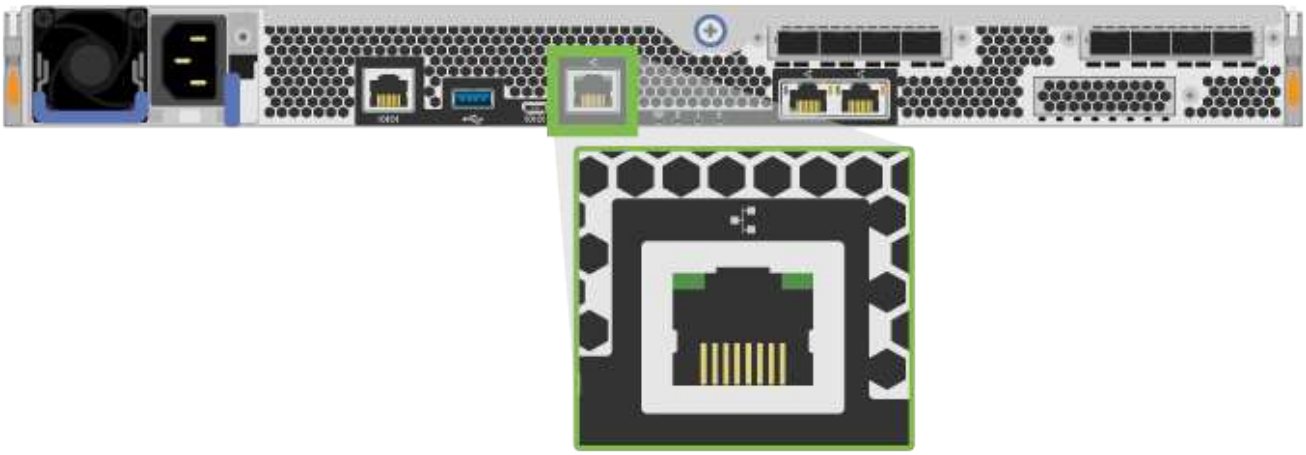
Prima di iniziare

- Configurare il server DHCP per associare un indirizzo IP, una subnet mask e un indirizzo gateway come lease permanente per ciascun controller.
- Ottenere gli indirizzi IP assegnati che si desidera utilizzare per connettersi al sistema di storage dall'amministratore di rete.

Fasi

1. Collegare un cavo Ethernet alla porta di gestione di ciascun controller e l'altra estremità alla rete.


Cavi Ethernet RJ-45 (se ordinati)

La figura seguente mostra un esempio della posizione della porta di gestione del controller (EF600 mostrato):


2. Aprire un browser e connettersi al sistema di storage utilizzando uno degli indirizzi IP del controller forniti dall'amministratore di rete.

Opzione 2: Indirizzo IP statico

Informazioni su come configurare manualmente le porte di gestione immettendo l'indirizzo IP e la subnet mask.

Prima di iniziare

- Richiedere all'amministratore di rete l'indirizzo IP, la subnet mask, l'indirizzo del gateway e le informazioni relative al server DNS e NTP dei controller`.
- Assicurarsi che il portatile in uso non riceva la configurazione di rete da un server DHCP.

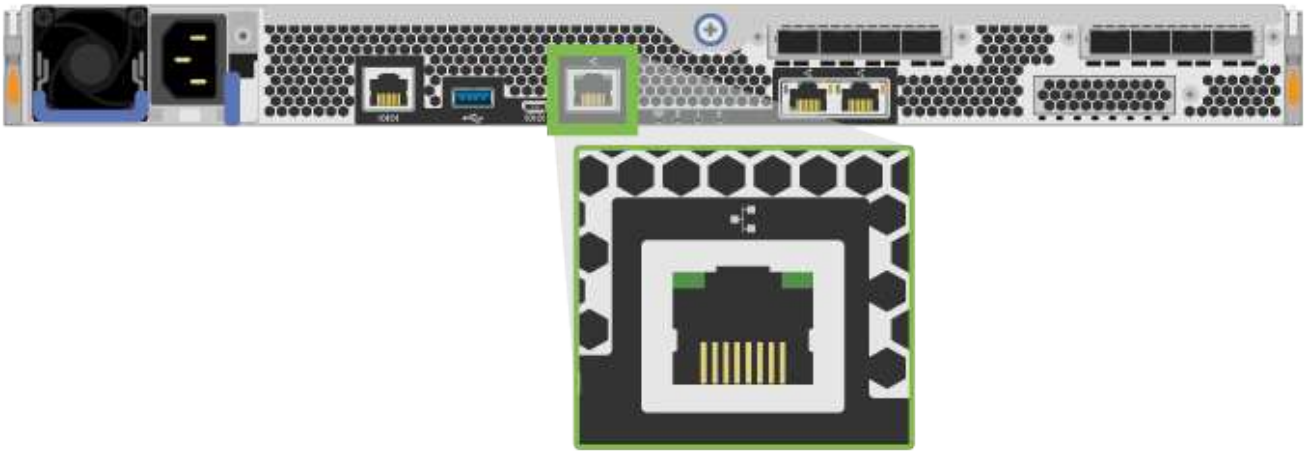
Fasi

1. Utilizzando un cavo Ethernet, collegare la porta di gestione Del controller A alla porta Ethernet di un laptop.

> Il controller A è il contenitore del controller superiore e il controller B è il contenitore del controller inferiore.

	
Cavi Ethernet RJ-45 (se ordinati)	

La figura seguente mostra un esempio della posizione della porta di gestione del controller (EF600 mostrato):



2. Aprire un browser e utilizzare l'indirizzo IP predefinito (169.254.128.101) per stabilire una connessione al controller. Il controller restituisce un certificato autofirmato. Il browser informa che la connessione non è sicura.
3. Seguire le istruzioni del browser per procedere e avviare Gestione di sistema di SANtricity.

   Se non si riesce a stabilire una connessione, verificare di non ricevere la configurazione di rete da un server DHCP.

4. Impostare la password di accesso del sistema di storage.
5. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller A, quindi selezionare **fine**.

   Poiché l'indirizzo IP viene ripristinato, System Manager perde la connessione al controller.

6. Scollegare il laptop dal sistema storage e collegare la porta di gestione del controller A alla rete.
7. Aprire un browser su un computer connesso alla rete e immettere l'indirizzo IP appena configurato del controller A.

   Se si perde la connessione al controller A, è possibile collegare un cavo ethernet al controller B per ristabilire la connessione al controller A attraverso il controller B (169.254.128.102).

8. Accedere utilizzando la password impostata in precedenza.

   Viene visualizzata la procedura guidata Configure Network Settings (Configura impostazioni di rete).

9. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller B, quindi selezionare **fine**.
10. Collegare il controller B alla rete.
11. Convalidare le impostazioni di rete del controller B immettendo l'indirizzo IP configurato del controller B in un browser.

> Se si perde la connessione al controller B, è possibile utilizzare la connessione precedentemente convalidata al controller A per ristabilire la connessione al controller B attraverso il controller A.

Fase 3: Configurazione del sistema storage

Dopo aver installato l'hardware EF300 o EF600, utilizzare il software SANtricity per configurare e gestire il sistema storage.

Prima di iniziare

- Configurare le porte di gestione.
- Verificare e registrare la password e gli indirizzi IP.

Fasi

1. Collegare il controller a un browser Web.
2. Utilizza Gestore di sistema SANtricity per gestire il tuo sistema storage EF300 o EF600. Consultare la guida in linea inclusa in System Manager.

Per accedere a System Manager, utilizzare gli stessi indirizzi IP utilizzati per configurare le porte di gestione.

Se si sta cablando EF300 per l'espansione SAS, vedere "Manutenzione dell'hardware EF600" Per l'installazione della scheda di espansione SAS e di "Cablaggio dell'hardware e-Series" Per il cablaggio di espansione SAS.

E2800 ed E5700

Installare e configurare i sistemi storage E2800 ed E5700

Scopri come installare e configurare il sistema storage E2800 o E5700.

È possibile scegliere uno dei seguenti formati per l'installazione e la configurazione del nuovo sistema di storage.

- **PDF**

  Questo è un PDF stampabile di istruzioni passo-passo con collegamenti in tempo reale a contenuti aggiuntivi. Scegli uno dei seguenti poster per iniziare.

  - "Poster in formato PDF E2860, E5760 e DE460C"
  - "E5724, EF570, EF280, E2812, E2824, Poster in formato PDF DE212C e DE224C"

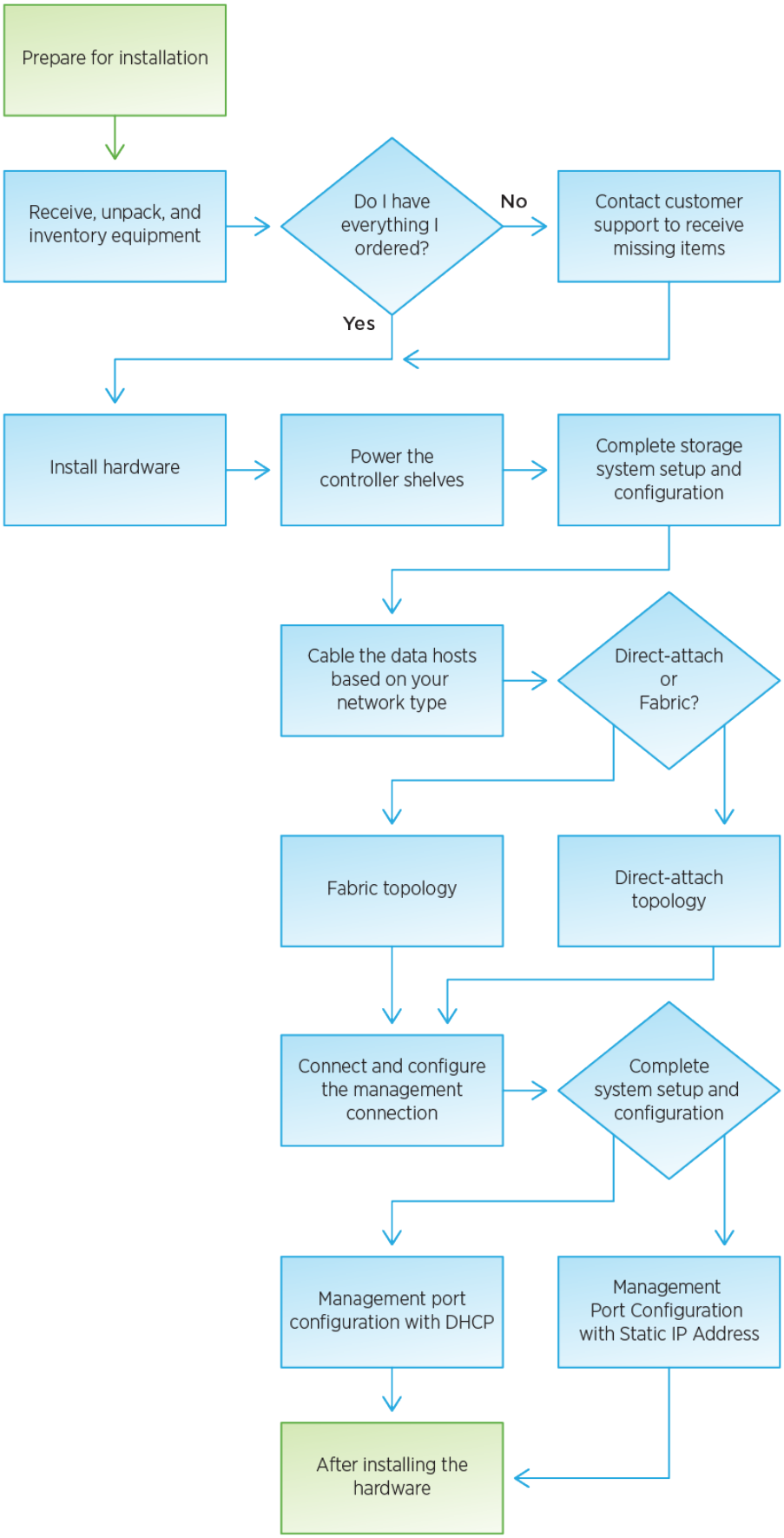
- **Istruzioni online**

  Queste sono le istruzioni di installazione descritte in questo sito. Inizia con uno dei seguenti argomenti per iniziare.

  - Preparazione all'installazione di E2860, E5760 e DE460C
  - Preparazione all'installazione di E5724, EF570, EF280, E2812, E2824, DE212C e DE224C

Panoramica

Prima di installare e configurare il nuovo sistema storage, acquisire familiarità con il processo di installazione:


Prepare for installation
Receive, unpack, and inventory equipment
Do I have everything I ordered?
No
Contact customer support to receive missing items
Yes
Install hardware
Power the controller shelves
Complete storage system setup and configuration
Cable the data hosts based on your network type
Direct-attach or Fabric?
Fabric topology
Direct-attach topology
Connect and configure the management connection
Complete system setup and configuration
Management port configuration with DHCP
Management Port Configuration with Static IP Address
After installing the hardware

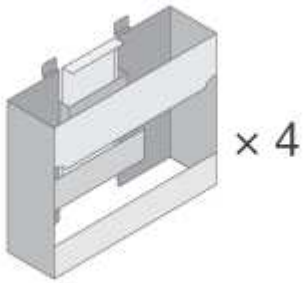
Installazione e configurazione di 60 dischi

Preparazione per l'installazione

Scopri come preparare l'installazione del tuo sistema storage E2860, E5760 o DE460.

Fasi

1. Creare un account e registrare l'hardware all'indirizzo "Supporto NetApp".
2. Assicurarsi che nella confezione ricevuta siano presenti i seguenti elementi.


Shelf, pannello frontale e hardware per il montaggio in rack

4 maniglie per scaffali

La seguente tabella identifica i tipi di cavi che potrebbero essere ricevuti. Se si riceve un cavo non elencato nella tabella, vedere "Hardware Universe" individuare il cavo e identificarne l'utilizzo.

Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi Ethernet (se ordinato)	Connessione di gestione

Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi i/O. (se ordinato)	Cablaggio degli host di dati
	Cavi di alimentazione x2 per shelf (se ordinato)	Accensione del sistema storage
	Cavi SAS (inclusi solo con gli shelf di dischi)	Cablaggio degli shelf

3. Assicurarsi di fornire i seguenti elementi.


Cacciavite Phillips n. 2

Torcia


Braccialetto ESD

Spazio rack 4U: Uno standard da 19" Rack da 48.30 cm per rack 4U delle seguenti dimensioni. **Profondità**: 38.25" (97.16 cm) **Larghezza**: 17.66" (44.86 cm) **Altezza**: 6.87" (17.46 cm) **Peso massimo**: 113 kg (250 lb)

Un browser supportato per il software di gestione: • Google Chrome (versione 89 e successive) • Microsoft Edge (versione 90 e successive) • Mozilla Firefox (versione 80 e successive) • Safari (versione 14 e successive)

Installare l'hardware

Scopri come installare un sistema storage E2860, E5760 o DE460 in un rack a due montanti o in un cabinet di sistema NetApp.

Prima di iniziare

- Registrare l'hardware all'indirizzo "Supporto NetApp".
- Preparare un'area di lavoro piana e priva di elettricità statica.
- Procurarsi un braccialetto ESD e adottare precauzioni antistatiche.

Leggere tutte le istruzioni prima di procedere con i passaggi riportati di seguito.

Fasi

1. Disimballare il contenuto dell'hardware, quindi inventariare l'hardware contenuto in base alla distinta di imballaggio.
2. Montare le guide.

   Se le istruzioni sono state fornite con l'hardware per il montaggio in rack, fare riferimento a tali istruzioni per informazioni su come installare le guide. Per ulteriori istruzioni sul montaggio in rack, vedere "Hardware per il montaggio in rack".

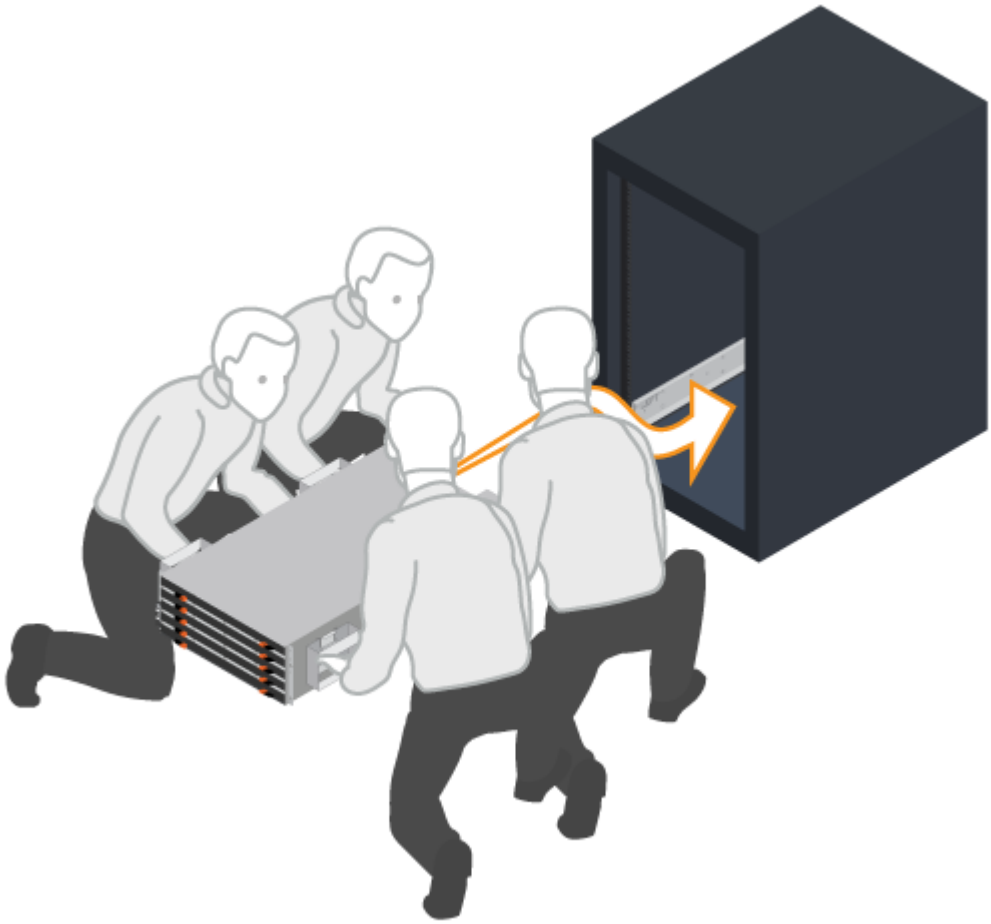
   > Per gli armadi a foro quadrato, è necessario installare i dadi della gabbia in dotazione per fissare la parte anteriore e posteriore del ripiano con le viti.

3. Installare lo shelf.

   > Un ripiano vuoto pesa circa 60 kg (132 lb). Per spostare in sicurezza uno scaffale vuoto, sono necessari un sollevatore meccanico o quattro persone che utilizzano le maniglie di sollevamento.

a. Se si solleva il ripiano manualmente, collegare le quattro maniglie di sollevamento. Spingere verso l'alto ciascuna maniglia fino a farla scattare in posizione.

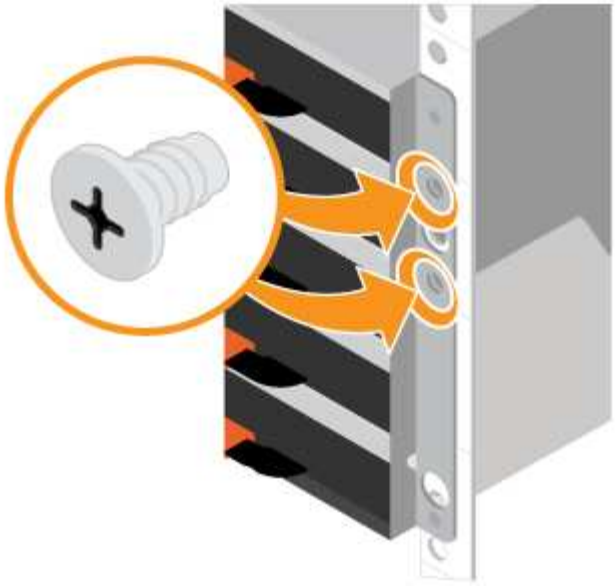
b. Sostenendo lo shelf dal basso, farlo scorrere nel cabinet. Se si utilizzano le maniglie di sollevamento, rimuoverle una alla volta mentre lo scaffale scorre nell'armadio. Per rimuovere le maniglie, tirare indietro il fermo di rilascio, spingere verso il basso, quindi allontanarlo dallo scaffale.



4. Fissare lo shelf.

   a. Inserire le viti nel primo e nel terzo foro dalla parte superiore del ripiano su entrambi i lati per fissarlo alla parte anteriore del cabinet.

   b. Posizionare due staffe posteriori su ciascun lato della sezione posteriore superiore del ripiano. Inserire le viti nel primo e nel terzo foro di ciascuna staffa per fissare la parte posteriore del cabinet.



5. Installare i dischi.
   a. Avvolgere l'estremità del braccialetto ESD intorno al polso e fissare l'estremità a una messa a terra metallica per evitare scariche elettrostatiche.
   b. Partendo dallo slot anteriore sinistro del cassetto superiore, installare ciascuna unità posizionandola delicatamente nello slot e abbassando la maniglia sollevata fino a farla scattare in posizione.
      - Se si installano meno di 60 dischi, se si dispone di dischi a stato solido (SSD) o se i dischi hanno capacità diverse:
        - Mantenere un minimo di 20 dischi per shelf. Installare prima le unità nei quattro slot anteriori di ciascun cassetto, per ottenere un flusso d'aria adeguato per il raffreddamento.
        - Distribuire le unità rimanenti nei cassetti. Se possibile, installare un numero uguale di ciascun tipo di disco in ciascun cassetto per consentire la creazione di gruppi di volumi o pool di dischi protetti da perdita del cassetto.
        - Distribuisci gli SSD in modo uniforme nei cassetti.
   c. Far scorrere con cautela il cassetto all'interno spingendo il centro e chiudendo delicatamente entrambi i fermi.
      - Non forzare il cassetto in posizione.
      - Utilizzare lo strumento di connessione, scollegare il connettore del cavo di serpente e ricollegarlo, assicurarsi di sentire uno scatto per determinare che la riconnessione sia stata eseguita correttamente.
      - La disconnessione e la riconnessione devono essere necessarie solo durante la configurazione iniziale o se il vassoio viene spedito in una posizione diversa.
   d. Fissare il pannello anteriore.

Rischio di danni all'apparecchiatura — interrompere la spinta del cassetto se si sente l'inceppamento. Utilizzare le leve di rilascio nella parte anteriore del cassetto per far scorrere il cassetto all'indietro. Quindi, reinserire con cautela il cassetto nell'alloggiamento.

Cablare gli scaffali

Scopri come collegare i cavi di alimentazione e alimentare gli shelf di dischi.

Prima di iniziare

- Installare l'hardware.
- Adottare precauzioni antistatiche.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Fasi

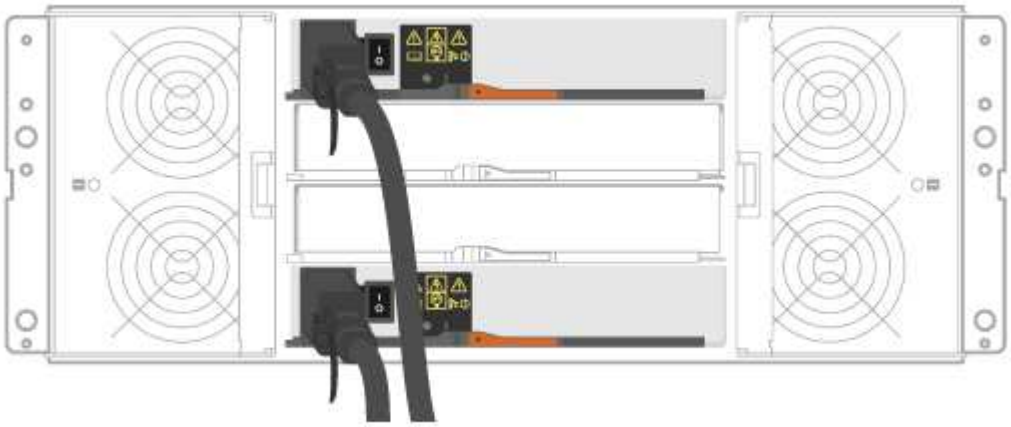
1. Cablare gli scaffali.

   Collegare il sistema in base alla configurazione. Se sono necessarie più opzioni di cablaggio rispetto agli esempi illustrati in questa sezione, vedere "Cablaggio".

   Per gli esempi illustrati in questa sezione, sono necessari i seguenti cavi:

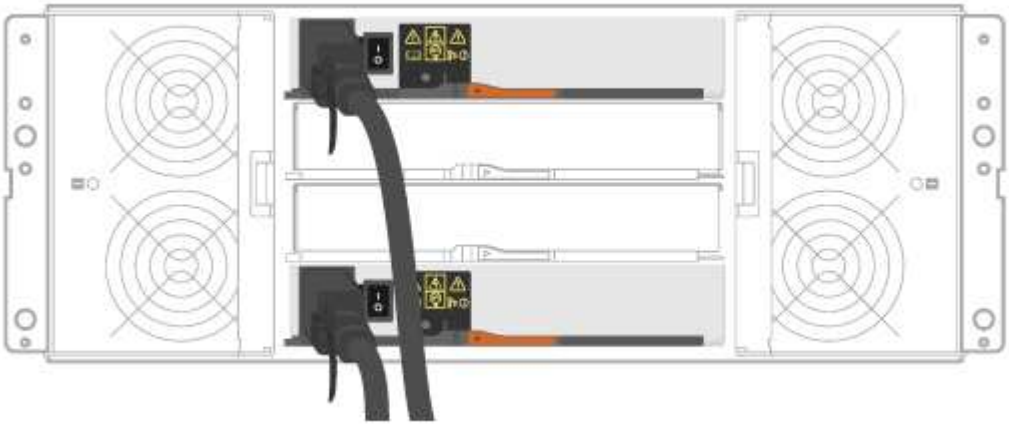
Cavi SAS

Esempio A: Shelf di controller E2860 con due shelf di dischi DE460C in una configurazione SAS standard.



a. Collegare il controller a al modulo IOM A del primo shelf di dischi.
b. Collegare IOM A del primo shelf di dischi a IOM A del secondo shelf di dischi.
c. Cavo IOM B del primo shelf di dischi a IOM B del secondo shelf di dischi.
d. Collegare il controller B all'IOM B del secondo shelf di dischi.

Esempio B: Uno shelf di controller E2860 con uno shelf di dischi DE460C in una configurazione SAS standard.



e. Collegare il controller a al modulo IOM A.
f. Cavo controller B a IOM B.

2. Alimentare gli shelf di dischi.

Sono necessari i seguenti cavi:

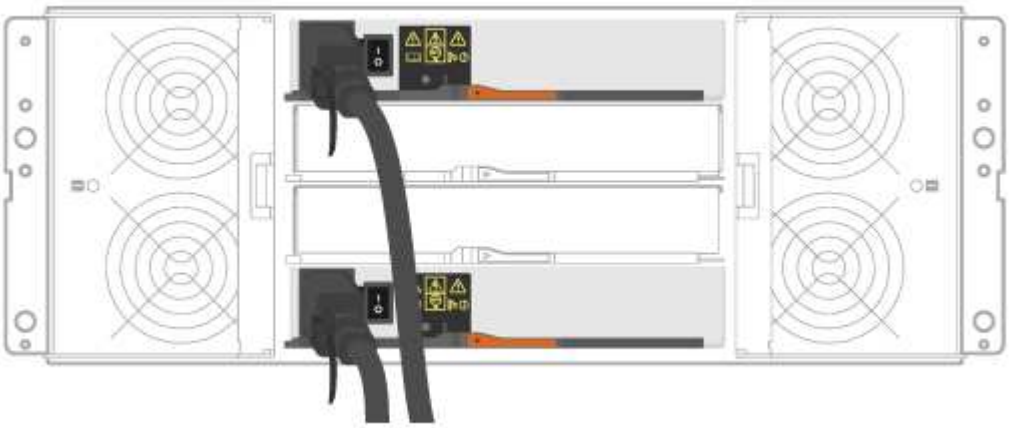
Cavi di alimentazione

Verificare che gli interruttori di alimentazione dello shelf siano spenti.

a. Collegare i due cavi di alimentazione per ogni shelf a diverse unità di distribuzione dell'alimentazione (PDU) nell'armadio o nel rack.
b. Se si dispone di shelf di dischi, accendere prima i due interruttori di alimentazione. Attendere 2 minuti prima di alimentare lo shelf del controller.
c. Accendere i due interruttori di alimentazione sullo shelf del controller.
d. Controllare i LED e il display a sette segmenti su ciascun controller.

   Durante l'avvio, il display a sette segmenti mostra la sequenza ripetuta di OS, SD, vuoto per indicare che il controller sta eseguendo l'elaborazione all'inizio della giornata. Dopo l'avvio del controller, viene visualizzato l'ID dello shelf.

*Esempio: I collegamenti di alimentazione si trovano sul retro dello



shelf.*

Configurazione e configurazione complete del sistema storage

Scopri come collegare i controller alla rete e completare la configurazione e la configurazione del sistema storage.

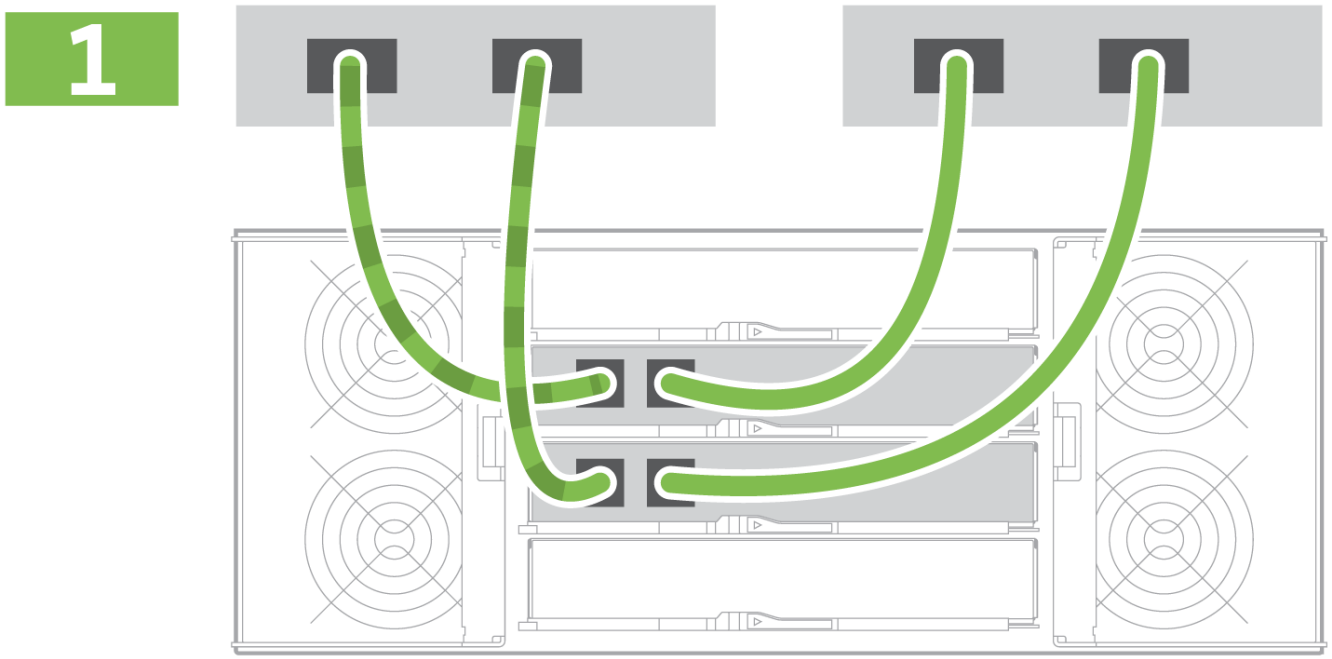
Fase 1: Collegare via cavo gli host dati

Collegare il sistema in base alla topologia di rete.

Se si utilizza AIX®, è necessario installare il driver multipath e-Series sull'host prima di collegarlo all'array.

Opzione 1: Topologia a collegamento diretto

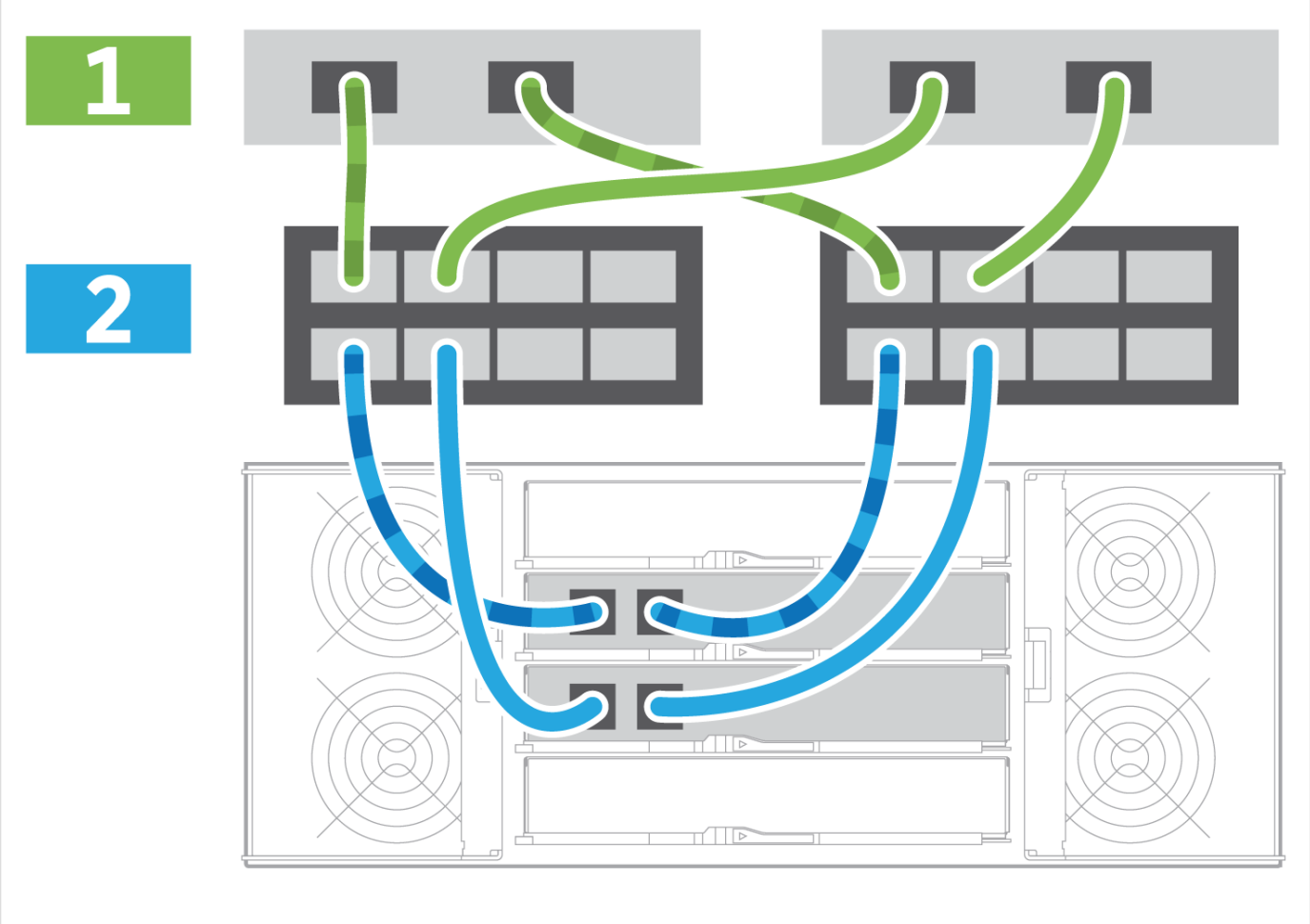
Nell'esempio seguente viene illustrato il collegamento dei cavi agli host di dati utilizzando una topologia a collegamento diretto.



1. Collegare ciascun adattatore host direttamente alle porte host dei controller.

Opzione 2: Topologia del fabric

Nell'esempio seguente viene illustrato il collegamento degli host di dati mediante una topologia fabric.



1. Collegare ciascun adattatore host direttamente allo switch.
2. Collegare ogni switch direttamente alle porte host dei controller.

Fase 2: Connessione e configurazione della connessione di gestione

È possibile configurare le porte di gestione del controller utilizzando un server DHCP o un indirizzo IP statico.

Opzione 1: Server DHCP

Scopri come configurare le porte di gestione con un server DHCP.

Prima di iniziare

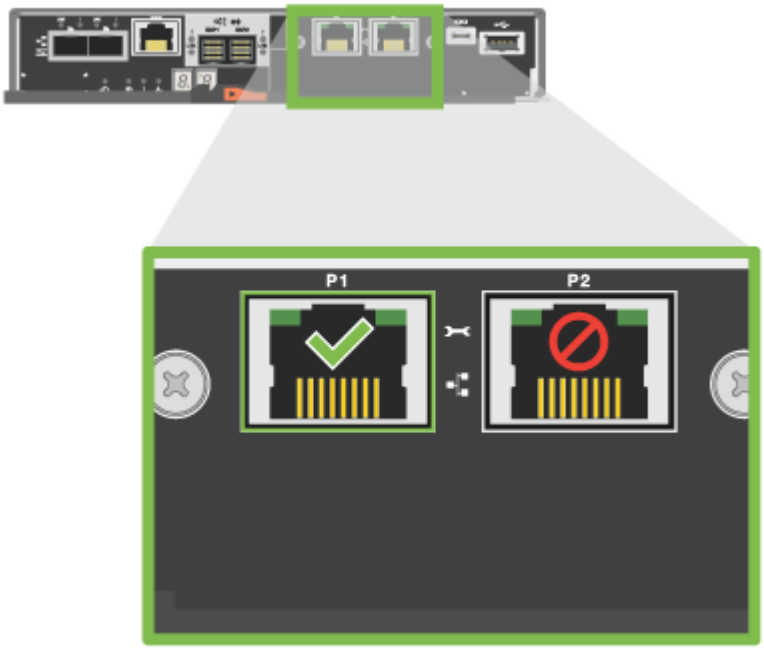
- Configurare il server DHCP per associare un indirizzo IP, una subnet mask e un indirizzo gateway come lease permanente per ciascun controller.
- Ottenere gli indirizzi IP assegnati per la connessione al sistema di storage dall'amministratore di rete.

Fasi

1. Collegare un cavo Ethernet alla porta di gestione di ciascun controller e l'altra estremità alla rete.

Cavi Ethernet (se ordinati)

Le seguenti figure mostrano esempi della posizione della porta di gestione del controller:



Porta di gestione P1 del controller E2800

Porta di gestione P1 del controller E5700

2. Aprire un browser e connettersi al sistema di storage utilizzando uno degli indirizzi IP del controller forniti dall'amministratore di rete.

Opzione 2: Indirizzo IP statico

Informazioni su come configurare manualmente le porte di gestione immettendo l'indirizzo IP e la subnet mask.

Prima di iniziare

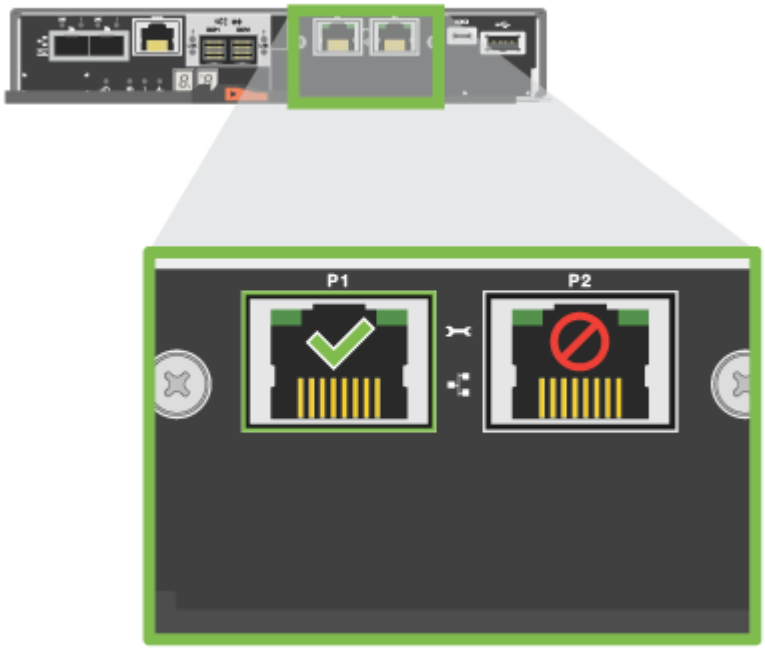
- Richiedere all'amministratore di rete l'indirizzo IP, la subnet mask, l'indirizzo del gateway e le informazioni sul server DNS e NTP dei controller.
- Assicurarsi che il portatile in uso non riceva la configurazione di rete da un server DHCP.

Fasi

1. Utilizzando un cavo Ethernet, collegare la porta di gestione Del controller A alla porta Ethernet di un laptop.

Cavi Ethernet (se ordinati)

Le seguenti figure mostrano esempi della posizione della porta di gestione del controller:



Porta di gestione P1 del controller E2800

Porta di gestione P1 del controller E5700

2. Aprire un browser e utilizzare l'indirizzo IP predefinito (169.254.128.101) per stabilire una connessione al controller. Il controller restituisce un certificato autofirmato. Il browser informa che la connessione non è sicura.
3. Seguire le istruzioni del browser per procedere e avviare Gestione di sistema di SANtricity.

   Se non si riesce a stabilire una connessione, verificare di non ricevere la configurazione di rete da un server DHCP.

4. Impostare la password di accesso del sistema di storage.
5. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller A, quindi selezionare **fine**.

   Poiché l'indirizzo IP viene ripristinato, System Manager perde la connessione al controller.

6. Scollegare il laptop dal sistema storage e collegare la porta di gestione del controller A alla rete.
7. Aprire un browser su un computer connesso alla rete e immettere l'indirizzo IP appena configurato del controller A.

   Se si perde la connessione al controller A, è possibile collegare un cavo ethernet al controller B per ristabilire la connessione al controller A attraverso il controller B (169.254.128.102).

8. Accedere utilizzando la password impostata in precedenza.

   Viene visualizzata la procedura guidata Configure Network Settings (Configura impostazioni di rete).

9. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller B, quindi selezionare **fine**.
10. Collegare il controller B alla rete.
11. Convalidare le impostazioni di rete del controller B inserendo l'indirizzo IP appena configurato del controller B in un browser.

> Se si perde la connessione al controller B, è possibile utilizzare la connessione precedentemente convalidata al controller A per ristabilire la connessione al controller B attraverso il controller A.

Fase 3: Configurare e gestire il sistema storage

Dopo aver installato l'hardware, utilizzare il software SANtricity per configurare e gestire il sistema di storage.

Prima di iniziare

- Configurare le porte di gestione.
- Verificare e registrare la password e gli indirizzi IP.

Fasi

1. Utilizza il software SANtricity per configurare e gestire gli array di storage.
2. Nella configurazione di rete più semplice, collegare il controller a un browser Web e utilizzare Gestione di sistema di SANtricity per gestire un singolo array di storage della serie E2800 o E5700.

Per accedere a System Manager, utilizzare gli stessi indirizzi IP utilizzati per configurare le porte di gestione.

Installare e configurare 12 e 24 dischi

Preparazione per l'installazione

Scopri come preparare l'installazione di E5724, EF570, EF280, E2812, E2824, Sistema storage DE212C o DE224C.

Fasi

1. Creare un account e registrare l'hardware all'indirizzo "Supporto NetApp".
2. Assicurarsi che nella confezione ricevuta siano presenti i seguenti elementi.

	
Shelf con dischi installati (pannello in confezione separata)	
	
Hardware per il montaggio in rack	

La seguente tabella identifica i tipi di cavi che potrebbero essere ricevuti. Se si riceve un cavo non elencato nella tabella, vedere "Hardware Universe" individuare il cavo e identificarne l'utilizzo.

Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi Ethernet (se ordinato)	Connessione di gestione
	Cavi i/O. (se ordinato)	Cablaggio degli host di dati
	Cavi di alimentazione (se ordinato)	Accensione del sistema storage

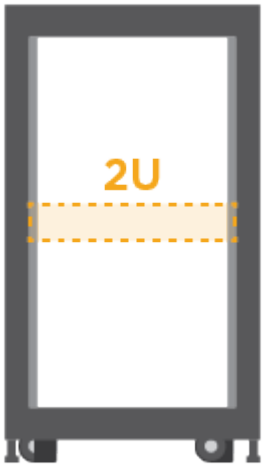
Tipo di connettore	Tipo di cavo	Utilizzare
	Cavi SAS inclusi solo con gli shelf di dischi	Cavi SAS

3. Assicurarsi di fornire i seguenti elementi.


Cacciavite Phillips n. 2

Torcia

Braccialetto ESD



Spazio rack 2U: Uno standard da 19" Rack da 48.30 cm per rack 2U delle seguenti dimensioni.

Profondità: 19.0" (48.3 cm)

Larghezza: 17.6" (44.7 cm)

Altezza: 3.34" (8.48 cm)

Shelf: 24 dischi

Peso massimo: 27.4 kg (60.5 lb)

Un browser supportato per il software di gestione:

- Google Chrome (versione 89 e successive)
- Microsoft Edge (versione 90 e successive)
- Mozilla Firefox (versione 80 e successive)
- Safari (versione 14 e successive)

Installare l'hardware

Scopri come installare E5724, EF570, EF280, E2812, E2824, Sistema storage DE212C o DE224C in un rack a due montanti o in un cabinet di sistema NetApp.

Prima di iniziare

Assicurarsi di eseguire le seguenti operazioni:

- Registrare l'hardware all'indirizzo "Supporto NetApp".
- Preparare un'area di lavoro piana e priva di elettricità statica.
- Procurarsi un braccialetto ESD e adottare precauzioni antistatiche.

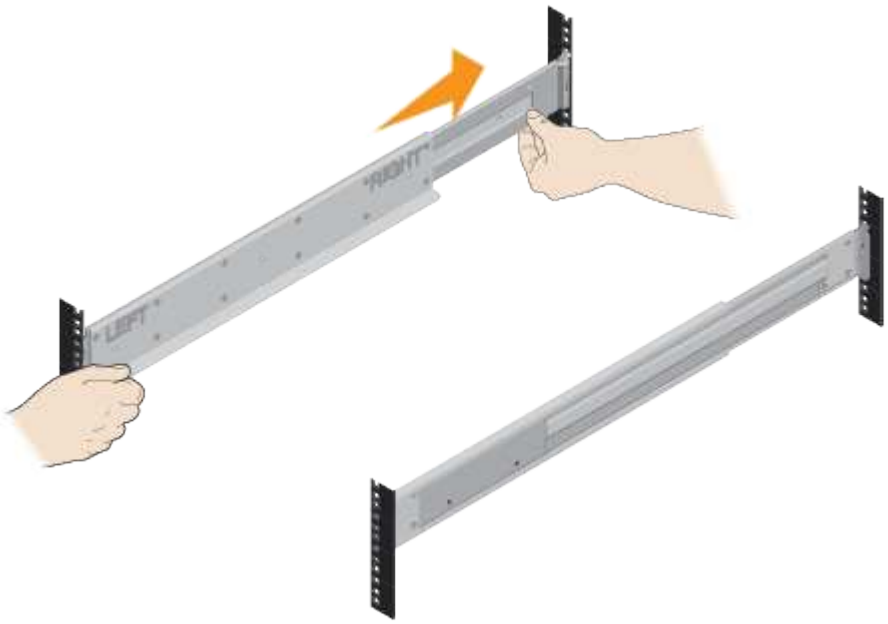
Leggere tutte le istruzioni prima di procedere con i passaggi riportati di seguito.

Fasi

1. Disimballare il contenuto dell'hardware, quindi inventariare l'hardware contenuto in base alla distinta di imballaggio.
2. Montare le guide.

   Se le istruzioni sono state fornite con l'hardware per il montaggio in rack, fare riferimento a tali istruzioni per informazioni dettagliate su come installare le guide. Per ulteriori istruzioni sul montaggio in rack, vedere "Hardware per il montaggio in rack".

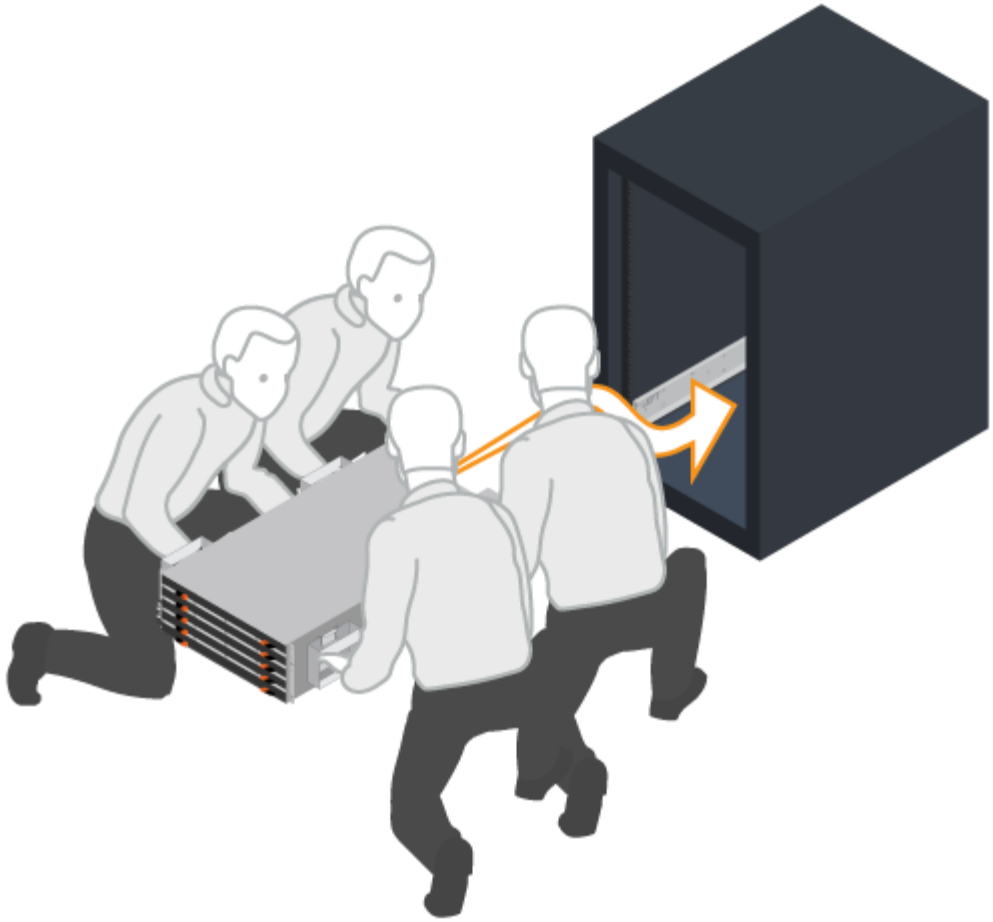
   > Installare l'hardware dalla parte inferiore del rack o dell'armadietto fino alla parte superiore per evitare che l'apparecchiatura si rovescii.



3. Installare lo shelf.

   > Quando è completamente caricato con dischi, ogni shelf pesa circa 29 kg (64 lb). Per spostare il ripiano in modo sicuro sono necessarie due persone o un sollevatore meccanico.

   a. Partendo dal ripiano che si desidera posizionare sul fondo del cabinet, posizionare il retro del ripiano (l'estremità con i connettori) sulle guide.
   b. Sostenendo lo shelf dal basso, farlo scorrere nel

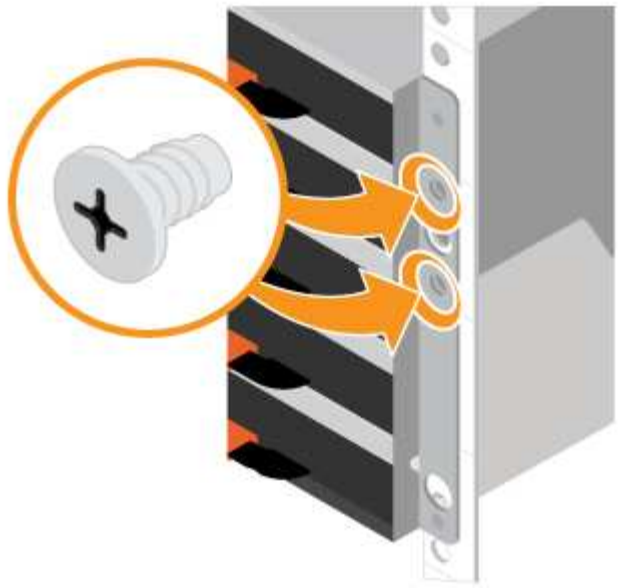


cabinet.

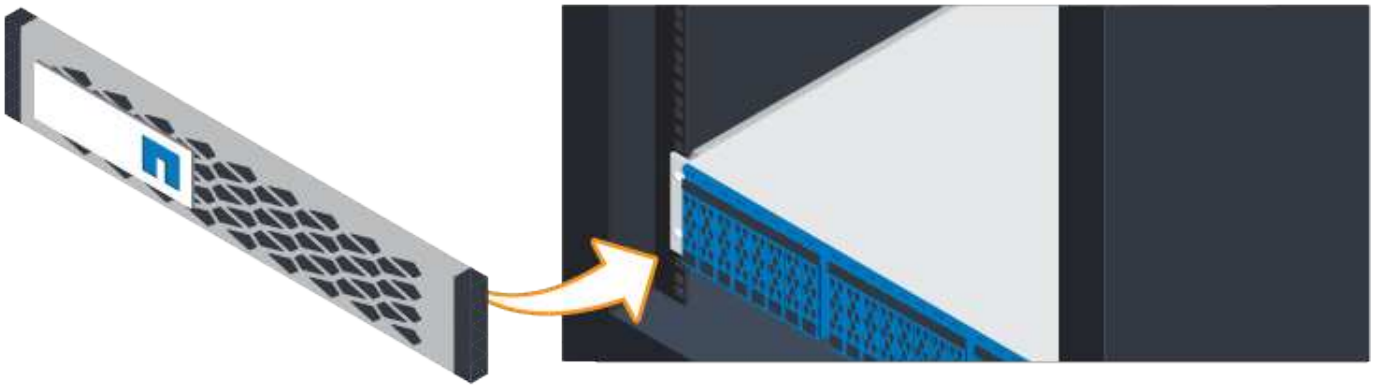
4. Fissare lo shelf.

   Fissare lo shelf al rack come indicato nella "Hardware per il montaggio in rack".

   a. Inserire le viti nel primo e nel terzo foro dalla parte superiore del ripiano su entrambi i lati per fissarlo alla parte anteriore del cabinet.
   b. Posizionare due staffe posteriori su ciascun lato della sezione posteriore superiore del ripiano. Inserire le viti nel primo e nel terzo foro di ciascuna staffa per fissare la parte posteriore del cabinet.



5. Installare il pannello o i cappucci terminali.
   a. Posizionare il pannello anteriore davanti allo shelf del controller in modo che i fori su ciascuna estremità siano allineati con i dispositivi di fissaggio sullo shelf del controller.
   b. Far scattare il pannello in posizione.
   c. Se si dispone di shelf di dischi opzionali, posizionare il cappuccio terminale sinistro davanti allo shelf di dischi in modo che i fori nel cappuccio terminale siano allineati con i dispositivi di fissaggio sul lato sinistro dello shelf.
   d. Inserire il cappuccio terminale in posizione.
   e. Ripetere i passaggi precedenti per il cappuccio terminale destro.



Collegare i cavi

Scopri come collegare i cavi di alimentazione e alimentare gli shelf di dischi.

Prima di iniziare

- Installare l'hardware.
- Adottare precauzioni antistatiche.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Fasi

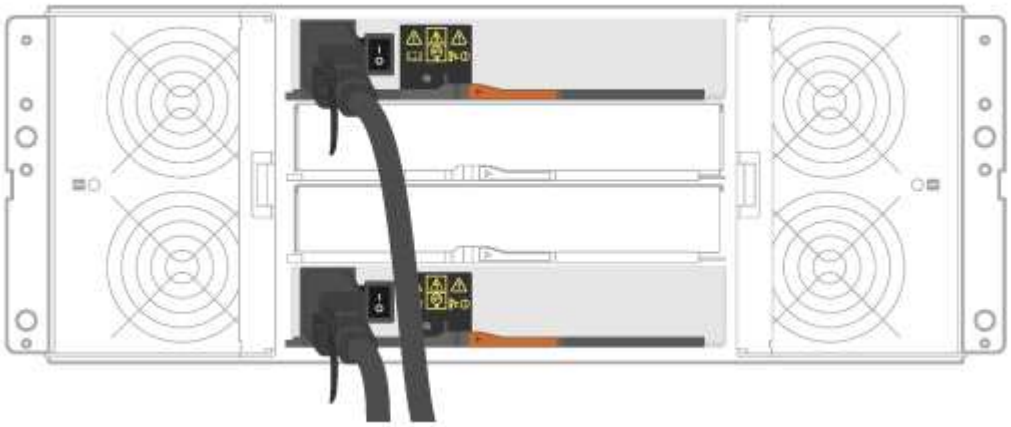
1. Cablare gli scaffali.

   Collegare il sistema in base alla configurazione. Se sono necessarie più opzioni di cablaggio rispetto agli esempi illustrati, vedere "Cablaggio".

   Per gli esempi illustrati, sono necessari i seguenti cavi:

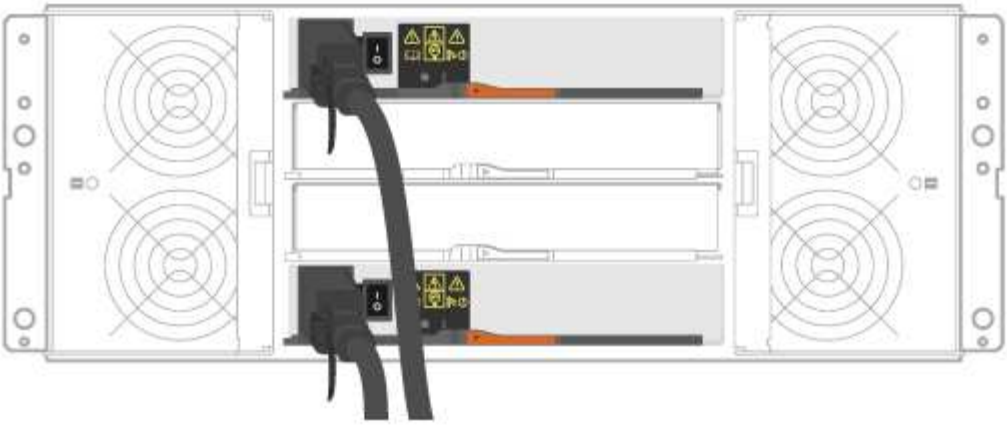
	
Cavi SAS	

   Esempio A: Shelf di controller E5700 con tre shelf di dischi DE212C/DE224 in una configurazione SAS standard.



   a. Collegare il controller a al modulo IOM A del primo shelf di dischi.
   b. Collegare IOM A del primo shelf di dischi a IOM A del secondo shelf di dischi.
   c. Collegare IOM A del secondo shelf di dischi a IOM A del terzo shelf di dischi.
   d. Collegare il controller B all'IOM B del terzo shelf di dischi.
   e. Cavo IOM B del secondo shelf di dischi a IOM B del terzo shelf di dischi.
   f. Cavo IOM B del primo shelf di dischi a IOM B del secondo shelf di dischi.

   Esempio B: Shelf di controller E5700 con shelf di dischi DE212C/DE224 in una configurazione SAS standard.



g. Collegare il controller a al modulo IOM A.

h. Cavo controller B a IOM B.

2. Alimentare gli shelf di dischi.

Sono necessari i seguenti cavi:

	
Cavi di alimentazione	

Verificare che gli interruttori di alimentazione dello shelf siano spenti.

a. Collegare i due cavi di alimentazione per ogni shelf a diverse unità di distribuzione dell'alimentazione (PDU) nell'armadio o nel rack.

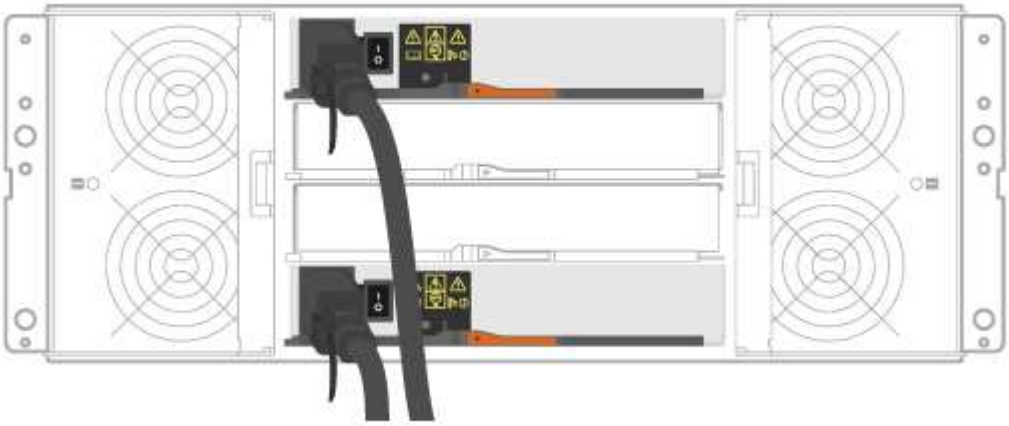
b. Se si dispone di shelf di dischi, accendere prima i due interruttori di alimentazione. Attendere 2 minuti prima di alimentare lo shelf del controller.

c. Accendere i due interruttori di alimentazione sullo shelf del controller.

d. Controllare i LED e il display a sette segmenti su ciascun controller.

   Durante l'avvio, il display a sette segmenti mostra la sequenza ripetuta di OS, SD, vuoto per indicare che il controller sta eseguendo l'elaborazione all'inizio della giornata. Dopo l'avvio del controller, viene visualizzato l'ID dello shelf.

*Esempio: I collegamenti di alimentazione si trovano sul retro dello



shelf.*

Configurazione e configurazione complete del sistema storage

Scopri come collegare i controller alla rete e completare la configurazione e la configurazione del sistema storage.

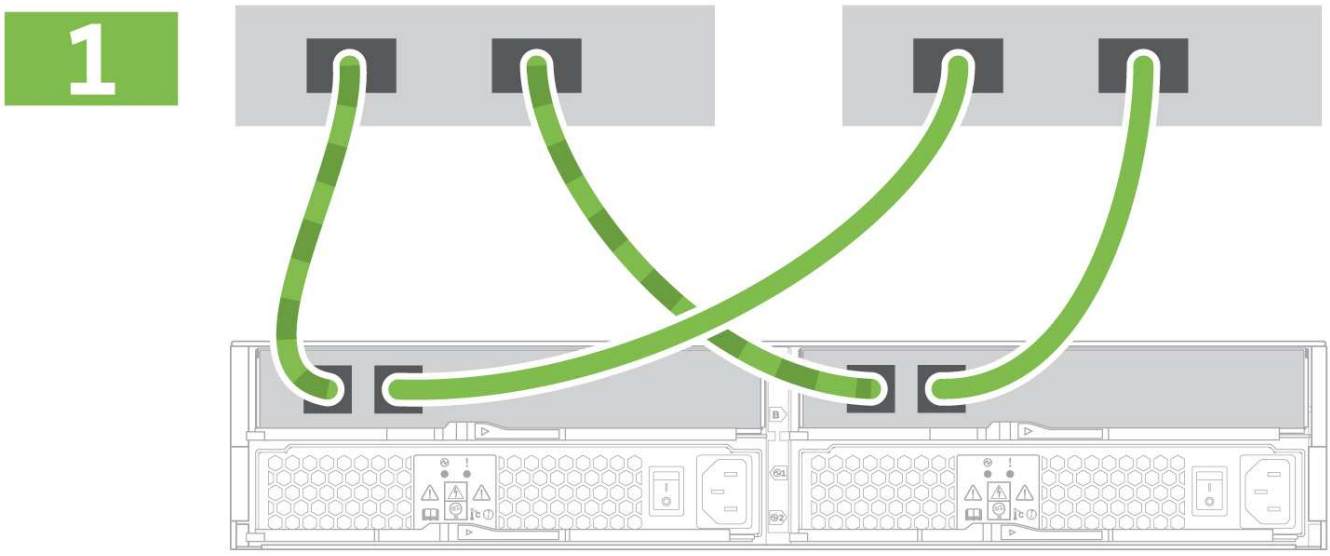
Fase 1: Collegare via cavo gli host dati

Collegare il sistema in base alla topologia di rete.

> Se si utilizza AIX®, è necessario installare il driver multipath e-Series sull'host prima di collegarlo all'array.

Opzione 1: Topologia a collegamento diretto

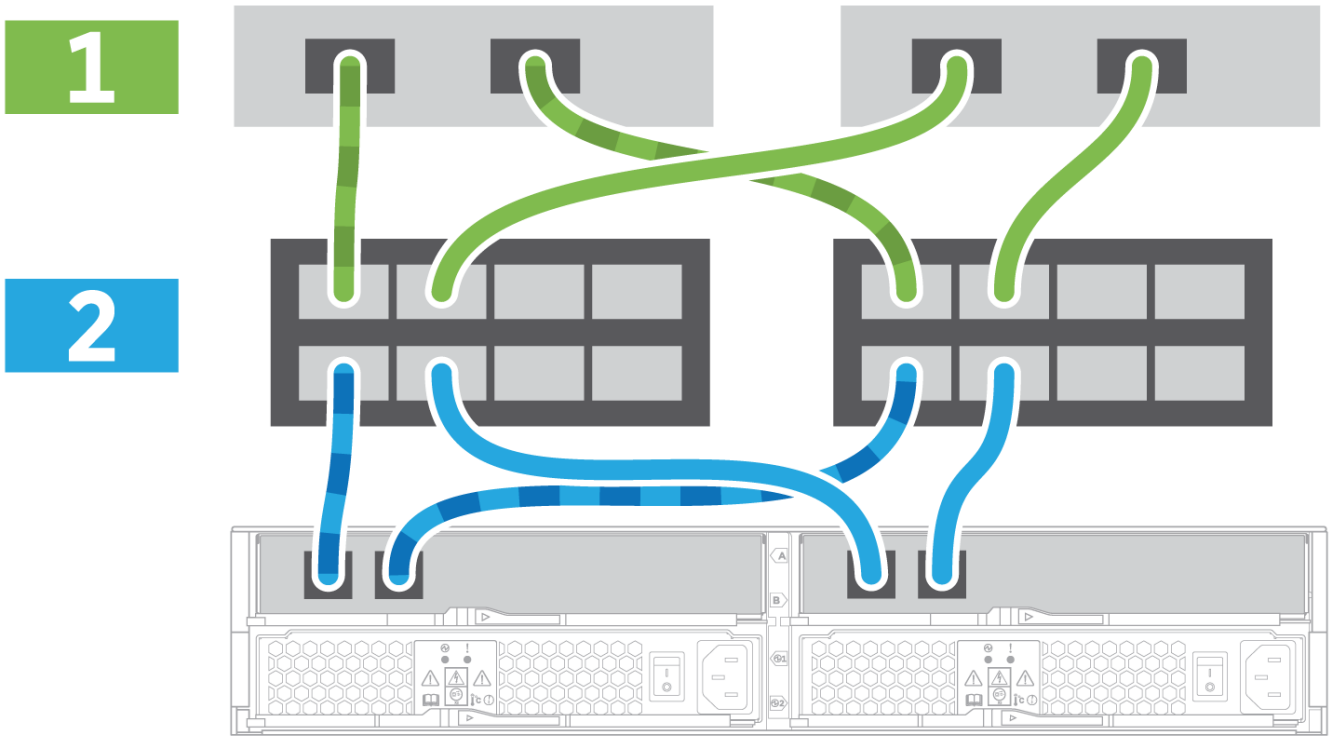
Nell'esempio seguente viene illustrato il collegamento dei cavi agli host di dati utilizzando una topologia a collegamento diretto.



1. Collegare ciascun adattatore host direttamente alle porte host dei controller.

Opzione 2: Topologia del fabric

Nell'esempio seguente viene illustrato il collegamento degli host di dati mediante una topologia fabric.



1. Collegare ciascun adattatore host direttamente allo switch.
2. Collegare ogni switch direttamente alle porte host dei controller.

Fase 2: Connessione e configurazione della connessione di gestione

È possibile configurare le porte di gestione del controller utilizzando una delle due opzioni disponibili: Utilizzando un server DHCP o un indirizzo IP statico.

Opzione 1: Server DHCP

Scopri come configurare le porte di gestione con un server DHCP.

Prima di iniziare

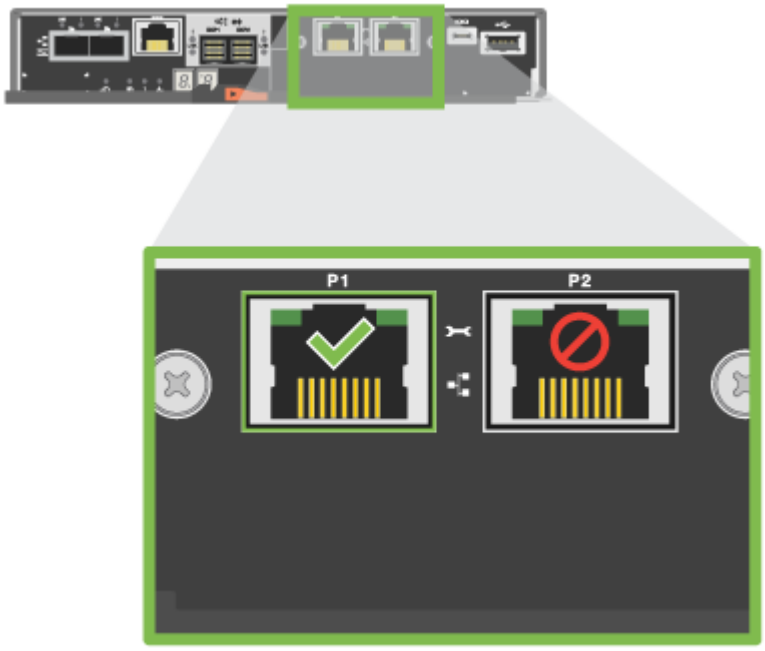
- Configurare il server DHCP per associare un indirizzo IP, una subnet mask e un indirizzo gateway come lease permanente per ciascun controller.
- Ottenere gli indirizzi IP assegnati che si desidera utilizzare per connettersi al sistema di storage dall'amministratore di rete.

Fasi

1. Collegare un cavo Ethernet alla porta di gestione di ciascun controller e l'altra estremità alla rete.

Cavi Ethernet (se ordinati)

Le seguenti figure mostrano esempi della posizione della porta di gestione del controller:



Porta di gestione P1 del controller E2800

Porta di gestione P1 del controller E5700

2. Aprire un browser e connettersi al sistema di storage utilizzando uno degli indirizzi IP del controller forniti dall'amministratore di rete.

Opzione 2: Indirizzo IP statico

Informazioni su come configurare manualmente le porte di gestione immettendo l'indirizzo IP e la subnet mask.

Prima di iniziare

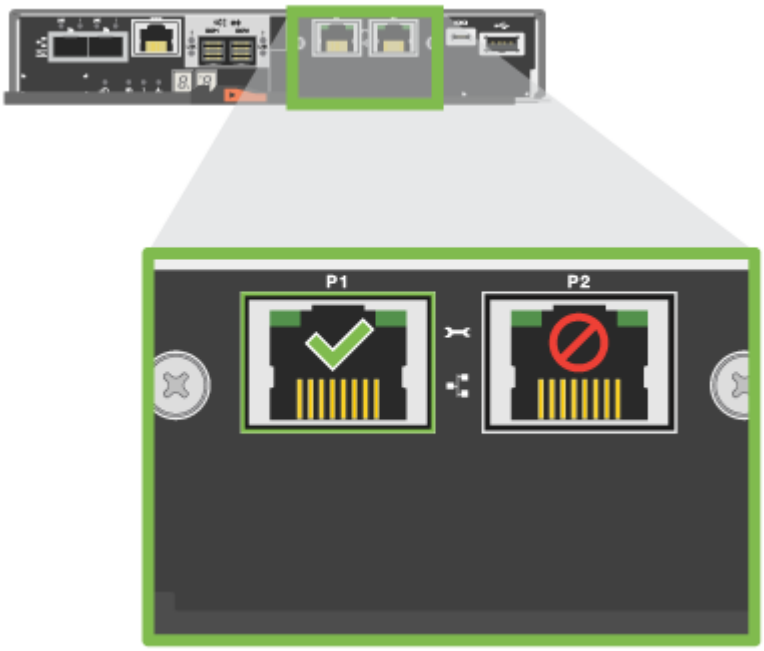
- Richiedere all'amministratore di rete l'indirizzo IP, la subnet mask, l'indirizzo del gateway e le informazioni relative al server DNS e NTP dei controller`.
- Assicurarsi che il portatile in uso non riceva la configurazione di rete da un server DHCP.

Fasi

1. Utilizzando un cavo Ethernet, collegare la porta di gestione Del controller A alla porta Ethernet di un laptop.

Cavi Ethernet (se ordinati)

Le seguenti figure mostrano esempi della posizione della porta di gestione del controller:



Porta di gestione P1 del controller E2800

Porta di gestione P1 del controller E5700

2. Aprire un browser e utilizzare l'indirizzo IP predefinito (169.254.128.101) per stabilire una connessione al controller. Il controller restituisce un certificato autofirmato. Il browser informa che la connessione non è sicura.
3. Seguire le istruzioni del browser per procedere e avviare Gestione di sistema di SANtricity.

> Se non si riesce a stabilire una connessione, verificare di non ricevere la configurazione di rete da un server DHCP.

4. Impostare la password di accesso del sistema di storage.
5. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller A, quindi selezionare **fine**.

> Poiché l'indirizzo IP viene ripristinato, System Manager perde la connessione al controller.

6. Scollegare il laptop dal sistema storage e collegare la porta di gestione del controller A alla rete.
7. Aprire un browser su un computer connesso alla rete e immettere l'indirizzo IP appena configurato del controller A.

> Se si perde la connessione al controller A, è possibile collegare un cavo ethernet al controller B per ristabilire la connessione al controller A attraverso il controller B (169.254.128.102).

8. Accedere utilizzando la password impostata in precedenza.

   Viene visualizzata la procedura guidata Configure Network Settings (Configura impostazioni di rete).

9. Utilizzare le impostazioni di rete fornite dall'amministratore di rete nella procedura guidata **Configura impostazioni di rete** per configurare le impostazioni di rete del controller B, quindi selezionare **fine**.
10. Collegare il controller B alla rete.
11. Convalidare le impostazioni di rete del controller B inserendo l'indirizzo IP appena configurato del controller B in un browser.

> Se si perde la connessione al controller B, è possibile utilizzare la connessione precedentemente convalidata al controller A per ristabilire la connessione al controller B attraverso il controller A.

Fase 3: Configurazione del sistema storage

Dopo aver installato l'hardware, utilizzare il software SANtricity per configurare e gestire il sistema di storage.

Prima di iniziare

- Configurare le porte di gestione.
- Verificare e registrare la password e gli indirizzi IP.

Fasi

1. Utilizza il software SANtricity per configurare e gestire gli array di storage.
2. Nella configurazione di rete più semplice, collegare il controller a un browser Web e utilizzare Gestione di sistema di SANtricity per gestire un singolo array di storage della serie E2800 o E5700.

Per accedere a System Manager, utilizzare gli stessi indirizzi IP utilizzati per configurare le porte di gestione.

Cabinet 3040 40U

Installare i vassoi nel cabinet 3040 40U

Nel cabinet e-Series 3040 40U è possibile installare i seguenti vassoi del controller e dei dischi di espansione:

- Tray di dischi controller E2612, E2624 e E2660
- Tray di dischi controller E2712, E2724 e E2760
- Tray di dischi controller E5412, E5424 e E5460
- Tray di dischi controller E5512, E5524 e E5560
- Tray di dischi controller E5612, E5624 e E5660
- Array flash EF540, EF550 e EF560
- Tray di dischi DE1600, DE5600 e DE6600

È inoltre possibile installare i seguenti shelf di controller SAS-3 e shelf di dischi nel cabinet.

- Shelf di controller E2812, E2824 e E5724
- Shelf di dischi DE212C e DE224C

Tuttavia, le specifiche di questi shelf non sono elencate in queste procedure. Fare riferimento a. "NetApp Hardware Universe".

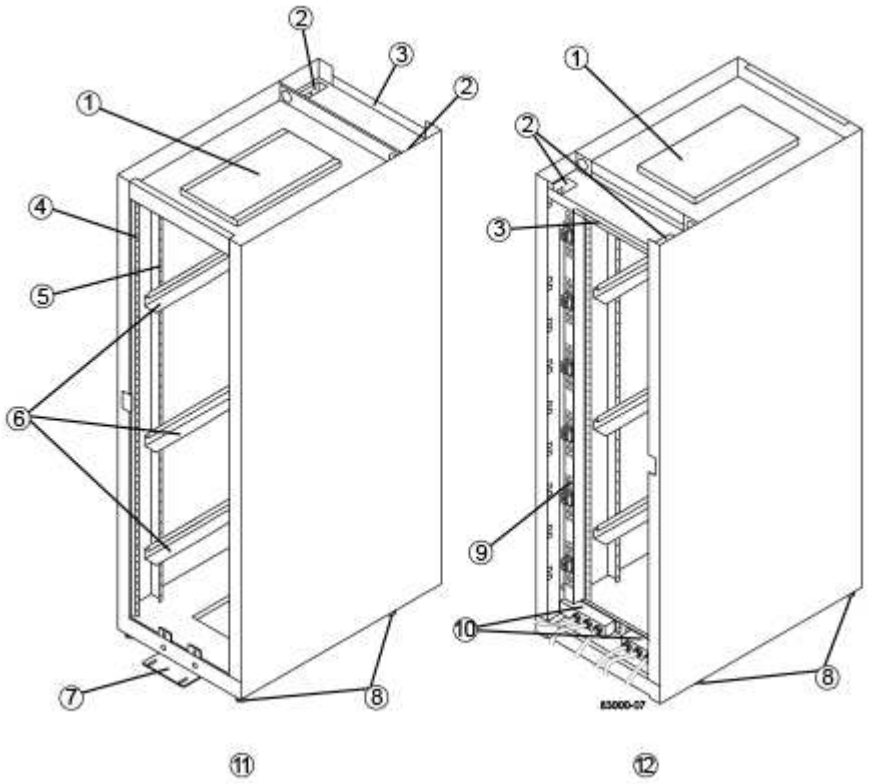
Specifiche del cabinet

Il cabinet modello 3040 40U presenta le seguenti caratteristiche standard:

- Una porta posteriore che può essere bloccata e bloccata
- Le guide di supporto EIA (Electronic Industry Association) standard forniscono fori di montaggio per l'installazione dei dispositivi in un sistema standard da 48.3 cm (19") ampio cabinet
- Quattro rotelle a rulli e quattro piedini regolabili posizionati sotto l'armadietto per spostare l'armadio e quindi livellarlo nella posizione finale

- Un piede di stabilità che stabilizza l’armadio dopo averlo installato nella sua posizione permanente
- Aperture di accesso per i cavi di interfaccia
- Due unità di distribuzione dell’alimentazione CA (PDU) che forniscono una connessione di alimentazione integrata e capacità di gestione dell’alimentazione

Le seguenti figure mostrano una vista frontale (sinistra) e una vista posteriore (destra) dell’armadio.



1.
Coperchio di ventilazione
2.
Aperture di accesso ai cavi di interfaccia
3.
Piastra posteriore
4.
Guide di supporto EIA
5.

Guide di supporto verticali
6.
Guide di montaggio per cabinet
7.
Piede di stabilità
8.
Piedini regolabili
9.
Unità di distribuzione dell'alimentazione (una di due)
10.
Scatole di alimentazione CA
11.
Parte anteriore del cabinet
12.
Parte posteriore del cabinet

Rischio di lesioni fisiche — se la metà inferiore del cabinet è vuota, non installare i componenti nella metà superiore del cabinet. Se la metà superiore del cabinet è troppo pesante per la metà inferiore, il cabinet potrebbe cadere e causare lesioni personali. Installare sempre un componente nella posizione più bassa disponibile nell'armadio.

Rischio di lesioni fisiche — spostare solo un armadio popolato con un carrello elevatore a forche o con un adeguato aiuto da parte di altre persone. Spingere sempre il cabinet dalla parte anteriore per evitare che cada. Un cabinet completamente popolato può pesare più di 909 kg (2000 lb). Il cabinet è difficile da spostare, anche su una superficie piana. Se è necessario spostare il cabinet lungo una superficie inclinata, rimuovere i componenti dalla metà superiore del cabinet e assicurarsi di disporre di un aiuto adeguato.

Non è possibile installare shelf di controller E2860 o E5760 o uno shelf di dischi DE460C in un cabinet 3040 40U.

Se un cabinet 3040 è completamente popolato con i vassoi DE6600, pesa più di 1250.1 kg (2756 lb).

Requisiti di alimentazione e dissipazione del calore

L'armadio include le seguenti specifiche per l'alimentazione e la dissipazione del calore.

Potenza nominale

L'armadio 3040 40U ha una potenza nominale di 200 V CA - 240 V CA a 50 Hz - 60 Hz e funziona fino a ±10% di tale intervallo.

Unità di distribuzione dell'alimentazione (PDU)

L'armadio include due unità di distribuzione dell'alimentazione CA (PDU) identiche, ciascuna PDU fornisce fino a 72A di alimentazione utilizzabile. Le PDU sono montate verticalmente sul retro dell'armadio e ciascuna PDU include sei power bank 12 A. Ciascun power bank contiene quattro prese di alimentazione IEC 60320-C19 e un interruttore automatico da 15 A. Ogni PDU ha un totale di 24 prese e 6 interruttori automatici.

Ciascuna delle due PDU è dotata di tre scatole di alimentazione, situate nella parte inferiore dell'armadio. Ciascuna scatola di alimentazione fornisce l'alimentazione a otto delle prese di corrente, come indicato di seguito:

- La scatola di ingresso dell'alimentazione 1, dotata di cavo di alimentazione C1, alimenta le otto prese inferiori
- La scatola di ingresso dell'alimentazione 2, dotata di cavo di alimentazione C2, alimenta le otto prese centrali
- La scatola di ingresso alimentazione 3, dotata di cavo di alimentazione C3, alimenta le otto prese superiori

Le scatole di alimentazione sono contrassegnate con C1, C2 e C3, dove i cavi di alimentazione si collegano ai moduli.

Calcolo dell'alimentazione e calcolo del calore per l'armadio

Componente	KVA	Watt	BTU/HR
PDU cabinet (72A PDU)	14.4	14400	49176
Cabinet PDU/banco 12A (72A PDU)	2.40*	2400*	8196*
Tray di dischi controller E2612	0.437	433	1476
Tray di dischi controller E2624	0.487	482	1644
Tray di dischi controller E2660	1.128	1117	3810

Componente	KVA	Watt	BTU/HR
E2712 tray di dischi controller	0.516	511	1744
Vassoio del disco controller E2724	0.561	555	1894
Tray di dischi controller E2760	1.205	1193	4072
Tray di dischi controller E5412	0.558	552	1883
Tray di dischi controller E5424 e flash array EF540	0.607	601	2051
Tray di dischi controller E5460	1.254	1242	4237
Tray di dischi controller E5512	0.587	581	1982
Tray di dischi controller E5524 e flash array EF550	0.637	630	2150
Tray di dischi controller E5560	1.285	1272	4342
Tray di dischi controller E5612	0.625	619	2111
Tray di dischi controller E5624 e flash array EF560	0.675	668	2279
Tray di dischi controller E5660	1.325	1312	4477
Vassoio del disco DE1600	0.325	322	1099
Vassoio del disco DE5600	0.375	371	1267
Vassoio del disco DE6600	0.1.011	1001	3415

Numero massimo di vassoi

Il numero massimo di vassoi che è possibile installare in un cabinet 3040 40U dipende dall'altezza di ciascun vassoio nelle unità rack (U).

Altezze dei vassoi nelle unità rack (U)

Ogni unità rack è di 4.45 cm (1.75 pollici). Ad esempio, è possibile installare fino a dieci vassoi 4U, fino a venti vassoi 2U o una combinazione di vassoi 2U e 4U, fino a 40U.

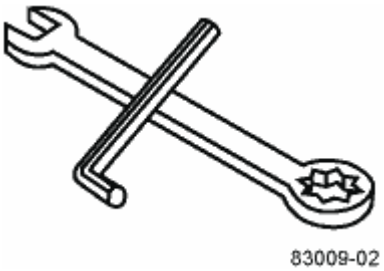
Vassoio	Unità rack (U)
Tray di dischi controller E2x12 o E2x24	2U
Tray di dischi controller E2x60	4U
Tray di dischi controller E5x12 o E5x24	2U
Tray di dischi controller E5x60	4U
Flash Array EF5x0	2U
Vassoio del disco DE1600	2U
Vassoio del disco DE5600	2U
Vassoio del disco DE6600	4U

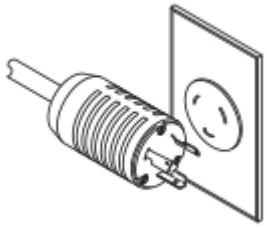
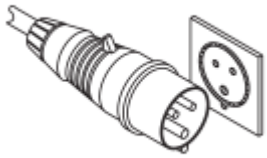
Raccogliere gli strumenti e le apparecchiature necessari

Prima di installare l'armadio 3040 40U, assicurarsi di disporre degli strumenti e delle apparecchiature necessari.

Fase

1. Raccogliere tutti gli elementi elencati nella seguente tabella.

	Elemento	Incluso con il cabinet
	**3/4" Chiave** (fornita nella cassa di spedizione) — per sollevare e abbassare i piedini di livellamento sotto l'armadietto. **1/4-in. Chiave Allen** — per sollevare e abbassare il piede di stabilità nella parte anteriore dell'armadio.	✓

	Elemento	Incluso con il cabinet
NEMA L6-30 	**Cavi di alimentazione CA** — per collegare l'armadio a fonti di alimentazione esterne (prese a muro). • I connettori NEMA L6-30 sono destinati all'uso negli Stati Uniti e in Canada. • I connettori IEC-60309 sono destinati all'uso in tutto il mondo, ad eccezione di Stati Uniti e Canada. Ciascuna PDU deve essere collegata a una fonte di alimentazione indipendente.	✔
IEC-60309 		**Cavi SAS** (opzionali): Due cavi sono inclusi in ogni tray di dischi, mentre i cavi lato host devono essere acquistati separatamente. **Cavi di comunicazione** (opzionali) – per collegare il vassoio all'host. Per ulteriori informazioni, consultare la guida di installazione del vassoio del disco del controller appropriata.
		**Spole per cavi montabili** – installate lungo entrambi i lati delle prese di distribuzione dell'alimentazione verticale per alloggiare cavi di lunghezza e instradamento in eccesso. Ogni cassetto del disco del controller include due spool per i cavi Gli spool dei cavi vengono forniti anche con i tray di dischi standalone.
✔		**Shears** – per tagliare le fasce metalliche sulla cassa di spedizione.

	Elemento	Incluso con il cabinet
		Carrello elevatore (opzionale) – per rimuovere il cabinet dal pallet di spedizione.
		Kit pannello anteriore (opzionale) – per coprire gli alloggiamenti vuoti nella parte anteriore del cabinet.
		Buste antistatiche (opzionali) – per proteggere i componenti rimossi durante la procedura di installazione del cabinet.

Preparazione per lo spostamento del cabinet

Prepararsi a spostare il cabinet dalla posizione nell'area di ricevimento stimandone il peso totale, acclimatando il cabinet, rimuovendo i materiali di imballaggio e controllando il contenuto della spedizione.

Fase 1: Stima del peso del cabinet

Il cabinet trasporta in modo affidabile e sicuro fino a 909.1 kg (2000 lb) di capacità. È necessario conoscere il peso approssimativo del cabinet in modo da poterlo spostare in sicurezza.

Fasi

1. Utilizzare la seguente tabella per calcolare il peso totale approssimativo del cabinet.

   Il peso totale del cabinet dipende dal numero e dal tipo di vassoi installati nel cabinet.

Componente	Peso	Note
Cabinet	138.80 kg (306.0 lb)	Svuotare con lo sportello posteriore installato
Unità di distribuzione dell'alimentazione (PDU [coppia])	19.96 kg (44.0 lb)	
Guide di montaggio (coppia)	1.59 kg (3.50 lb)	
Tray di dischi controller E2612	27 kg (59.52 lb)	Configurazione massima
Tray di dischi controller E2624	26.12 kg (57.32 lb)	Configurazione massima
Tray di dischi controller E2660	105.2 kg (232 lb)	Configurazione massima

Componente	Peso	Note
E2712 tray di dischi controller	27.12 kg (59.8 lb)	Configurazione massima
Vassoio del disco controller E2724	26 kg (57.32 lb)	Configurazione massima
Tray di dischi controller E2760	105.2 kg (232 lb)	Configurazione massima
Tray di dischi controller E5412	27.92 (61.52 lb)	Configurazione massima
Vassoio del disco controller E5424	26.92 kg (59.32 lb)	Configurazione massima
Tray di dischi controller E5460	105.2 kg (232 lb)	Configurazione massima
Tray di dischi controller E5512	28.89 kg (63.7 lb)	Configurazione massima
Tray di dischi controller E5524	27.9 kg (61.52 lb)	Configurazione massima
Tray di dischi controller E5560	107.13 kg (236.2 lb)	Configurazione massima
Tray di dischi controller E5612	28.89 kg (63.7 lb)	Configurazione massima
Tray di dischi controller E5624	27.9 kg (61.52 lb)	Configurazione massima
Tray di dischi controller E5660	107.13 kg (236.2 lb)	Configurazione massima
Flash array EF540	23.64 kg (52.12 lb)	Configurazione massima
Flash array EF550	24.63 kg (54.32 lb)	Configurazione massima
Flash array EF560	24.63 kg (54.32 lb)	Configurazione massima
Vassoio del disco DE1600	26.3 kg (58 lb)	Configurazione massima
Vassoio del disco DE5600	25.31 kg (55.8 lb)	Configurazione massima
Vassoio del disco DE6600	104.1 kg (229.6 lb)	Configurazione massima

2. Rivedere le seguenti note.

Rimuovere tutti i dischi dal vassoio del disco DE6600 prima di spostare il cabinet nella posizione finale.

Possibili danni alle apparecchiature — gli armadi con i cassetti per unità DE6600 vengono forniti senza unità per ridurre il peso di spedizione. Poiché un cabinet completamente popolato con cassetti per dischi DE6600 può pesare più di 1247.3 kg (2750 lb), assicurarsi di spostare il cabinet in posizione prima di caricare i dischi e assicurarsi che la capacità di carico a pavimento del cabinet di destinazione supporti tale peso.

Possibili danni ai componenti dei vassoi — non posizionare un vassoio per unità DE6600 su una superficie piana. Installare il vassoio dell'unità DE6600 nel cabinet prima di utilizzare o spostare i cassetti.

Fase 2: Acclimatare il cabinet

Prima di rimuovere i materiali di imballaggio, assicurarsi che l'armadietto e i vassoi siano in grado di essere utilizzati in ambienti interni.

Fasi

1. Se la temperatura esterna è inferiore a 0°C (32°F), lasciare il cabinet e i vassoi all'interno delle cassette per almeno 24 ore per evitare la formazione di condensa.
2. Aumentare o diminuire il periodo di stabilizzazione di 24 ore in base alla temperatura esterna all'arrivo.

Possibili danni ai componenti del vassoio — se la temperatura esterna è inferiore a 0°C (32°F) quando si riceve il cabinet e i vassoi, non disimballarli immediatamente o non estrarli. L'esposizione di componenti freddi a temperature interne calde può causare condensa, con conseguenti danni o guasti ai componenti.

Fase 3: Rimuovere i materiali di imballaggio

Rimuovere i materiali di imballaggio solo dopo che il cabinet si è acclimatato alla temperatura interna.

Fasi

1. Fare riferimento alle istruzioni di disimballaggio riportate sul lato anteriore della cassa di spedizione.
2. Rimuovere il materiale di imballaggio seguendo le istruzioni allegate.

Fase 4: Controllare il contenuto della spedizione

Controllare il contenuto della spedizione per assicurarsi che tutte le apparecchiature siano arrivate al sito.

Fasi

1. Confrontare la distinta di imballaggio con l'apparecchiatura ricevuta.
2. Assicurarsi che tutte le apparecchiature siano arrivate al sito.
3. In caso di elementi mancanti, contattare il rappresentante commerciale.

Fase 5: Rimuovere i componenti pesanti dal cabinet

Rimuovere alcuni dei componenti più pesanti posizionati nella parte superiore dell'armadio per garantire la massima stabilità.

Prima di iniziare

- Assicurarsi che il peso massimo non superi i 2000 libbre prima di spostare l'armadietto.

- Prendere nota della posizione di ciascun vassoio, componente e cavo prima di rimuoverlo, in modo da poter reinstallare ciascun elemento nella posizione originale.

Fasi

1. Registrare la configurazione del cavo per il riassemblaggio futuro se è necessario scollegare i cavi.
2. Rimuovere i vassoi delle unità e dei dischi controller nella metà superiore del cabinet. Tenere tutti i componenti dello stesso vassoio insieme.

   Non è necessario rimuovere gli alimentatori o altri componenti dal retro di ciascun vassoio

3. Collocare ciascun componente in un sacchetto antistatico separato. Se sono disponibili le scatole di spedizione originali, utilizzarle per trasportare i componenti.

Spostare il cabinet nella posizione permanente

L'armadio 3040 40U è dotato di rotelle per impieghi pesanti che consentono di spostare l'armadio nella sua posizione permanente.

Prima di iniziare

- Leggere le istruzioni per rimuovere il cabinet dal pallet senza utilizzare un carrello elevatore a forche.

  Le casse di spedizione forniscono rampe e istruzioni integrate. Fare riferimento alle istruzioni di disimballaggio riportate sul lato anteriore della cassa di spedizione.

- Valutare tutte le rampe tra il dock di caricamento e la destinazione finale del cabinet.

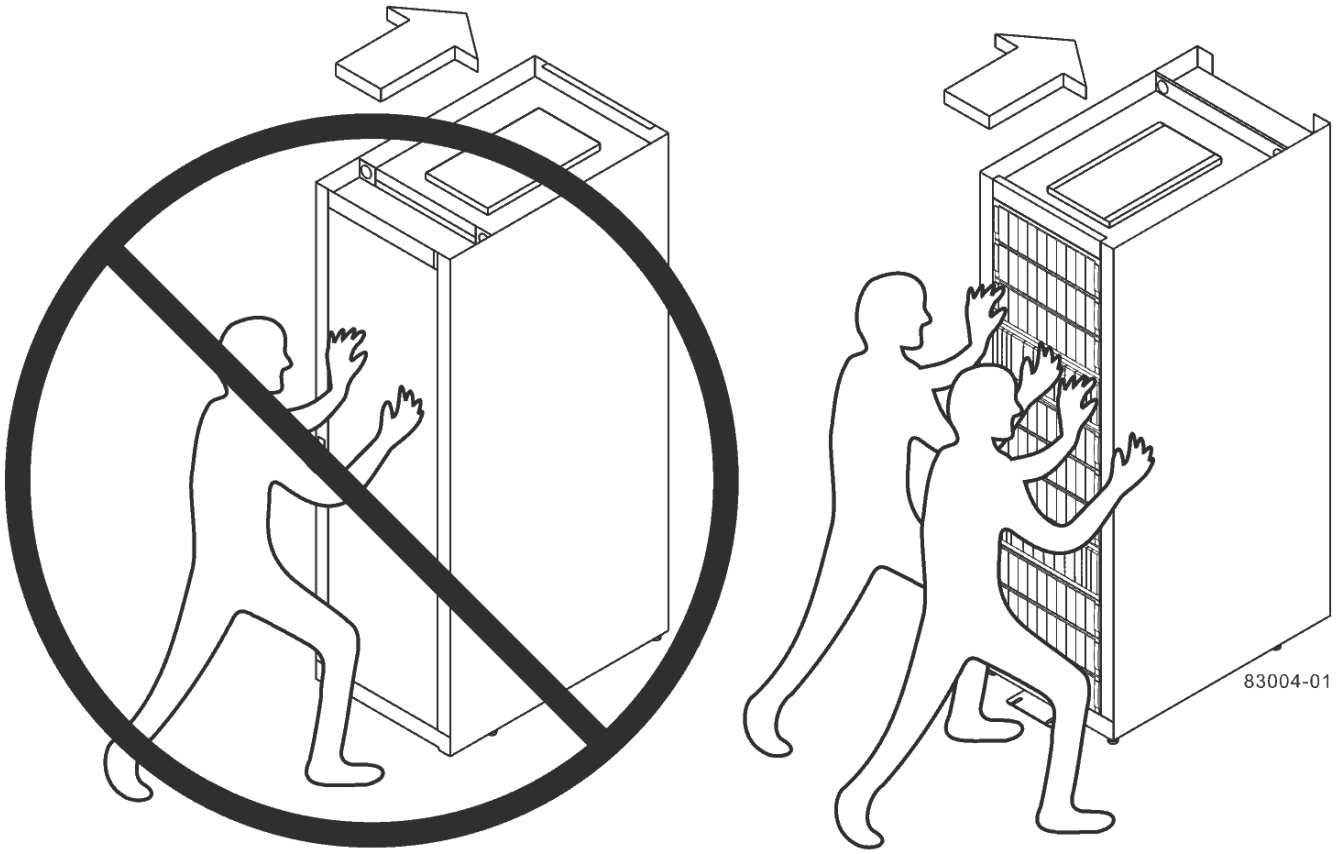
  È necessario valutare tutte le rampe per assicurarsi che il baricentro del cabinet (quando il cabinet si trova su una rampa e si trova ad angolo) non si estenda oltre l'ingombro del cabinet.

A proposito di questa attività

Molti cabinet sono popolati con i vassoi delle unità. Questa situazione comporta la maggior parte del peso nella parte anteriore dell'armadio, rendendo il baricentro più vicino alla parte anteriore.

Fasi

1. Rimuovere i dispositivi più in alto nel cabinet per assicurarsi che il cabinet venga trasportato in modo sicuro nella posizione finale. Ciò è particolarmente importante se una rampa presenta un'inclinazione o un calo superiore a 10 gradi.
2. Spostare il cabinet nella sua posizione permanente utilizzando il metodo corretto mostrato nella figura seguente. Assicurarsi di premere la parte anteriore del cabinet e non la parte posteriore.



Rear of Cabinet

Front of Cabinet

Installazione completa del cabinet

Dopo aver spostato il cabinet, abbassare i piedini di livellamento e il piedino di stabilità, reinstallare i componenti rimossi, installare gli altri componenti necessari e collegare il cabinet all'alimentazione.

Fase 1: Abbassare i piedini di livellamento e il piedino di stabilità

È possibile stabilizzare il cabinet regolando i relativi piedini. I piedini di livellamento sostengono l'armadio dalle rotelle. Il piedino di stabilità impedisce al cabinet di cadere dopo che è stato collocato nella sua posizione permanente.

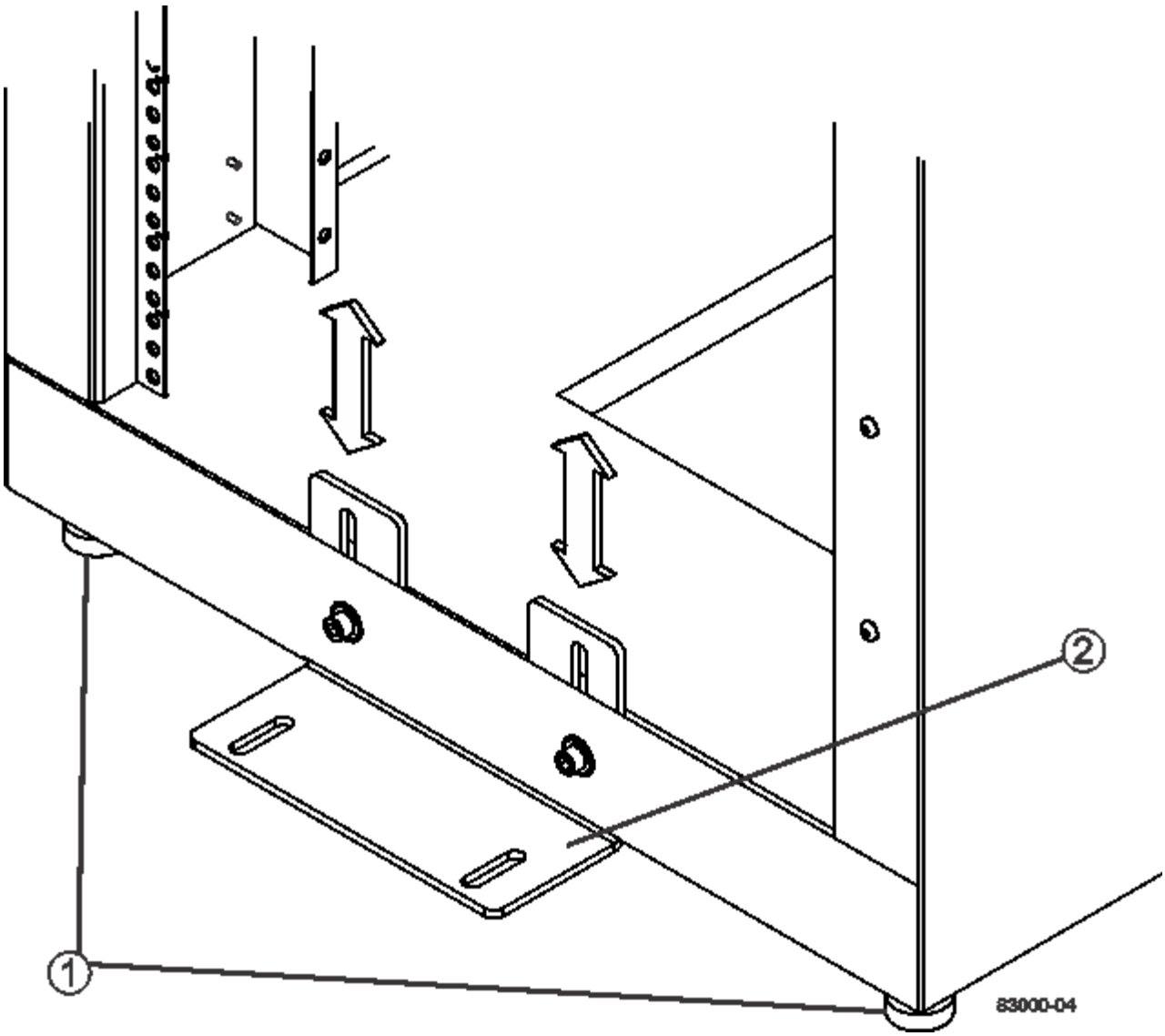
Fasi

1. Abbassare i piedini di livellamento per sostenere l'armadio dalle rotelle.

   I piedini di livellamento si trovano vicino a ciascun angolo inferiore del cabinet.

2. Assicurarsi che l'armadio sia il più possibile in piano.

   La figura seguente fornisce una vista ravvicinata del piede di stabilità e dei piedini di livellamento.



1.	
Piedini di livellamento	
2.	
Piede di stabilità	

Fase 2: Reinstallazione dei vassoi

Dopo aver spostato il cabinet, è possibile reinstallare i vassoi nelle posizioni originali.

> *Non* installare i seguenti vassoi nella parte superiore del cabinet sopra la testa. Una volta popolati, ciascuno di questi vassoi pesa oltre 100 kg (220 lb). Se installati nella parte superiore del cabinet, questi vassoi creano un cabinet pesante che può facilmente sbilanciarsi: E2660, E2660, E2760, E5460, E5560, E i vassoi del disco controller E5660, nonché il vassoio del disco DE6600

Fasi

1. Reinstallare tutti i vassoi nella posizione originale nel cabinet.

> **Rischio di lesioni fisiche** — un vassoio vuoto pesa circa 56.7 kg (125 lb). Sono necessarie tre persone per spostare in sicurezza un vassoio vuoto Se il vassoio contiene dei componenti, è necessario un sollevamento meccanico per spostare il vassoio in modo sicuro

2. Reinstallare tutti i componenti nelle posizioni originali nei vassoi.

   Per evitare conflitti di indirizzi e perdita di accesso ai dati, sostituire tutti i componenti nello stesso vassoio e nella stessa posizione nel vassoio

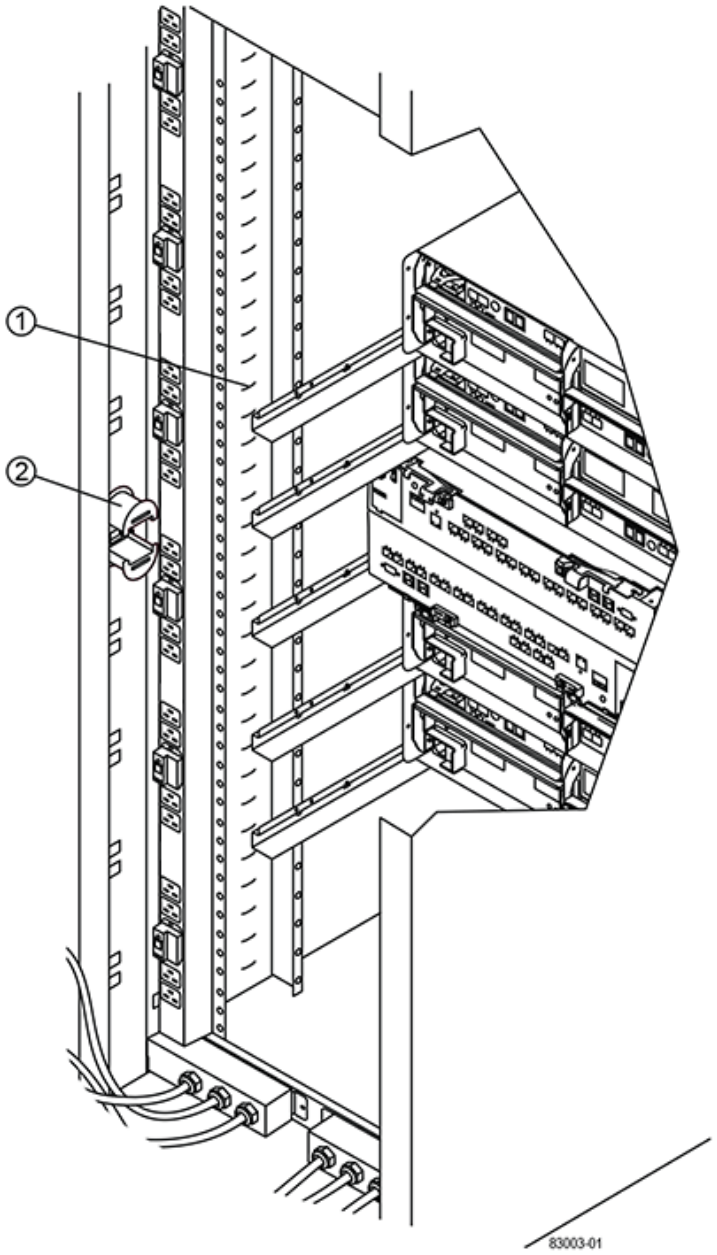
3. Reinstallare tutti i cavi nelle posizioni originali nei vassoi.
4. Instradare i cavi di interfaccia verso il cabinet.
5. Instradare i cavi di alimentazione principale dal cabinet alle due fonti di alimentazione esterne. *Non* collegare i cavi di alimentazione.

Fase 3: Installare gli spool dei cavi e le fascette

Dopo aver reinstallato i vassoi, installare gli spool dei cavi e le fascette. Gli spool dei cavi e le fascette sono adatti alla lunghezza e all'instradamento dei cavi in eccesso per i controller e i vassoi.

Fase

1. Installare gli steli dei cavi e le fascette avvolti lungo entrambi i lati delle prese di distribuzione dell'alimentazione verticali.



1.	
Ubicazione della fascetta	
2.	
Spola del cavo	

Fase 4: Installare vassoi aggiuntivi

Se necessario, è possibile installare vassoi aggiuntivi. Per garantire il corretto flusso d'aria, è necessario coprire le posizioni inutilizzate dei vassoi.

Fasi

1. Se si dispone di vassoi aggiuntivi che devono essere installati, installare la bulloneria di montaggio per questi vassoi.
2. Se la parte anteriore del cabinet non è completamente piena di vassoi, utilizzare i kit del pannello anteriore per coprire gli spazi vuoti sopra o sotto i vassoi installati.

   La copertura degli spazi vuoti è necessaria per mantenere il corretto flusso d'aria attraverso l'armadio.

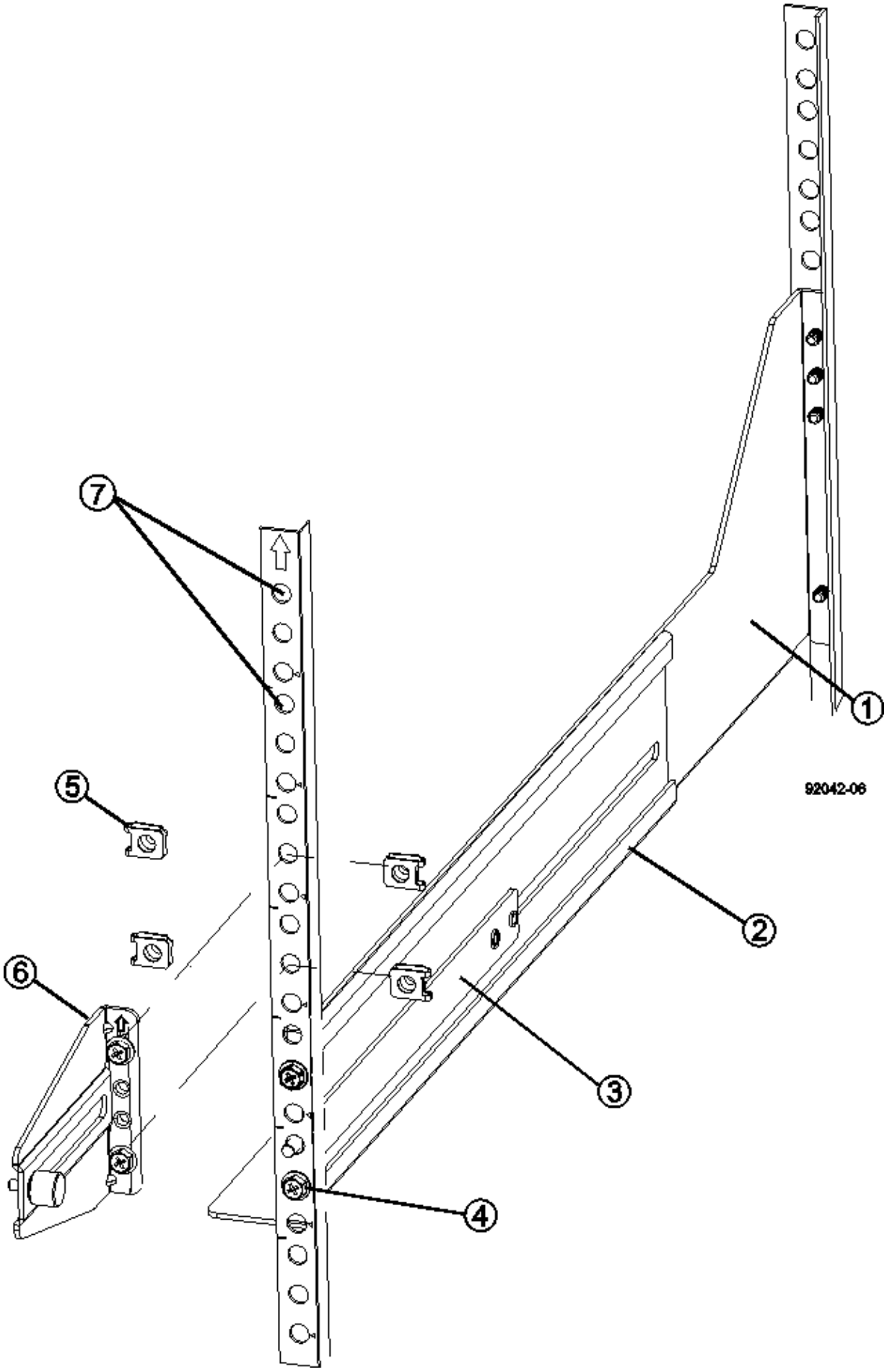
3. Accendere i vassoi.

Fase 5: Installare guide di montaggio aggiuntive

Se si installano i vassoi del disco controller o i vassoi del disco forniti separatamente (non già installati nel cabinet), potrebbe essere necessario installare ulteriori guide di montaggio nel cabinet.

Fasi

1. Determinare la posizione delle guide di montaggio.
   - **Sopra un vassoio esistente** — posizionare le guide di montaggio immediatamente sopra il vassoio superiore nel cabinet.
   - **Sotto un vassoio esistente** — posizionare le guide di montaggio con spazio sufficiente per sostenere il vassoio da installare:
     - 8.9 cm (3.5") Per vassoi di dischi o controller 2U
     - 17.8 cm Per vassoi di dischi o controller 4U
2. Utilizzare i contrassegni di misurazione sui supporti verticali anteriori destro e sinistro per fissare le guide di montaggio nella stessa posizione su ciascun lato dell'armadio.


7
1
92042-06
5
2
6
3
4

1.
Guida regolabile anteriore
2.
Guida regolabile posteriore
3.
Piastra di regolazione e viti
4.
Viti M5×10 mm per montaggio su guida
5.
Dadi di fissaggio
6.
Staffa di fissaggio posteriore
7.
Supporto verticale

> I dadi a clip e la staffa di fissaggio posteriore non vengono utilizzati quando le guide sono installate in un cabinet 3040.

3. Posizionare la guida regolabile posteriore sul supporto verticale.
4. Sulla guida regolabile posteriore, allineare i fori delle guide regolabili davanti ai fori del supporto verticale.
5. Fissare due viti M5×10 mm.
   a. Fissare le viti attraverso la guida di supporto verticale e la guida regolabile posteriore.
   b. Serrare le viti.
6. Posizionare la guida regolabile anteriore sul supporto verticale.
7. Sulla guida regolabile anteriore, allineare i fori delle guide regolabili davanti ai fori del supporto verticale.
8. Fissare due viti M5×10 mm.
   a. Inserire una vite attraverso la guida di supporto verticale e il foro inferiore della guida regolabile anteriore.
   b. Inserire una vite nella guida di supporto verticale e al centro dei tre fori superiori nella guida regolabile anteriore.

c. Serrare le viti.

> I due fori per le viti rimanenti vengono utilizzati per montare il vassoio

9. Ripetere i passaggi da 3 a 8 per fissare la seconda guida sull'altro lato del cabinet.
10. Installare ciascun vassoio attenendosi alle istruzioni di installazione applicabili.
11. Scegliere una delle seguenti opzioni:
    - Se tutte le posizioni dei vassoi sono piene, accendergli.
    - Se non tutte le posizioni dei vassoi sono piene, utilizzare i kit del pannello anteriore per coprire gli spazi vuoti sopra o sotto i vassoi installati.

Fase 6: Collegare il cabinet all'alimentazione

Per completare l'installazione del cabinet, accendere i componenti del cabinet.

A proposito di questa attività

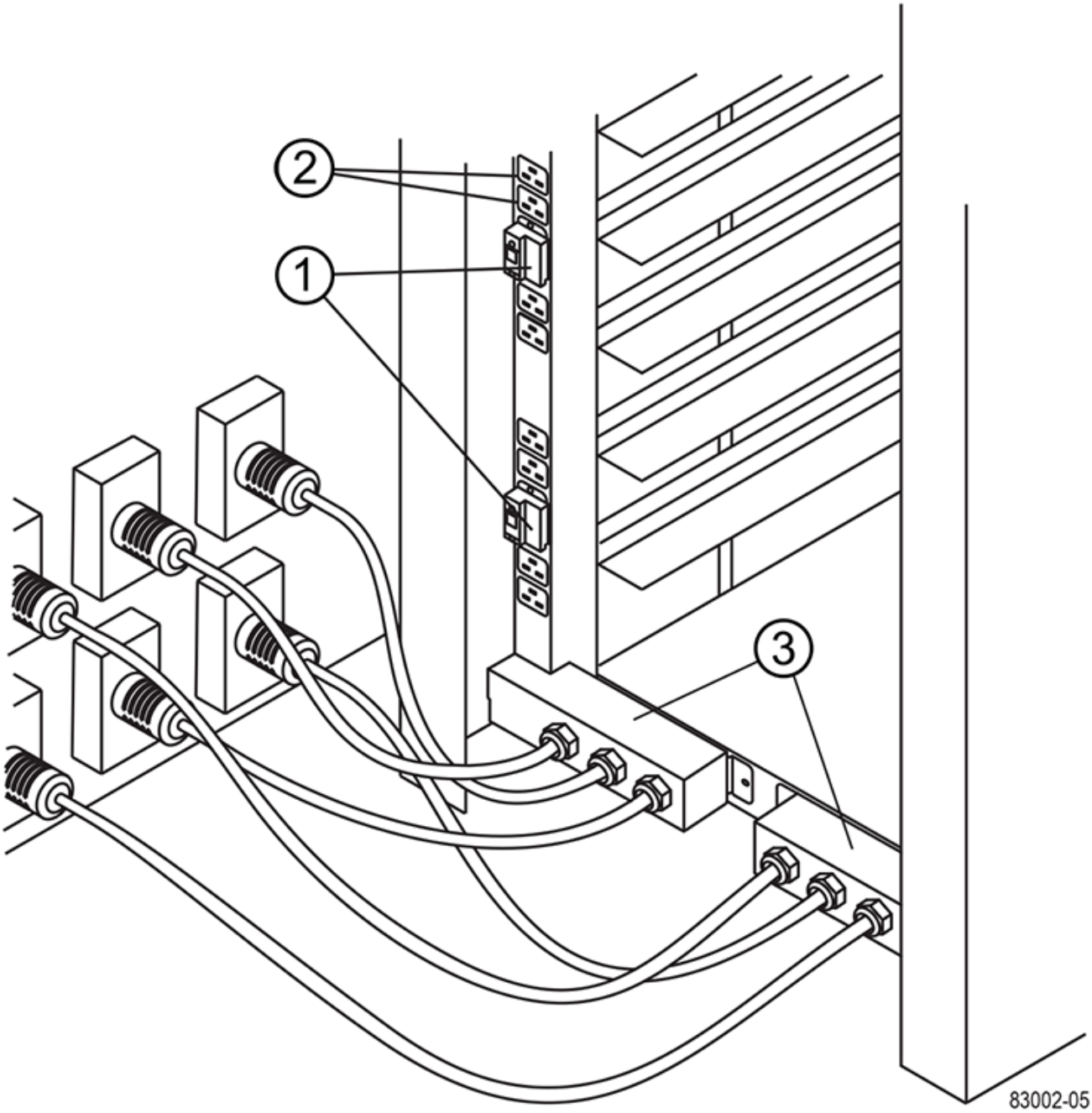
Mentre i vassoi eseguono la procedura di accensione, i LED sulla parte anteriore e posteriore dei vassoi lampeggiano. A seconda della configurazione, il completamento della procedura di accensione può richiedere alcuni minuti.

Fasi

1. Spegnere tutti i componenti del cabinet.
2. Portare tutti e 12 gli interruttori automatici in posizione Off (giù).
3. Collegare ciascuno dei sei connettori NEMA L6-30 (Stati Uniti e Canada) o i sei connettori IEC 60309 (in tutto il mondo, ad eccezione di Stati Uniti e Canada) a una presa elettrica disponibile.

> È necessario collegare ciascuna PDU a una fonte di alimentazione indipendente all'esterno dell'armadio.

4. Portare tutti e 12 gli interruttori automatici nella posizione ON (su).



1.
Interruttori automatici
2.
Prese elettriche
3.
Scatole di alimentazione

5. Accendere tutti i vassoi delle unità del cabinet.

> Attendere 30 secondi dopo aver acceso i vassoi delle unità prima di accendere i vassoi delle unità del controller.

6. Dopo aver acceso i vassoi delle unità, attendere 30 secondi, quindi accendere tutti i vassoi dei dischi del controller nel cabinet.

Risultato

L'installazione del cabinet è completata. È possibile riprendere le normali operazioni.

Hardware per il montaggio in rack

Utilizzare i collegamenti riportati di seguito per accedere alla documentazione che descrive come installare l'hardware per il montaggio su rack.

Guide di supporto regolabili

Accesso "Installazione delle guide di supporto regolabili" per l'installazione di un vassoio del disco controller o di un vassoio del disco spedito separatamente (non già installato nel cabinet). Questa procedura si applica ai seguenti vassoi 2U (9 cm o 3.5 pollici):

- DE1600 o DE5600
- E2612 o E2624
- E5412, E5424, E5512 O E5524

Rack a due montanti — 2U

Accesso "Installazione dell'apparecchiatura 2U in un rack a due montanti".

Rack o cabinet a quattro montanti — 2U

Accesso "Installazione di un enclosure 2U da 12 dischi in un rack o cabinet a quattro montanti".

Rack a quattro montanti - SuperRail

Accesso "Installazione di SuperRail in un rack a quattro montanti (shelf DE224C/DE460C)".

Cablaggio

Panoramica dei cavi

È possibile collegare un host direttamente a un controller o utilizzare gli switch per collegare un host a un controller.

Se il sistema di storage include uno o più shelf di dischi, è necessario collegarlo al proprio shelf di controller. È possibile aggiungere un nuovo shelf di dischi mentre l'alimentazione è ancora applicata ad altri componenti del sistema di storage. Inoltre, è possibile collegare il sistema storage a una rete per la gestione fuori banda.

Le informazioni sui cavi sono destinate a un installatore dell'hardware o a un amministratore di sistema che sta installando o espandendo un sistema storage. Si presuppone che il sistema storage sia stato installato come descritto nelle *istruzioni di installazione e configurazione* dell'hardware.

Modello hardware applicabile

Le informazioni sul cablaggio si applicano ai seguenti modelli hardware.

Ripiano controller	Shelf di dischi
EF300, EF600	DE212C, DE224C, DE460
E5724, EF570, E2812, E2824, EF280	DE212C, DE224C
E2860, E5760	DE460C

Ulteriori informazioni sul cablaggio

Se si utilizzano cavi per la seguente configurazione, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente."

Ripiano controller	Shelf di dischi
E2712, E2724, E5612, E5624, EF560	DE212C, DE224C
E2760, E5660	DE460C

Per informazioni sul cablaggio per il supporto delle funzioni di mirroring, consultare "Guida alla distribuzione e descrizioni delle funzionalità di mirroring sincrono e asincrono".

Requisiti

Oltre agli shelf di controller e agli shelf di dischi, potrebbero essere necessari alcuni o tutti i seguenti componenti per il cablaggio del sistema storage:

- Cavi: SAS, Fibre Channel (FC), Ethernet, InfiniBand
- Ricetrasmettitori SFP (Small form-factor pluggable) o QSFP (Quad SFP)
- Switch
- HBA (host bus adapter)
- Host Channel Adapter (HCA)
- Schede di interfaccia di rete (NIC)

Cablaggio host

È possibile collegare un host direttamente a un controller (topologia direct-attached) o utilizzare switch (topologia switch) per collegare un host a un controller.

Cablaggio per una topologia a collegamento diretto

Una topologia direct-attached connette gli adattatori host direttamente ai controller del sistema storage.

La figura seguente mostra un esempio di connessione. Per garantire le massime prestazioni, utilizzare tutte le porte dell'adattatore host disponibili.

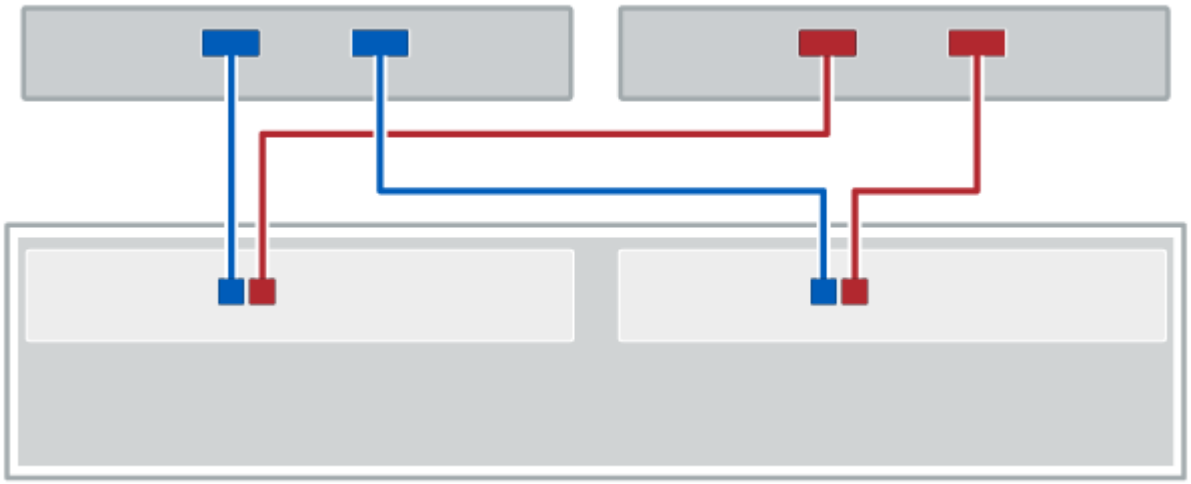


Figura 1. Due host e due controller

(1) *collegare ciascuna porta dell'adattatore host direttamente alle porte host dei controller.*

Cablaggio per una topologia di switch

Una topologia di switch utilizza gli switch per connettere gli host ai controller del sistema storage. Lo switch deve supportare il tipo di connessione utilizzato tra l'host e il controller.

La figura seguente mostra un esempio di connessione. Per gli switch che offrono funzionalità di provisioning, è necessario isolare ogni coppia di iniziatori e di destinazione.

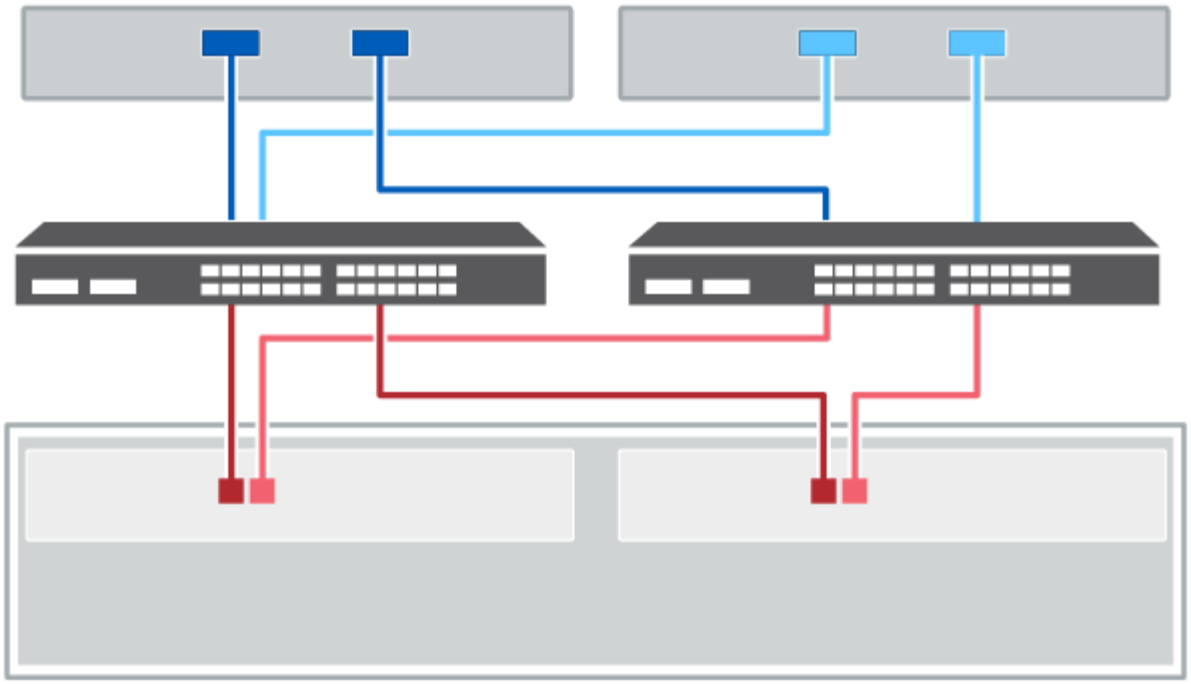


Figura 2. Due host e due switch

(1) *collegare ogni adattatore host direttamente allo switch.*

(2) *collegare ogni switch direttamente alle porte host dei controller. Per garantire le massime prestazioni, utilizzare tutte le porte dell'adattatore host disponibili.*

Cablaggio dello shelf di dischi

È necessario collegare ciascun controller nello shelf di controller a un modulo i/o (IOM) in uno shelf di dischi.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

Cablaggio E2800 ed E5700

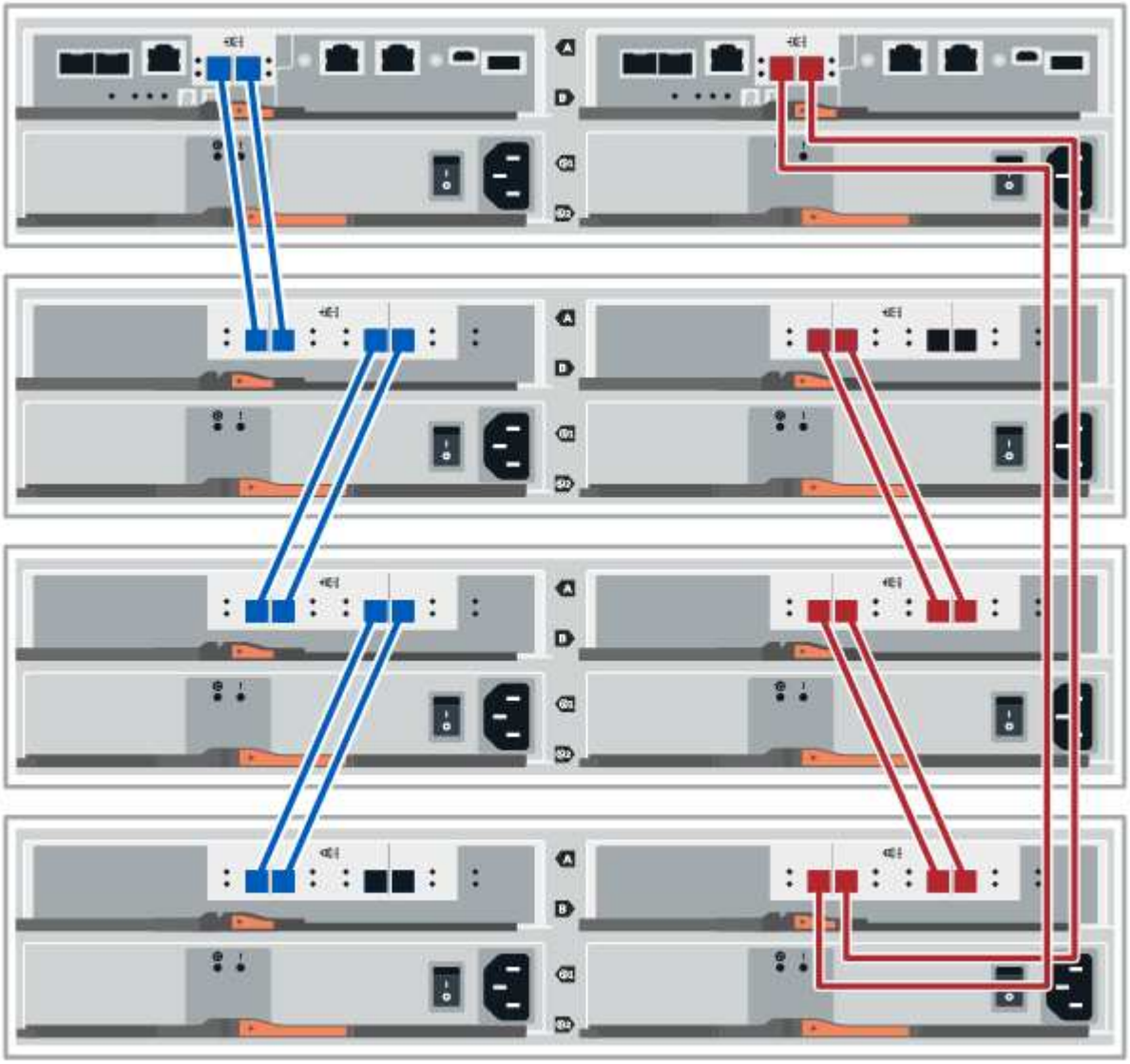
Le seguenti informazioni si applicano al cablaggio di E2800, E2800, EF280, E5700, EF5700B, Oppure EF570 su uno shelf di dischi DE212C, DE224C o DE460.

Cablaggio di uno shelf da 12 o 24 dischi

È possibile collegare lo shelf del controller a uno o più shelf da 12 o 24 dischi.

L'immagine seguente mostra una rappresentazione dello shelf del controller e degli shelf di dischi. Per individuare le porte sul modello in uso, vedere "Hardware Universe".

Uno shelf di controller e shelf da 12 o 24 dischi

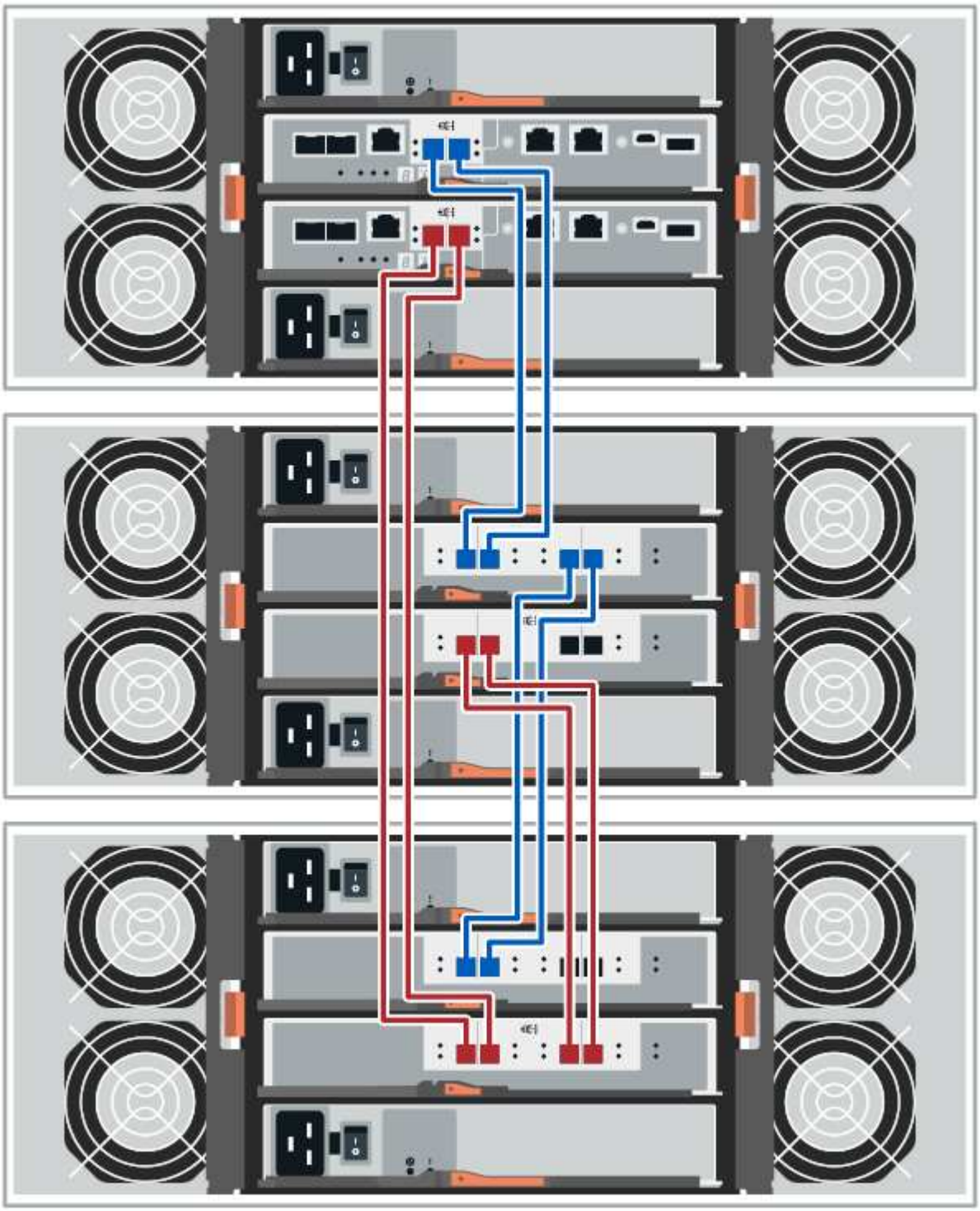


Cablaggio di uno shelf da 60 dischi

È possibile collegare lo shelf del controller a uno o più shelf da 60 dischi.

L'immagine seguente mostra una rappresentazione dello shelf del controller e degli shelf di dischi. Per individuare le porte sul modello in uso, vedere "Hardware Universe".

Uno shelf di controller e 60 shelf di dischi



Cablaggio EF300 ed EF600

Le seguenti informazioni si applicano al cablaggio di uno shelf di controller EF300 o EF600 su uno shelf di dischi DE212C, DE224C o DE460.

Prima di iniziare

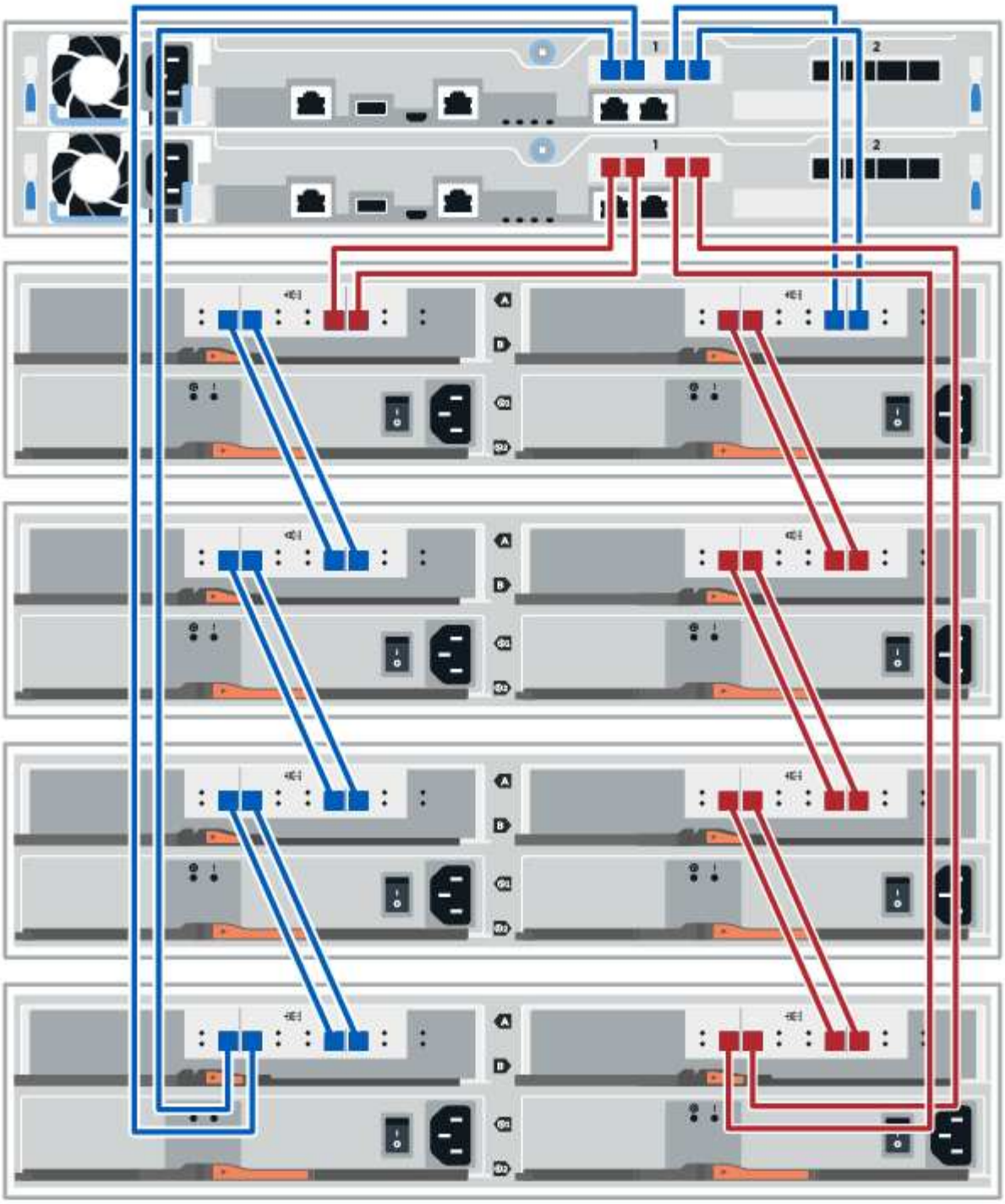
Prima di collegare un dispositivo EF300 o EF600, assicurarsi che il firmware sia aggiornato alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".

Cablaggio di uno shelf da 12 o 24 dischi

È possibile collegare lo shelf del controller a uno o più shelf da 12 o 24 dischi.

L'immagine seguente mostra una rappresentazione dello shelf del controller e degli shelf di dischi. Per individuare le porte sul modello in uso, vedere "Hardware Universe".

Uno shelf di controller e shelf da 12 o 24 dischi

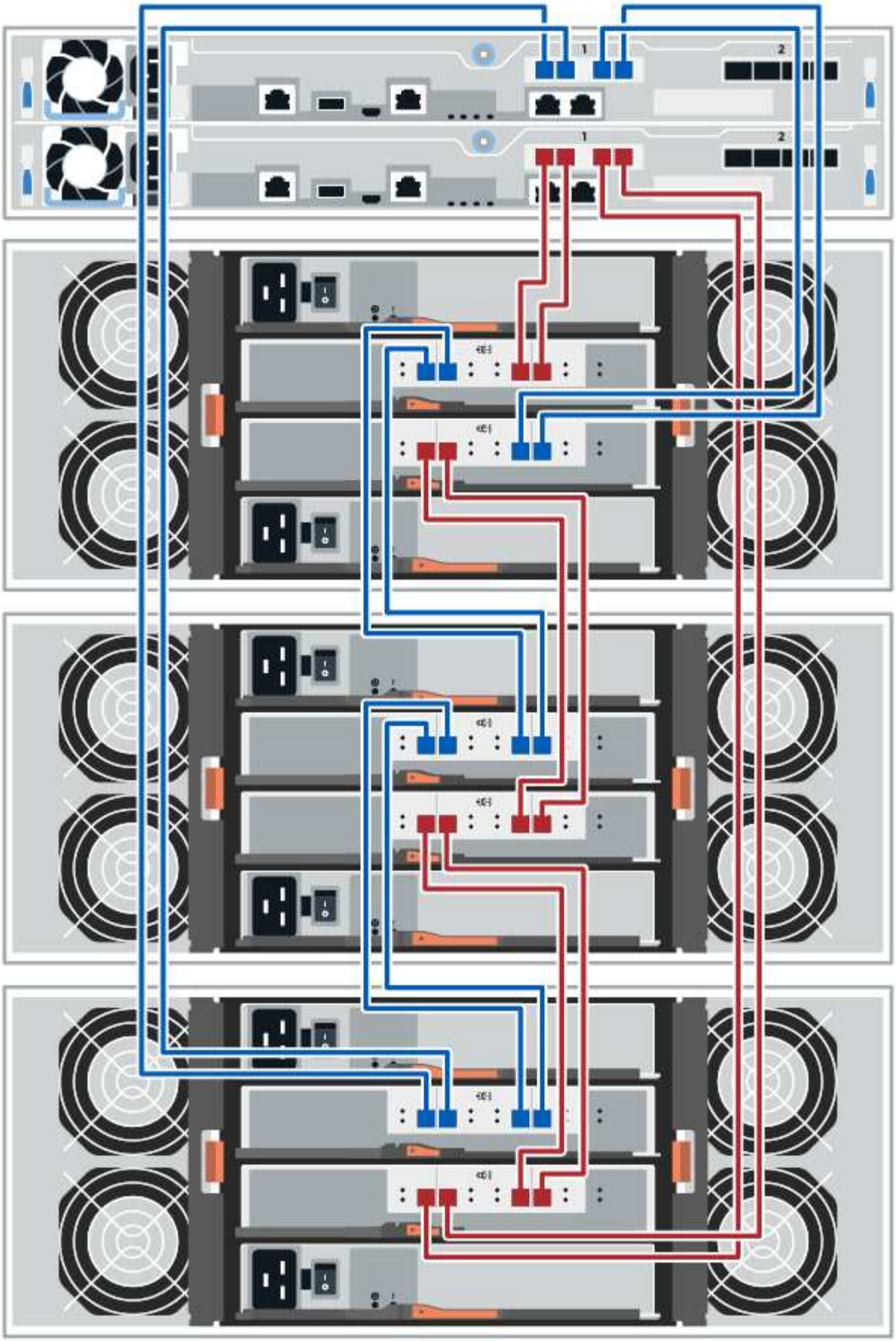


Cablaggio di uno shelf da 60 dischi

È possibile collegare lo shelf del controller a uno o più shelf da 60 dischi.

L'immagine seguente mostra una rappresentazione dello shelf del controller e degli shelf di dischi. Per individuare le porte sul modello in uso, vedere "Hardware Universe".

Uno shelf di controller e 60 shelf di dischi



Cavi di alimentazione

È necessario collegare gli alimentatori di ciascun componente a circuiti di alimentazione separati.

Prima di iniziare

- Hai confermato che la tua posizione fornisce l'alimentazione necessaria.
- I due interruttori di alimentazione sui due alimentatori dello shelf devono essere spenti.

A proposito di questa attività

La fonte di alimentazione del sistema storage deve essere in grado di soddisfare i requisiti di alimentazione del nuovo shelf di dischi. Per informazioni sul consumo energetico del sistema storage, consultare "Hardware Universe".

Fase

1. Collegare i due cavi di alimentazione per ogni shelf a diverse unità di distribuzione dell'alimentazione (PDU) nell'armadio o nel rack.

Aggiunta a caldo di uno shelf di dischi

È possibile aggiungere un nuovo shelf di dischi mentre gli altri componenti del sistema di storage sono ancora in funzione. È possibile configurare, riconfigurare, aggiungere o spostare la capacità del sistema storage senza interrompere l'accesso degli utenti ai dati.

Prima di iniziare

A causa della complessità di questa procedura, si consiglia quanto segue:

- Leggere tutti i passaggi prima di iniziare la procedura.
- Assicurarsi che l'aggiunta a caldo di uno shelf di dischi sia la procedura necessaria.

A proposito di questa attività

Questa procedura si applica all'aggiunta a caldo di uno shelf di dischi DE212C, DE224C o DE460C a E2800, E2800, EF280, E5700, E5700B, Shelf di controller EF570, EF300 o EF600.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

> Per mantenere l'integrità del sistema, seguire la procedura esattamente nell'ordine suggerito.

Fase 1: Preparazione all'aggiunta dello shelf di dischi

Per prepararsi all'aggiunta a caldo di uno shelf di dischi, è necessario verificare la presenza di eventi critici e lo stato degli IOM.

Prima di iniziare

- La fonte di alimentazione del sistema storage deve essere in grado di soddisfare i requisiti di alimentazione del nuovo shelf di dischi. Per le specifiche di alimentazione dello shelf di dischi, consultare "Hardware Universe".
- Lo schema di cablaggio per il sistema storage esistente deve corrispondere a uno degli schemi applicabili illustrati in questa procedura.

Fasi

1. In Gestore di sistema di SANtricity, selezionare **supporto** > **Centro di supporto** > **Diagnostica**.
2. Selezionare **Collect Support Data**.

   Viene visualizzata la finestra di dialogo Collect Support Data (raccolta dati di supporto).

3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome support-data.7z. I dati non vengono inviati automaticamente al supporto tecnico.

4. Selezionare **supporto** > **Registro eventi**.

   La pagina Registro eventi visualizza i dati dell'evento.

5. Selezionare l'intestazione della colonna **priorità** per ordinare gli eventi critici all'inizio dell'elenco.
6. Esaminare gli eventi critici di sistema per gli eventi che si sono verificati nelle ultime due o tre settimane e verificare che gli eventi critici recenti siano stati risolti o altrimenti risolti.

   > Se si sono verificati eventi critici non risolti nelle due o tre settimane precedenti, interrompere la procedura e contattare il supporto tecnico. Continuare la procedura solo dopo aver risolto il problema.

7. Selezionare **hardware**.
8. Selezionare l'icona **IOM (ESM)**.

   Viene visualizzata la finestra di dialogo Shelf Component Settings (Impostazioni componenti shelf) con la scheda **IOM (ESM)** selezionata.

9. Assicurarsi che lo stato visualizzato per ogni IOM/ESM sia *ottimale*.
10. Fare clic su **Mostra altre impostazioni**.
11. Verificare che sussistano le seguenti condizioni:
    - Il numero di ESM/IOM rilevati corrisponde al numero di ESM/IOM installati nel sistema e a quello di ogni shelf di dischi.
    - Entrambi gli ESM/IOM mostrano che la comunicazione è corretta.
    - La velocità di trasferimento dati è di 12 GB/s per gli shelf di dischi DE212C, DE224C e DE460C o di 6

GB/s per gli altri tray di dischi.

Fase 2: Installare lo shelf di dischi e alimentare

Si installa un nuovo shelf di dischi o uno shelf di dischi precedentemente installato, si accende l'alimentazione e si verifica la presenza di eventuali LED che richiedono attenzione.

Fasi

1. Se si sta installando uno shelf di dischi precedentemente installato in un sistema storage, rimuovere i dischi. I dischi devono essere installati uno alla volta più avanti in questa procedura.

   Se la cronologia di installazione dello shelf di dischi che si sta installando non è nota, si deve presumere che sia stato precedentemente installato in un sistema storage.

2. Installare lo shelf di dischi nel rack che contiene i componenti del sistema di storage.

   > Consultare le istruzioni di installazione del modello in uso per la procedura completa per l'installazione fisica e il cablaggio di alimentazione. Le istruzioni di installazione del modello in uso includono note e avvisi da tenere in considerazione per installare in sicurezza uno shelf di dischi.

3. Accendere il nuovo shelf di dischi e verificare che sullo shelf non siano accesi LED di attenzione color ambra. Se possibile, risolvere eventuali condizioni di guasto prima di continuare con questa procedura.

Fase 3: Collegare il sistema via cavo

Selezionare una delle seguenti opzioni:

- Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700
- Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

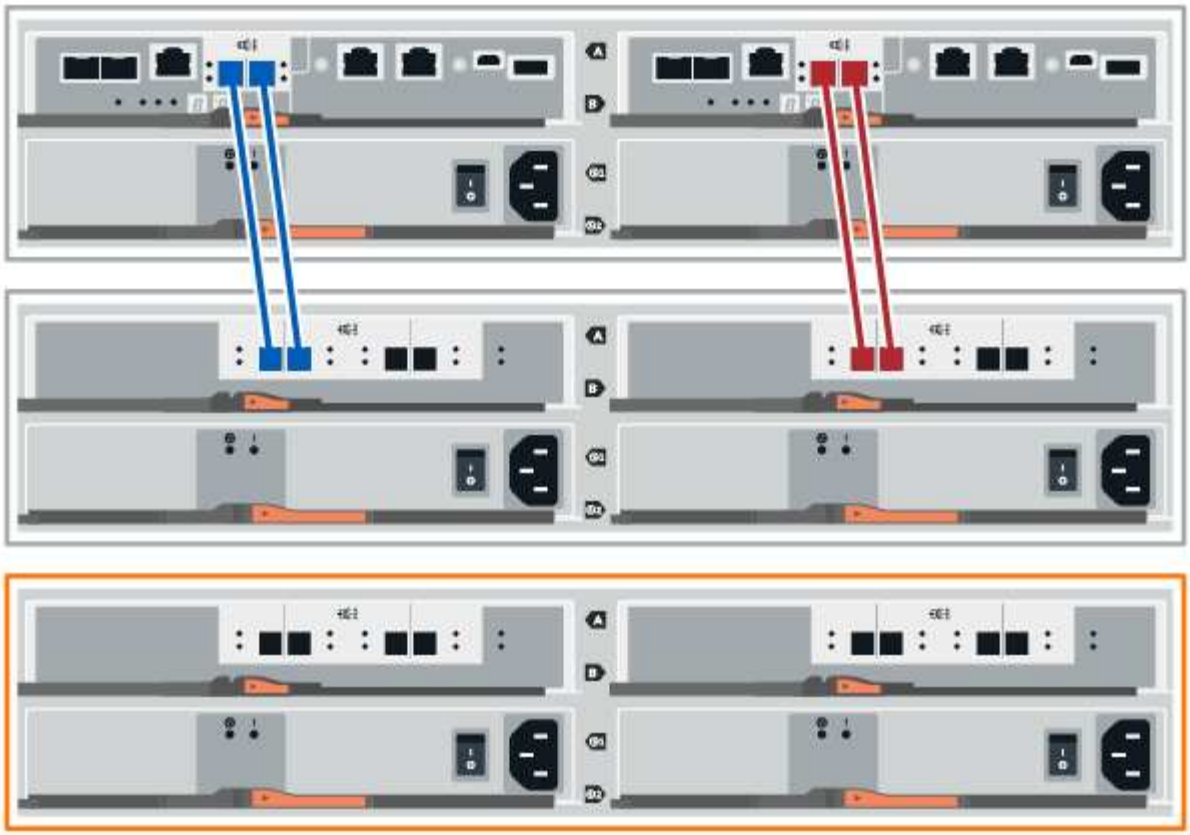
Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700

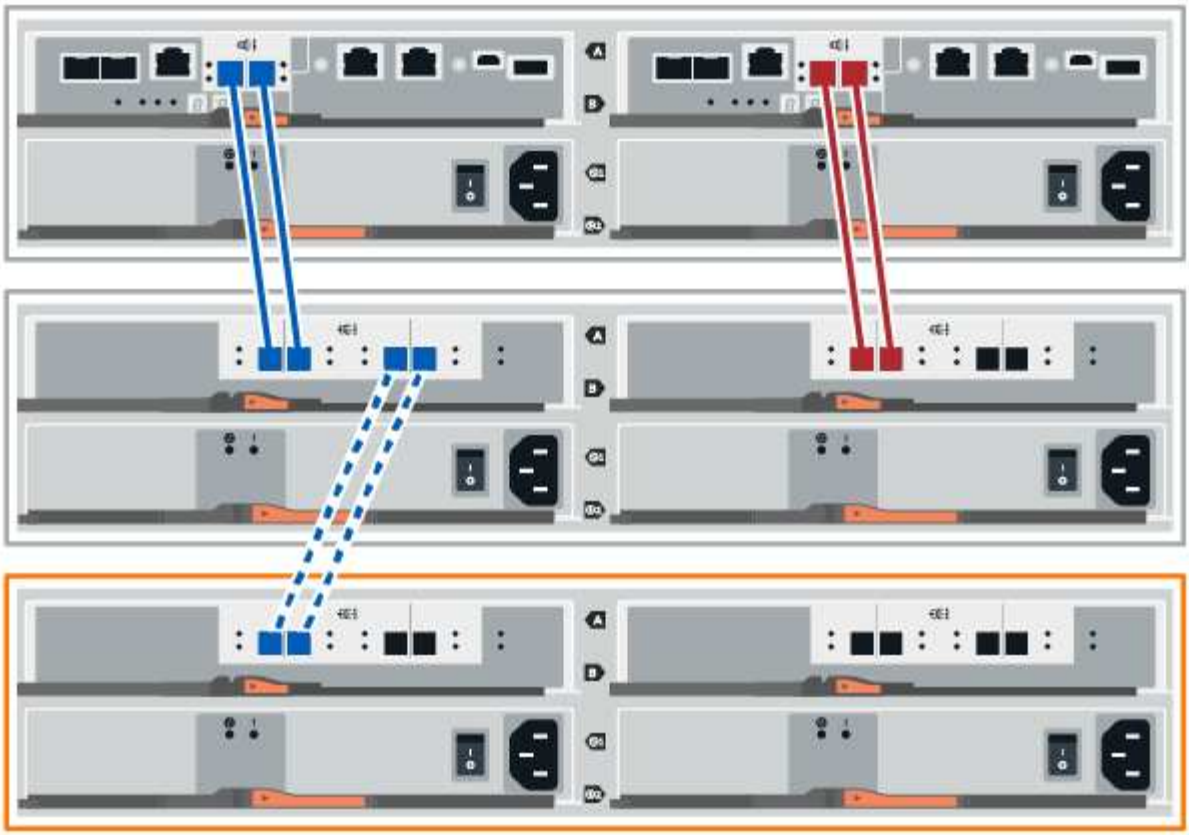
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Fasi

1. Collegare lo shelf di dischi al controller A.

   La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller A. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".





2. In Gestione sistema di SANtricity, fare clic su **hardware**.

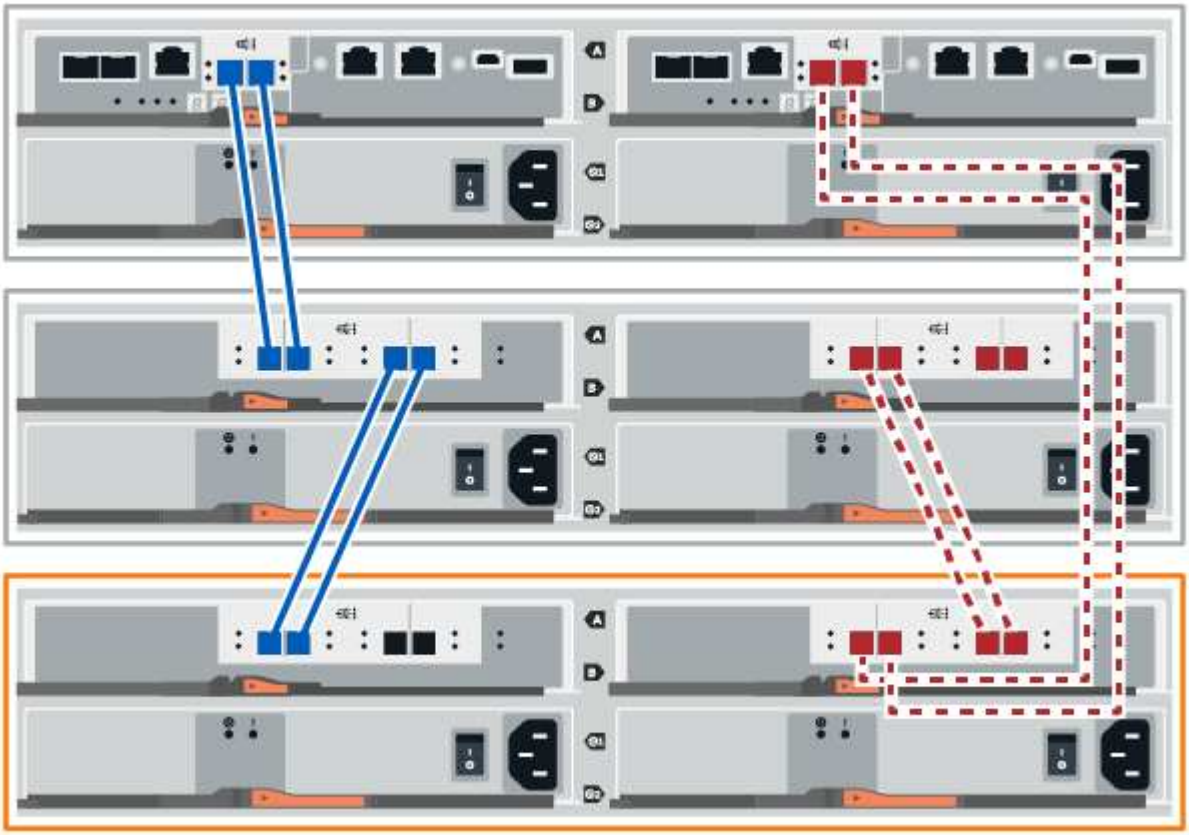
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

3. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
4. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

   Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

5. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
6. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
7. Scollegare tutti i cavi di espansione dal controller B.
8. Collegare lo shelf di dischi al controller B.

La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller B. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



9. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

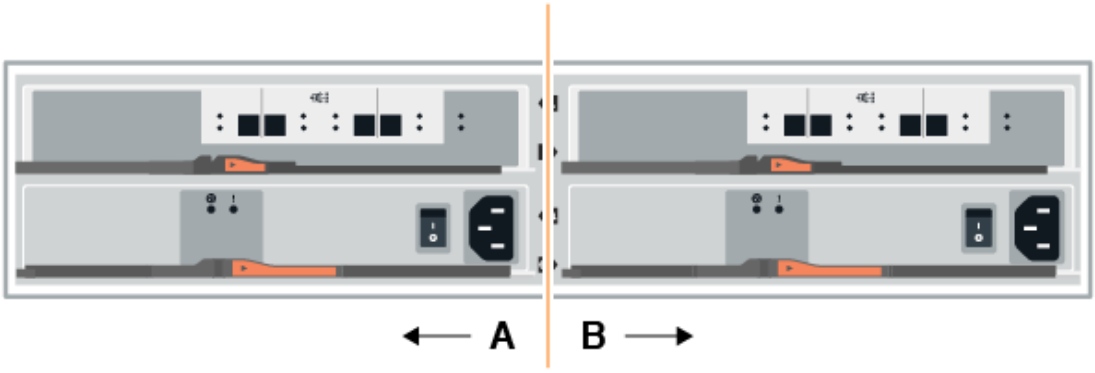
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Prima di iniziare

- Il firmware è stato aggiornato alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".

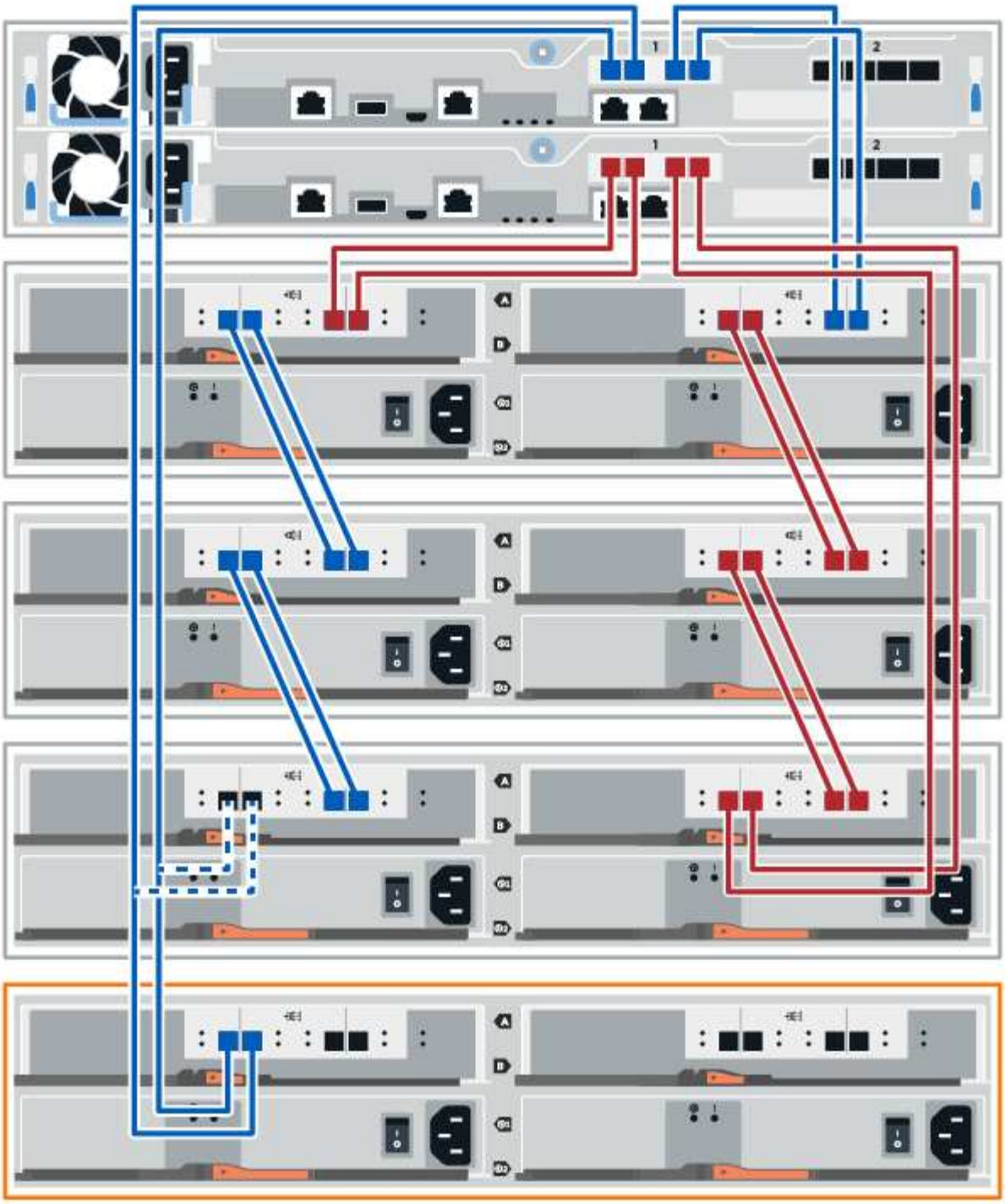
Fasi

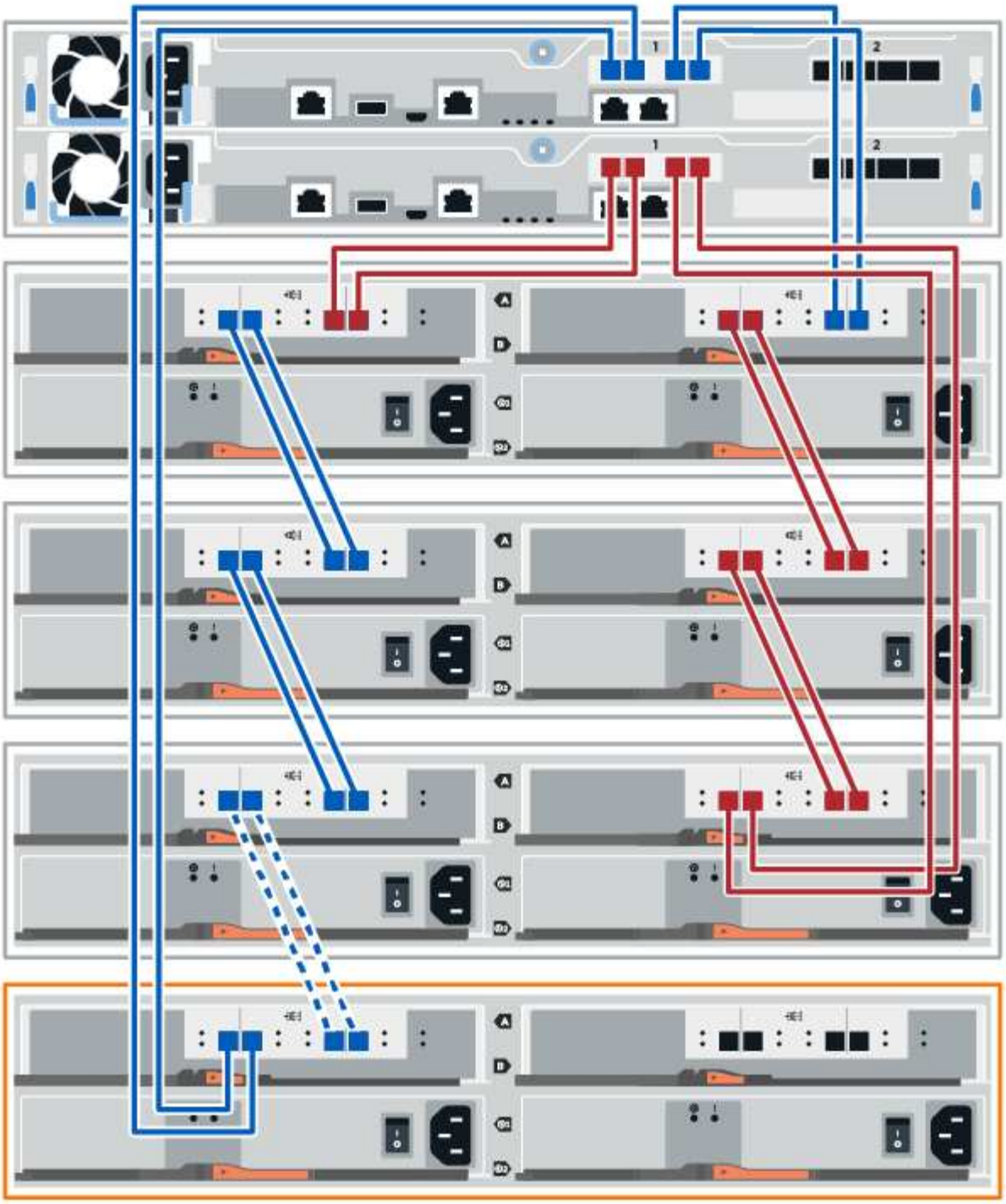
1. Scollegare entrambi i cavi del controller Lato A dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.



2. Collegare i cavi alle porte IOM12 lato A tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di connessione per un lato tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".


1
2
1
2
A
B



3. In Gestione sistema di SANtricity, fare clic su **hardware**.

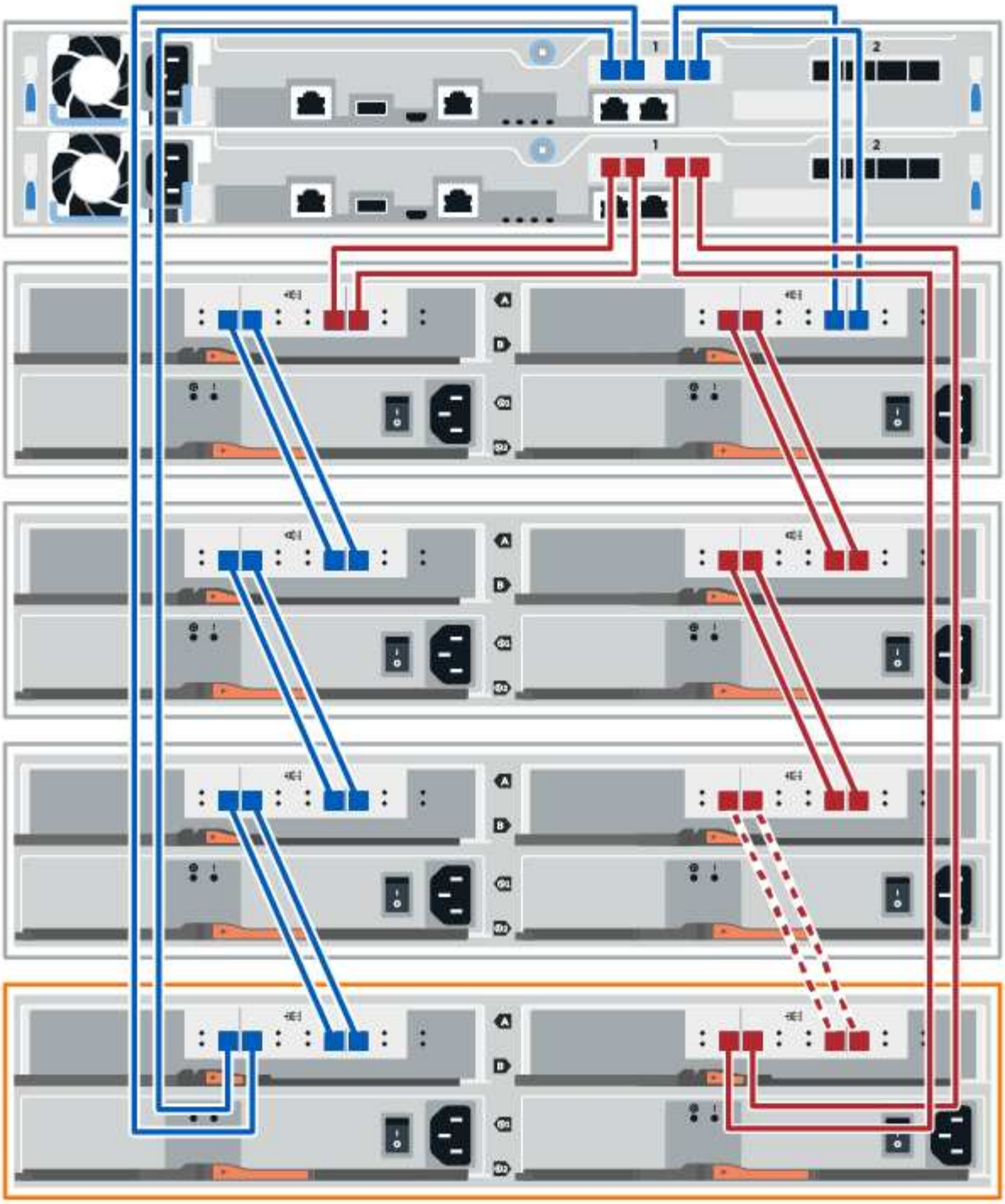
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

4. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
5. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

6. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
7. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
8. Scollegare entrambi i cavi del controller lato B dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.
9. Collegare i cavi alle porte IOM12 lato B tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di collegamento per il lato B tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



10. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Fase 4: Completare l'aggiunta a caldo

Per completare l'aggiunta a caldo, verificare la presenza di eventuali errori e confermare che lo shelf di dischi appena aggiunto utilizzi il firmware più recente.

Fasi

1. In Gestore di sistema di SANtricity, fare clic su **Home**.
2. Se il collegamento **Recover from Problems** (Ripristina da problemi) viene visualizzato al centro della pagina, fare clic sul collegamento e risolvere eventuali problemi indicati nel Recovery Guru.
3. In Gestione sistema di SANtricity, fare clic su **hardware** e scorrere verso il basso, se necessario, per visualizzare lo shelf di dischi appena aggiunto.
4. Per i dischi precedentemente installati in un sistema storage diverso, aggiungere un disco alla volta allo shelf di dischi appena installato. Attendere che ogni disco venga riconosciuto prima di inserire il disco successivo.

   Quando un disco viene riconosciuto dal sistema di storage, la rappresentazione dello slot nella pagina **hardware** viene visualizzata come un rettangolo blu.

5. Selezionare la scheda **Support** > **Support Center** > **Support Resources**.
6. Fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware) e verificare quali versioni del firmware IOM/ESM e del firmware del disco sono installate sul nuovo shelf di dischi.

   > Potrebbe essere necessario scorrere la pagina verso il basso per individuare questo collegamento.

7. Se necessario, aggiornare il firmware del disco.

   Il firmware IOM/ESM viene aggiornato automaticamente alla versione più recente, a meno che non sia stata disattivata la funzione di aggiornamento.

La procedura di aggiunta a caldo è stata completata. È possibile riprendere le normali operazioni.

Cablaggio Ethernet per una stazione di gestione

È possibile collegare il sistema storage a una rete Ethernet per la gestione out-of-band degli array di storage. È necessario utilizzare cavi Ethernet per tutte le connessioni di gestione degli array di storage.

Topologia diretta

Una topologia diretta collega il controller direttamente a una rete Ethernet.

È necessario collegare la porta di gestione 1 su ciascun controller per la gestione out-of-band e lasciare la porta 2 disponibile per l'accesso allo storage array da parte del supporto tecnico.

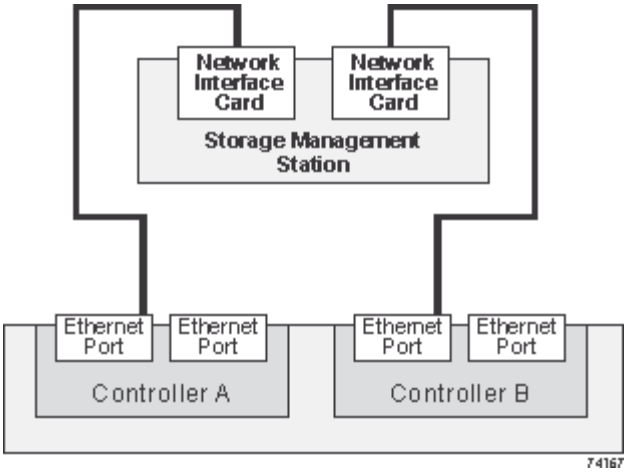


Figura 3. Connessioni per la gestione diretta dello storage

Topologia del fabric

Una topologia fabric utilizza uno switch per collegare il controller a una rete Ethernet.

È necessario collegare la porta di gestione 1 su ciascun controller per la gestione out-of-band e lasciare la porta 2 disponibile per l'accesso allo storage array da parte del supporto tecnico.

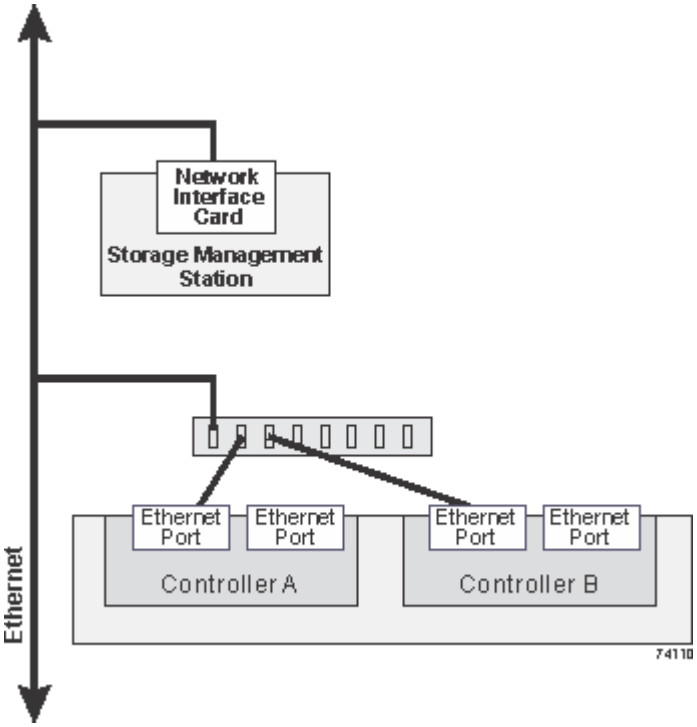


Figura 4. Connessioni per la gestione dello storage fabric

Implementare il software

Configurazione di Linux Express

Panoramica sulla configurazione di Linux Express

Il metodo Linux Express per l'installazione dello storage array e l'accesso a Gestore di sistema SANtricity è appropriato per la configurazione di un host Linux standalone su un sistema storage e-Series. È progettato per rendere operativo il sistema storage il più rapidamente possibile, con un numero minimo di punti decisionali.

Panoramica della procedura

Il metodo Linux Express include i seguenti passaggi.

1. Configurare uno dei seguenti ambienti di comunicazione:
    - Fibre Channel (FC)
    - ISCSI
    - SAS
    - Iiser su Infiniband
    - SRP su Infiniband
    - NVMe su Infiniband
    - NVMe su RoCE
    - NVMe su Fibre Channel
2. Creare volumi logici sull'array di storage.
3. Rendere i volumi disponibili per l'host dati.

Trova ulteriori informazioni

- Guida in linea — descrive come utilizzare Gestione di sistema di SANtricity per completare le attività di configurazione e gestione dello storage. È disponibile all'interno del prodotto.
- "Knowledge base di NetApp" (Un database di articoli) — fornisce informazioni sulla risoluzione dei problemi, FAQ e istruzioni per un'ampia gamma di prodotti e tecnologie NetApp.
- "Tool di matrice di interoperabilità NetApp" — consente di cercare configurazioni di prodotti e componenti NetApp che soddisfino gli standard e i requisiti specificati da NetApp.
- "Guida all'installazione di Linux Unified host Utilities 7.1" — descrive come utilizzare Linux Unified host Utilities 7.1.

Presupposti

Il metodo Linux Express si basa sui seguenti presupposti:

Componente	Presupposti
Hardware	• Per installare l'hardware, sono state utilizzate le istruzioni di installazione e configurazione fornite con gli shelf dei controller. • Sono stati collegati i cavi tra gli shelf di dischi opzionali e i controller. • Il sistema storage è alimentato. • Hai installato tutto l'altro hardware (ad esempio, stazione di gestione, switch) e hai effettuato le connessioni necessarie. • Se si utilizza NVMe su Infiniband, NVMe su RoCE o NVMe su Fibre Channel, ciascun controller EF300, EF600, EF570 o E5700 contiene almeno 32 GB di RAM.
Host	• È stata stabilita una connessione tra il sistema storage e l'host dati. • Il sistema operativo host è stato installato. • Non stai utilizzando Linux come guest virtualizzato. • Non si sta configurando l'host dati (i/o collegato) per l'avvio da SAN. • Sono stati installati gli aggiornamenti del sistema operativo elencati nella sezione "Tool di matrice di interoperabilità NetApp".
Stazione di gestione dello storage	• Si utilizza una rete di gestione a 1 Gbps o più veloce. • Si sta utilizzando una stazione separata per la gestione piuttosto che l'host dei dati (i/o collegato). • Si sta utilizzando 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. • La stazione di gestione è stata collegata alla stessa subnet delle porte di gestione dello storage.
Indirizzamento IP	• È stato installato e configurato un server DHCP. • È stata ancora stabilita una connessione Ethernet tra la stazione di gestione e il sistema di storage.
Provisioning dello storage	• Non verranno utilizzati volumi condivisi. • Verranno creati pool anziché gruppi di volumi.

Componente	Presupposti
Protocollo: FC	• Sono state effettuate tutte le connessioni FC sul lato host e lo zoning dello switch attivato. • Stai utilizzando HBA e switch FC supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA FC elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: ISCSI	• Si utilizzano switch Ethernet in grado di trasportare il traffico iSCSI. • Gli switch Ethernet sono stati configurati in base alle raccomandazioni del vendor per iSCSI.
Protocollo: SAS	• Stai utilizzando HBA SAS supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA SAS elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: Er su InfiniBand	• Si sta utilizzando un fabric InfiniBand. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA IB-iSER elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: SRP su InfiniBand	• Si sta utilizzando un fabric InfiniBand. • Si stanno utilizzando le versioni del driver e del firmware IB-SRP elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: NVMe su InfiniBand	• Sono state ricevute le schede di interfaccia host 100G o 200G in un sistema storage EF300, EF600, EF570 o E5700 preconfigurato con il protocollo NVMe over InfiniBand oppure i controller sono stati ordinati con porte IB standard e devono essere convertiti in porte NVMe-of. • Si sta utilizzando un fabric InfiniBand. • Si stanno utilizzando le versioni del driver e del firmware NVMe/IB elencate nella "Tool di matrice di interoperabilità NetApp".

Componente	Presupposti
Protocollo: NVMe su RoCE	• Sono state ricevute le schede di interfaccia host 100G o 200G in un sistema storage EF300, EF600, EF570 o E5700 preconfigurato con il protocollo NVMe over RoCE oppure i controller sono stati ordinati con porte IB standard e devono essere convertiti in porte NVMe-of. • Si stanno utilizzando le versioni del driver e del firmware NVMe/RoCE elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: NVMe su Fibre Channel	• Le schede di interfaccia host 32G sono state ricevute in un sistema storage EF300, EF600, EF570 o E5700 preconfigurato con il protocollo NVMe over Fibre Channel oppure i controller sono stati ordinati con porte FC standard e devono essere convertiti in porte NVMe-of. • Si utilizzano driver NVMe/FC e versioni firmware come indicato nella "Tool di matrice di interoperabilità NetApp".

Queste istruzioni del metodo espresso includono esempi per SUSE Linux Enterprise Server (SLES) e per Red Hat Enterprise Linux (RHEL).

Configurazione Express Fibre Channel

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

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

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

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

   - Controller A, porta 1: 169.254.128.101
   - Controller B, porta 1: 169.254.128.102
   - Subnet mask: 255.255.0.0
2. Individuare l'etichetta dell'indirizzo MAC sul retro di ciascun controller, quindi fornire all'amministratore di rete l'indirizzo MAC per la porta 1 di ciascun controller.

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

Installare e configurare Linux Unified host Utilities

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

Fasi

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

- Nessuna notifica configurata.

Fasi

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

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

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

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

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

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

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

Configurare il software multipath

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

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

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

operativo.

A proposito di questa attività

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

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

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.
2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

   ```
   # systemctl start multipathd
   ```

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

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

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

5. Abilitare il daemon multipath all'avvio.

   ```
   systemctl enable multipathd
   ```

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

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

7. Assicurarsi che l'immagine /boot/initrams-* o /boot/initrd-* appena creata sia selezionata nel file di configurazione del boot.

   Ad esempio, per GRUB è così `/boot/grub/menu.lst` e per grub2 lo è `/boot/grub2/menu.cfg`.

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

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

1. Riavviare l'host.

Impostare il file multipath.conf

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

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

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

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

Configurare gli switch FC

La configurazione (zoning) degli switch Fibre Channel (FC) consente agli host di connettersi allo storage array e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Credenziali di amministratore per gli switch.
- Il numero WWPN di ciascuna porta di iniziatore host e di ciascuna porta di destinazione del controller collegata allo switch. (Utilizzare l'utility HBA per il rilevamento).

A proposito di questa attività

Ciascuna porta dell'iniziatore deve trovarsi in una zona separata con tutte le porte di destinazione corrispondenti. Per ulteriori informazioni sulla suddivisione in zone degli switch, consultare la documentazione del vendor dello switch.

Fasi

1. Accedere al programma di amministrazione dello switch FC, quindi selezionare l'opzione di configurazione dello zoning.
2. Creare una nuova zona che includa la prima porta iniziatore host e che includa anche tutte le porte di destinazione che si connettono allo stesso switch FC dell'iniziatore.
3. Creare zone aggiuntive per ciascuna porta iniziatore host FC nello switch.
4. Salvare le zone, quindi attivare la nuova configurazione di zoning.

Determinare le WWPN host ed effettuare le impostazioni consigliate

Installare un'utility HBA FC in modo da visualizzare il nome della porta globale (WWPN) di ciascuna porta host.

Inoltre, è possibile utilizzare l'utility HBA per modificare le impostazioni consigliate nella colonna Note di "Tool di matrice di interoperabilità NetApp" per la configurazione supportata.

A proposito di questa attività

Consulta le seguenti linee guida per le utility HBA:

- La maggior parte dei vendor HBA offre un'utility HBA. È necessaria la versione corretta dell'HBA per il sistema operativo host e la CPU. Esempi di utility HBA FC includono:
  - Emulex OneCommand Manager per HBA Emulex
  - QLogic QConverge Console per HBA QLogic
- Le porte i/o host potrebbero essere registrate automaticamente se è installato l'agente di contesto host.

Fasi

1. Scaricare l'utility appropriata dal sito Web del vendor HBA.
2. Installare l'utility.
3. Selezionare le impostazioni appropriate nell'utility HBA.

   Le impostazioni appropriate per la configurazione sono elencate nella colonna Note di "Tool di matrice di interoperabilità NetApp".

Creare partizioni e filesystem

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

```
# sanlun lun show -p

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

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

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

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

3. Creare un file system sulla partizione.

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

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

4. Creare una cartella per montare la nuova partizione.

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

5. Montare la partizione.

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

Verificare l'accesso allo storage sull'host

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

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

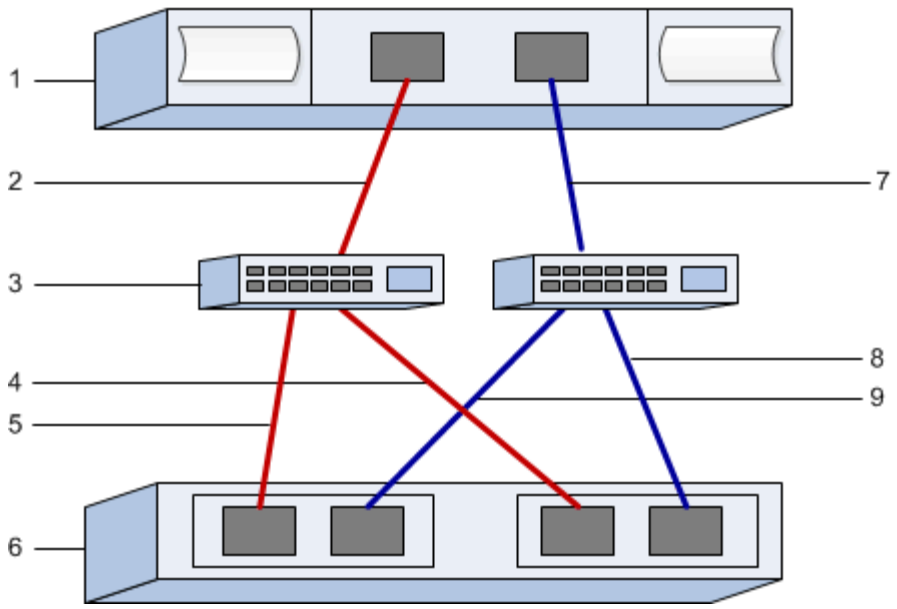
Al termine

Rimuovere il file e la cartella copiati.

Registrare la configurazione FC

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

La figura mostra un host collegato a un array di storage e-Series in due zone. Una zona è indicata dalla linea blu, mentre l'altra è indicata dalla linea rossa. Ogni singola porta ha due percorsi per lo storage (uno per ciascun controller).



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	PN. WWN
1	Host	*non applicabile*
2	Porta host 0 a switch FC zona 0	
7	Dalla porta host 1 allo switch FC zona 1	

Identificatori di destinazione

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
3	Switch	*non applicabile*
6	Controller di array (destinazione)	*non applicabile*
5	Dal controller A, dalla porta 1 allo switch FC 1	
9	Dal controller A, dalla porta 2 allo switch FC 2	
4	Dal controller B, porta 1 allo switch FC 1	

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
8	Controller B, dalla porta 2 allo switch FC 2	

Host di mappatura

Nome host di mapping
Tipo di sistema operativo host

Installazione SAS

Verificare che la configurazione Linux sia supportata

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

Fasi

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

   Viene visualizzata la sezione Criteri di ricerca più precisi. In questa sezione è possibile selezionare il protocollo applicabile e altri criteri per la configurazione, ad esempio sistema operativo, sistema operativo NetApp e driver host multipath. Selezionare i criteri desiderati per la configurazione, quindi visualizzare gli elementi di configurazione compatibili applicabili. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo prescritti nello strumento. Per informazioni dettagliate sulla configurazione scelta, fare clic sulla freccia a destra della pagina Visualizza configurazioni supportate.

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

Installare e configurare Linux Unified host Utilities

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

Fasi

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

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

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

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

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

Se si utilizza il software SANtricity versione 11.53 o precedente, è possibile installare il

software Gestione archiviazione SANtricity sulla stazione di gestione per semplificare la gestione dell'array.

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

- Nessuna notifica configurata.

Fasi

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

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

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

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

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

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

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

Configurare il software multipath

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

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

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

operativo.

A proposito di questa attività

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

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

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.
2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

   ```
   # systemctl start multipathd
   ```

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

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

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

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

   ```
   systemctl enable multipathd
   ```

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

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

7. Assicurarsi che l'immagine /boot/initrams-* o /boot/initrd-* appena creata sia selezionata nel file di configurazione del boot.

   Ad esempio, per GRUB è così `/boot/grub/menu.lst` e per grub2 lo è `/boot/grub2/menu.cfg`.

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

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

1. Riavviare l'host.

Impostare il file multipath.conf

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

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

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

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

Determinare gli identificatori host SAS - Linux

Per il protocollo SAS, individuare gli indirizzi SAS utilizzando l'utility HBA, quindi utilizzare il BIOS HBA per definire le impostazioni di configurazione appropriate.

Prima di iniziare questa procedura, consultare le seguenti linee guida per le utility HBA:

- La maggior parte dei vendor HBA offre un'utility HBA. A seconda del sistema operativo host e della CPU, utilizzare l'utility LSI-sas2flash(6G) o sas3flash(12G).
- Le porte i/o host potrebbero essere registrate automaticamente se è installato l'agente di contesto host.

Fasi

1. Scaricare l'utility HBA dal sito Web del vendor HBA.
2. Installare l'utility.
3. Utilizzare il BIOS HBA per selezionare le impostazioni appropriate per la configurazione.

   Vedere la colonna Note di "Tool di matrice di interoperabilità NetApp" per consigli.

Creare partizioni e filesystem

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

```
# sanlun lun show -p

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

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

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

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

3. Creare un file system sulla partizione.

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

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

4. Creare una cartella per montare la nuova partizione.

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

5. Montare la partizione.

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

Verificare l'accesso allo storage sull'host

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

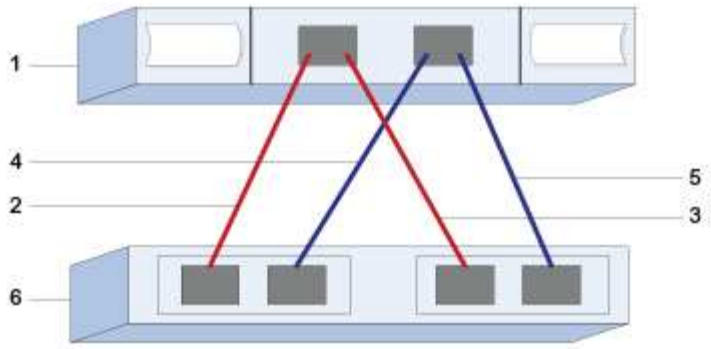
1. Sull'host, copiare uno o più file nel punto di montaggio del disco.
2. Copiare di nuovo i file in un'altra cartella sul disco originale.
3. Eseguire `diff` per confrontare i file copiati con gli originali.

Al termine

Rimuovere il file e la cartella copiati.

Registrare la configurazione SAS

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



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	Indirizzo SAS
1	Host	*non applicabile*
2	Porta host (iniziatore) 1 collegata al controller A, porta 1	
3	Porta host (iniziatore) 1 collegata al controller B, porta 1	
4	Porta host (iniziatore) 2 collegata al controller A, porta 1	
5	Porta host (iniziatore) 2 collegata al controller B, porta 1	

Identificatori di destinazione

Le configurazioni consigliate sono costituite da due porte di destinazione.

Host di mappatura

Mapping host Name (Nome host mapping)
Tipo di sistema operativo host

Configurazione di iSCSI

Verificare che la configurazione Linux sia supportata

Per garantire un funzionamento affidabile, è necessario creare un piano di implementazione e utilizzare lo strumento matrice di interoperabilità NetApp (IMT) per

verificare che l'intera configurazione sia supportata.

Fasi

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

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

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

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

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

   Se lo storage array non riesce a ottenere gli indirizzi IP assegnati da DHCP entro 30 secondi, vengono

impostati i seguenti indirizzi IP predefiniti:

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

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

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

Installare e configurare Linux Unified host Utilities

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

Fasi

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Software SANtricity 11.53 o precedente.

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Gestione fuori banda.

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

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

A proposito di questa attività

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

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

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

Fasi

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

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

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

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

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

3. Utilizzare l'installazione guidata per eseguire le seguenti operazioni:
   - **Verifica dell'hardware (controller e dischi)** — verifica del numero di controller e dischi nell'array di storage. Assegnare un nome all'array.
   - **Verifica di host e sistemi operativi** — verifica dei tipi di host e sistemi operativi a cui lo storage array può accedere.
   - **Accept Pools** — accettare la configurazione del pool consigliata per il metodo di installazione rapida. Un pool è un gruppo logico di dischi.

- **Configura avvisi** — consente a System Manager di ricevere notifiche automatiche quando si verifica un problema con lo storage array.
- **Enable AutoSupport** — monitora automaticamente lo stato dello storage array e invia le spedizioni al supporto tecnico.

4. Se non hai ancora creato un volume, creane uno dal **Storage › Volumes › Create › Volume**.

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

Configurare il software multipath

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

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

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

A proposito di questa attività

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

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

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.
2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

   ```
   # systemctl start multipathd
   ```

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

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

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

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

```
systemctl enable multipathd
```

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

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

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

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

8. Riavviare l'host.

Impostare il file multipath.conf

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

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

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

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

Configurare gli switch

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

È necessario assicurarsi quanto segue:

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

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

Configurare il networking

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

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

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

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

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

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

Configurare il networking lato array

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

3. Chiudere l'installazione guidata.

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

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

   Il grafico cambia per mostrare i controller invece dei dischi.

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

   Viene visualizzato il menu di scelta rapida del controller.

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

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

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

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

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità desiderata. Le opzioni visualizzate nell'elenco a discesa dipendono dalla velocità massima supportata dalla rete (ad esempio, 10 Gbps). Le schede di interfaccia host iSCSI da 25 GB opzionali disponibili sui controller non consentono la negoziazione automatica delle velocità. È necessario impostare la velocità di ciascuna porta su 10 GB o 25 GB. Tutte le porte devono essere impostate alla stessa velocità.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.
Porta TCP in ascolto (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.

Impostazione della porta	Descrizione
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

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

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

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

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

Configurare la rete lato host

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

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

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

   a. Determinare i nomi delle porte iSCSI utilizzando `ifconfig -a` comando.
   b. Impostare l'indirizzo IP per le porte iSCSI Initiator. Le porte dell'iniziatore devono essere presenti sulla stessa sottorete delle porte di destinazione iSCSI.

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

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

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

Aggiunte opzionali per IPv6:

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

Red Hat Enterprise Linux 9 (RHEL 9)

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

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

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

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

Aggiunta opzionale per IPv6:

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

+

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

a. Riavviare i servizi di rete.

```
# systemctl restart network
```

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

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

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

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

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

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

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

Metodo 1 (con ifache)

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

Metodo 2 (senza ifache)

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

L'IQN è simile al seguente:

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

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

Metodo 1 (con ifache)

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

Metodo 2 (senza ifache)

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

a. Elencare le sessioni iSCSI stabilite sull'host.

```
# iscsiadm -m session
```

Verificare le connessioni di rete IP

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

Fasi

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

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

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

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

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

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

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

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

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

Creare partizioni e filesystem

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

```
# sanlun lun show -p

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

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

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

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

3. Creare un file system sulla partizione.

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

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

4. Creare una cartella per montare la nuova partizione.

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

5. Montare la partizione.

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

Verificare l'accesso allo storage sull'host

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

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

Al termine

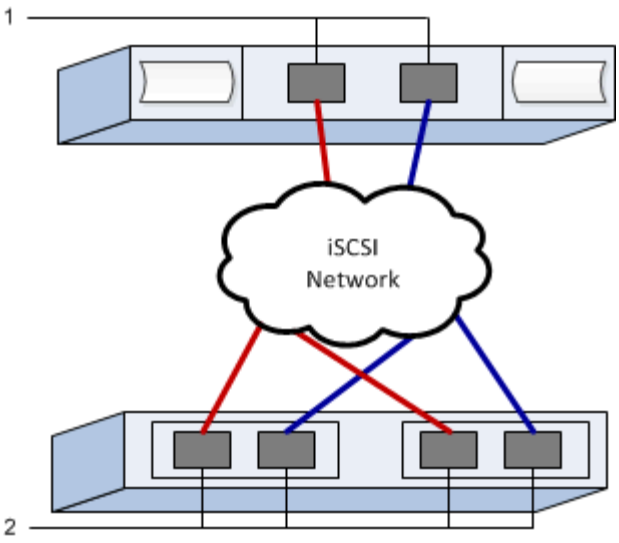
Rimuovere il file e la cartella copiati.

Registrare la configurazione iSCSI

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

Configurazione consigliata

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



IQN di destinazione

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

Nome host di mapping

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

Setup di liser su InfiniBand

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

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

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

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:
* Un server DHCP installato e configurato sulla stessa subnet delle porte di gestione dello storage.

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

   - Controller A, porta 1: 169.254.128.101
   - Controller B, porta 1: 169.254.128.102
   - Subnet mask: 255.255.0.0
2. Individuare l'etichetta dell'indirizzo MAC sul retro di ciascun controller, quindi fornire all'amministratore di rete l'indirizzo MAC per la porta 1 di ciascun controller.

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

Determinare i GUID della porta host ed effettuare le impostazioni consigliate

Il pacchetto infiniband-DIAGS include comandi per visualizzare il GUID (Globally Unique ID) di ciascuna porta InfiniBand (IB). La maggior parte delle distribuzioni Linux con OFED/RDMA supportato attraverso i pacchetti inclusi dispone anche del pacchetto infiniband-diags, che include comandi per visualizzare informazioni su HCA.

Fasi

1. Installare `infiniband-diags` che utilizza i comandi di gestione dei pacchetti del sistema operativo.
2. Eseguire `ibstat` per visualizzare le informazioni sulla porta.
3. Registrare i GUID dell'iniziatore su Foglio di lavoro di Iiser over InfiniBand.
4. Selezionare le impostazioni appropriate nell'utility HBA.

   Le impostazioni appropriate per la configurazione sono elencate nella colonna Note di "Tool di matrice di interoperabilità NetApp".

Configurare il gestore di subnet

Nell'ambiente in uso sullo switch o sugli host deve essere in esecuzione un gestore di subnet. Se si utilizza il lato host, attenersi alla procedura riportata di seguito per configurarlo.

> Prima di configurare il gestore di subnet, è necessario installare il pacchetto infiniband-DIAGS per ottenere il GUID (Globally Unique ID) tramite `ibstat -p` comando. Vedere Determinare i GUID della porta host ed effettuare le impostazioni consigliate per informazioni su come installare il pacchetto infiniband-diags.

Fasi

1. Installare `opensm` pacchetto su tutti gli host che eseguiranno il gestore di subnet.
2. Utilizzare `ibstat -p` comando per trovare `GUID0` e. `GUID1` Delle porte HBA. Ad esempio:

   ```
   # ibstat -p
   0x248a070300a80a80
   0x248a070300a80a81
   ```

3. Creare uno script di gestione delle subnet che venga eseguito una volta come parte del processo di avvio.

   ```
   # vim /usr/sbin/subnet-manager.sh
   ```

4. Aggiungere le seguenti righe. Sostituire i valori trovati al punto 2 `GUID0` e. `GUID1`. Per `P0` e. `P1`, utilizzare le priorità del gestore di subnet, con 1 come minimo e 15 come massimo.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

Un esempio del comando con sostituzioni di valori:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Creare un file system service unit denominato `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Aggiungere le seguenti righe.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notificare al sistema il nuovo servizio.

```
# systemctl daemon-reload
```

8. Attivare e avviare `subnet-manager` servizio.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Installare e configurare Linux Unified host Utilities

Gli strumenti delle utility host unificate di Linux consentono di gestire lo storage NetApp,

incluse policy di failover e percorsi fisici.

Fasi

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

La procedura guidata viene riavviata automaticamente quando si apre System Manager o si aggiorna il

browser e viene soddisfatta almeno una delle seguenti condizioni:

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

Fasi

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

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

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

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

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

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

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

Configurare il software multipath

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

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

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

A proposito di questa attività

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

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

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.
2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

   ```
   # systemctl start multipathd
   ```

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

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

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

5. Abilitare il daemon multipath all'avvio.

   ```
   systemctl enable multipathd
   ```

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

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

7. Assicurarsi che l'immagine /boot/initrams-* o /boot/initrd-* appena creata sia selezionata nel file di configurazione del boot.

   Ad esempio, per GRUB è così `/boot/grub/menu.lst` e per grub2 lo è `/boot/grub2/menu.cfg`.

8. Utilizzare "Creare l'host manualmente" procedura nella guida in linea per verificare se gli host sono definiti.

Verificare che ogni impostazione del tipo di host sia basata sulle informazioni del kernel raccolte in fase 4.

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

1. Riavviare l'host.

Impostare il file multipath.conf

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

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

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

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

Configurare le connessioni di rete

Se la configurazione utilizza il protocollo iSER su InfiniBand, eseguire la procedura descritta in questa sezione per configurare le connessioni di rete.

Fasi

1. Da System Manager, andare a **Impostazioni › sistema › Configura iSER su porte Infiniband**. Per ulteriori informazioni, consultare la guida in linea di System Manager.

   Inserire gli indirizzi iSCSI dell'array nella stessa subnet delle porte host che verranno utilizzate per creare sessioni iSCSI. Per gli indirizzi, consultare il Foglio di lavoro di iser.

2. Registrare l'IQN.

   Queste informazioni potrebbero essere necessarie quando si creano sessioni iSER da sistemi operativi che non supportano il rilevamento delle destinazioni di invio. Inserire queste informazioni nel campo Foglio di lavoro di iser.

Configurare il networking per gli host collegati allo storage

Se la configurazione utilizza il protocollo iSER su InfiniBand, eseguire la procedura descritta in questa sezione.

Lo stack di driver InfiniBand OFED supporta l'esecuzione simultanea di iSER e SRP sulle stesse porte, pertanto non è necessario alcun hardware aggiuntivo.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un OFED consigliato da NetApp installato sul sistema. Per ulteriori informazioni, consultare "Tool di matrice di interoperabilità NetApp".

Fasi

1. Abilitare e avviare i servizi iSCSI sugli host:

   Red Hat Enterprise Linux 7, 8 e 9 (RHEL 7, RHEL 8 e RHEL 9)

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

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

   ```
   # systemctl start iscsid.service
   # systemctl enable iscsid.service
   ```

2. Configurare le interfacce di rete della scheda InfiniBand:
   a. Identificare le porte InfiniBand che verranno utilizzate. Documentare l'indirizzo HW (indirizzo MAC) di ciascuna porta.
   b. Configurare i nomi persistenti per i dispositivi di interfaccia di rete InfiniBand.
   c. Configurare l'indirizzo IP e le informazioni di rete per le interfacce InfiniBand identificate.

      La configurazione specifica dell'interfaccia richiesta potrebbe variare a seconda del sistema operativo utilizzato. Consultare la documentazione del sistema operativo del vendor per informazioni specifiche sull'implementazione.

   d. Avviare le interfacce di rete IB riavviando il servizio di rete o riavviando manualmente ciascuna interfaccia. Ad esempio:

      ```
      systemctl restart network
      ```

   e. Verificare la connettività alle porte di destinazione. Dall'host, eseguire il ping degli indirizzi IP configurati durante la configurazione delle connessioni di rete.
3. Riavviare i servizi per caricare il modulo iSER.
4. Modificare le impostazioni iSCSI in /etc/iscsi/iscsid.conf

   ```
   node.startup = automatic
   replacement_timeout = 20
   ```

5. Creare configurazioni di sessione iSCSI:
   a. Creare file di configurazione iface per ogni interfaccia InfiniBand.

      La posizione della directory per i file iface iSCSI dipende dal sistema operativo. Questo esempio è per l'utilizzo di Red Hat Enterprise Linux:

```
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces/iface-ib0
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces/iface-ib1
```

b. Modificare ciascun file iface per impostare il nome dell'interfaccia e l'IQN dell'iniziatore. Impostare i seguenti parametri in modo appropriato per ogni file iface:

Opzione	Valore
iface.net_ifacename	Il nome del dispositivo di interfaccia (es. ib0).
iface.initiatorname	L'iniziatore host IQN documentato nel foglio di lavoro.

c. Creare sessioni iSCSI per la destinazione.

Il metodo preferito per creare le sessioni consiste nell'utilizzare il metodo di ricerca SendTargets. Tuttavia, questo metodo non funziona su alcune versioni del sistema operativo.

> Utilizzare **Method 2** per RHEL 6.x o SLES 11.3 o versione successiva.

- **Metodo 1 - rilevamento SendTargets:** utilizzare il meccanismo di rilevamento SendTargets per uno degli indirizzi IP del portale di destinazione. In questo modo verranno create sessioni per ciascuno dei portali di destinazione.

```
iscsiadm -m discovery -t st -p 192.168.130.101 -I iser
```

- **Metodo 2 - creazione manuale:** per ogni indirizzo IP del portale di destinazione, creare una sessione utilizzando la configurazione appropriata dell'interfaccia host iface. In questo esempio, l'interfaccia ib0 si trova sulla subnet A e l'interfaccia ib1 sulla subnet B. Per queste variabili, sostituire il valore appropriato dal foglio di lavoro:
  - <Target IQN> = IQN di destinazione dello storage array
  - <Target Port IP> = indirizzo IP configurato sulla porta di destinazione specificata

```
# Controller A Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l -o new
# Controller B Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l -o new
# Controller A Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l -o new
# Controller B Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l -o new
```

6. Accedere alle sessioni iSCSI.

   Per ogni sessione, eseguire il comando iscsiadm per accedere alla sessione.

```
# Controller A Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l
# Controller B Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l
# Controller A Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l
# Controller B Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l
```

7. Verificare le sessioni iSER/iSCSI.
   a. Controllare lo stato della sessione iscsi dall'host:

```
iscsiadm -m session
```

   b. Controllare lo stato della sessione iscsi dall'array. Da Gestore di sistema SANtricity, selezionare **array di storage** > **iSER** > **Visualizza/termina sessioni**.

All'avvio del servizio OFED/RDMA, i moduli kernel iSER vengono caricati per impostazione predefinita quando i servizi iSCSI sono in esecuzione. Per completare la configurazione della connessione iSER, è necessario caricare i moduli iSER. Attualmente richiede un riavvio dell'host.

Creare partizioni e filesystem

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

```
# sanlun lun show -p

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

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

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

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

3. Creare un file system sulla partizione.

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

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

4. Creare una cartella per montare la nuova partizione.

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

5. Montare la partizione.

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

Verificare l'accesso allo storage sull'host

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

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

Al termine

Rimuovere il file e la cartella copiati.

Registra la tua configurazione iSER su IB

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

Identificatori host

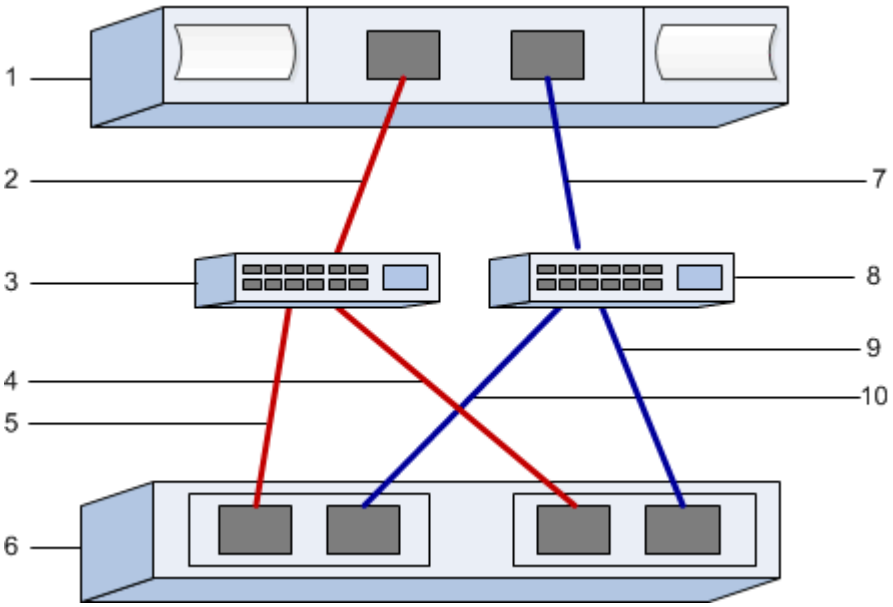
> Il software Initiator IQN viene determinato durante l'attività, Configurare il networking per gli host collegati allo storage.

Individuare e documentare l'IQN iniziatore da ciascun host. Per gli iniziatori software, l'IQN si trova in genere nel file /etc/iscsi/initatorname.iscsi.

N. didascalia	Connessioni alla porta host	IQN iniziatore software
1	Host (iniziatore) 1	
n/a.		
n/a.		
n/a.		
n/a.		

Configurazione consigliata

Le configurazioni consigliate sono costituite da due porte host (iniziatore) e quattro porte di destinazione.



IQN di destinazione

Documentare l'IQN di destinazione per lo storage array. Queste informazioni verranno utilizzate in Configurare il networking per gli host collegati allo storage.

Individuare il nome IQN dell'array di storage utilizzando SANtricity: **Array di storage** > **iSER** > **Gestisci impostazioni**. Queste informazioni potrebbero essere necessarie quando si creano sessioni iSER da sistemi operativi che non supportano il rilevamento delle destinazioni di invio.

N. didascalia	Nome array	IQN di destinazione
6	Controller di array (destinazione)	

Configurazione di rete

Documentare la configurazione di rete che verrà utilizzata per gli host e lo storage sul fabric InfiniBand. Queste istruzioni presuppongono che vengano utilizzate due subnet per la ridondanza completa.

L'amministratore di rete può fornire le seguenti informazioni. Queste informazioni vengono utilizzate nell'argomento, Configurare il networking per gli host collegati allo storage.

Subnet A

Definire la subnet da utilizzare.

Indirizzo di rete	Netmask

Documentare gli IQN che devono essere utilizzati dalle porte dell'array e da ciascuna porta host.

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	IQN
3	Switch	*non applicabile*
5	Controller A, porta 1	
4	Controller B, porta 1	
2	Host 1, porta 1	
	(Opzionale) host 2, porta 1	

Subnet B

Definire la subnet da utilizzare.

Indirizzo di rete	Netmask

Documentare gli IQN che devono essere utilizzati dalle porte dell'array e da ciascuna porta host.

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	IQN
8	Switch	*non applicabile*
10	Controller A, porta 2	
9	Controller B, porta 2	
7	Host 1, porta 2	
	(Opzionale) host 2, porta 2	

Nome host di mapping

Il nome host del mapping viene creato durante il flusso di lavoro.

Nome host di mapping
Tipo di sistema operativo host

Configurazione SRP su InfiniBand

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

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

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

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

   - Controller A, porta 1: 169.254.128.101
   - Controller B, porta 1: 169.254.128.102
   - Subnet mask: 255.255.0.0
2. Individuare l'etichetta dell'indirizzo MAC sul retro di ciascun controller, quindi fornire all'amministratore di rete l'indirizzo MAC per la porta 1 di ciascun controller.

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

Determinare i GUID della porta host ed effettuare le impostazioni consigliate

Il pacchetto infiniband-DIAGS include comandi per visualizzare il GUID (Globally Unique ID) di ciascuna porta InfiniBand (IB). La maggior parte delle distribuzioni Linux con OFED/RDMA supportato attraverso i pacchetti inclusi dispone anche del pacchetto infiniband-diags, che include comandi per visualizzare informazioni su HCA.

Fasi

1. Installare `infiniband-diags` che utilizza i comandi di gestione dei pacchetti del sistema operativo.
2. Eseguire `ibstat` per visualizzare le informazioni sulla porta.
3. Registrare i GUID dell'iniziatore su Foglio di lavoro SRP.
4. Selezionare le impostazioni appropriate nell'utility HBA.

   Le impostazioni appropriate per la configurazione sono elencate nella colonna Note di "Tool di matrice di interoperabilità NetApp".

Configurare il gestore di subnet

Nell'ambiente in uso sullo switch o sugli host deve essere in esecuzione un gestore di subnet. Se si utilizza il lato host, attenersi alla procedura riportata di seguito per

configurarlo.

> Prima di configurare il gestore di subnet, è necessario installare il pacchetto infiniband-DIAGS per ottenere il GUID (Globally Unique ID) tramite `ibstat -p` comando. Vedere Determinare i GUID della porta host ed effettuare le impostazioni consigliate per informazioni su come installare il pacchetto infiniband-diags.

Fasi

1. Installare `opensm` pacchetto su tutti gli host che eseguiranno il gestore di subnet.
2. Utilizzare `ibstat -p` comando per trovare `GUID0` e. `GUID1` Delle porte HBA. Ad esempio:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Creare uno script di gestione delle subnet che venga eseguito una volta come parte del processo di avvio.

```
# vim /usr/sbin/subnet-manager.sh
```

4. Aggiungere le seguenti righe. Sostituire i valori trovati al punto 2 `GUID0` e. `GUID1`. Per `P0` e. `P1`, utilizzare le priorità del gestore di subnet, con 1 come minimo e 15 come massimo.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

   Un esempio del comando con sostituzioni di valori:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Creare un file system service unit denominato `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Aggiungere le seguenti righe.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notificare al sistema il nuovo servizio.

```
# systemctl daemon-reload
```

8. Attivare e avviare `subnet-manager` servizio.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Installare e configurare le utility host Linux

Il pacchetto Linux Unified host Utilities include strumenti per la gestione dello storage NetApp, tra cui policy di failover e percorsi fisici.

Fasi

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

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

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

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

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

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

Gestione storage SANtricity include l'interfaccia a riga di comando (CLI) per ulteriori attività di gestione e

l'agente di contesto host per l'invio delle informazioni di configurazione degli host ai controller degli array di storage attraverso il percorso i/O.

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

Configurare il software multipath

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

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

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

A proposito di questa attività

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

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

Fasi

1. Se non è già stato creato un file multipath.conf, eseguire `# touch /etc/multipath.conf` comando.
2. Utilizzare le impostazioni di multipath predefinite lasciando vuoto il file multipath.conf.
3. Avviare il servizio multipath.

```
# systemctl start multipathd
```

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

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

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

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

```
systemctl enable multipathd
```

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

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

7. Assicurarsi che l'immagine /boot/initrams-* o /boot/initrd-* appena creata sia selezionata nel file di configurazione del boot.

   Ad esempio, per GRUB è così `/boot/grub/menu.lst` e per grub2 lo è `/boot/grub2/menu.cfg`.

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

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

1. Riavviare l'host.

Impostare il file multipath.conf

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

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

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

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

Configurazione delle connessioni di rete: SRP su Infiniband

Se la configurazione utilizza il protocollo SRP su Infiniband, attenersi alla procedura descritta in questa sezione.

Prima di iniziare

Per collegare l'host Linux allo storage array, è necessario attivare lo stack di driver InfiniBand con le opzioni appropriate. Impostazioni specifiche possono variare a seconda delle distribuzioni Linux. Controllare "Tool di matrice di interoperabilità NetApp" per istruzioni specifiche e impostazioni aggiuntive consigliate specifiche per la soluzione.

Fasi

1. Installare lo stack di driver OFED/RDMA per il sistema operativo in uso.

   SLES

   ```
   zypper install rdma-core
   ```

   RHEL

   ```
   yum install rdma-core
   ```

2. Configurare OFED/RDMA per caricare il modulo SRP.

   SLES

   ```
   zypper install srp_daemon
   ```

   RHEL

   ```
    yum install srp_daemon
   ```

3. Nel file di configurazione OFED/RDMA, impostare `SRP_LOAD=yes` e. `SRP_DAEMON_ENABLE=yes`.

   Il file di configurazione RDMA si trova nella seguente posizione:

   ```
   /etc/rdma/rdma.conf
   ```

4. Attivare e avviare il servizio OFED/RDMA.

   RHEL 7.x e SLES 12.x o superiore

   - Per abilitare il caricamento dei moduli InfiniBand all'avvio:

     ```
     systemctl enable rdma
     ```

   - Per caricare immediatamente i moduli InfiniBand:

```
systemctl start rdma
```

5. Attivare il daemon SRP.

   RHEL 7.x e SLES 12 o superiore

   - Per abilitare il daemon SRP all'avvio:

     ```
     systemctl enable srp_daemon
     ```

   - Per avviare immediatamente il daemon SRP:

     ```
     systemctl start srp_daemon
     ```

6. Se si desidera modificare la configurazione SRP, immettere il seguente comando per creare `/etc/modprobe.d/ib_srp.conf` .

   ```
   options ib_srp cmd_sg_entries=255 allow_ext_sg=y
   indirect_sg_entries=2048
   ```

   a. Sotto il `/etc/srp_daemon.conf`, aggiungere la seguente riga.

      ```
      a    max_sect=4096
      ```

Creare partizioni e filesystem

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

```
# sanlun lun show -p

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

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

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

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

3. Creare un file system sulla partizione.

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

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

4. Creare una cartella per montare la nuova partizione.

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

5. Montare la partizione.

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

Verificare l'accesso allo storage sull'host

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Volume inizializzato formattato con un file system.

Fasi

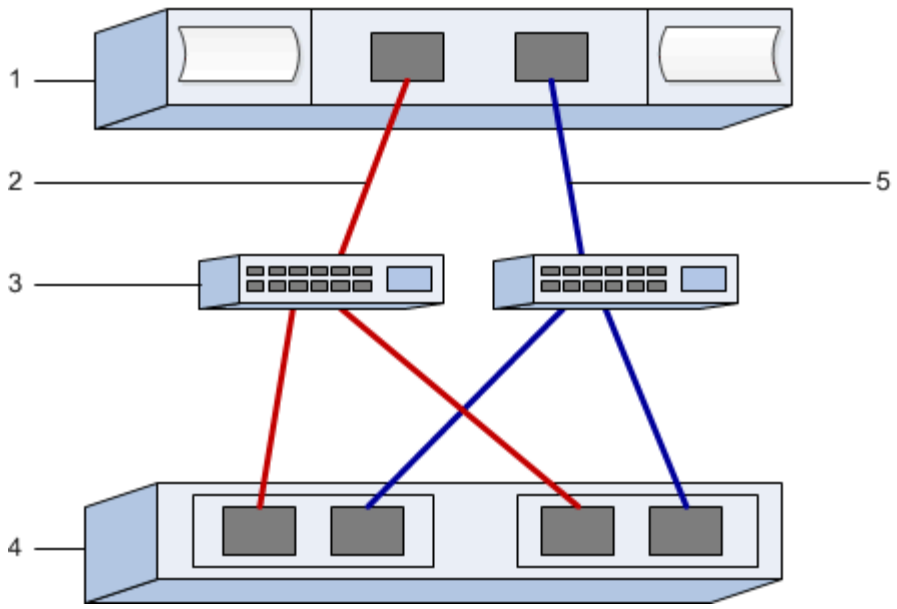
1. Sull'host, copiare uno o più file nel punto di montaggio del disco.
2. Copiare di nuovo i file in un'altra cartella sul disco originale.
3. Eseguire `diff` per confrontare i file copiati con gli originali.

Al termine

Rimuovere il file e la cartella copiati.

Registrare la configurazione SRP su IB

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



Identificatori host

> I GUID iniziatori vengono determinati nell'attività, Determinare i GUID della porta host ed effettuare le impostazioni consigliate.

N. didascalia	Connessioni porta host (iniziatore)	GUID
1	Host	*non applicabile*
3	Switch	*non applicabile*
4	Destinazione (storage array)	*non applicabile*
2	Porta host 1 allo switch IB 1 (percorso "A")	
5	Porta host 2 allo switch IB 2 (percorso "B")	

Configurazione consigliata

Le configurazioni consigliate sono costituite da due porte initiator e quattro porte di destinazione.

Nome host di mapping

> Il nome host del mapping viene creato durante il flusso di lavoro.

Nome host di mapping

Tipo di sistema operativo host

NVMe over InfiniBand Setup

Verificare il supporto di Linux ed esaminare le restrizioni

Come prima fase, è necessario verificare che la configurazione Linux sia supportata ed esaminare anche le restrizioni relative a controller, host e ripristino.

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

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

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

Esaminare le restrizioni NVMe su InfiniBand

Prima di utilizzare NVMe su InfiniBand, consultare "Tool di matrice di interoperabilità NetApp" per esaminare le restrizioni più recenti relative a controller, host e recovery.

Limitazioni di storage e disaster recovery

- Il mirroring asincrono e sincrono non è supportato.
- Il thin provisioning (creazione di thin volumi) non è supportato.

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

3. Utilizzare l'installazione guidata per eseguire le seguenti operazioni:
   - **Verifica dell'hardware (controller e dischi)** — verifica del numero di controller e dischi nell'array di storage. Assegnare un nome all'array.
   - **Verifica di host e sistemi operativi** — verifica dei tipi di host e sistemi operativi a cui lo storage array può accedere.
   - **Accept Pools** — accettare la configurazione del pool consigliata per il metodo di installazione rapida.

Un pool è un gruppo logico di dischi.

- **Configura avvisi** — consente a System Manager di ricevere notifiche automatiche quando si verifica un problema con lo storage array.
- **Enable AutoSupport** — monitora automaticamente lo stato dello storage array e invia le spedizioni al supporto tecnico.

4. Se non hai ancora creato un volume, creane uno dal **Storage › Volumes › Create › Volume**.

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

Determinare i GUID della porta host ed effettuare le impostazioni consigliate

Il pacchetto infiniband-DIAGS include comandi per visualizzare il GUID (Globally Unique ID) di ciascuna porta InfiniBand (IB). La maggior parte delle distribuzioni Linux con OFED/RDMA supportato attraverso i pacchetti inclusi dispone anche del pacchetto infiniband-diags, che include comandi per visualizzare informazioni su HCA.

Fasi

1. Installare `infiniband-diags` che utilizza i comandi di gestione dei pacchetti del sistema operativo.
2. Eseguire `ibstat` per visualizzare le informazioni sulla porta.
3. Registrare i GUID dell'iniziatore su Foglio di lavoro SRP.
4. Selezionare le impostazioni appropriate nell'utility HBA.

   Le impostazioni appropriate per la configurazione sono elencate nella colonna Note di "Tool di matrice di interoperabilità NetApp".

Configurare il gestore di subnet

Nell'ambiente in uso sullo switch o sugli host deve essere in esecuzione un gestore di subnet. Se si utilizza il lato host, attenersi alla procedura riportata di seguito per configurarlo.

> Prima di configurare il gestore di subnet, è necessario installare il pacchetto infiniband-DIAGS per ottenere il GUID (Globally Unique ID) tramite `ibstat -p` comando. Vedere Determinare i GUID della porta host ed effettuare le impostazioni consigliate per informazioni su come installare il pacchetto infiniband-diags.

Fasi

1. Installare `opensm` pacchetto su tutti gli host che eseguiranno il gestore di subnet.
2. Utilizzare `ibstat -p` comando per trovare `GUID0` e. `GUID1` Delle porte HCA. Ad esempio:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Creare uno script di gestione delle subnet che venga eseguito una volta come parte del processo di avvio.

```
# vim /usr/sbin/subnet-manager.sh
```

4. Aggiungere le seguenti righe. Sostituire i valori trovati al punto 2 `GUID0` e. `GUID1`. Per `P0` e. `P1`, utilizzare le priorità del gestore di subnet, con 1 come minimo e 15 come massimo.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

Un esempio del comando con sostituzioni di valori:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Creare un file system service unit denominato `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Aggiungere le seguenti righe.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notificare al sistema il nuovo servizio.

```
# systemctl daemon-reload
```

8. Attivare e avviare `subnet-manager` servizio.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Impostare NVMe su InfiniBand sul lato host

La configurazione di un iniziatore NVMe in un ambiente InfiniBand include l'installazione e la configurazione dei pacchetti infiniband, nvme-cli e rdma, la configurazione degli indirizzi IP dell'iniziatore e l'impostazione del layer NVMe-of sull'host.

Prima di iniziare

È necessario utilizzare il sistema operativo RHEL 7, RHEL 8, RHEL 9, SUSE Linux Enterprise Server 12 o 15 Service Pack più recente. Vedere "Tool di matrice di interoperabilità NetApp" per un elenco completo dei requisiti più recenti.

Fasi

1. Installare i pacchetti rdma, nvme-cli e infiniband:

   SLES 12 o SLES 15

   ```
   # zypper install infiniband-diags
   # zypper install rdma-core
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8 O RHEL 9

   ```
   # yum install infiniband-diags
   # yum install rdma-core
   # yum install nvme-cli
   ```

2. Per RHEL 8 o RHEL 9, installare gli script di rete:

   RHEL 8

   ```
   # yum install network-scripts
   ```

   RHEL 9

   ```
   # yum install NetworkManager-initscripts-updown
   ```

3. Per RHEL 7, attivare `ipoib`. Modificare il file /etc/rdma/rdma.conf e modificare la voce per il caricamento `ipoib`:

```
IPOIB_LOAD=yes
```

4. Ottenere l'NQN host, che verrà utilizzato per configurare l'host in un array.

```
# cat /etc/nvme/hostnqn
```

5. Verificare che entrambi i collegamenti delle porte IB siano attivi e che lo stato sia attivo:

```
# ibstat
```

```
CA 'mlx4_0'
        CA type: MT4099
        Number of ports: 2
        Firmware version: 2.40.7000
        Hardware version: 1
        Node GUID: 0x0002c90300317850
        System image GUID: 0x0002c90300317853
        Port 1:
                State: Active
                Physical state: LinkUp
                Rate: 40
                Base lid: 4
                LMC: 0
                SM lid: 4
                Capability mask: 0x0259486a
                Port GUID: 0x0002c90300317851
                Link layer: InfiniBand
        Port 2:
                State: Active
                Physical state: LinkUp
                Rate: 56
                Base lid: 5
                LMC: 0
                SM lid: 4
                Capability mask: 0x0259486a
                Port GUID: 0x0002c90300317852
                Link layer: InfiniBand
```

6. Impostare gli indirizzi IP IPv4 sulle porte ib.

SLES 12 o SLES 15

Creare il file /etc/sysconfig/network/ifcfg-ib0 con il seguente contenuto.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='10.10.10.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

Quindi, creare il file /etc/sysconfig/network/ifcfg-ib1:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='11.11.11.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 7 o RHEL 8

Creare il file /etc/sysconfig/network-scripts/ifcfg-ib0 con il seguente contenuto.

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='10.10.10.100/24'
DEFROUTE=no
IPV4=FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib0
ONBOOT=yes
```

Quindi, creare il file /etc/sysconfig/network-scripts/ifcfg-ib1:

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='11.11.11.100/24'
DEFROUTE=no
IPV4=FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib1
ONBOOT=yes
```

RHEL 9

Utilizzare `nmtui` per attivare e modificare una connessione. Di seguito è riportato un file di esempio `/etc/NetworkManager/system-connections/ib0.nmconnection` il tool genera:

```
[connection]
id=ib0
uuid=<unique uuid>
type=infiniband
interface-name=ib0

[infiniband]
mtu=4200

[ipv4]
address1=10.10.10.100/24
method=manual

[ipv6]
addr-gen-mode=default
method=auto

[proxy]
```

Di seguito è riportato un file di esempio `/etc/NetworkManager/system-connections/ib1.nmconnection` il tool genera:

```
[connection]
id=ib1
uuid=<unique uuid>
type=infiniband
interface-name=ib1

[infiniband]
mtu=4200

[ipv4]
address1=11.11.11.100/24'
method=manual

[ipv6]
addr-gen-mode=default
method=auto

[proxy]
```

7. Attivare il `ib` interfaccia:

```
# ifup ib0
# ifup ib1
```

8. Verificare gli indirizzi IP utilizzati per la connessione all'array. Eseguire questo comando per entrambi `ib0` e. `ib1`:

```
# ip addr show ib0
# ip addr show ib1
```

Come illustrato nell'esempio riportato di seguito, l'indirizzo IP di `ib0` è `10.10.10.255`.

```
10: ib0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast
state UP group default qlen 256
    link/infiniband
80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd
00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff:ff
    inet 10.10.10.255 brd 10.10.10.255 scope global ib0
       valid_lft forever preferred_lft forever
    inet6 fe80::202:c903:31:7851/64 scope link
       valid_lft forever preferred_lft forever
```

Come illustrato nell'esempio riportato di seguito, l'indirizzo IP di `ib1` è `11.11.11.255`.

```
10: ib1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast
state UP group default qlen 256
    link/infiniband
80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd
00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff:ff
    inet 11.11.11.255 brd 11.11.11.255 scope global ib0
       valid_lft forever preferred_lft forever
    inet6 fe80::202:c903:31:7851/64 scope link
       valid_lft forever preferred_lft forever
```

9. Impostare il livello NVMe-of sull'host. Creare i seguenti file in /etc/modules-load.d/ per caricare `nvme_rdma` kernel e assicurarsi che il modulo kernel sia sempre attivo, anche dopo un riavvio:

```
# cat /etc/modules-load.d/nvme_rdma.conf
  nvme_rdma
```

10. Riavviare l'host.

    Per verificare `nvme_rdma` kernel module è stato caricato, eseguire questo comando:

```
# lsmod | grep nvme
nvme_rdma              36864  0
nvme_fabrics           24576  1 nvme_rdma
nvme_core             114688  5 nvme_rdma,nvme_fabrics
rdma_cm               114688  7
rpcrdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm
ib_core               393216  15
rdma_cm,ib_ipoib,rpcrdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_umad,
ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm
t10_pi                 16384  2 sd_mod,nvme_core
```

Configurare le connessioni NVMe dell'array di storage su InfiniBand

Se il controller include una porta NVMe su InfiniBand, è possibile configurare l'indirizzo IP di ciascuna porta utilizzando Gestione di sistema di SANtricity.

Fasi

1. Dall'interfaccia di System Manager, 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 NVMe over InfiniBand che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

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

   > L'opzione Configure NVMe over InfiniBand ports (Configura porte NVMe su InfiniBand) viene visualizzata solo se System Manager rileva NVMe sulle porte InfiniBand del controller.

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

5. Nell'elenco a discesa, selezionare la porta HIC che si desidera configurare, quindi immettere l'indirizzo IP della porta.
6. Fare clic su **Configura**.
7. Ripetere i passaggi 5 e 6 per le altre porte HIC che verranno utilizzate.

Rilevare e connettersi allo storage dall'host

Prima di definire ciascun host in Gestore di sistema di SANtricity, è necessario individuare le porte del controller di destinazione dall'host, quindi stabilire connessioni NVMe.

Fasi

1. Individuare i sottosistemi disponibili sulla destinazione NVMe-of per tutti i percorsi utilizzando il seguente comando:

   ```
   nvme discover -t rdma -a target_ip_address
   ```

   In questo comando, `target_ip_address` È l'indirizzo IP della porta di destinazione.

   > Il `nvme discover` il comando rileva tutte le porte del controller nel sottosistema, indipendentemente dall'accesso all'host.

```
# nvme discover -t rdma -a 10.10.10.200
 Discovery Log Number of Records 2, Generation counter 0
 =====Discovery Log Entry 0======
 trtype:  rdma
 adrfam:  ipv4
 subtype: nvme subsystem
 treq:    not specified
 portid:  0
 trsvcid: 4420
 subnqn:  nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
 traddr: 10.10.10.200
 rdma_prtype: infiniband
 rdma_qptype: connected
 rdma_cms:    rdma-cm
 rdma_pkey: 0x0000
=====Discovery Log Entry 1======
 trtype:  rdma
 adrfam:  ipv4
 subtype: nvme subsystem
 treq:    not specified
 portid:  1
 trsvcid: 4420
 subnqn:  nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
 traddr: 11.11.11.100
 rdma_prtype: infiniband
 rdma_qptype: connected
 rdma_cms:    rdma-cm
 rdma_pkey: 0x0000
```

2. Ripetere il passaggio 1 per qualsiasi altra connessione.
3. Connettersi al sottosistema rilevato sul primo percorso utilizzando il comando: `nvme connect -t rdma -n discovered_sub_nqn -a target_ip_address -Q queue_depth_setting -l controller_loss_timeout_period`

> Il comando precedente non persiste durante il riavvio. Il `nvme connect` Il comando deve essere eseguito dopo ogni riavvio per ristabilire le connessioni NVMe.

> Le connessioni NVMe non persistono durante il riavvio del sistema o per periodi prolungati di indisponibilità del controller.

> Le connessioni non vengono stabilite per nessuna porta rilevata inaccessibile dall'host.

> Se si specifica un numero di porta utilizzando questo comando, la connessione non riesce. La porta predefinita è l'unica porta configurata per le connessioni.

L'impostazione consigliata per la profondità della coda è 1024. Eseguire il override dell'impostazione predefinita di 128 con 1024 utilizzando `-Q 1024`opzione della riga di comando, come illustrato nell'esempio seguente.

Il periodo di timeout consigliato per la perdita del controller in secondi è di 60 minuti (3600 secondi). Ignorare l'impostazione predefinita di 600 secondi con 3600 secondi utilizzando `-l 3600` opzione della riga di comando, come mostrato nell'esempio seguente:

```
# nvme connect -t rdma -a 10.10.10.200 -n nqn.1992-
08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

4. Utilizzare `nvme list-subsys` Per visualizzare un elenco dei dispositivi NVMe attualmente connessi.
5. Connettersi al sottosistema rilevato sul secondo percorso:

```
  # nvme connect -t rdma -a 11.11.11.100 -n nqn.1992-
08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

6. Utilizzare Linux `lsblk` e. `grep` comandi per visualizzare informazioni aggiuntive su ciascun dispositivo a blocchi:

```
 # lsblk | grep nvme

 nvme0n1    259:0    0     5G  0 disk
 nvme1n1    259:0    0     5G  0 disk
```

7. Utilizzare `nvme list` Per visualizzare un nuovo elenco dei dispositivi NVMe attualmente connessi. Nell'esempio riportato di seguito, è così `nvme0n1` e. `nvme0n1`.

```
 # nvme list
 Node          SN            Model                    Namespace
 ------------------------------------------------------------
 /dev/nvme0n1  021648023161  NetApp E-Series          1
 /dev/nvme1n1  021648023161  NetApp E-Series          1
```

```
Usage                  Format           FW Rev
-----------------------------------------------------------------
5.37 GB /5.37 GB          512 B + 0 B      0842XXXX
5.37 GB /5.37 GB          512 B + 0 B      0842XXXX
```

Definire un host

Utilizzando Gestore di sistema di SANtricity, è possibile definire gli host che inviano i dati allo storage array. La definizione 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 definisce 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.

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare una delle seguenti opzioni dall'elenco a discesa: • **Linux** per SANtricity 11.60 e versioni successive • **Linux DM-MP (kernel 3.10 o successivo)** per pre-SANtricity 11.60
Tipo di interfaccia host	Selezionare il tipo di interfaccia host che si desidera utilizzare.

Impostazione	Descrizione
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare interfaccia i/o** Se le porte host hanno effettuato l'accesso, è possibile selezionare gli identificatori delle porte host dall'elenco. Questo è il metodo consigliato. • **Aggiunta manuale** Se le porte host non hanno effettuato l'accesso, controllare /etc/nvme/hostnqn sull'host per trovare gli identificatori hostnqn e associarli alla definizione dell'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dal file /etc/nvme/hostnqn (uno alla volta) nel campo **host ports** (Porte host). È necessario aggiungere 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.

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

Risultato

Una volta creato correttamente l'host, Gestore di sistema di SANtricity crea un nome predefinito per ogni porta host configurata per l'host.

L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per `host IPT is IPT_1`.

Assegnare un volume

È necessario assegnare un volume (spazio dei nomi) 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 spazi dei nomi in un array di storage.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

- 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 ID dello spazio dei nomi (NSID) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un NSID univoco.

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.
- Sono state definite tutte le assegnazioni dei volumi.

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.

Risultato

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 NSID disponibile. L'host utilizza l'NSID per accedere al volume.
- Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host.

Visualizzare i volumi visibili all'host

È possibile utilizzare lo strumento SMdevices per visualizzare i volumi attualmente visibili sull'host. Questo tool fa parte del pacchetto nvme-cli e può essere utilizzato in alternativa a `nvme list` comando.

Per visualizzare informazioni su ciascun percorso NVMe a un volume e-Series, utilizzare `nvme netapp smdevices [-o <format>]` comando. L'output `<format>` può essere normale (il valore predefinito se -o non viene utilizzato), column o json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Impostare il failover

Per fornire un percorso ridondante all'array di storage, è possibile configurare l'host per eseguire il failover.

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

> Fare riferimento a. "Tool di matrice di interoperabilità NetApp" Per garantire l'installazione degli aggiornamenti necessari, il multipathing potrebbe non funzionare correttamente con le versioni GA di SLES o RHEL.

A proposito di questa attività

RHEL 7 e SLES 12 utilizzano il multipath DMMP (Device Mapper Multipath) per il multipathing quando si utilizza NVMe su Infiniband. RHEL 8, RHEL9 e SLES 15 utilizzano un failover NVMe nativo integrato. A seconda del sistema operativo in esecuzione, è necessaria una configurazione aggiuntiva di multipath per il

corretto funzionamento.

Attiva DMMP (Device Mapper Multipath) per RHEL 7 o SLES 12

Per impostazione predefinita, DM-MP è disattivato in RHEL e SLES. Per abilitare i componenti DM-MP sull'host, attenersi alla seguente procedura.

Fasi

1. Aggiungere la voce NVMe e-Series Device alla sezione devices del file /etc/multipath.conf, come mostrato nell'esempio seguente:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configurare `multipathd` per iniziare all'avvio del sistema.

```
# systemctl enable multipathd
```

3. Inizio `multipathd` se non è in esecuzione.

```
# systemctl start multipathd
```

4. Verificare lo stato di `multipathd` per assicurarsi che sia attivo e in esecuzione:

```
# systemctl status multipathd
```

Configurazione di RHEL 8 con NVMe Multipathing nativo

NVMe Multipathing nativo è disattivato per impostazione predefinita in RHEL 8 e deve essere attivato seguendo la procedura riportata di seguito.

1. Setup (Configurazione) `modprobe` Regola per attivare NVMe Multipathing nativo.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` con il nuovo `modprobe` parametro.

```
# dracut -f
```

3. Riavviare il server per attivarlo con NVMe Multipathing nativo attivato.

```
# reboot
```

4. Verificare che il multipathing NVMe nativo sia stato attivato dopo l'avvio del backup dell'host.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. Se l'output del comando è `N`, Quindi NVMe Multipathing nativo è ancora disattivato.
   b. Se l'output del comando è `Y`, Quindi viene attivato NVMe Multipathing nativo e tutti i dispositivi NVMe rilevati lo utilizzeranno.

> Per SLES 15 e RHEL 9, il multipathing NVMe nativo è attivato per impostazione predefinita e non è richiesta alcuna configurazione aggiuntiva.

Accedere ai volumi NVMe per le destinazioni dei dispositivi virtuali

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 7 e SLES 12, l'i/o viene indirizzato alle destinazioni dei dispositivi virtuali dall'host Linux. DM-MP gestisce i percorsi fisici sottostanti queste destinazioni virtuali.

I dispositivi virtuali sono destinazioni di i/O.

Assicurarsi di eseguire l'i/o solo sui dispositivi virtuali creati da DM-MP e non sui percorsi fisici dei dispositivi. Se si esegue l'i/o sui percorsi fisici, DM-MP non può gestire un evento di failover e l'i/o non riesce.

È possibile accedere a questi dispositivi a blocchi tramite `dm` o a. `symlink` in /dev/mapper. Ad esempio:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Output di esempio

Il seguente esempio di output da `nvme list` Il comando mostra il nome del nodo host e la sua correlazione con l'ID dello spazio dei nomi.

```
NODE         SN            MODEL           NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Colonna	Descrizione
`Node`	Il nome del nodo comprende due parti: • La notazione `nvme1` Rappresenta il controller A e. `nvme2` Rappresenta il controller B. • La notazione `n1`, `n2`, e così via rappresentano l'identificatore dello spazio dei nomi dal punto di vista dell'host. Questi identificatori vengono ripetuti nella tabella, una volta per il controller A e una volta per il controller B.
`Namespace`	La colonna namespace elenca l'ID dello spazio dei nomi (NSID), che è l'identificatore dal punto di vista dello storage array.

Di seguito `multipath -ll` output, i percorsi ottimizzati vengono visualizzati con una `prio` valore di 50, mentre i percorsi non ottimizzati vengono visualizzati con un `prio` valore di 10.

Il sistema operativo Linux indirizza i/o al gruppo di percorsi indicato come `status=active`, mentre i gruppi di percorsi sono elencati come `status=enabled` sono disponibili per il failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Voce	Descrizione
`policy='service-time 0' prio=50 status=active`	Questa riga e la riga seguente lo mostrano `nvme1n1`, Che è lo spazio dei nomi con un NSID di 10, è ottimizzato sul percorso con un `prio` valore di 50 e a. `status` valore di `active`. Questo namespace è di proprietà del controller A.
`policy='service-time 0' prio=10 status=enabled`	Questa riga mostra il percorso di failover per lo spazio dei nomi 10, con un `prio` valore di 10 e a. `status` valore di `enabled`. Al momento l'i/o non viene indirizzato allo spazio dei nomi di questo percorso. Questo namespace è di proprietà del controller B.
`policy='service-time 0' prio=0 status=enabled`	Questo esempio mostra `multipath -ll`Output da un punto diverso nel tempo, mentre il controller A viene riavviato. Il percorso verso lo spazio dei nomi 10 viene mostrato come con un `prio` valore di 0 e a. `status` valore di `enabled`.
`policy='service-time 0' prio=10 status=active`	Tenere presente che il `active` percorso a cui si riferisce `nvme2`, Quindi l'i/o viene indirizzato su questo percorso al controller B.

Accedere ai volumi NVMe per le destinazioni fisiche dei dispositivi NVMe

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 8, RHEL 9 e SLES 15, l'i/o viene indirizzato alle destinazioni fisiche del dispositivo NVMe dall'host Linux. Una soluzione NVMe multipathing nativa gestisce i percorsi fisici sottostanti il singolo dispositivo fisico

apparente visualizzato dall'host.

I dispositivi NVMe fisici sono destinazioni di i/O.

È consigliabile eseguire i/o ai collegamenti in `/dev/disk/by-id/nvme-eui.[uuid#]` piuttosto che direttamente al percorso fisico del dispositivo nvme `/dev/nvme[subsys#]n[id#]`. Il collegamento tra queste due posizioni può essere trovato usando il seguente comando:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/o eseguito a. `/dev/disk/by-id/nvme-eui.[uuid#]` verrà passata direttamente `/dev/nvme[subsys#]n[id#]` Che ha tutti i percorsi virtualizzati sotto l'IT utilizzando la soluzione di multipathing NVMe nativa.

Puoi visualizzare i tuoi percorsi eseguendo:

```
# nvme list-subsys
```

Output di esempio:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

Se si specifica un dispositivo nvme fisico quando si utilizza il comando 'nvme list-subsys', vengono fornite ulteriori informazioni sui percorsi per lo spazio dei nomi:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

Sono inoltre presenti collegamenti ai comandi multipath per consentire di visualizzare le informazioni sul percorso per il failover nativo attraverso di essi:

```
#multipath -ll
```

Per visualizzare le informazioni sul percorso, impostare quanto segue in /etc/multipath.conf:

```
defaults {
        enable_foreign nvme
}
```

Output di esempio:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Creazione di filesystem (RHEL 7 e SLES 12)

Per RHEL 7 e SLES 12, si crea un file system sullo spazio dei nomi e si monta il file system.

Fasi

1. Eseguire `multipath -ll` per ottenere un elenco di `/dev/mapper/dm` dispositivi.

   ```
   # multipath -ll
   ```

   Il risultato di questo comando mostra due dispositivi, `dm-19` e. `dm-16`:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n19 259:19  active ready running
| `- #:#:#:# nvme1n19 259:115 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n19 259:51  active ready running
  `- #:#:#:# nvme3n19 259:83  active ready running
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n16 259:16  active ready running
| `- #:#:#:# nvme1n16 259:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n16 259:48  active ready running
  `- #:#:#:# nvme3n16 259:80  active ready running
```

2. Creare un file system sulla partizione per ciascuno di essi `/dev/mapper/eui-` dispositivo.

   Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Creazione di file system (RHEL 8, RHEL 9, SLES 15)

Per RHEL 8, RHEL 9, SLES 15, si crea un file system sul dispositivo nvme nativo e si monta il file system.

Fasi

1. Eseguire `multipath -ll` per ottenere un elenco di dispositivi nvme.

```
# multipath -ll
```

Il risultato di questo comando può essere utilizzato per trovare i dispositivi associati a `/dev/disk/by-id/nvme-eui.[uuid#]` posizione. Per l'esempio riportato di seguito, questo sarebbe `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
Series,08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=50 status=optimized
| `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=10 status=non-optimized
| `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`-+- policy='n/a' prio=10 status=non-optimized
  `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Creare un file system sulla partizione per il dispositivo nvme desiderato utilizzando la posizione `/dev/disk/by-id/nvme-eui.[id#]`.

Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verificare l'accesso allo storage sull'host

Prima di utilizzare lo spazio dei nomi, verificare che l'host possa scrivere i dati nello spazio dei nomi e leggerli.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Namespace inizializzato formattato con un file system.

Fasi

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

Al termine

Rimuovere il file e la cartella copiati.

Registra la tua configurazione NVMe over IB

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

Identificatori host

L'iniziatore software NQN viene determinato durante l'attività.

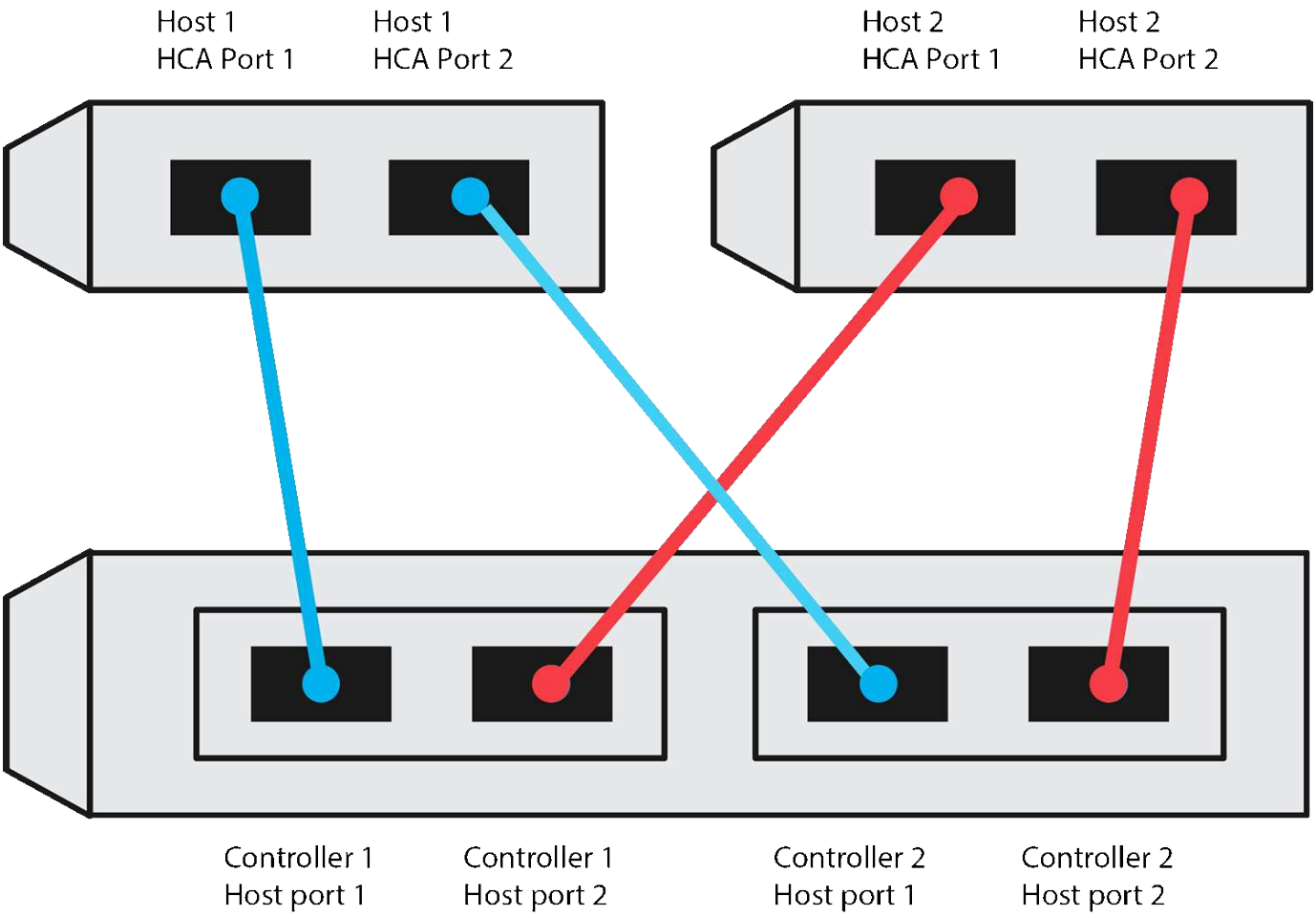
Individuare e documentare l'NQN iniziatore da ciascun host. L'NQN si trova generalmente nel file /etc/nvme/hostnqn.

N. didascalia	Connessioni alla porta host	NQN host
1	Host (iniziatore) 1	
n/a.		

N. didascalia	Connessioni alla porta host	NQN host
n/a.		
n/a.		
n/a.		

Configurazione consigliata

In una topologia a connessione diretta, uno o più host sono collegati direttamente al sottosistema. Nella versione SANtricity OS 11.50, supportiamo una singola connessione da ciascun host a un controller del sottosistema, come mostrato di seguito. In questa configurazione, una porta HCA (host Channel Adapter) di ciascun host deve trovarsi sulla stessa subnet della porta del controller e-Series a cui è collegato, ma su una subnet diversa dall'altra porta HCA.



NQN di destinazione

Documentare l'NQN di destinazione per lo storage array. Queste informazioni verranno utilizzate in Configurare le connessioni NVMe dell'array di storage su InfiniBand.

Individuare il nome NQN dell'array di storage utilizzando SANtricity: **Array di storage** > **NVMe su Infiniband** > **Gestisci impostazioni**. Queste informazioni potrebbero essere necessarie quando si creano sessioni NVMe su InfiniBand da sistemi operativi che non supportano il rilevamento delle destinazioni di invio.

N. didascalia	Nome array	IQN di destinazione
6	Controller di array (destinazione)	

Configurazione di rete

Documentare la configurazione di rete che verrà utilizzata per gli host e lo storage sul fabric InfiniBand. Queste istruzioni presuppongono che vengano utilizzate due subnet per la ridondanza completa.

L'amministratore di rete può fornire le seguenti informazioni. Queste informazioni vengono utilizzate nell'argomento, Configurare le connessioni NVMe dell'array di storage su InfiniBand.

Subnet A

Definire la subnet da utilizzare.

Indirizzo di rete	Netmask

Documentare gli NQN che devono essere utilizzati dalle porte dell'array e da ciascuna porta host.

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	NQN
3	Switch	*non applicabile*
5	Controller A, porta 1	
4	Controller B, porta 1	
2	Host 1, porta 1	
	(Opzionale) host 2, porta 1	

Subnet B

Definire la subnet da utilizzare.

Indirizzo di rete	Netmask

Documentare gli IQN che devono essere utilizzati dalle porte dell'array e da ciascuna porta host.

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	NQN
8	Switch	*non applicabile*

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	NQN
10	Controller A, porta 2	
9	Controller B, porta 2	
7	Host 1, porta 2	
	(Opzionale) host 2, porta 2	

Nome host di mapping

Il nome host del mapping viene creato durante il flusso di lavoro.

Nome host di mapping
Tipo di sistema operativo host

NVMe over RoCE Setup (Configurazione NVMe su RoCE)

Verificare il supporto di Linux ed esaminare le restrizioni

Come prima fase, è necessario verificare che la configurazione Linux sia supportata ed esaminare anche le restrizioni relative a controller, switch, host e ripristino.

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

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

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

Verificare le restrizioni NVMe su RoCE

Prima di utilizzare NVMe su RoCE, consultare la "Tool di matrice di interoperabilità NetApp" per esaminare le restrizioni più recenti relative a controller, host e recovery.

Limitazioni dello switch

RISCHIO DI PERDITA DI DATI. è necessario attivare il controllo di flusso per l'utilizzo con Global Pause Control sullo switch per eliminare il rischio di perdita di dati in un ambiente NVMe over RoCE.

Limitazioni di storage e disaster recovery

- Il mirroring asincrono e sincrono non è supportato.
- Il thin provisioning (creazione di thin volumi) non è supportato.

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

- Nessuna notifica configurata.

Fasi

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

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

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

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

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

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

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

Configurare lo switch

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

> **RISCHIO DI PERDITA DI DATI.** è necessario attivare il controllo di flusso per l'utilizzo con Global Pause Control sullo switch per eliminare il rischio di perdita di dati in un ambiente NVMe over RoCE.

Fasi

1. Attiva il controllo del flusso di frame di pausa Ethernet **end-to-end** come configurazione Best practice.

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

Impostare NVMe su RoCE sul lato host

La configurazione di NVMe Initiator in un ambiente RoCE include l'installazione e la configurazione dei pacchetti rdma-core e nvme-cli, la configurazione degli indirizzi IP dell'iniziatore e l'impostazione del layer NVMe-of sull'host.

Prima di iniziare

È necessario utilizzare il sistema operativo RHEL 7, RHEL 8, RHEL 9, SUSE Linux Enterprise Server 12 o 15 Service Pack più recente. Vedere "Tool di matrice di interoperabilità NetApp" per un elenco completo dei requisiti più recenti.

Fasi

1. Installare i pacchetti rdma e nvme-cli:

   SLES 12 o SLES 15

   ```
   # zypper install rdma-core
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8 E RHEL 9

   ```
   # yum install rdma-core
   # yum install nvme-cli
   ```

2. Per RHEL 8 e RHEL 9, installare gli script di rete:

   RHEL 8

   ```
   # yum install network-scripts
   ```

   RHEL 9

   ```
   # yum install NetworkManager-initscripts-updown
   ```

3. Ottenere l'NQN host, che verrà utilizzato per configurare l'host in un array.

   ```
   # cat /etc/nvme/hostnqn
   ```

4. Impostare gli indirizzi IP IPv4 sulle porte ethernet utilizzate per collegare NVMe su RoCE. Per ciascuna interfaccia di rete, creare uno script di configurazione che contenga le diverse variabili per tale interfaccia.

Le variabili utilizzate in questa fase si basano sull'hardware del server e sull'ambiente di rete. Le variabili includono `IPADDR` e. `GATEWAY`. Queste sono istruzioni di esempio per SLES e RHEL:

SLES 12 e SLES 15

Creare il file di esempio `/etc/sysconfig/network/ifcfg-eth4` con i seguenti contenuti.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.1.87/24'
GATEWAY='192.168.1.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

Quindi, creare il file di esempio `/etc/sysconfig/network/ifcfg-eth5`:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 7 o RHEL 8

Creare il file di esempio `/etc/sysconfig/network-scripts/ifcfg-eth4` con i seguenti contenuti.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.1.87/24’
GATEWAY='192.168.1.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

Quindi, creare il file di esempio `/etc/sysconfig/network-scripts/ifcfg-eth5`:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 9

Utilizzare `nmtui` per attivare e modificare una connessione. Di seguito è riportato un file di esempio `/etc/NetworkManager/system-connections/eth4.nmconnection` il tool genera:

```
[connection]
id=eth4
uuid=<unique uuid>
type=ethernet
interface-name=eth4

[ethernet]
mtu=4200

[ipv4]
address1=192.168.1.87/24
method=manual

[ipv6]
addr-gen-mode=default
method=auto

[proxy]
```

Di seguito è riportato un file di esempio `/etc/NetworkManager/system-connections/eth5.nmconnection` il tool genera:

```
[connection]
id=eth5
uuid=<unique uuid>
type=ethernet
interface-name=eth5

[ethernet]
mtu=4200

[ipv4]
address1=192.168.2.87/24
method=manual

[ipv6]
addr-gen-mode=default
method=auto

[proxy]
```

5. Abilitare le interfacce di rete:

```
# ifup eth4
# ifup eth5
```

6. Impostare il livello NVMe-of sull'host. Creare il seguente file in `/etc/modules-load.d/` per caricare `nvme_rdma` kernel e assicurarsi che il modulo kernel sia sempre attivo, anche dopo un riavvio:

```
# cat /etc/modules-load.d/nvme_rdma.conf
  nvme_rdma
```

7. Riavviare l'host.

   Per verificare `nvme_rdma` kernel module è stato caricato, eseguire questo comando:

```
# lsmod | grep nvme
nvme_rdma              36864  0
nvme_fabrics           24576  1 nvme_rdma
nvme_core             114688  5 nvme_rdma,nvme_fabrics
rdma_cm               114688  7
rpcrdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm
ib_core               393216  15
rdma_cm,ib_ipoib,rpcrdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_umad,
ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm
t10_pi                 16384  2 sd_mod,nvme_core
```

Configurare NVMe array di storage su connessioni RoCE

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Una porta host NVMe over RoCE sul controller; in caso contrario, le impostazioni NVMe over RoCE non sono disponibili in System Manager.
- L'indirizzo IP della connessione host.

A proposito di questa attività

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

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

Fasi

1. Dall'interfaccia di System Manager, selezionare **hardware**.
2. Fare clic sul controller con la porta NVMe over RoCE che si desidera configurare.

   Viene visualizzato il menu di scelta rapida del controller.

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

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

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

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

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità desiderata. Le opzioni visualizzate nell'elenco a discesa dipendono dalla velocità massima supportata dalla rete (ad esempio, 10 Gbps). I valori possibili includono: • Negoziazione automatica • 10 Gbps • 25 Gbps • 40 Gbps • 50 Gbps • 100 Gbps • 200 Gbps Quando un HIC da 200 GB è collegato con un cavo QSFP56, la negoziazione automatica è disponibile solo quando si effettua la connessione a switch e/o adattatori Mellanox. La velocità della porta NVMe su RoCE configurata deve corrispondere alla velocità del modulo SFP sulla porta selezionata. Tutte le porte devono essere impostate alla stessa velocità.
Abilitare IPv4 e/o abilitare IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.

Impostazione della porta	Descrizione
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 MTU predefinita è 1500 byte per frame. Immettere un valore compreso tra 1500 e 4200.

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.

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

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione dal server DHCP	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere gli indirizzi IP instradabili e l'indirizzo IP del router. Se è presente un solo indirizzo IP instradabile, impostare l'indirizzo rimanente su 0:0:0:0:0:0:0:0.
Abilitare il supporto VLAN (disponibile facendo clic su **Mostra altre impostazioni**).	Questa opzione è disponibile solo in un ambiente iSCSI. Non è disponibile in un ambiente NVMe over RoCE.
Abilitare la priorità ethernet (disponibile facendo clic su **Mostra altre impostazioni**).	Questa opzione è disponibile solo in un ambiente iSCSI. Non è disponibile in un ambiente NVMe over RoCE.

7. Fare clic su **fine**.

Rilevare e connettersi allo storage dall'host

Prima di definire ciascun host in Gestore di sistema di SANtricity, è necessario individuare le porte del controller di destinazione dall'host, quindi stabilire connessioni NVMe.

Fasi

1. Individuare i sottosistemi disponibili sulla destinazione NVMe-of per tutti i percorsi utilizzando il seguente comando:

```
nvme discover -t rdma -a target_ip_address
```

In questo comando, `target_ip_address` È l'indirizzo IP della porta di destinazione.

> Il `nvme discover` il comando rileva tutte le porte del controller nel sottosistema, indipendentemente dall'accesso all'host.

```
# nvme discover -t rdma -a 192.168.1.77
Discovery Log Number of Records 2, Generation counter 0
=====Discovery Log Entry 0======
trtype:  rdma
adrfam:  ipv4
subtype: nvme subsystem
treq:    not specified
portid:  0
trsvcid: 4420
subnqn:  nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr:  192.168.1.77
rdma_prtype: roce
rdma_qptype: connected
rdma_cms:    rdma-cm
rdma_pkey: 0x0000
=====Discovery Log Entry 1======
trtype:  rdma
adrfam:  ipv4
subtype: nvme subsystem
treq:    not specified
portid:  1
trsvcid: 4420
subnqn:  nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr:  192.168.2.77
rdma_prtype: roce
rdma_qptype: connected
rdma_cms:    rdma-cm
rdma_pkey: 0x0000
```

2. Ripetere il passaggio 1 per qualsiasi altra connessione.
3. Connettersi al sottosistema rilevato sul primo percorso utilizzando il comando: `nvme connect -t rdma -n discovered_sub_nqn -a target_ip_address -Q queue_depth_setting -l controller_loss_timeout_period`

Il comando elencato in precedenza non persiste durante il riavvio. Il `NVMe connect` Il comando deve essere eseguito dopo ogni riavvio per ristabilire le connessioni NVMe.

Le connessioni non vengono stabilite per nessuna porta rilevata inaccessibile dall'host.

Se si specifica un numero di porta utilizzando questo comando, la connessione non riesce. La porta predefinita è l'unica porta configurata per le connessioni.

L'impostazione consigliata per la profondità della coda è 1024. Eseguire il override dell'impostazione predefinita di 128 con 1024 utilizzando `-Q 1024`opzione della riga di comando, come illustrato nell'esempio seguente.

Il periodo di timeout consigliato per la perdita del controller in secondi è di 60 minuti (3600 secondi). Ignorare l'impostazione predefinita di 600 secondi con 3600 secondi utilizzando `-l 3600` opzione della riga di comando, come illustrato nell'esempio seguente.

```
# nvme connect -t rdma -a 192.168.1.77 -n nqn.1992-
08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
# nvme connect -t rdma -a 192.168.2.77 -n nqn.1992-
08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
```

4. Ripetere il passaggio 3 per collegare il sottosistema rilevato al secondo percorso.

Definire un host

Utilizzando Gestore di sistema di SANtricity, è possibile definire gli host che inviano i dati allo storage array. La definizione 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 definisce 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.

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare una delle seguenti opzioni dall'elenco a discesa: • **Linux** per SANtricity 11.60 e versioni successive • **Linux DM-MP (kernel 3.10 o successivo)** per pre-SANtricity 11.60
Tipo di interfaccia host	Selezionare il tipo di interfaccia host che si desidera utilizzare. Se l'array configurato dispone di un solo tipo di interfaccia host, questa impostazione potrebbe non essere disponibile per la selezione.
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare interfaccia i/o** Se le porte host hanno effettuato l'accesso, è possibile selezionare gli identificatori delle porte host dall'elenco. Questo è il metodo consigliato. • **Aggiunta manuale** Se le porte host non hanno effettuato l'accesso, controllare /etc/nvme/hostnqn sull'host per trovare gli identificatori hostnqn e associarli alla definizione dell'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dal file /etc/nvme/hostnqn (uno alla volta) nel campo **host ports** (Porte host). È necessario aggiungere 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.

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

Risultato

Una volta creato correttamente l'host, Gestore di sistema di SANtricity crea un nome predefinito per ogni porta host configurata per l'host.

L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per `host IPT is IPT_1`.

Assegnare un volume

È necessario assegnare un volume (spazio dei nomi) 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 spazi dei nomi in un array di storage.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

- 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 ID dello spazio dei nomi (NSID) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un NSID univoco.

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.
- Sono state definite tutte le assegnazioni dei volumi.

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.

Risultato

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 NSID disponibile. L'host utilizza l'NSID per accedere al volume.
- Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host.

Visualizzare i volumi visibili all'host

È possibile utilizzare lo strumento SMdevices per visualizzare i volumi attualmente visibili sull'host. Questo tool fa parte del pacchetto nvme-cli e può essere utilizzato in alternativa a `nvme list` comando.

Per visualizzare informazioni su ciascun percorso NVMe a un volume e-Series, utilizzare `nvme netapp smdevices [-o <format>]` comando. L'<format> di output può essere normale (l'impostazione predefinita se -o non viene utilizzato), column o json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Impostare il failover sull'host

Per fornire un percorso ridondante all'array di storage, è possibile configurare l'host per eseguire il failover.

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

> Fare riferimento a. "Tool di matrice di interoperabilità NetApp" Per garantire l'installazione degli aggiornamenti necessari, poiché il multipathing potrebbe non funzionare correttamente con le versioni GA di SLES o RHEL.

A proposito di questa attività

RHEL 7 e SLES 12 utilizzano il multipath DMMP (Device Mapper Multipath) per il multipathing per NVMe su RoCE. RHEL 8, RHEL 9 e SLES 15 utilizzano un failover NVMe nativo integrato. A seconda del sistema operativo in esecuzione, è necessaria una configurazione aggiuntiva di multipath per il corretto funzionamento.

Attiva DMMP (Device Mapper Multipath) per RHEL 7 o SLES 12

Per impostazione predefinita, DM-MP è disattivato in RHEL e SLES. Per abilitare i componenti DM-MP sull'host, attenersi alla seguente procedura.

Fasi

1. Aggiungere la voce NVMe e-Series Device (dispositivo NVMe e-Series) alla sezione Devices (dispositivi) di `/etc/multipath.conf` come mostrato nell'esempio seguente:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configurare `multipathd` per iniziare all'avvio del sistema.

```
# systemctl enable multipathd
```

3. Inizio `multipathd` se non è in esecuzione.

```
# systemctl start multipathd
```

4. Verificare lo stato di `multipathd` per assicurarsi che sia attivo e in esecuzione:

```
# systemctl status multipathd
```

Configurare RHEL 8 con NVMe Multipathing nativo

Il multipathing NVMe nativo è disattivato per impostazione predefinita in RHEL 8 e deve essere attivato utilizzando la procedura seguente.

1. Configurare `modprobe` Regola per attivare NVMe Multipathing nativo.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` con il nuovo `modprobe` parametro.

```
# dracut -f
```

3. Riavviare il server per attivarlo con NVMe Multipathing nativo attivato.

```
# reboot
```

4. Verificare che NVMe Multipathing nativo sia attivato dopo l'avvio del backup dell'host.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. Se l'output del comando è `N`, Quindi NVMe Multipathing nativo è ancora disattivato.
   b. Se l'output del comando è `Y`, Quindi viene attivato NVMe Multipathing nativo e tutti i dispositivi NVMe rilevati lo utilizzeranno.

> Per RHEL 9 e SLES 15, il multipathing NVMe nativo è attivato per impostazione predefinita e non è richiesta alcuna configurazione aggiuntiva.

Accedere ai volumi NVMe per le destinazioni dei dispositivi virtuali

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 7 e SLES 12, l'i/o viene indirizzato alle destinazioni dei dispositivi virtuali dall'host Linux. DM-MP gestisce i percorsi fisici sottostanti queste destinazioni virtuali.

I dispositivi virtuali sono destinazioni di i/O.

Assicurarsi di eseguire l'i/o solo sui dispositivi virtuali creati da DM-MP e non sui percorsi fisici dei dispositivi. Se si esegue l'i/o sui percorsi fisici, DM-MP non può gestire un evento di failover e l'i/o non riesce.

È possibile accedere a questi dispositivi a blocchi tramite `dm` o a. `symlink` in /dev/mapper. Ad esempio:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Esempio

Il seguente esempio di output da `nvme list` Il comando mostra il nome del nodo host e la sua correlazione con l'ID dello spazio dei nomi.

```
NODE         SN           MODEL           NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Colonna	Descrizione
`Node`	Il nome del nodo comprende due parti: • La notazione `nvme1` Rappresenta il controller A e. `nvme2` Rappresenta il controller B. • La notazione `n1`, `n2`, e così via rappresentano l'identificatore dello spazio dei nomi dal punto di vista dell'host. Questi identificatori vengono ripetuti nella tabella, una volta per il controller A e una volta per il controller B.
`Namespace`	La colonna namespace elenca l'ID dello spazio dei nomi (NSID), che è l'identificatore dal punto di vista dello storage array.

Di seguito `multipath -ll` output, i percorsi ottimizzati vengono visualizzati con una `prio` valore di 50, mentre i percorsi non ottimizzati vengono visualizzati con un `prio` valore di 10.

Il sistema operativo Linux indirizza i/o al gruppo di percorsi indicato come `status=active`, mentre i gruppi di percorsi sono elencati come `status=enabled` sono disponibili per il failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Voce	Descrizione
`policy='service-time 0' prio=50 status=active`	Questa riga e la riga seguente lo mostrano `nvme1n1`, Che è lo spazio dei nomi con un NSID di 10, è ottimizzato sul percorso con un `prio` valore di 50 e a. `status` valore di `active`. Questo namespace è di proprietà del controller A.
`policy='service-time 0' prio=10 status=enabled`	Questa riga mostra il percorso di failover per lo spazio dei nomi 10, con un `prio` valore di 10 e a. `status` valore di `enabled`. Al momento l'i/o non viene indirizzato allo spazio dei nomi di questo percorso. Questo namespace è di proprietà del controller B.
`policy='service-time 0' prio=0 status=enabled`	Questo esempio mostra `multipath -ll`Output da un punto diverso nel tempo, mentre il controller A viene riavviato. Il percorso verso lo spazio dei nomi 10 viene mostrato come con un `prio` valore di 0 e a. `status` valore di `enabled`.
`policy='service-time 0' prio=10 status=active`	Tenere presente che il `active` percorso a cui si riferisce `nvme2`, Quindi l'i/o viene indirizzato su questo percorso al controller B.

Accesso ai volumi NVMe per le destinazioni fisiche dei dispositivi NVMe

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 8, RHEL 9 e SLES 15, l'i/o viene indirizzato alle destinazioni fisiche del dispositivo NVMe dall'host Linux. Una soluzione NVMe multipathing nativa gestisce i percorsi fisici sottostanti il singolo dispositivo fisico

apparente visualizzato dall'host.

I dispositivi NVMe fisici sono destinazioni di i/O.

È consigliabile eseguire i/o ai collegamenti in `/dev/disk/by-id/nvme-eui.[uuid#]` piuttosto che direttamente al percorso fisico del dispositivo nvme `/dev/nvme[subsys#]n[id#]`. Il collegamento tra queste due posizioni può essere trovato usando il seguente comando:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/o eseguito a. `/dev/disk/by-id/nvme-eui.[uuid#]` verrà passata direttamente `/dev/nvme[subsys#]n[id#]` Che ha tutti i percorsi virtualizzati sotto l'IT utilizzando la soluzione di multipathing NVMe nativa.

Puoi visualizzare i tuoi percorsi eseguendo:

```
# nvme list-subsys
```

Output di esempio:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

Se si specifica un dispositivo namespace quando si utilizza `nvme list-subsys` fornisce informazioni aggiuntive sui percorsi per lo spazio dei nomi:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

Sono inoltre presenti collegamenti ai comandi multipath per consentire di visualizzare le informazioni sul percorso per il failover nativo attraverso di essi:

```
#multipath -ll
```

Per visualizzare le informazioni sul percorso, impostare quanto segue in /etc/multipath.conf:

```
defaults {
        enable_foreign nvme
}
```

Output di esempio:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Creazione di filesystem (RHEL 7 e SLES 12)

Per RHEL 7 e SLES 12, si crea un file system sullo spazio dei nomi e si monta il file system.

Fasi

1. Eseguire `multipath -ll` per ottenere un elenco di `/dev/mapper/dm` dispositivi.

   ```
   # multipath -ll
   ```

   Il risultato di questo comando mostra due dispositivi, `dm-19` e. `dm-16`:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n19 259:19  active ready running
| `- #:#:#:# nvme1n19 259:115 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n19 259:51  active ready running
  `- #:#:#:# nvme3n19 259:83  active ready running
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n16 259:16  active ready running
| `- #:#:#:# nvme1n16 259:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n16 259:48  active ready running
  `- #:#:#:# nvme3n16 259:80  active ready running
```

2. Creare un file system sulla partizione per ciascuno di essi `/dev/mapper/eui-` dispositivo.

   Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Creazione di file system (RHEL 8, RHEL 9 e SLES 15)

Per RHEL 8, RHEL 9 e SLES 15, si crea un file system sul dispositivo nvme nativo e si monta il file system.

Fasi

1. Eseguire `multipath -ll` per ottenere un elenco di dispositivi nvme.

```
# multipath -ll
```

Il risultato di questo comando può essere utilizzato per trovare i dispositivi associati `/dev/disk/by-id/nvme-eui.[uuid#]` posizione. Per l'esempio riportato di seguito, questo potrebbe essere `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
Series,08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=50 status=optimized
| `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=10 status=non-optimized
| `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`-+- policy='n/a' prio=10 status=non-optimized
  `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Creare un file system sulla partizione per il dispositivo nvme desiderato utilizzando la posizione `/dev/disk/by-id/nvme-eui.[id#]`.

Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verificare l'accesso allo storage sull'host

Prima di utilizzare lo spazio dei nomi, verificare che l'host possa scrivere i dati nello spazio dei nomi e leggerli.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Namespace inizializzato formattato con un file system.

Fasi

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

Al termine

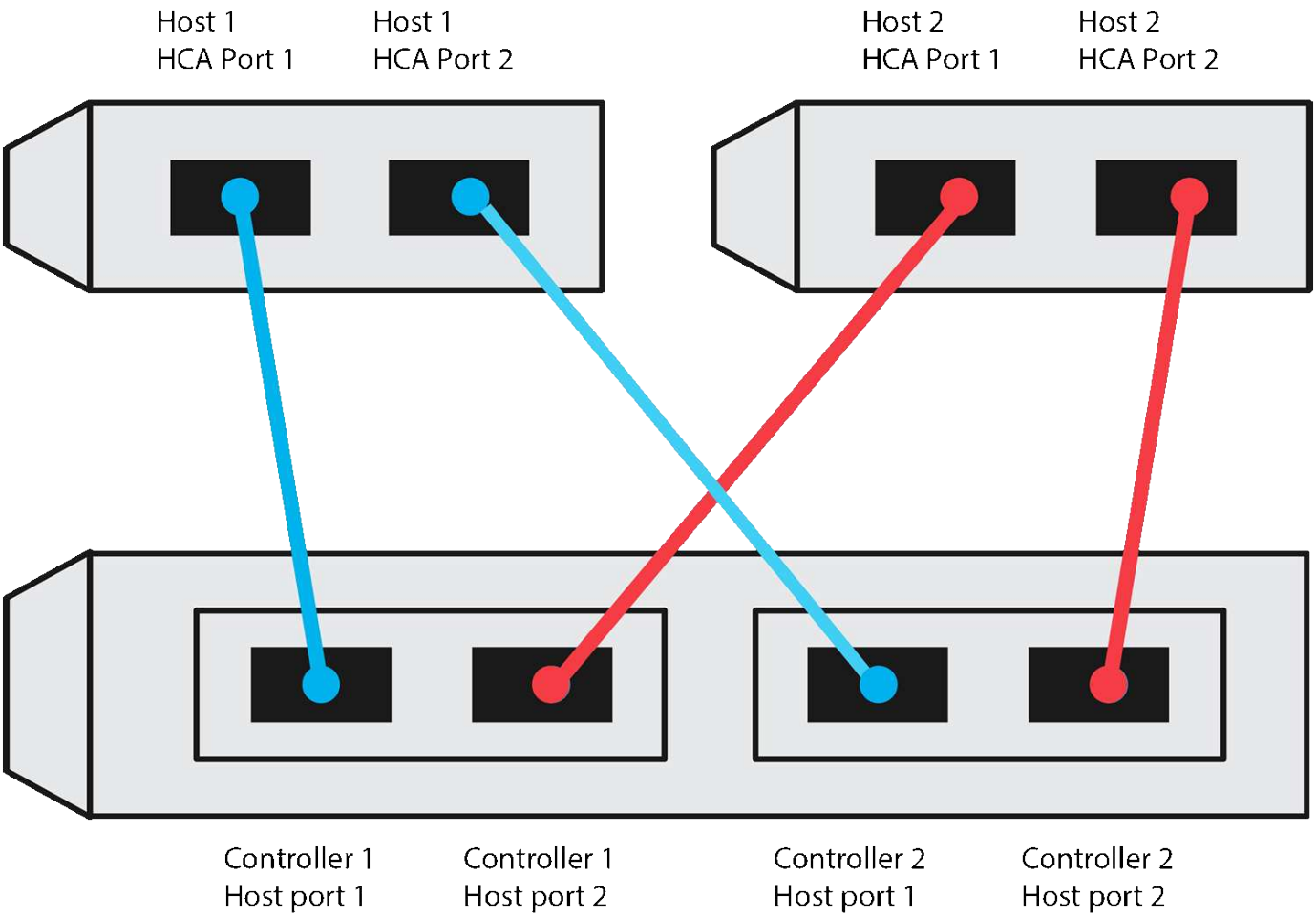
Rimuovere il file e la cartella copiati.

Registrare la configurazione NVMe over RoCE

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

Topologia a connessione diretta

In una topologia a connessione diretta, uno o più host sono collegati direttamente al sottosistema. Nella versione SANtricity OS 11.50, supportiamo una singola connessione da ciascun host a un controller del sottosistema, come mostrato di seguito. In questa configurazione, una porta HCA (host Channel Adapter) di ciascun host deve trovarsi sulla stessa subnet della porta del controller e-Series a cui è collegato, ma su una subnet diversa dall'altra porta HCA.

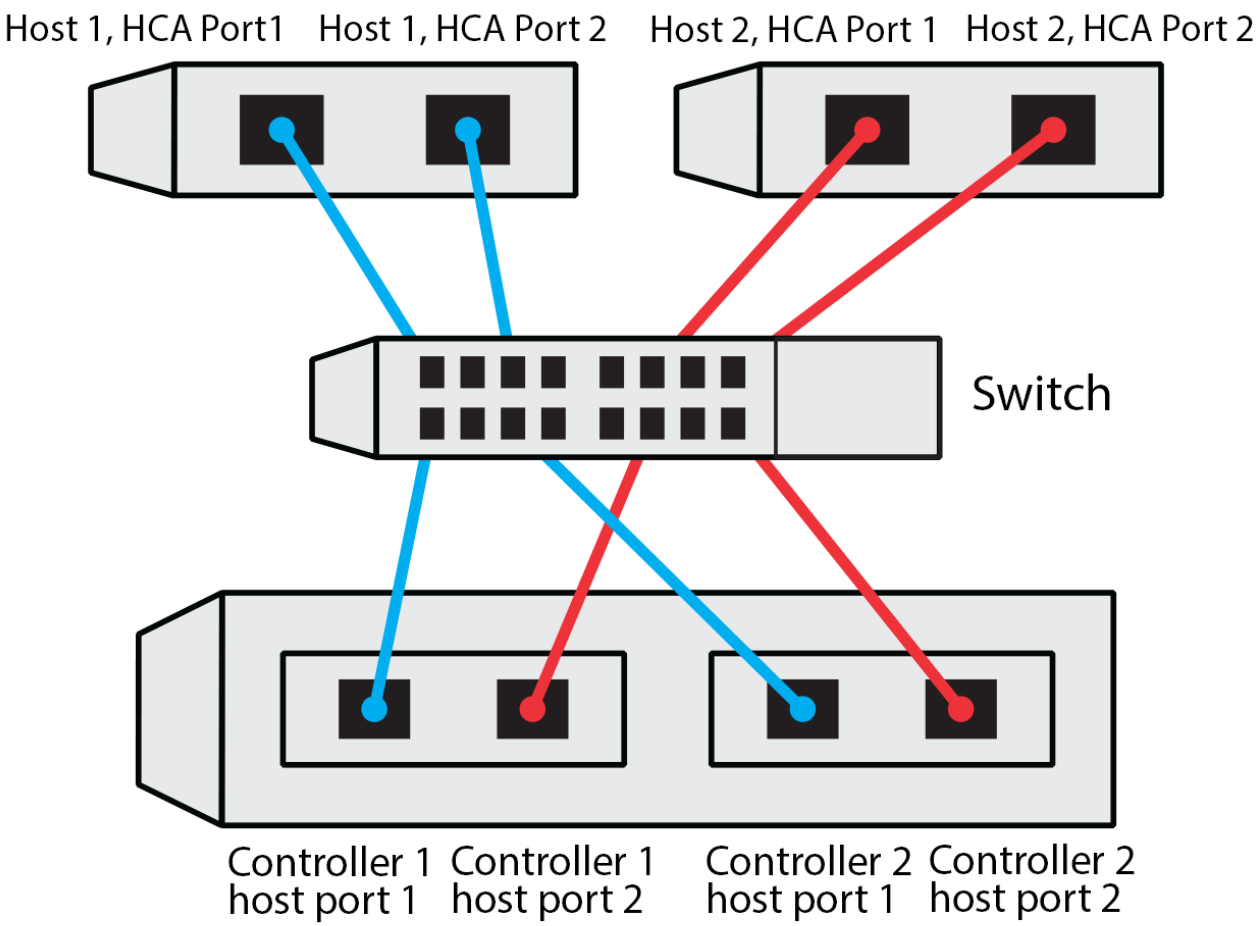


Una configurazione di esempio che soddisfa i requisiti è costituita da quattro subnet di rete come segue:

- Subnet 1: Host 1 porta HCA 1 e Controller 1 porta host 1
- Subnet 2: Host 1 porta HCA 2 e Controller 2 porta host 1
- Subnet 3: Host 2 porta HCA 1 e Controller 1 porta host 2
- Subnet 4: Host 2 HCA Port 2 e Controller 2 host Port 2

Topologia di connessione dello switch

In una topologia fabric, vengono utilizzati uno o più switch. Fare riferimento a. "Tool di matrice di interoperabilità NetApp" per un elenco degli switch supportati.



Identificatori host

Individuare e documentare l'NQN iniziatore da ciascun host.

Connessioni alla porta host	NQN iniziatore software
Host (iniziatore) 1	
Host (iniziatore) 2	

NQN di destinazione

Documentare l'NQN di destinazione per lo storage array.

Nome array	NQN di destinazione
Controller di array (destinazione)	

NQN di destinazione

Documentare gli NQN che devono essere utilizzati dalle porte dell'array.

Connessioni delle porte (di destinazione) degli array controller	NQN
Controller A, porta 1	
Controller B, porta 1	
Controller A, porta 2	
Controller B, porta 2	

Nome host di mapping

Il nome host del mapping viene creato durante il flusso di lavoro.

Nome host di mapping
Tipo di sistema operativo host

Configurazione NVMe su Fibre Channel

Verificare il supporto di Linux ed esaminare le restrizioni

Come prima fase, è necessario verificare che la configurazione Linux sia supportata ed esaminare anche le restrizioni relative a controller, host e ripristino.

Verificare che la configurazione Linux sia supportata

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

Fasi

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

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

5. Selezionare i criteri desiderati per la configurazione, quindi visualizzare gli elementi di configurazione compatibili applicabili.

6. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo prescritti nello strumento.

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

Esaminare le restrizioni per NVMe su FC

Prima di utilizzare NVMe su Fibre Channel, consultare "Tool di matrice di interoperabilità NetApp" per esaminare le restrizioni più recenti relative a controller, host e recovery.

Limitazioni di storage e disaster recovery

- Il mirroring asincrono e sincrono non è supportato.
- Il thin provisioning (creazione di thin volumi) non è supportato.

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

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

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

- Nessuna notifica configurata.

Fasi

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

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

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

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

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

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

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

Configurare gli switch FC

La configurazione (zoning) degli switch Fibre Channel (FC) consente agli host di connettersi allo storage array e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Credenziali di amministratore per gli switch.
- Il numero WWPN di ciascuna porta di iniziatore host e di ciascuna porta di destinazione del controller collegata allo switch. (Utilizzare l'utility HBA per il rilevamento).

A proposito di questa attività

Per ulteriori informazioni sulla suddivisione in zone degli switch, consultare la documentazione del vendor dello switch.

Ciascuna porta dell'iniziatore deve trovarsi in una zona separata con tutte le porte di destinazione corrispondenti.

Fasi

1. Accedere al programma di amministrazione dello switch FC, quindi selezionare l'opzione di configurazione dello zoning.
2. Creare una nuova zona che includa la prima porta iniziatore host e che includa anche tutte le porte di destinazione che si connettono allo stesso switch FC dell'iniziatore.
3. Creare zone aggiuntive per ciascuna porta iniziatore host FC nello switch.
4. Salvare le zone, quindi attivare la nuova configurazione di zoning.

Impostare NVMe su Fibre Channel sul lato host

La configurazione di NVMe Initiator in un ambiente Fibre Channel include l'installazione e la configurazione del pacchetto nvme-cli e l'abilitazione di NVMe/FC Initiator sull'host.

A proposito di questa attività

La procedura seguente riguarda RHEL 7, RHEL 8, RHEL 9, SLES 12 e SLES 15 utilizzando HBA FC Broadcom Emulex o QLogic compatibili con NVMe/FC. Per ulteriori informazioni sulle versioni supportate di questi sistemi operativi o HBA, consultare "Tool di matrice di interoperabilità NetApp".

Fasi

1. Installare `nvme-cli` pacchetto:

   SLES 12 o SLES 15

   ```
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8 O RHEL 9

   ```
   # yum install nvme-cli
   ```

   a. Solo per RHEL 7, scaricare e installare uno script Broadcom AutoConnect esterno per le connessioni NVMe/FC tramite "Sito Web Broadcom". Immettere la parola chiave **Autoconnect script file for Inbox NVMe over FC Drivers** e scegliere la versione più recente specifica per il sistema operativo in uso.

   b. Per Qlogic, modificare `/lib/systemd/system/nvmefc-boot-connections.service` Dopo aver installato lo script di connessione automatica Broadcom NVMe/FC in modo che contenga quanto segue:

```
[Unit]
Description=Auto-connect to subsystems on FC-NVME devices found
during boot

[Service]
Type=oneshot
ExecStart=/bin/sh -c "echo add >
/sys/class/fc/fc_udev_device/nvme_discovery"

[Install]
WantedBy=default.target
```

2. Attivare e avviare `nvmefc-boot-connections` servizio.

```
systemctl enable nvmefc-boot-connections.service
```

```
systemctl start nvmefc-boot-connections.service
```

Configurazione lato host per HBA Emulex:

La procedura seguente riguarda solo gli HBA Emulex.

1. Impostare `lpfc_enable_fc4_type` a. `3` Per attivare SLES12 SP4 come iniziatore NVMe/FC.

```
# cat /etc/modprobe.d/lpfc.conf
options lpfc lpfc_enable_fc4_type=3
```

2. Ricostruire il `initrd` Per ottenere la modifica Emulex e la modifica del parametro di boot.

```
# dracut --force
```

3. Riavviare l'host per caricare le modifiche in `Ipfc` driver.

```
# reboot
```

L'host viene riavviato e l'iniziatore NVMe/FC viene attivato sull'host.

Una volta completata la configurazione lato host, la connessione NVMe tramite le porte Fibre Channel avviene automaticamente.

Definire un host

Utilizzando Gestore di sistema di SANtricity, è possibile definire gli host che inviano i dati allo storage array. La definizione 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 definisce 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.

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare una delle seguenti opzioni dall'elenco a discesa: • **Linux** per SANtricity 11.60 e versioni successive • **Linux DM-MP (kernel 3.10 o successivo)** per pre-SANtricity 11.60
Tipo di interfaccia host	Selezionare il tipo di interfaccia host che si desidera utilizzare. Se l'array configurato dispone di un solo tipo di interfaccia host, questa impostazione potrebbe non essere disponibile per la selezione.

Impostazione	Descrizione
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare interfaccia i/o** Se le porte host hanno effettuato l'accesso, è possibile selezionare gli identificatori delle porte host dall'elenco. Questo è il metodo consigliato. • **Aggiunta manuale** Se le porte host non hanno effettuato l'accesso, controllare /etc/nvme/hostnqn sull'host per trovare gli identificatori hostnqn e associarli alla definizione dell'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dal file /etc/nvme/hostnqn (uno alla volta) nel campo **host ports** (Porte host). È necessario aggiungere 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.

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

Risultato

Una volta creato correttamente l'host, Gestore di sistema di SANtricity crea un nome predefinito per ogni porta host configurata per l'host.

L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per `host IPT is IPT_1`.

Assegnare un volume

È necessario assegnare un volume (spazio dei nomi) 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 spazi dei nomi in un array di storage.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

- 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 ID dello spazio dei nomi (NSID) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un NSID univoco.

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.
- Sono state definite tutte le assegnazioni dei volumi.

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.

Risultato

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 NSID disponibile. L'host utilizza l'NSID per accedere al volume.
- Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host.

Visualizzare i volumi visibili all'host

È possibile utilizzare lo strumento SMdevices per visualizzare i volumi attualmente visibili sull'host. Questo tool fa parte del pacchetto nvme-cli e può essere utilizzato in alternativa a `nvme list` comando.

Per visualizzare informazioni su ciascun percorso NVMe a un volume e-Series, utilizzare `nvme netapp smdevices [-o <format>]` comando.

L'output `<format>` può essere normale (il valore predefinito se -o non viene utilizzato), column o json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Impostare il failover sull'host

Per fornire un percorso ridondante all'array di storage, è possibile configurare l'host per eseguire il failover.

Prima di iniziare

È necessario installare i pacchetti richiesti sul sistema.

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

A proposito di questa attività

RHEL 7 e SLES 12 utilizzano il multipath DMMP (Device Mapper Multipath) per il multipathing quando si utilizza NVMe su Fibre Channel. RHEL 8, RHEL 9 e SLES 15 utilizzano un failover NVMe nativo integrato. A seconda del sistema operativo in esecuzione, è necessaria una configurazione aggiuntiva di multipath per il corretto funzionamento.

Attiva DMMP (Device Mapper Multipath) per RHEL 7 o SLES 12

Per impostazione predefinita, DM-MP è disattivato in RHEL e SLES. Per abilitare i componenti DM-MP sull'host, attenersi alla seguente procedura.

Fasi

1. Aggiungere la voce NVMe e-Series Device alla sezione devices del file /etc/multipath.conf, come mostrato nell'esempio seguente:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configurare `multipathd` per iniziare all'avvio del sistema.

```
# systemctl enable multipathd
```

3. Inizio `multipathd` se non è in esecuzione.

```
# systemctl start multipathd
```

4. Verificare lo stato di `multipathd` per assicurarsi che sia attivo e in esecuzione:

```
# systemctl status multipathd
```

Impostare NVMe Multipathing nativo per RHEL 8

A proposito di questa attività

NVMe Multipathing nativo è disattivato per impostazione predefinita in RHEL 8 e deve essere attivato seguendo la procedura riportata di seguito.

Fasi

1. Setup (Configurazione) `modprobe` Regola per attivare NVMe Multipathing nativo.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` con il nuovo parametro modprobe.

```
# dracut -f
```

3. Riavviare il server per attivarlo con NVMe Multipathing nativo attivato

```
# reboot
```

4. Verificare che il multipathing NVMe nativo sia stato attivato dopo l'avvio del backup dell'host.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. Se l'output del comando è `N`, Quindi NVMe Multipathing nativo è ancora disattivato.
   b. Se l'output del comando è `Y`, Quindi viene attivato NVMe Multipathing nativo e tutti i dispositivi NVMe rilevati lo utilizzeranno.

> Per RHEL 9 e SLES 15, il multipathing NVMe nativo è attivato per impostazione predefinita e non è richiesta alcuna configurazione aggiuntiva.

Accedere ai volumi NVMe per le destinazioni dei dispositivi virtuali

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 7 e SLES 12, l'i/o viene indirizzato alle destinazioni dei dispositivi virtuali dall'host Linux. DM-MP gestisce i percorsi fisici sottostanti queste destinazioni virtuali.

I dispositivi virtuali sono destinazioni di i/O.

Assicurarsi di eseguire l'i/o solo sui dispositivi virtuali creati da DM-MP e non sui percorsi fisici dei dispositivi. Se si esegue l'i/o sui percorsi fisici, DM-MP non può gestire un evento di failover e l'i/o non riesce.

È possibile accedere a questi dispositivi a blocchi tramite `dm` o a. `symlink` poll `/dev/mapper`; ad esempio:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Esempio

Il seguente esempio di output da `nvme list` Il comando mostra il nome del nodo host e la sua correlazione con l'ID dello spazio dei nomi.

```
NODE         SN            MODEL           NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Colonna	Descrizione
`Node`	Il nome del nodo comprende due parti: • La notazione `nvme1` Rappresenta il controller A e. `nvme2` Rappresenta il controller B. • La notazione `n1`, `n2`, e così via rappresentano l'identificatore dello spazio dei nomi dal punto di vista dell'host. Questi identificatori vengono ripetuti nella tabella, una volta per il controller A e una volta per il controller B.
`Namespace`	La colonna namespace elenca l'ID dello spazio dei nomi (NSID), che è l'identificatore dal punto di vista dello storage array.

Di seguito `multipath -ll` output, i percorsi ottimizzati vengono visualizzati con una `prio` valore di 50, mentre i percorsi non ottimizzati vengono visualizzati con un `prio` valore di 10.

Il sistema operativo Linux indirizza i/o al gruppo di percorsi indicato come `status=active`, mentre i gruppi di percorsi sono elencati come `status=enabled` sono disponibili per il failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Voce	Descrizione
`policy='service-time 0' prio=50 status=active`	Questa riga e la riga seguente lo mostrano `nvme1n1`, Che è lo spazio dei nomi con un NSID di 10, è ottimizzato sul percorso con un `prio` valore di 50 e a. `status` valore di `active`. Questo namespace è di proprietà del controller A.
`policy='service-time 0' prio=10 status=enabled`	Questa riga mostra il percorso di failover per lo spazio dei nomi 10, con un `prio` valore di 10 e a. `status` valore di `enabled`. Al momento l'i/o non viene indirizzato allo spazio dei nomi di questo percorso. Questo namespace è di proprietà del controller B.
`policy='service-time 0' prio=0 status=enabled`	Questo esempio mostra `multipath -ll`Output da un punto diverso nel tempo, mentre il controller A viene riavviato. Il percorso verso lo spazio dei nomi 10 viene mostrato come con un `prio` valore di 0 e a. `status` valore di `enabled`.
`policy='service-time 0' prio=10 status=active`	Tenere presente che il `active` percorso a cui si riferisce `nvme2`, Quindi l'i/o viene indirizzato su questo percorso al controller B.

Accedere ai volumi NVMe per le destinazioni fisiche dei dispositivi NVMe

È possibile configurare l'i/o diretto alla destinazione del dispositivo in base al sistema operativo in uso (e al metodo multipathing interno).

Per RHEL 8, RHEL 9 e SLES 15, l'i/o viene indirizzato alle destinazioni fisiche del dispositivo NVMe dall'host Linux. Una soluzione NVMe multipathing nativa gestisce i percorsi fisici sottostanti il singolo dispositivo fisico

apparente visualizzato dall'host.

I dispositivi NVMe fisici sono destinazioni di i/O.

È consigliabile eseguire i/o ai collegamenti in `/dev/disk/by-id/nvme-eui.[uuid#]` piuttosto che direttamente al percorso fisico del dispositivo nvme `/dev/nvme[subsys#]n[id#]`. Il collegamento tra queste due posizioni può essere trovato usando il seguente comando:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/o eseguito a. `/dev/disk/by-id/nvme-eui.[uuid#]` verrà passata direttamente `/dev/nvme[subsys#]n[id#]` Che ha tutti i percorsi virtualizzati sotto l'IT utilizzando la soluzione di multipathing NVMe nativa.

Puoi visualizzare i tuoi percorsi eseguendo:

```
# nvme list-subsys
```

Output di esempio:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

Se si specifica un dispositivo namespace quando si utilizza `nvme list-subsys` fornisce informazioni aggiuntive sui percorsi per lo spazio dei nomi:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

Sono inoltre presenti collegamenti ai comandi multipath per consentire di visualizzare le informazioni sul percorso per il failover nativo attraverso di essi:

```
#multipath -ll
```

Per visualizzare le informazioni sul percorso, è necessario impostare le seguenti opzioni in `/etc/multipath.conf`:

```
defaults {
        enable_foreign nvme
}
```

Output di esempio:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Creazione di filesystem (RHEL 7 e SLES 12)

Per RHEL 7 e SLES 12, si crea un file system sul dispositivo dm desiderato e si monta il filesystem.

Fasi

1. Eseguire `multipath -ll` per ottenere un elenco di `/dev/mapper/dm` dispositivi.

   ```
   # multipath -ll
   ```

   Il risultato di questo comando mostra due dispositivi, `dm-19` e. `dm-16`:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n19 259:19  active ready running
| `- #:#:#:# nvme1n19 259:115 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n19 259:51  active ready running
  `- #:#:#:# nvme3n19 259:83  active ready running
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n16 259:16  active ready running
| `- #:#:#:# nvme1n16 259:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n16 259:48  active ready running
  `- #:#:#:# nvme3n16 259:80  active ready running
```

2. Creare un file system sulla partizione per ciascuno di essi `/dev/mapper/eui-` dispositivo.

   Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Creazione di file system (RHEL 8, RHEL 9, SLES 15)

Per RHEL 8, RHEL 9 e SLES 15, si crea un file system sul dispositivo nvme nativo e si monta il file system.

Fasi

1. Eseguire il comando multipath -ll per ottenere un elenco di dispositivi nvme.

   ```
   # multipath -ll
   ```

   Il risultato di questo comando può essere utilizzato per trovare i dispositivi associati `/dev/disk/by-id/nvme-eui.[uuid#]` posizione. Per l'esempio riportato di seguito, questo potrebbe essere `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

   ```
   eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
   Series,08520000
   size=4194304 features='n/a' hwhandler='ANA' wp=rw
   |-+- policy='n/a' prio=50 status=optimized
   | `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
   |-+- policy='n/a' prio=50 status=optimized
   | `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
   |-+- policy='n/a' prio=10 status=non-optimized
   | `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
   `-+- policy='n/a' prio=10 status=non-optimized
     `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
   ```

2. Creare un file system sulla partizione per il dispositivo nvme desiderato utilizzando la posizione `/dev/disk/by-id/nvme-eui.[id#]`.

   Il metodo per creare un file system varia a seconda del file system scelto. Questo esempio mostra la creazione di un file system ext4.

   ```
   # mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
   mke2fs 1.42.11 (22-Oct-2019)
   Creating filesystem with 2620928 4k blocks and 655360 inodes
   Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
   Superblock backups stored on blocks:
           32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

   Allocating group tables: done
   Writing inode tables: done
   Creating journal (32768 blocks): done
   Writing superblocks and filesystem accounting information: done
   ```

3. Creare una cartella per montare il nuovo dispositivo.

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

4. Montare il dispositivo.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verificare l'accesso allo storage sull'host

Prima di utilizzare lo spazio dei nomi, verificare che l'host possa scrivere i dati nello spazio dei nomi e leggerli.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Namespace inizializzato formattato con un file system.

Fasi

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

Al termine

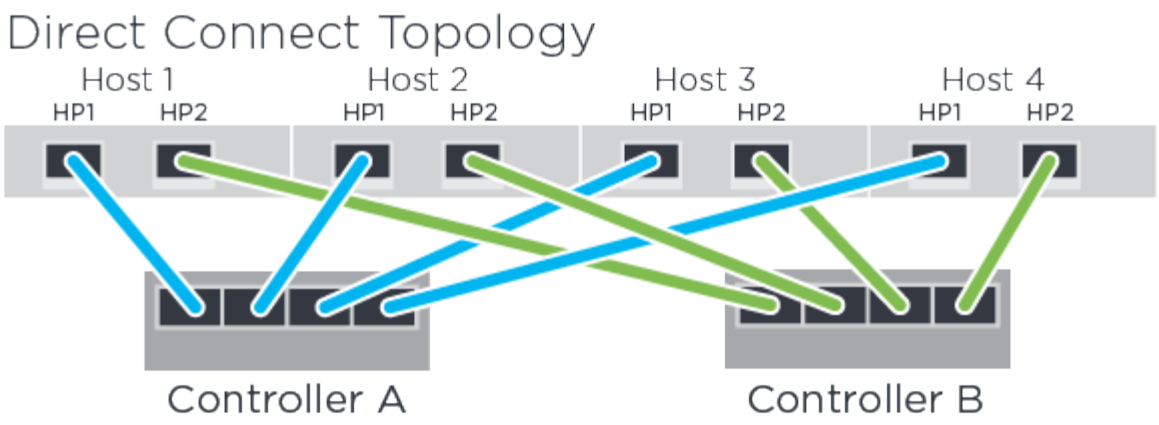
Rimuovere il file e la cartella copiati.

Registrare la configurazione NVMe over FC

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

Topologia a connessione diretta

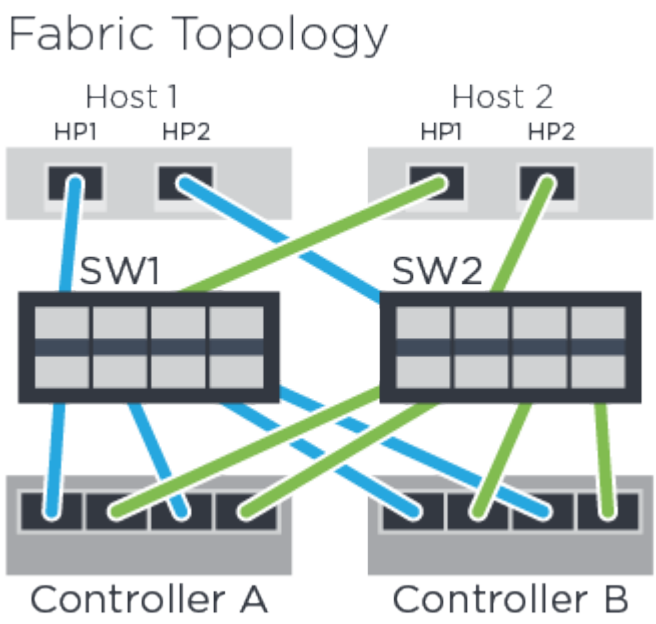
In una topologia a connessione diretta, uno o più host sono collegati direttamente al controller.



- Host 1 HBA Port 1 e Controller A host Port 1
- Host 1 HBA Port 2 e Controller B host Port 1
- Host 2 HBA Port 1 e Controller A host Port 2
- Host 2 HBA Port 2 e Controller B host Port 2
- Host 3 HBA Port 1 e Controller A host Port 3
- Host 3 HBA Port 2 e Controller B host Port 3
- Host 4 HBA Port 1 e Controller A host Port 4
- Host 4 HBA Port 2 e Controller B host Port 4

Topologia di connessione dello switch

In una topologia fabric, vengono utilizzati uno o più switch. Vedere "Tool di matrice di interoperabilità NetApp" per un elenco degli switch supportati.



Identificatori host

Individuare e documentare l'NQN iniziatore da ciascun host.

Connessioni alla porta host	NQN host
Host (iniziatore) 1	
Host (iniziatore) 2	

NQN di destinazione

Documentare l'NQN di destinazione per lo storage array.

Nome array	NQN di destinazione
Controller di array (destinazione)	

NQN di destinazione

Documentare gli NQN che devono essere utilizzati dalle porte dell'array.

Connessioni delle porte (di destinazione) degli array controller	NQN
Controller A, porta 1	
Controller B, porta 1	
Controller A, porta 2	
Controller B, porta 2	

Nome host di mapping

Il nome host del mapping viene creato durante il flusso di lavoro.

Nome host di mapping
Tipo di sistema operativo host

Configurazione di VMware Express

Panoramica della configurazione di VMware Express

Il metodo VMware Express per l'installazione dello storage array e l'accesso a Gestore di

sistema SANtricity è appropriato per la configurazione di un host VMware standalone su un sistema storage e-Series. È progettato per rendere operativo il sistema storage il più rapidamente possibile, con un numero minimo di punti decisionali.

Panoramica della procedura

Il metodo espresso include i seguenti passaggi, descritti anche nella "Workflow VMware".

1. Configurare uno dei seguenti ambienti di comunicazione:
   - "NVMe su Fibre Channel"
   - "Fibre Channel"
   - "ISCSI"
   - "SAS"
2. Creare volumi logici sull'array di storage.
3. Rendere i volumi disponibili per l'host dati.

Trova ulteriori informazioni

- Guida in linea — descrive come utilizzare Gestione di sistema di SANtricity per completare le attività di configurazione e gestione dello storage. È disponibile all'interno del prodotto.
- "Knowledge base di NetApp" (Un database di articoli) — fornisce informazioni sulla risoluzione dei problemi, FAQ e istruzioni per un'ampia gamma di prodotti e tecnologie NetApp.
- "Tool di matrice di interoperabilità NetApp" — consente di cercare configurazioni di prodotti e componenti NetApp che soddisfino gli standard e i requisiti specificati da NetApp.
- "Guida alla configurazione VMware per l'integrazione iSCSI di e-Series SANtricity con ESXi 6.X." — fornisce dettagli tecnici sull'integrazione iSCSI con VMware.
- "Massimi di configurazione VMware" — descrive come configurare lo storage fisico e virtuale in modo che rimanga entro i limiti massimi consentiti supportati da ESX/ESXi.
- "Requisiti e limitazioni dello storage VMware NVMe".
- "Documentazione VMware vSphere" — fornisce la documentazione di ESXi vCenter Server.

Presupposti

Il metodo VMware Express si basa sui seguenti presupposti:

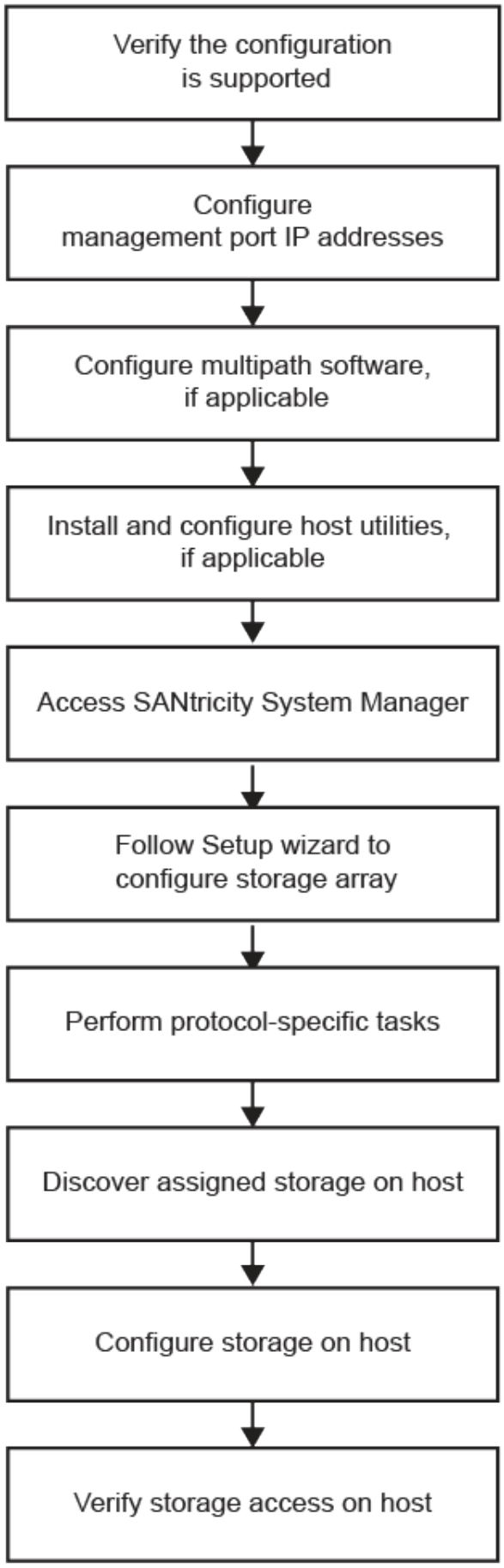
Componente	Presupposti
Hardware	• Per installare l'hardware, sono state utilizzate le istruzioni di installazione e configurazione fornite con gli shelf dei controller. • Sono stati collegati i cavi tra gli shelf di dischi opzionali e i controller. • Il sistema storage è alimentato. • Hai installato tutto l'altro hardware (ad esempio, stazione di gestione, switch) e hai effettuato le connessioni necessarie.
Host	• È stata stabilita una connessione tra il sistema storage e l'host dati. • Il sistema operativo host è stato installato. • Non stai utilizzando VMware come guest virtualizzato. • Non si sta configurando l'host dati (i/o collegato) per l'avvio da SAN.
Stazione di gestione dello storage	• Si utilizza una rete di gestione a 1 Gbps o più veloce. • Si sta utilizzando una stazione separata per la gestione piuttosto che l'host dei dati (i/o collegato). • Si sta utilizzando 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. • La stazione di gestione è stata collegata alla stessa subnet delle porte di gestione dello storage.
Indirizzamento IP	• È stato installato e configurato un server DHCP. • È stata ancora stabilita una connessione Ethernet tra la stazione di gestione e il sistema di storage.
Provisioning dello storage	• Non verranno utilizzati volumi condivisi. • Verranno creati pool anziché gruppi di volumi.

Componente	Presupposti
Protocollo: FC	• Sono state effettuate tutte le connessioni FC sul lato host e lo zoning dello switch attivato. • Stai utilizzando HBA e switch FC supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA FC elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: NVMe su Fibre Channel	• Sono state effettuate tutte le connessioni FC sul lato host e lo zoning dello switch attivato. • Stai utilizzando HBA e switch FC supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA FC elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: ISCSI	• Si utilizzano switch Ethernet in grado di trasportare il traffico iSCSI. • Gli switch Ethernet sono stati configurati in base alle raccomandazioni del vendor per iSCSI.
Protocollo: SAS	• Stai utilizzando HBA SAS supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA SAS elencate nella "Tool di matrice di interoperabilità NetApp".

Se questi presupposti non sono corretti per l'installazione o se si desidera ottenere informazioni di base più concettuali, consultare il seguente report tecnico: "Guida alla configurazione VMware per l'integrazione iSCSI di e-Series SANtricity con ESXi 6.X."

Comprendere il workflow VMware

Questo flusso di lavoro guida l'utente attraverso il "metodo rapido" per la configurazione dello storage array e del gestore di sistema SANtricity in modo da rendere lo storage disponibile per un host VMware.


Verify the configuration is supported
Configure management port IP addresses
Configure multipath software, if applicable
Install and configure host utilities, if applicable
Access SANtricity System Manager
Follow Setup wizard to configure storage array
Perform protocol-specific tasks
Discover assigned storage on host
Configure storage on host
Verify storage access on host

Verificare che la configurazione VMware sia supportata

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

Fasi

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

   Viene visualizzata la sezione Criteri di ricerca più precisi. In questa sezione è possibile selezionare il protocollo applicabile e altri criteri per la configurazione, ad esempio sistema operativo, sistema operativo NetApp e driver host multipath. Selezionare i criteri desiderati per la configurazione, quindi visualizzare gli elementi di configurazione compatibili applicabili. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo prescritti nello strumento. Per informazioni dettagliate sulla configurazione scelta, fare clic sulla freccia a destra della pagina Visualizza configurazioni supportate.

5. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo come indicato nella tabella.

Aggiornamenti del sistema operativo	Protocollo	Aggiornamenti relativi al protocollo
• Potrebbe essere necessario installare driver pronti all'uso per garantire funzionalità e supportabilità adeguate. È possibile installare i driver HBA utilizzando la shell ESXi o una connessione SSH remota all'host ESXi. Per accedere all'host utilizzando uno di questi metodi, è necessario abilitare la shell ESXi e l'accesso SSH. Per ulteriori informazioni sulla shell ESXi, fare riferimento alla Knowledge base VMware relativa all'utilizzo della shell ESXi in ESXi. Per i comandi di installazione, fare riferimento alle istruzioni fornite con i driver HBA. • Ogni vendor HBA dispone di metodi specifici per aggiornare il codice di avvio e il firmware. Alcuni di questi metodi potrebbero includere l'utilizzo di un plugin vCenter o l'installazione del provider CIM sull'host ESXi. I plug-in vCenter possono essere utilizzati per ottenere informazioni sull'HBA specifico del vendor. Fare riferimento alla sezione di supporto del sito Web del vendor per ottenere le istruzioni e il software necessari per aggiornare il firmware o il codice di avvio HBA. Fare riferimento alla *VMware Compatibility Guide* o al sito Web del vendor HBA per ottenere il firmware o il codice di avvio corretto.	FC	Driver, firmware e codice di avvio dell'HBA (host bus adapter)
ISCSI	Driver, firmware e codice di avvio della scheda di interfaccia di rete (NIC)	SAS

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

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

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

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

Configurare il software multipath

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

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

che aggiorna il dispositivo virtuale. Per VMware, NVMe/FC utilizza il plug-in ad alte prestazioni (HPP).

Applicabile solo per i protocolli FC, iSCSI e SAS, VMware fornisce plug-in, noti come Storage Array Type Plug-in (SATP), per gestire le implementazioni di failover di array di storage` di vendor specifici.

L'SATP da utilizzare è **VMW_SATP_ALUA**.

Per ulteriori informazioni, vedere "VMware SATP".

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

A proposito di questa attività

Se si utilizza iSCSI, assicurarsi di aver chiuso l'installazione guidata durante la configurazione di iSCSI.

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

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

Se l'installazione guidata non viene visualizzata automaticamente, contattare il supporto tecnico.

Fasi

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

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

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

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

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

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

> Per EF300 e EF600, è necessario impostare la dimensione del blocco su 512 byte per garantire la compatibilità con VMware. Per ulteriori informazioni sull'impostazione di un volume a 512 byte, consultare la guida in linea di Gestione di sistema di SANtricity.

Eseguire attività specifiche di FC

Per il protocollo Fibre Channel, configurare gli switch e determinare gli identificatori delle porte host.

> Per EF300 e EF600, è necessario impostare la dimensione del blocco su 512 byte per garantire la compatibilità con VMware. Per ulteriori informazioni sull'impostazione di un volume a 512 byte, consultare la guida in linea di Gestione di sistema di SANtricity.

Fase 1: Configurazione degli switch FC - VMware

La configurazione (zoning) degli switch Fibre Channel (FC) consente agli host di connettersi allo storage array e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Credenziali di amministratore per gli switch.
- Il numero WWPN di ciascuna porta di iniziatore host e di ciascuna porta di destinazione del controller collegata allo switch. (Utilizzare l'utility HBA per il rilevamento).

> È possibile utilizzare l'utility HBA di un vendor per aggiornare e ottenere informazioni specifiche sull'HBA. Per istruzioni su come ottenere l'utility HBA, consultare la sezione dedicata al supporto del sito Web del vendor.

A proposito di questa attività

Ciascuna porta dell'iniziatore deve trovarsi in una zona separata con tutte le porte di destinazione corrispondenti. Per ulteriori informazioni sulla suddivisione in zone degli switch, consultare la documentazione del vendor dello switch.

Fasi

1. Accedere al programma di amministrazione dello switch FC, quindi selezionare l'opzione di configurazione dello zoning.
2. Creare una nuova zona che includa la prima porta iniziatore host e che includa anche tutte le porte di destinazione che si connettono allo stesso switch FC dell'iniziatore.
3. Creare zone aggiuntive per ciascuna porta iniziatore host FC nello switch.
4. Salvare le zone, quindi attivare la nuova configurazione di zoning.

Fase 2: Determinare le WWPN della porta host—FC

Per configurare lo zoning FC, è necessario determinare il nome della porta globale (WWPN) di ciascuna porta initiator.

Fasi

1. Connettersi all'host ESXi utilizzando SSH o la shell ESXi.
2. Eseguire il seguente comando:

```
esxcfg-scsidevs -a
```

3. Registrare gli identificatori dell'iniziatore. L'output sarà simile a questo esempio:

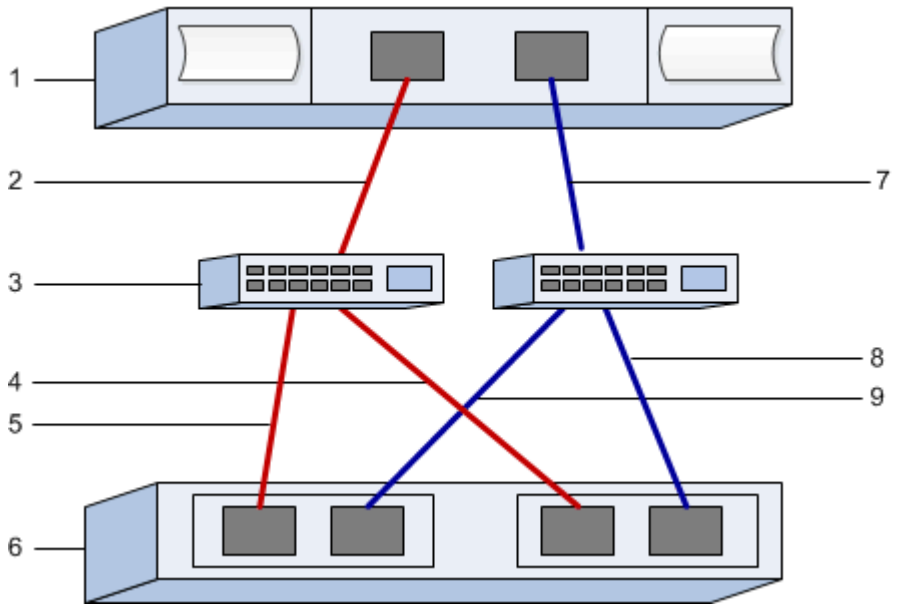
```
vmhba3 lpfc link-up  fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vmhba4 lpfc link-up  fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Fase 3: Registrare la configurazione

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

La figura mostra un host collegato a un array di storage e-Series in due zone. Una zona è indicata dalla linea

blu, mentre l'altra è indicata dalla linea rossa. Ogni zona contiene una porta iniziatore e tutte le porte di destinazione.



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	PN. WWN
1	Host	*non applicabile*
2	Porta host 0 a switch FC zona 0	
7	Dalla porta host 1 allo switch FC zona 1	

Identificatori di destinazione

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
3	Switch	*non applicabile*
6	Controller di array (destinazione)	*non applicabile*
5	Dal controller A, dalla porta 1 allo switch FC 1	
9	Dal controller A, dalla porta 2 allo switch FC 2	

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
4	Dal controller B, porta 1 allo switch FC 1	
8	Controller B, dalla porta 2 allo switch FC 2	

Host di mappatura

Nome host di mapping
Tipo di sistema operativo host

Eseguire NVMe su attività specifiche di FC

Per il protocollo NVMe over Fibre Channel, configurare gli switch e determinare gli identificatori delle porte host.

Fase 1: Configurazione degli switch NVMe/FC

La configurazione (zoning) degli switch NVMe over Fibre Channel (FC) consente agli host di connettersi allo storage array e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Credenziali di amministratore per gli switch.
- Il numero WWPN di ciascuna porta di iniziatore host e di ciascuna porta di destinazione del controller collegata allo switch. (Utilizzare l'utility HBA per il rilevamento).

> È possibile utilizzare l'utility HBA di un vendor per aggiornare e ottenere informazioni specifiche sull'HBA. Per istruzioni su come ottenere l'utility HBA, consultare la sezione dedicata al supporto del sito Web del vendor.

A proposito di questa attività

Ciascuna porta dell'iniziatore deve trovarsi in una zona separata con tutte le porte di destinazione corrispondenti. Per ulteriori informazioni sulla suddivisione in zone degli switch, consultare la documentazione del vendor dello switch.

Fasi

1. Accedere al programma di amministrazione dello switch FC, quindi selezionare l'opzione di configurazione dello zoning.
2. Creare una nuova zona che includa la prima porta iniziatore host e che includa anche tutte le porte di destinazione che si connettono allo stesso switch FC dell'iniziatore.

3. Creare zone aggiuntive per ciascuna porta iniziatore host FC nello switch.
4. Salvare le zone, quindi attivare la nuova configurazione di zoning.

Fase 2: Determinare le porte host WWPN—NVMe/FC VMware

Per configurare lo zoning FC, è necessario determinare il nome della porta globale (WWPN) di ciascuna porta initiator.

Fasi

1. Connettersi all'host ESXi utilizzando SSH o la shell ESXi.
2. Eseguire il seguente comando:

```
esxcfg-scsidevs -a
```

3. Registrare gli identificatori dell'iniziatore. L'output sarà simile a questo esempio:

```
vmhba3 lpfc link-up  fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vmhba4 lpfc link-up  fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Fase 3: Abilitare i driver HBA

Il supporto per NVMe deve essere abilitato nei driver Broadcom/Emulex e HBA Marvell/Qlogic.

Fasi

1. Eseguire uno dei seguenti comandi dalla shell ESXi:
   - **Driver HBA Broadcom/Emulex**

     ```
     esxcli system module parameters set -m lpfc -p
     "lpfc_enable_fc4_type=3"
     ```

   - **Driver HBA Marvell/Qlogic**

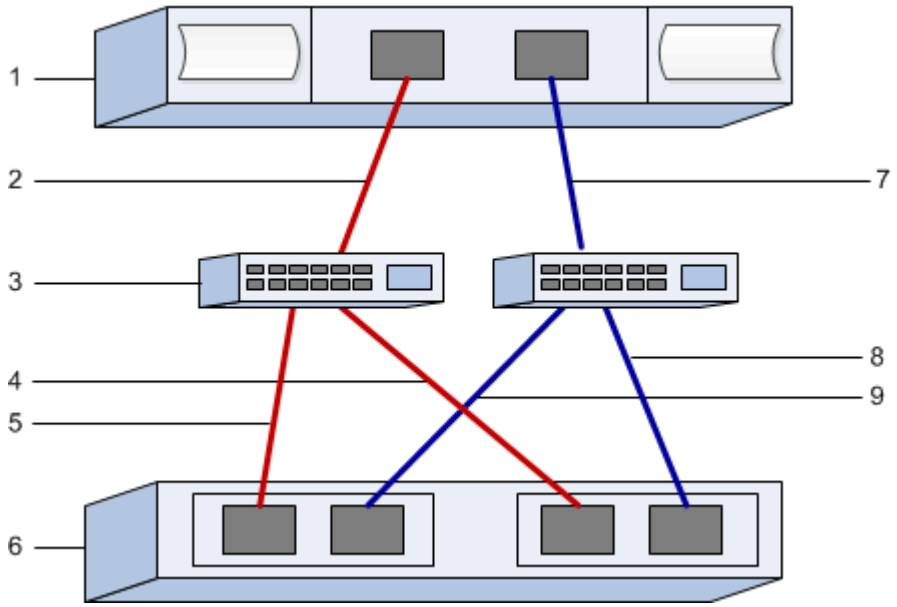
     ```
     esxcfg-module -s "ql2xnvmesupport=1" qlnativefc
     ```

2. Riavviare l'host.

Fase 4: Registrare la configurazione

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

La figura mostra un host collegato a un array di storage e-Series in due zone. Una zona è indicata dalla linea blu, mentre l'altra è indicata dalla linea rossa. Ogni zona contiene una porta iniziatore e tutte le porte di destinazione.



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	PN. WWN
1	Host	*non applicabile*
2	Porta host 0 a switch FC zona 0	
7	Dalla porta host 1 allo switch FC zona 1	

Identificatori di destinazione

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
3	Switch	*non applicabile*
6	Controller di array (destinazione)	*non applicabile*
5	Dal controller A, dalla porta 1 allo switch FC 1	
9	Dal controller A, dalla porta 2 allo switch FC 2	

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
4	Dal controller B, porta 1 allo switch FC 1	
8	Controller B, dalla porta 2 allo switch FC 2	

Host di mappatura

Nome host di mapping
Tipo di sistema operativo host

Eseguire attività specifiche di iSCSI

Per il protocollo iSCSI, configurare gli switch e la rete sul lato array e sul lato host. Quindi, verificare le connessioni di rete IP.

Fase 1: Configurazione degli switch - iSCSI, VMware

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Due reti separate per l'alta disponibilità. Assicurarsi di isolare il traffico iSCSI per separare i segmenti di rete.
- Controllo di flusso hardware di invio e ricezione abilitato **end-to-end**.
- Controllo di flusso prioritario disattivato.
- Se appropriato, abilitare i frame jumbo.

> Port channels/LACP non è supportato sulle porte switch del controller. LACP lato host non è consigliato; il multipathing offre gli stessi vantaggi o meglio.

Fasi

Consultare la documentazione del fornitore dello switch.

Fase 2: Configurazione del networking - iSCSI VMware

È possibile configurare la rete iSCSI in diversi modi, a seconda dei requisiti di storage dei dati. Rivolgersi all'amministratore di rete per suggerimenti sulla scelta della configurazione migliore per l'ambiente in uso.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Controllo di flusso hardware di invio e ricezione abilitato **end-to-end**.
- Controllo di flusso prioritario disattivato.
- Se appropriato, abilitare i frame jumbo.

  Se si utilizzano frame jumbo all'interno della SAN IP per motivi di performance, assicurarsi di configurare l'array, gli switch e gli host in modo che utilizzino frame jumbo. Consultare la documentazione del sistema operativo e dello switch per informazioni su come abilitare i frame jumbo sugli host e sugli switch. Per abilitare i frame jumbo sull'array, completare la procedura descritta nella fase 3.

A proposito di questa attività

Durante la pianificazione della rete iSCSI, tenere presente che "Massimi di configurazione VMware" La guida indica che il numero massimo di percorsi di storage iSCSI supportati è 8. È necessario considerare questo requisito per evitare di configurare troppi percorsi.

Per impostazione predefinita, l'iniziatore software iSCSI VMware crea una singola sessione per target iSCSI quando non si utilizza il binding della porta iSCSI.

> VMware iSCSI port binding è una funzionalità che obbliga tutte le porte VMkernel associate ad accedere a tutte le porte di destinazione accessibili sui segmenti di rete configurati. Deve essere utilizzato con array che presentano un singolo indirizzo di rete per la destinazione iSCSI. NetApp consiglia di non utilizzare il binding della porta iSCSI. Per ulteriori informazioni, consultare "Knowledge base VMware" Per l'articolo relativo alle considerazioni sull'utilizzo del binding della porta iSCSI software in ESX/ESXi. Se l'host ESXi è collegato allo storage di un altro vendor, NetApp consiglia di utilizzare porte vmkernel iSCSI separate per evitare qualsiasi conflitto con il binding delle porte.

Per le Best practice, NON utilizzare l'associazione delle porte sugli array di storage e-Series.

Per garantire una buona configurazione multipathing, utilizzare più segmenti di rete per la rete iSCSI. Posizionare almeno una porta lato host e almeno una porta da ciascun controller di array su un segmento di rete e un gruppo identico di porte lato host e lato array su un altro segmento di rete. Se possibile, utilizzare più switch Ethernet per fornire ulteriore ridondanza.

Fasi

Consultare la documentazione del fornitore dello switch.

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

Fase 3: Configurare il networking lato array - iSCSI, VMware

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- L'indirizzo IP o il nome di dominio di uno dei controller degli array di storage.
- La password per la GUI di System Manager, RBAC (Role-Based Access Control) o LDAP e un servizio di directory è configurata per l'accesso di sicurezza appropriato allo storage array. Per ulteriori informazioni

sulla gestione degli accessi, consultare la guida in linea di Gestione di sistema SANtricity.

A proposito di questa attività

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

> Per ulteriori informazioni su come configurare la rete lato array nella configurazione VMware, consultare il seguente report tecnico: "Guida alla configurazione VMware per l'integrazione iSCSI di e-Series SANtricity con ESXi 6.x e 7.x.".

Fasi

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

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

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

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

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

3. Chiudere l'installazione guidata.

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

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

   Il grafico cambia per mostrare i controller invece dei dischi.

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

   Viene visualizzato il menu di scelta rapida del controller.

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

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

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

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

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

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

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

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

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

Fase 4: Configurare il protocollo iSCSI (host-side networking)

La configurazione della rete iSCSI sul lato host consente all'iniziatore iSCSI VMware di stabilire una sessione con l'array.

A proposito di questa attività

In questo metodo rapido per la configurazione della rete iSCSI sul lato host, è possibile consentire all'host ESXi di trasportare il traffico iSCSI sullo storage su quattro percorsi ridondanti.

Una volta completata questa attività, l'host viene configurato con un singolo vSwitch contenente entrambe le porte VMkernel ed entrambe le VMNIC.

Per ulteriori informazioni sulla configurazione della rete iSCSI per VMware, consultare "Documentazione VMware vSphere" Per la versione di vSphere in uso.

Fasi

1. Configurare gli switch che verranno utilizzati per trasportare il traffico dello storage iSCSI.
2. Attiva il controllo di flusso hardware di invio e ricezione **end-to-end**.
3. Disattiva il controllo del flusso di priorità.
4. Completare la configurazione iSCSI lato array.
5. Utilizzare due porte NIC per il traffico iSCSI.
6. Utilizzare il client vSphere o il client Web vSphere per eseguire la configurazione lato host.

   Le interfacce variano in termini di funzionalità e il flusso di lavoro esatto varia.

Fase 5: Verifica delle connessioni di rete IP - iSCSI, VMware

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

Fasi

1. Sull'host, eseguire uno dei seguenti comandi, a seconda che i frame jumbo siano abilitati:
   - Se i frame jumbo non sono abilitati, eseguire questo comando:

```
vmkping <iSCSI_target_IP_address\>
```

- Se i frame jumbo sono abilitati, eseguire il comando ping con una dimensione del payload di 8,972 byte. Le intestazioni combinate IP e ICMP sono di 28 byte, che quando vengono aggiunte al payload equivale a 9,000 byte. L'interruttore -s imposta il `packet size` bit. Lo switch -d imposta il bit DF (non frammentare) sul pacchetto IPv4. Queste opzioni consentono di trasmettere correttamente frame jumbo di 9,000 byte tra l'iniziatore iSCSI e la destinazione.

```
vmkping -s 8972 -d <iSCSI_target_IP_address\>
```

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

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

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

> Se il comando non riesce e viene visualizzato il messaggio `sendto() failed (Message too long)`, Verificare le dimensioni MTU (supporto frame jumbo) per le interfacce Ethernet sul server host, sul controller storage e sulle porte dello switch.

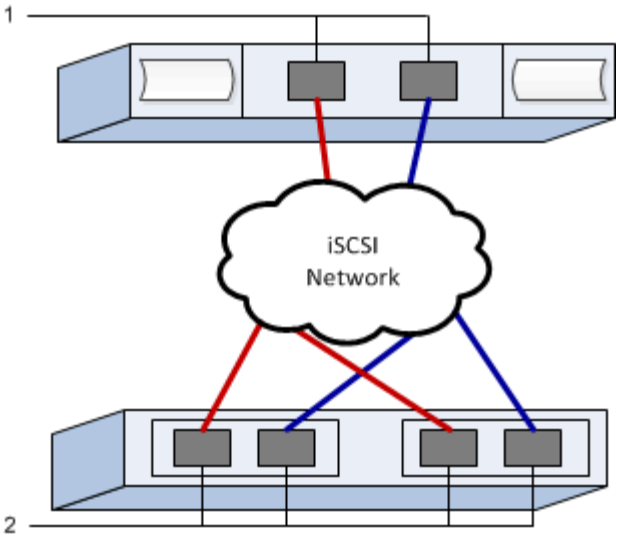
3. Tornare alla procedura di configurazione iSCSI per completare il rilevamento della destinazione.

Fase 6: Registrare la configurazione

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

Configurazione consigliata

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



IQN di destinazione

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

Nome host di mapping

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

Eseguire attività specifiche di SAS

Per il protocollo SAS, determinare gli indirizzi delle porte host ed effettuare le impostazioni consigliate.

Fase 1: Determinare gli identificatori host SAS - VMware

Individuare gli indirizzi SAS utilizzando l'utility HBA, quindi utilizzare il BIOS HBA per definire le impostazioni di configurazione appropriate.

A proposito di questa attività

Consulta le linee guida per le utility HBA:

- La maggior parte dei vendor HBA offre un'utility HBA.
- Le porte i/o host potrebbero essere registrate automaticamente se è installato l'agente di contesto host.

Fasi

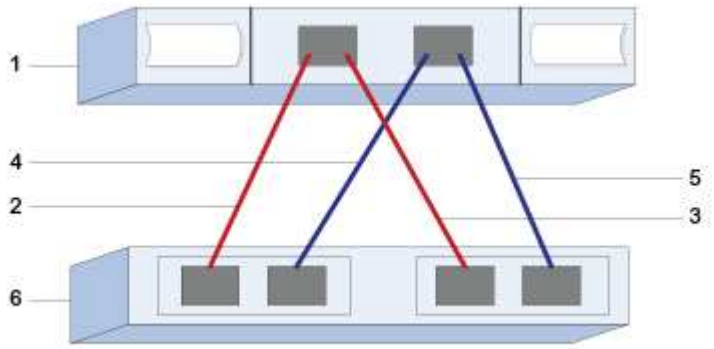
1. Scaricare l'utility HBA dal sito Web del vendor HBA.

2. Installare l'utility.
3. Utilizzare il BIOS HBA per selezionare le impostazioni appropriate per la configurazione.

   Per le impostazioni appropriate, vedere la colonna Note di "Tool di matrice di interoperabilità NetApp" per consigli.

Fase 2: Registrare la configurazione

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



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	Indirizzo SAS
1	Host	*non applicabile*
2	Porta host (iniziatore) 1 collegata al controller A, porta 1	
3	Porta host (iniziatore) 1 collegata al controller B, porta 1	
4	Porta host (iniziatore) 2 collegata al controller A, porta 1	
5	Porta host (iniziatore) 2 collegata al controller B, porta 1	

Identificatori di destinazione

Le configurazioni consigliate sono costituite da due porte di destinazione.

Nome host di mapping

Nome host di mapping
Tipo di sistema operativo host

Rilevare lo storage sull'host

Dopo aver assegnato i volumi all'host, eseguire una nuova scansione in modo che l'host rilevi e configuri i volumi per il multipathing.

Per impostazione predefinita, un host ESXi esegue automaticamente una nuova scansione ogni cinque minuti. Prima di eseguire una nuova scansione manuale, è possibile che venga visualizzato un volume tra un momento e l'altro in cui viene creato e assegnato a un host. Indipendentemente da ciò, è possibile eseguire una nuova scansione manuale per garantire che tutti i volumi siano configurati correttamente.

Fasi

1. Creare uno o più volumi e assegnarli all'host ESXi.
2. Se si utilizza un vCenter Server, aggiungere l'host all'inventario del server.
3. Utilizzare vSphere Client o vSphere Web Client per connettersi direttamente al vCenter Server o all'host ESXi.
4. Per istruzioni su come eseguire una nuova scansione dello storage su un host ESXi, cercare "Knowledge base VMware" articolo su questo argomento.

Configurare lo storage sull'host

È possibile utilizzare lo storage assegnato a un host ESXi come datastore VMFS (Virtual Machine file System) o RDM (Raw Device Mapping). Gli RDM non sono supportati dal protocollo NVMe over Fibre Channel.

Tutte le versioni 6.*x* e 7 *x* di ESXi supportano le versioni 5 e 6 di VMFS.

Fasi

1. Assicurarsi che i volumi mappati all'host ESXi siano stati rilevati correttamente.
2. Per istruzioni sulla creazione di datastore VMFS o sull'utilizzo di volumi come RDM con vSphere Client o vSphere Web Client, consultare la "Sito Web della documentazione VMware".

Verificare l'accesso allo storage sull'host

Prima di utilizzare un volume, verificare che l'host sia in grado di scrivere i dati nel volume e di leggerli.

A tale scopo, verificare che il volume sia stato utilizzato come archivio dati VMFS (Virtual Machine file System) o sia stato mappato direttamente a una macchina virtuale per l'utilizzo come RDM (Raw Device Mapping).

Configurazione di Windows Express

Panoramica della configurazione di Windows Express

Il metodo Windows Express per l'installazione dello storage array e l'accesso a Gestore di sistema di SANtricity è appropriato per la configurazione di un host Windows standalone su un sistema e-Series. È progettato per rendere operativo il sistema storage il più rapidamente possibile, con un numero minimo di punti decisionali.

Panoramica della procedura

Il metodo espresso include i seguenti passaggi, descritti anche nella "Workflow di Windows".

1. Configurare uno dei seguenti ambienti di comunicazione:
   - "Fibre Channel (FC)"
   - "ISCSI"
   - "SAS"
2. Creare volumi logici sull'array di storage.
3. Rendere i volumi disponibili per l'host dati.

Trova ulteriori informazioni

- Guida in linea — descrive come utilizzare Gestione di sistema di SANtricity per completare le attività di configurazione e gestione dello storage. È disponibile all'interno del prodotto.
- "Knowledge base di NetApp" (Un database di articoli) — fornisce informazioni sulla risoluzione dei problemi, FAQ e istruzioni per un'ampia gamma di prodotti e tecnologie NetApp.
- "Tool di matrice di interoperabilità NetApp" — consente di cercare configurazioni di prodotti e componenti NetApp che soddisfino gli standard e i requisiti specificati da NetApp.
- "Documentazione NetApp: Utility host" — fornisce la documentazione per la versione corrente di Windows Unified host Utilities.

Presupposti

Il metodo Windows Express si basa sui seguenti presupposti:

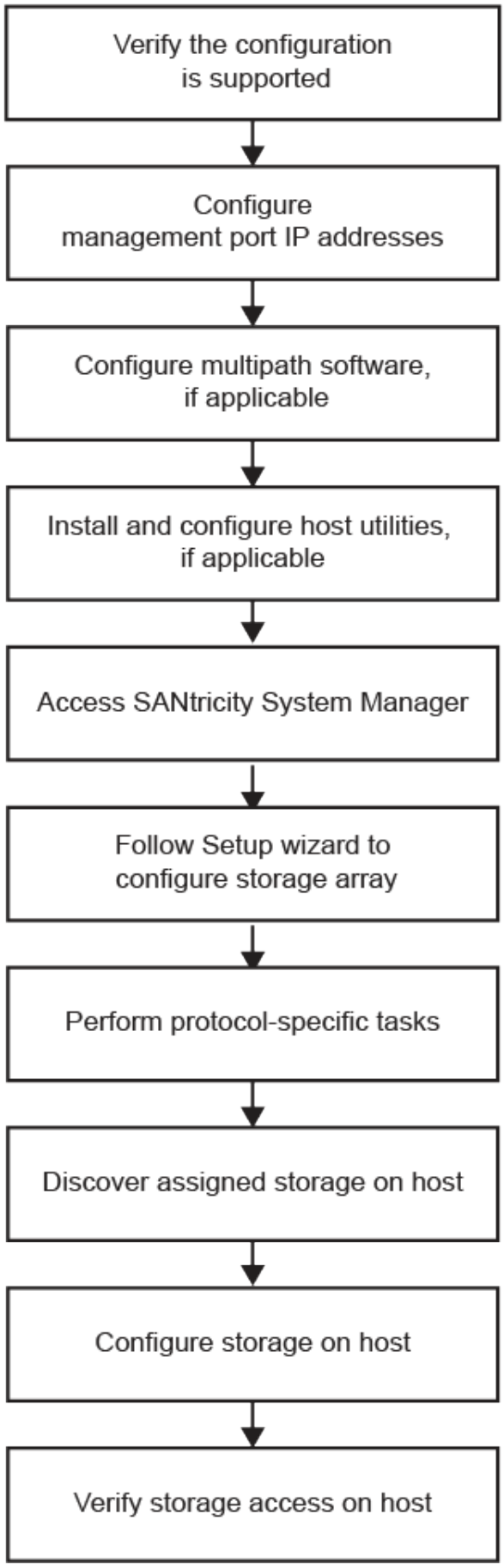
Componente	Presupposti
Hardware	• Per installare l'hardware, sono state utilizzate le istruzioni di installazione e configurazione fornite con gli shelf dei controller. • Sono stati collegati i cavi tra gli shelf di dischi opzionali e i controller. • Il sistema storage è alimentato. • Hai installato tutto l'altro hardware (ad esempio, stazione di gestione, switch) e hai effettuato le connessioni necessarie.

Componente	Presupposti
Host	• È stata stabilita una connessione tra il sistema storage e l'host dati. • Il sistema operativo host è stato installato. • Non stai utilizzando Windows come guest virtualizzato. • Non si sta configurando l'host dati (i/o collegato) per l'avvio da SAN.
Stazione di gestione dello storage	• Si utilizza una rete di gestione a 1 Gbps o più veloce. • Si sta utilizzando una stazione separata per la gestione piuttosto che l'host dei dati (i/o collegato). • Si sta utilizzando 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. • La stazione di gestione è stata collegata alla stessa subnet delle porte di gestione dello storage.
Indirizzamento IP	• È stato installato e configurato un server DHCP. • È stata ancora stabilita una connessione Ethernet tra la stazione di gestione e il sistema di storage.
Provisioning dello storage	• Non verranno utilizzati volumi condivisi. • Verranno creati pool anziché gruppi di volumi.
Protocollo: FC	• Sono state effettuate tutte le connessioni FC sul lato host e lo zoning dello switch attivato. • Stai utilizzando HBA e switch FC supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA FC elencate nella "Tool di matrice di interoperabilità NetApp".
Protocollo: ISCSI	• Si utilizzano switch Ethernet in grado di trasportare il traffico iSCSI. • Gli switch Ethernet sono stati configurati in base alle raccomandazioni del vendor per iSCSI.

Componente	Presupposti
Protocollo: SAS	• Stai utilizzando HBA SAS supportati da NetApp. • Si stanno utilizzando le versioni del driver e del firmware dell'HBA SAS elencate nella "Tool di matrice di interoperabilità NetApp".

Comprendere il flusso di lavoro di Windows

Questo flusso di lavoro guida l'utente attraverso il metodo rapido per la configurazione dello storage array e di Gestore di sistema di SANtricity per rendere lo storage disponibile a un host Windows.


Verify the configuration is supported
Configure management port IP addresses
Configure multipath software, if applicable
Install and configure host utilities, if applicable
Access SANtricity System Manager
Follow Setup wizard to configure storage array
Perform protocol-specific tasks
Discover assigned storage on host
Configure storage on host
Verify storage access on host

Verificare che la configurazione di Windows sia supportata

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

Fasi

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

   Viene visualizzata la sezione Criteri di ricerca più precisi. In questa sezione è possibile selezionare il protocollo applicabile e altri criteri per la configurazione, ad esempio sistema operativo, sistema operativo NetApp e driver host multipath. Selezionare i criteri desiderati per la configurazione, quindi visualizzare gli elementi di configurazione compatibili applicabili. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo prescritti nello strumento. Per informazioni dettagliate sulla configurazione scelta, fare clic sulla freccia a destra della pagina Visualizza configurazioni supportate.

5. Se necessario, eseguire gli aggiornamenti per il sistema operativo e il protocollo come indicato nella tabella.

Aggiornamenti del sistema operativo	Protocollo	Aggiornamenti relativi al protocollo
Potrebbe essere necessario installare driver pronti all'uso per garantire funzionalità e supportabilità adeguate. Ogni vendor HBA dispone di metodi specifici per aggiornare il codice di avvio e il firmware. Fare riferimento alla sezione di supporto del sito Web del vendor per ottenere le istruzioni e il software necessari per aggiornare il firmware e il codice di avvio HBA.	FC	Driver, firmware e codice di avvio dell'HBA (host bus adapter)
ISCSI	Driver, firmware e codice di avvio della scheda di interfaccia di rete (NIC).	SAS

Configurare gli indirizzi IP utilizzando DHCP

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

A proposito di questa attività

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

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

Fasi

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

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

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

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

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

   - Controller A, porta 1: 169.254.128.101
   - Controller B, porta 1: 169.254.128.102
   - Subnet mask: 255.255.0.0
2. Individuare l'etichetta dell'indirizzo MAC sul retro di ciascun controller, quindi fornire all'amministratore di rete l'indirizzo MAC per la porta 1 di ciascun controller.

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

Configurare il software multipath

Per fornire un percorso ridondante all'array di storage, è possibile installare il pacchetto DSM Windows di SANtricity e utilizzare il pacchetto multipath per Windows.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- I privilegi di amministratore o superutente corretti.

A proposito di questa attività

Il software multipath fornisce un percorso ridondante all'array di storage in caso di interruzione di uno dei percorsi fisici. Prima di poter utilizzare il multipathing, è necessario installare il pacchetto DSM Windows di SANtricity. Questo pacchetto contiene il software multipath per Windows.

Le installazioni di Windows utilizzano il driver nativo DSM (Device Specific Module) di MPIO per il failover. Quando si installa e si attiva il pacchetto DSM Windows di SANtricity, non è necessario intraprendere ulteriori azioni per utilizzare multipath.

Fasi

1. Scaricare il pacchetto **SANtricity DSM** dal "Pagina del software del sistema operativo SANtricity". Selezionare la versione del software, accettare il contratto di licenza e selezionare **SANtricity Windows DSM** sotto Download aggiuntivi.
2. Eseguire il programma di installazione **SANtricity DSM**. Fare doppio clic sul pacchetto di installazione da eseguire.
3. Utilizzare l'installazione guidata per installare il pacchetto sulla stazione di gestione.

Installare e configurare Windows Unified host Utilities

Gli strumenti di Windows Unified host Utilities consentono di collegare i computer host ai sistemi di storage NetApp e di impostare i parametri richiesti sui computer host. È inoltre possibile impostare i timeout dei dischi appropriati per ottenere le migliori prestazioni di lettura/scrittura con lo storage NetApp.

> Per ulteriori informazioni, consultare la *Guida all'installazione delle utility host di Windows,* disponibile in "Documentazione NetApp: Utility host".

Fasi

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

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

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

   > Questo pacchetto di utility non può essere installato utilizzando il programma di installazione di Gestore storage SANtricity.

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

Installazione di SANtricity Storage Manager per SMcli e host Context Agent (HCA)

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

Fasi

1. Scaricare la versione del software SANtricity all'indirizzo "Supporto NetApp". Dalla scheda **Download**, **Download › Gestione storage e-Series SANtricity**.
2. Eseguire il programma di installazione di SANtricity. Fare doppio clic sul pacchetto di installazione SMIA*.exe per eseguirlo.
3. Utilizzare l'installazione guidata per installare il software sulla stazione di gestione.

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

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

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

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

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

Browser	Versione minima
Safari	14

A proposito di questa attività

Se si utilizza iSCSI, assicurarsi di aver chiuso l'installazione guidata durante la configurazione di iSCSI.

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

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

Se l'installazione guidata non viene visualizzata automaticamente, contattare il supporto tecnico.

Fasi

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

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

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

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

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

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

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

Eseguire attività specifiche di FC

Per il protocollo Fibre Channel, configurare gli switch e determinare gli identificatori delle porte host.

Fase 1: Configurazione degli switch FC - Windows

La configurazione (zoning) degli switch Fibre Channel (FC) consente agli host di connettersi allo storage array e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Credenziali di amministratore per gli switch.
- Il numero WWPN di ciascuna porta di iniziatore host e di ciascuna porta di destinazione del controller collegata allo switch. (Utilizzare l'utility HBA per il rilevamento).

A proposito di questa attività

È necessario eseguire la zona in base alla WWPN e non alla porta fisica. Ciascuna porta dell'iniziatore deve trovarsi in una zona separata con tutte le porte di destinazione corrispondenti. Per ulteriori informazioni sulla suddivisione in zone degli switch, consultare la documentazione del vendor dello switch.

Fasi

1. Accedere al programma di amministrazione dello switch FC, quindi selezionare l'opzione di configurazione dello zoning.
2. Creare una nuova zona che includa la prima porta iniziatore host e che includa anche tutte le porte di destinazione che si connettono allo stesso switch FC dell'iniziatore.
3. Creare zone aggiuntive per ciascuna porta iniziatore host FC nello switch.
4. Salvare le zone, quindi attivare la nuova configurazione di zoning.

Fase 2: Determinare le reti WWPN host ed effettuare le impostazioni consigliate: FC, Windows

Installare un'utility HBA FC in modo da visualizzare il nome della porta globale (WWPN) di ciascuna porta host. Inoltre, è possibile utilizzare l'utility HBA per modificare le impostazioni consigliate nella colonna Note di "Tool di matrice di interoperabilità NetApp" per la configurazione supportata.

A proposito di questa attività

Consulta le seguenti linee guida per le utility HBA:

- La maggior parte dei vendor HBA offre un'utility HBA. È necessaria la versione corretta dell'HBA per il sistema operativo host e la CPU. Esempi di utility HBA FC includono:
  - Emulex OneCommand Manager per HBA Emulex
  - QLogic QConverge Console per HBA QLogic
- Le porte i/o host potrebbero essere registrate automaticamente se è installato l'agente di contesto host.

Fasi

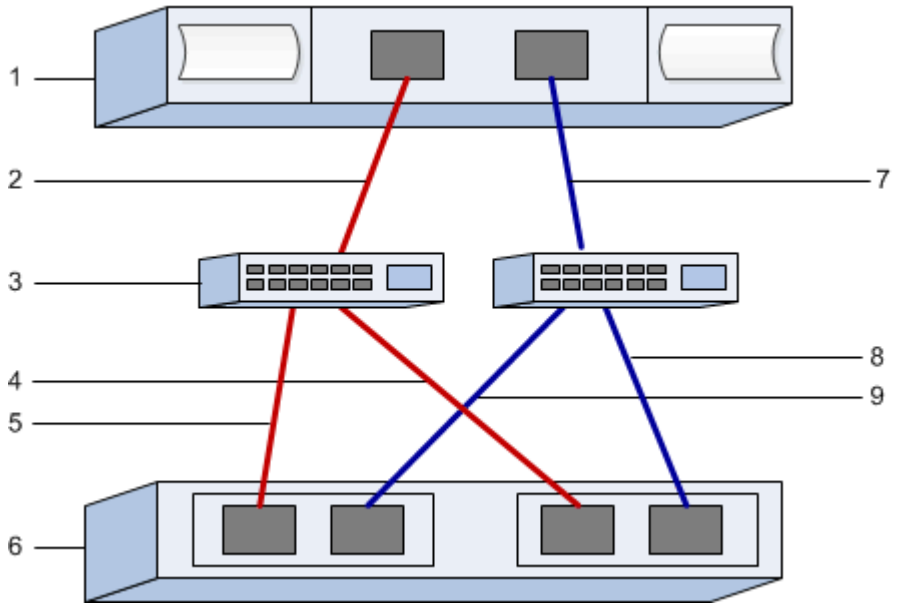
1. Scaricare l'utility appropriata dal sito Web del vendor HBA.
2. Installare l'utility.
3. Selezionare le impostazioni appropriate nell'utility HBA.

   Le impostazioni appropriate per la configurazione sono elencate nella colonna Note di "Tool di matrice di interoperabilità NetApp".

Fase 3: Registrare la configurazione

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

La figura mostra un host collegato a un array di storage e-Series in due zone. Una zona è indicata dalla linea blu, mentre l'altra è indicata dalla linea rossa. Ogni singola porta ha due percorsi per lo storage (uno per ciascun controller).



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	PN. WWN
1	Host	*non applicabile*
2	Porta host 0 a switch FC zona 0	
7	Dalla porta host 1 allo switch FC zona 1	

Identificatori di destinazione

N. didascalia	Connessioni delle porte (di destinazione) degli array controller	PN. WWN
3	Switch	*non applicabile*
6	Controller di array (destinazione)	*non applicabile*
5	Dal controller A, dalla porta 1 allo switch FC 1	
9	Dal controller A, dalla porta 2 allo switch FC 2	
4	Dal controller B, porta 1 allo switch FC 1	
8	Controller B, dalla porta 2 allo switch FC 2	

Nome host di mapping

Nome host di mapping
Tipo di sistema operativo host

Eseguire attività specifiche di iSCSI

Per il protocollo iSCSI, configurare gli switch, configurare la rete sul lato array e sul lato host, quindi verificare le connessioni di rete IP.

Fase 1: Configurazione degli switch - iSCSI, Windows

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

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Due reti separate per l'alta disponibilità. Assicurarsi di isolare il traffico iSCSI per separare i segmenti di rete utilizzando VLAN o due reti separate.
- Controllo di flusso hardware di invio e ricezione abilitato **end-to-end**.
- Controllo di flusso prioritario disattivato.
- Se appropriato, abilitare i frame jumbo.

> Port channels/LACP non è supportato sulle porte switch del controller. LACP lato host non è consigliato; il multipathing offre gli stessi vantaggi o meglio.

Fasi

Consultare la documentazione del fornitore dello switch.

Fase 2: Configurazione della rete - iSCSI Windows

È possibile configurare la rete iSCSI in diversi modi, a seconda dei requisiti di storage dei dati. Rivolgersi all'amministratore di rete per suggerimenti sulla scelta della configurazione migliore per l'ambiente in uso.

Una strategia efficace per configurare la rete iSCSI con ridondanza di base consiste nel collegare ciascuna porta host e una porta da ciascun controller per separare gli switch e partizionare ciascun set di porte host e controller su segmenti di rete separati utilizzando VLAN.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Controllo di flusso hardware di invio e ricezione abilitato **end-to-end**.
- Controllo di flusso prioritario disattivato.
- Se appropriato, abilitare i frame jumbo.

  Se si utilizzano frame jumbo all'interno della SAN IP per motivi di performance, assicurarsi di configurare l'array, gli switch e gli host in modo che utilizzino frame jumbo. Consultare la documentazione del sistema operativo e dello switch per informazioni su come abilitare i frame jumbo sugli host e sugli switch. Per abilitare i frame jumbo sull'array, completare la procedura descritta nella fase 3.

Fasi

Consultare la documentazione del fornitore dello switch.

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

Fase 3: Configurare la rete lato array - iSCSI, Windows

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

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

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

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

   Quando si apre System Manager e non sono stati configurati pool, gruppi di volumi, carichi di lavoro o notifiche, viene avviata l'installazione guidata.

3. Chiudere l'installazione guidata.

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

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

   Il grafico cambia per mostrare i controller invece dei dischi.

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

   Viene visualizzato il menu di scelta rapida del controller.

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

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

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

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

Impostazione della porta	Descrizione
Velocità della porta ethernet configurata	Selezionare la velocità desiderata. Le opzioni visualizzate nell'elenco a discesa dipendono dalla velocità massima supportata dalla rete (ad esempio, 10 Gbps). Le schede di interfaccia host iSCSI opzionali nei controller E5700 e EF570 non negoziano automaticamente le velocità. È necessario impostare la velocità di ciascuna porta su 10 GB o 25 GB. Tutte le porte devono essere impostate alla stessa velocità.
Attiva IPv4 / attiva IPv6	Selezionare una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.
Porta TCP in ascolto (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire un nuovo numero di porta. La porta di ascolto è il numero di porta TCP utilizzato dal controller per rilevare gli accessi iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. Immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile facendo clic su **Mostra altre impostazioni della porta**).	Se necessario, inserire una nuova dimensione in byte per l'unità di trasmissione massima (MTU). La dimensione massima predefinita dell'unità di trasmissione (MTU) è di 1500 byte per frame. Immettere un valore compreso tra 1500 e 9000.
Abilitare le risposte PING ICMP	Selezionare questa opzione per attivare il protocollo ICMP (Internet Control message Protocol). I sistemi operativi dei computer collegati in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per ottenere i pacchetti da e verso tale host.

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

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

Impostazione della porta	Descrizione
Ottenere automaticamente la configurazione	Selezionare questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Selezionare questa opzione, quindi inserire un indirizzo statico nei campi. Per IPv4, includere la subnet mask di rete e il gateway. Per IPv6, includere l'indirizzo IP instradabile e l'indirizzo IP del router.
Abilitare il supporto VLAN (disponibile facendo clic su **Mostra altre impostazioni**).	Questa opzione è disponibile solo in un ambiente iSCSI. Non è disponibile in un ambiente NVMe over RoCE. 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**).	Questa opzione è disponibile solo in un ambiente iSCSI. Non è disponibile in un ambiente NVMe over RoCE. 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 e 7. 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.

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

Fase 4: Configurare il protocollo iSCSI (host-side networking)

È necessario configurare la rete iSCSI sul lato host in modo che l'iniziatore iSCSI Microsoft possa stabilire sessioni con l'array.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Switch completamente configurati che verranno utilizzati per trasportare il traffico dello storage iSCSI.
- Controllo di flusso hardware di invio e ricezione abilitato **end-to-end**
- Controllo di flusso prioritario disattivato.
- Configurazione iSCSI lato array completata.
- L'indirizzo IP di ciascuna porta del controller.

A proposito di questa attività

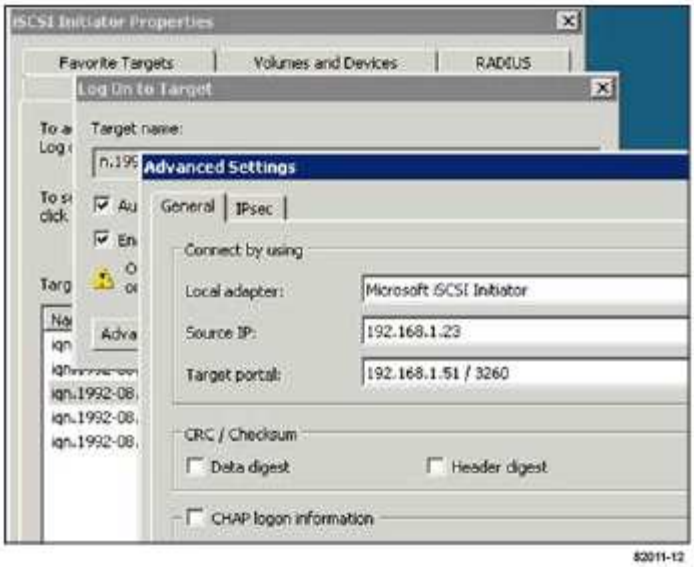
Queste istruzioni presuppongono che per il traffico iSCSI vengano utilizzate due porte NIC.

Fasi

1. Disattiva i protocolli della scheda di rete non utilizzati.

   Questi protocolli includono, a titolo esemplificativo ma non esaustivo, QoS, Condivisione file e stampanti e NetBIOS.

2. Eseguire `> iscsicpl.exe` Da una finestra terminale sull'host per aprire la finestra di dialogo **iSCSI Initiator Properties**.
3. Nella scheda **Discovery**, selezionare **Discover Portal**, quindi inserire l'indirizzo IP di una delle porte di destinazione iSCSI.
4. Nella scheda **targets**, selezionare il primo portale di destinazione rilevato, quindi selezionare **Connect**.
5. Selezionare **Enable multi-path** (attiva percorso multiplo), selezionare **Add this Connection to the list of favorite targets** (Aggiungi connessione all'elenco di destinazioni preferite), quindi selezionare **Advanced** (Avanzate).
6. Per **Local adapter**, selezionare **Microsoft iSCSI Initiator**.
7. Per **Initiator IP**, selezionare l'indirizzo IP di una porta sulla stessa subnet o VLAN di una delle destinazioni iSCSI.
8. Per **Target IP**, selezionare l'indirizzo IP di una porta sulla stessa subnet dell'indirizzo **Initiator IP** selezionato nel passaggio precedente.
9. Mantenere i valori predefiniti per le restanti caselle di controllo, quindi selezionare **OK**.
10. Selezionare di nuovo **OK** quando si torna alla finestra di dialogo **Connetti a destinazione**.
11. Ripetere questa procedura per ogni porta e sessione dell'iniziatore (percorso logico) verso l'array di storage che si desidera stabilire.



Fase 5: Verificare le connessioni di rete IP - iSCSI, Windows

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

1. Selezionare **Start › tutti i programmi › Accessori › prompt dei comandi**, quindi utilizzare l'interfaccia CLI di Windows per eseguire uno dei seguenti comandi, a seconda che i frame jumbo siano abilitati:

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

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

   - Se i frame jumbo sono abilitati, eseguire il comando ping con una dimensione del payload di 8,972 byte. Le intestazioni combinate IP e ICMP sono di 28 byte, che quando vengono aggiunte al payload equivale a 9,000 byte. L'interruttore -f imposta il `don't fragment (DF)` bit. L'interruttore -l consente di impostare le dimensioni. Queste opzioni consentono di trasmettere correttamente frame jumbo di 9,000 byte tra l'iniziatore iSCSI e la destinazione.

     ```
     ping -l 8972 -f <iSCSI_target_IP_address\>
     ```

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

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

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

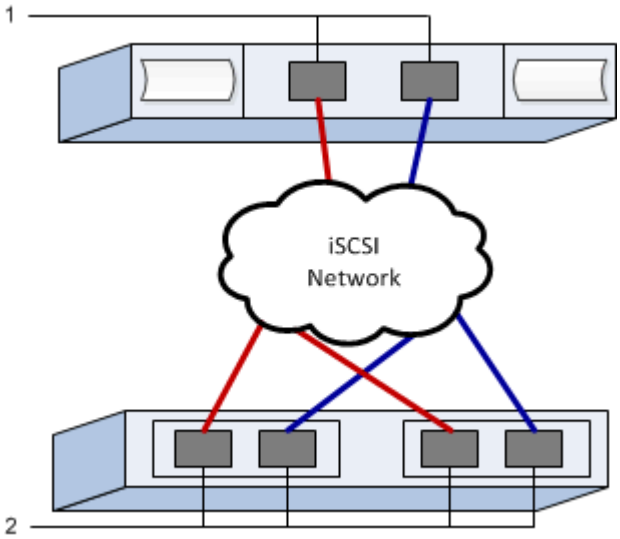
> Se il comando non riesce (ad esempio, restituisce `Packet needs to be fragmented but DF set`), verificare le dimensioni MTU (supporto frame jumbo) per le interfacce Ethernet sul server host, sul controller storage e sulle porte dello switch.

Fase 6: Registrare la configurazione

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

Configurazione consigliata

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



IQN di destinazione

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

Nome host di mapping

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

Eseguire attività specifiche di SAS

Per il protocollo SAS, determinare gli indirizzi delle porte host e definire le impostazioni appropriate.

Fase 1: Determinare gli identificatori host SAS - Windows

Individuare gli indirizzi SAS utilizzando l'utility HBA, quindi utilizzare il BIOS HBA per definire le impostazioni di configurazione appropriate.

A proposito di questa attività

Consulta le linee guida per le utility HBA:

- La maggior parte dei vendor HBA offre un'utility HBA. A seconda del sistema operativo host e della CPU, utilizzare l'utility LSI-sas2flash(6G) o sas3flash(12G).
- Le porte i/o host potrebbero essere registrate automaticamente se è installato l'agente di contesto host.

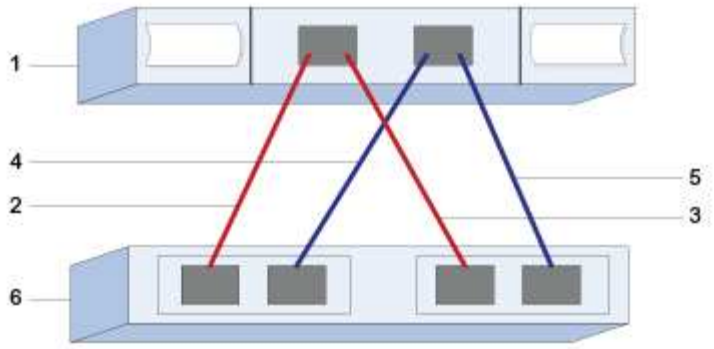
Fasi

1. Scaricare l'utility LSI-sas2flash(6G) o sas3flash(12G) dal sito Web del vendor HBA.
2. Installare l'utility.
3. Utilizzare il BIOS HBA per selezionare le impostazioni appropriate per la configurazione.

   Per informazioni sulle impostazioni consigliate, vedere la colonna Note di "Tool di matrice di interoperabilità NetApp".

Fase 2: Registrare la configurazione

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



Identificatori host

N. didascalia	Connessioni porta host (iniziatore)	Indirizzo SAS
1	Host	*non applicabile*
2	Porta host (iniziatore) 1 collegata al controller A, porta 1	
3	Porta host (iniziatore) 1 collegata al controller B, porta 1	
4	Porta host (iniziatore) 2 collegata al controller A, porta 1	
5	Porta host (iniziatore) 2 collegata al controller B, porta 1	

Identificatori di destinazione

Le configurazioni consigliate sono costituite da due porte di destinazione.

Nome host di mapping

Nome host di mapping
Tipo di sistema operativo host

Rilevare lo storage sull'host

Quando si aggiungono nuove LUN, è necessario eseguire una nuova scansione manuale dei dischi associati per rilevarli. L'host non rileva automaticamente i nuovi LUN.

I LUN del sistema storage vengono visualizzati come dischi sull'host Windows.

Fasi

1. Accedere come amministratore.
2. Per rilevare lo storage, eseguire il comando seguente dal prompt dei comandi di Windows.

```
# echo rescan | diskpart
```

3. Per verificare l'aggiunta di nuovo storage, eseguire il seguente comando.

```
# echo list disk | diskpart
```

Configurare lo storage sull'host

Poiché un nuovo LUN non è in linea e non dispone di partizione o file system quando un host Windows lo rileva per la prima volta, è necessario portare il volume in linea e inizializzarlo in Windows. In alternativa, è possibile formattare il LUN con un file system.

È possibile inizializzare il disco come disco di base con una tabella di partizione GPT o MBR. In genere, si formatta il LUN con un file system come New Technology file System (NTFS).

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un LUN rilevato dall'host.

Fasi

1. Dal prompt dei comandi di Windows, immettere `diskpart` contesto.

```
> diskpart
```

2. Visualizzare l'elenco dei dischi disponibili.

```
> list disk
```

3. Selezionare il disco da portare in linea.

```
> select disk 1
```

4. Portare il disco online.

```
> online disk
```

5. Creare una partizione.

```
> create partition primary
```

> In Windows Server 2008 e versioni successive, subito dopo la creazione della partizione viene richiesto di formattare il disco e assegnargli un nome. Selezionare **Cancel** (Annulla) per continuare a utilizzare queste istruzioni per la formattazione e la denominazione della partizione.

6. Assegnare una lettera di unità.

```
> assign letter=f
```

7. Formattare il disco.

```
> format FS=NTFS LABEL="New Volume" QUICK
```

8. Uscire dal contesto diskpart.

```
> exit
```

Verificare l'accesso allo storage sull'host

Prima di utilizzare il volume, verificare che l'host sia in grado di scrivere i dati sul LUN e di leggerli.

Prima di iniziare

Il LUN deve essere stato inizializzato e formattato con un file system.

Fasi

1. Creare e scrivere su un file sul nuovo LUN.

```
> echo test file > f:\\test.txt
```

2. Leggere il file e verificare che i dati siano stati scritti.

```
> type f:\\test.txt
```

3. Per verificare il funzionamento di multipath, modificare la proprietà del volume.
   a. Dalla GUI di Gestione di sistema di SANtricity, andare a **Storage** > **Volumes**, quindi selezionare **More** > **Change ownership**.

b. Nella finestra di dialogo Change Volume Ownership (Modifica proprietà volume), utilizzare l'elenco a discesa **Preferred Owner** (Proprietario preferito) per selezionare l'altro controller per uno dei volumi nell'elenco, quindi confermare l'operazione.

c. Verificare che sia ancora possibile accedere ai file sul LUN.

```
> dir f:\\
```

4. Individuare l'ID di destinazione.

L'utility dsmUtil distingue tra maiuscole e minuscole.

```
> C:\\Program Files \(x86\)\\DSMDrivers\\mppdsm\\dsmUtil.exe -a
```

5. Visualizzare i percorsi del LUN e verificare di disporre del numero di percorsi previsto. In `<target ID>` Parte del comando, utilizzare l'ID di destinazione trovato nel passaggio precedente.

```
> C:\\Program Files \(x86\)\\DSMDrivers\\mppdsm\\dsmUtil.exe –g <target
ID\>
```

Aggiornare i sistemi

Controller

Panoramica sull'upgrade dei controller

È possibile aggiornare lo storage array attraverso la sostituzione dei controller esistenti.

Componenti del controller

Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa anche le funzioni del software di gestione.

Quando utilizzare questa procedura

Questa procedura viene generalmente utilizzata quando si desidera aggiornare tutti i controller a un modello o a una piattaforma differente. Questa procedura comporta la sostituzione di tutti i controller in un vassoio del disco del controller

Questa procedura può essere utilizzata anche nelle seguenti situazioni:

- Quando tutti i controller di un vassoio del disco controller riscontrano guasti hardware e non sono più funzionanti.
- Per aggiornare i moduli DIMM (Dual Inline Memory Module) nel vassoio del controller sostituendo entrambi i controller con lo stesso modello di controller, ma con DIMM differenti.

> Gli scenari di aggiornamento HIC non sono trattati in questa procedura. Consultare invece le procedure di aggiunta, aggiornamento e sostituzione HIC per il sistema e-Series.

Considerazioni sull'upgrade

Prima di aggiornare i controller, esaminare le seguenti considerazioni.

Requisiti hardware e firmware

- **Aggiornamenti dei controller duplex e simplex**

  Per i vassoi del disco del controller duplex, sostituire entrambi i controller. Per i vassoi del disco del controller simplex, sostituire il controller singolo. In entrambi i casi, è necessario spegnere il vassoio del disco del controller Di conseguenza, non è possibile accedere ai dati sull'array di storage fino a quando la sostituzione non viene completata correttamente.

- **Vassoi e shelf**

  Gli array di storage con shelf di controller E2800 o E5700 vengono generalmente gestiti con l'interfaccia utente di Gestore di sistema di SANtricity. È inoltre possibile utilizzare l'interfaccia di gestione dello storage SANtricity per gestire gli shelf di controller E2800 o E5700. Tutti gli altri vassoi del controller a cui si fa riferimento in questa procedura utilizzano Gestione storage SANtricity.

- **Batterie del controller**

Un nuovo controller viene spedito senza una batteria installata. Quando possibile, rimuovere la batteria dal vecchio controller e installarla nel nuovo controller. Tuttavia, per alcuni aggiornamenti del controller, la batteria del vecchio controller non è compatibile con il nuovo controller. In questi casi, è necessario ordinare una batteria insieme al nuovo controller e tenere la batteria a disposizione prima di iniziare queste attività.

- **Identificazione del vendor**

  Alcuni aggiornamenti del controller comportano la modifica dell'ID del vendor in SCSI Inquiry Data from (dati di richiesta SCSI) `LSI` a. `NETAPP`. Quando l'ID fornitore cambia da `LSI` a. `NETAPP`, Per recuperare i dispositivi, sono necessari ulteriori passaggi sui sistemi operativi Windows, VMware e AIX. Questa procedura di aggiornamento include i passaggi per questi sistemi operativi.

- **Mirroring sincrono e mirroring asincrono**

  Se lo storage array partecipa al mirroring sincrono, tra il sito primario e il sito remoto sono supportate solo le connessioni iSCSI o Fibre Channel. Se la configurazione della scheda di interfaccia host (HIC) nei nuovi controller non include connessioni iSCSI o Fibre Channel, il mirroring sincrono non sarà supportato.

  Per il mirroring asincrono, l'array di storage locale e l'array di storage remoto possono eseguire diverse versioni del firmware. La versione minima del firmware supportata è la versione 7.84 del firmware SANtricity.

- **Limiti degli oggetti di storage**

  Se si cambiano i controller da modelli 5x00 a modelli 2x00, la nuova configurazione dello storage array supporterà un numero inferiore di alcuni oggetti storage (ad esempio, volumi) nel software di gestione dello storage rispetto alla configurazione precedente. Assicurarsi che la vecchia configurazione non superi i limiti degli oggetti di storage. Vedere "Hardware Universe" per ulteriori informazioni.

Eseguire l'aggiornamento a modelli più recenti

Se si stanno sostituendo i controller per eseguire l'aggiornamento a un nuovo modello, tenere presente che lo storage array attuale potrebbe disporre di funzionalità premium installate che il nuovo modello non è in grado di supportare. Ad esempio, i controller E2700 non supportano la funzionalità Premium di Snapshots legacy.

Se si sostituiscono i controller E2600 con i controller E2700 e lo storage array utilizzava la funzione Snapshots legacy, è necessario disattivare tale funzione ed eliminare o convertire tutti i volumi (ovvero snapshot, repository) associati a tale funzione prima di sostituire i controller. È possibile convertire le snapshot legacy nella funzione Snapshot aggiornata. Prima di aggiornare un tray di dischi controller, è necessario disattivare tutte le funzioni premium utilizzate sull'array di storage non supportate dai nuovi controller.

Compatibilità con gli aggiornamenti

Esaminare i percorsi di aggiornamento supportati per ciascun modello di array di storage.

Da E2x00 a E2x00

- **Batteria**: Riutilizzare la vecchia batteria.
- **ID vendor**: Sono necessari ulteriori passaggi.
- **Supporto delle funzioni**: Gli snapshot legacy non sono supportati su E2700.
- **Shelf SAS-2**: I controller E2800 non devono essere posizionati negli shelf SAS-2.

Da E2x00 a E5x00

- **Batteria**: Ordinare una nuova batteria.
- **ID vendor**: Sono necessari ulteriori passaggi per l'aggiornamento da E2600 a E5500 o E5600 o per l'aggiornamento da E2700 a E5400.
- **Supporto delle funzioni**:
  - Gli snapshot legacy non sono supportati su E5500 o E5600.
  - Il mirroring remoto dei volumi legacy (RVM) non è supportato su E5500 o E5600 con iSCSI HICS.
  - Data Assurance non è supportato su E5500 o E5600 con iSCSI HICS.
  - I controller E5700 non devono essere posizionati negli shelf SAS-2.
- **Shelf SAS-3**: I controller E5400, E5500 e E5600 non devono essere posizionati negli shelf SAS-3.

Da E5x00 a E2x00

- **Batteria**: Ordinare una nuova batteria.
- **ID vendor**: Sono necessari ulteriori passaggi per l'aggiornamento da E5500 o E5600 a E2600 o per l'aggiornamento da E5400 a E2700.
- **Supporto delle funzioni**: Gli snapshot legacy non sono supportati su E2700.
- **Shelf SAS-3**: I controller E5400, E5500 e E5600 non devono essere posizionati negli shelf SAS-3.

Da E5x00 a E5x00

- **Batteria**: Riutilizzare la vecchia batteria.
- **ID vendor**: Procedure aggiuntive necessarie per l'aggiornamento da E5400 a E5500 o E5600.
- **Supporto delle funzioni**:
  - Gli snapshot legacy non sono supportati su E5500 o E5600.
  - Il mirroring remoto dei volumi legacy (RVM) non è supportato su E5400 o E5500 con iSCSI HICS.
  - Data Assurance non è supportato su E5400 o E5500 con iSCSI HICS.
  - I controller E5700 non devono essere posizionati negli shelf SAS-2.
- **Shelf SAS-3**: I controller E5400, E5500 e E5600 non devono essere posizionati negli shelf SAS-3.

Da EF5x0 a EF5x0

- **Batteria**: Riutilizzare la vecchia batteria.
- **ID vendor**: Ulteriori passaggi necessari per l'aggiornamento da EF540 a EF550 o EF560.
- **Supporto delle funzioni**:
  - Nessuna snapshot legacy per EF550/EF560.
  - Nessuna Data Assurance per EF550/EF560 con iSCSI.
  - I controller EF570 non devono essere posizionati negli shelf SAS-3.
- **Shelf SAS-3**: I controller EF540, EF550 e EF560 non devono essere posizionati negli shelf SAS-3.

Enclosure SAS

E5700 supporta enclosure SAS-2 DE5600 e DE6600 tramite upgrade della testina. Quando un controller E5700 viene installato in enclosure SAS-2, il supporto per le porte host di base viene disattivato.

Shelf SAS-2	Shelf SAS-3
Gli shelf SAS-2 includono i seguenti modelli: • Tray di dischi DE1600, DE5600 e DE6600 • Tray di dischi controller E5400, E5500 e E5600 • Array flash EF540, EF550 e EF560 • Tray di dischi controller E2600 e E2700	Gli shelf SAS-3 includono i seguenti modelli: • Shelf di controller E2800 • Shelf di controller E5700 • Shelf di dischi DE212C, DE224C, DE460C

Protezione dell'investimento da SAS-2 a SAS-3

È possibile riconfigurare il sistema SAS-2 per l'utilizzo dietro un nuovo shelf di controller SAS-3 (E57XX/EF570/E28XX).

> Questa procedura richiede una richiesta di variazione del prodotto (FPVR). Per presentare un FPVR, contatta il tuo team di vendita.

Preparazione per l'aggiornamento dei controller

Preparare l'aggiornamento dei controller salvando la chiave Drive Security (se utilizzata), registrando il numero di serie, raccogliendo i dati di supporto, disattivando alcune funzioni (se utilizzate) e portando il controller offline.

> La raccolta dei dati di supporto può influire temporaneamente sulle performance dello storage array.

Fasi

1. Assicurarsi che lo storage array esistente sia aggiornato alla versione più recente del sistema operativo (firmware del controller) disponibile per i controller correnti. Da Gestore di sistema di SANtricity, andare al **supporto › Centro di aggiornamento** per visualizzare l'inventario di software e firmware.

   > Se si esegue l'aggiornamento a controller che supportano SANtricity OS versione 8.50, è necessario installare le versioni più recenti di SANtricity OS e L'ultima VERSIONE DI NVSRAM dopo aver installato e acceso i nuovi controller. Se non si esegue questo aggiornamento, potrebbe non essere possibile configurare lo storage array per il bilanciamento automatico del carico (ALB).

2. Se si dispone di dischi abilitati alla protezione installati e si prevede di eseguire una sostituzione completa del controller, fare riferimento alla tabella seguente per completare i passaggi appropriati per il tipo di sicurezza (interno o esterno) e lo stato del disco. Se si dispone di unità abilitate per la protezione * installate, saltare questo passaggio e passare al punto 3 sotto la tabella.

   > Alcuni passaggi della tabella richiedono i comandi dell'interfaccia a riga di comando (CLI). Per informazioni sull'utilizzo di questi comandi, vedere "Riferimento all'interfaccia della riga di comando".

Tipo di sicurezza e contesto	Fasi
Gestione interna delle chiavi, uno o più dischi bloccati	Esportare il file della chiave di sicurezza interna in una posizione nota sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Utilizzare `export storageArray securityKey` Comando CLI. Specificare la password associata alla chiave di sicurezza e la posizione in cui si desidera salvarla.
Gestione esterna delle chiavi, tutti i dischi bloccati, è possibile passare temporaneamente alla gestione interna delle chiavi per la sostituzione del controller (scelta consigliata).	Eseguire le seguenti operazioni nell'ordine indicato: a. Registrare l'indirizzo del server KMS esterno e il numero di porta. Da System Manager, andare a **Impostazioni › sistema › Gestione chiavi di sicurezza › Visualizza/Modifica impostazioni server di gestione chiavi**. b. Assicurarsi che i certificati del client e del server siano disponibili sull'host locale in modo che l'array di storage e il server di gestione delle chiavi possano autenticarsi una volta terminata la sostituzione del controller. Utilizzare `save storageArray keyManagementCertificate` Comando CLI per salvare i certificati. Eseguire il comando due volte, una volta con il `certificateType` parametro impostato su `client`e l'altro con il parametro impostato su `server`. c. Transizione alla gestione interna delle chiavi mediante l'esecuzione di `disable storageArray externalKeyManagement` Comando CLI. d. Esportare il file della chiave di sicurezza interna in una posizione nota sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Utilizzare `export storageArray securityKey` Comando CLI. Specificare la password associata alla chiave di sicurezza e la posizione in cui si desidera salvarla.

Tipo di sicurezza e contesto	Fasi
Gestione esterna delle chiavi, tutti i dischi bloccati, **non** è possibile passare temporaneamente alla gestione interna delle chiavi per la sostituzione del controller.	Eseguire le seguenti operazioni nell'ordine indicato: a. Registrare l'indirizzo del server KMS esterno e il numero di porta. Da System Manager, andare a **Impostazioni › sistema › Gestione chiavi di sicurezza › Visualizza/Modifica impostazioni server di gestione chiavi**. b. Assicurarsi che i certificati del client e del server siano disponibili sull'host locale in modo che l'array di storage e il server di gestione delle chiavi possano autenticarsi una volta terminata la sostituzione del controller. Utilizzare `save storageArray keyManagementCertificate` Comando CLI per salvare i certificati. Eseguire il comando due volte, una volta con il `certificateType` parametro impostato su `client`e l'altro con il parametro impostato su `server`. c. Esportare il file della chiave di sicurezza interna in una posizione nota sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Utilizzare `export storageArray securityKey` Comando CLI. Specificare la password associata alla chiave di sicurezza e la posizione in cui si desidera salvarla.
Gestione esterna delle chiavi, dischi parziali bloccati	Non sono necessari ulteriori passaggi.

> Lo storage array deve essere in uno stato ottimale per recuperare i certificati client e server. Se i certificati non sono recuperabili, è necessario creare una nuova CSR, ottenere la firma CSR e scaricare il certificato del server dal server di gestione delle chiavi esterno (EKMS).

3. Annotare il numero di serie dell'array di storage:
   a. Da System Manager, selezionare **Support › Support Center › scheda Support Resources**.
   b. Scorrere fino a **Launch Detailed storage array information**, quindi selezionare **Storage Array Profile**.

      Il report viene visualizzato sullo schermo.

   c. Per individuare il numero di serie dello chassis sotto il profilo dello storage array, digitare **numero di serie** nella casella di testo **trova**, quindi fare clic su **trova**.

      Vengono evidenziati tutti i termini corrispondenti. Per scorrere tutti i risultati uno alla volta, continuare a fare clic su **Find** (trova).

   d. Annotare il `Chassis Serial Number`.

Questo numero di serie è necessario per eseguire le operazioni descritte in "Aggiornamento completo del controller".

4. Raccogliere i dati di supporto relativi allo storage array utilizzando la GUI o la CLI:
   - Utilizzare System Manager o Array Management Window in Storage Manager per raccogliere e salvare un bundle di supporto dello storage array.
     - Da System Manager, selezionare **Support › Support Center › scheda Diagnostics**. Quindi selezionare **Collect Support Data** e fare clic su **Collect**.
     - Dalla barra degli strumenti della finestra Array Management (Gestione array), selezionare **Monitor › Health › Collect Support Data Manually** (Monitor[Salute > Collect Support Data Manually]). Quindi, immettere un nome e specificare una posizione nel sistema in cui si desidera memorizzare il bundle di supporto.

       Il file viene salvato nella cartella Download del browser con il nome `support-data.7z`.

   Se lo shelf contiene cassetti, i dati di diagnostica per lo shelf vengono archiviati in un file separato con zip denominato `tray-component-state-capture.7z`.

   - Utilizzare l'interfaccia CLI per eseguire `save storageArray supportData` per raccogliere dati di supporto completi sull'array di storage.
5. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi:
   a. Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   b. Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   c. Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

6. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
7. Se si utilizza il mirroring asincrono o sincrono, eliminare le coppie mirrorate e disattivare le relazioni di mirroring tramite System Manager o la finestra Array Management.
8. Se un volume con thin provisioning viene segnalato all'host come un thin volume e il vecchio array esegue un firmware (firmware 8.25 o superiore) che supporta la funzione UNMAP, disattivare Write Back Caching per tutti i thin volumi:
   a. Da System Manager, selezionare **Storage › Volumes** (Storage[volumi]).
   b. Selezionare un volume qualsiasi, quindi **More › Change cache settings** (Altro[Modifica impostazioni cache]).

      Viene visualizzata la finestra di dialogo Change cache Setting (Modifica impostazioni cache). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

c. Selezionare la scheda **Basic** e modificare le impostazioni per il caching in lettura e il caching in scrittura.

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

e. Attendere cinque minuti per consentire il trasferimento dei dati presenti nella memoria cache sul disco.

9. Se il linguaggio SAML (Security Assertion Markup Language) è attivato sul controller, contattare il supporto tecnico per disattivare l'autenticazione SAML.

> Una volta attivato, SAML non può essere disattivato tramite l'interfaccia di Gestione di sistema di SANtricity. Per disattivare la configurazione SAML, contattare il supporto tecnico per assistenza.

10. Attendere il completamento di tutte le operazioni in corso prima di passare alla fase successiva.

    a. Dalla pagina **Home** di System Manager, selezionare **View Operations in Progress** (Visualizza operazioni in corso).

    b. Prima di continuare, assicurarsi che tutte le operazioni visualizzate nella finestra **operazioni in corso** siano state completate.

11. Spegnere il vassoio del disco del controller

    Attendere che tutti i LED sul vassoio del disco del controller si spenano.

12. Spegnere tutti i vassoi delle unità collegati al vassoio del disco del controller

    Attendere due minuti affinché tutti i dischi si rallentino.

Quali sono le prossime novità?

Passare a. "Rimuovere i controller".

Rimuovere i controller

Una volta completata la preparazione per l'aggiornamento, è possibile rimuovere i controller e, se necessario, rimuovere la batteria.

Fase 1: Rimuovere il controller

Rimuovere il contenitore del controller in modo da poterlo aggiornare con uno nuovo. Scollegare tutti i cavi e rimuovere eventuali ricetrasmettitori SFP. Quindi, far scorrere il contenitore del controller fuori dallo shelf del controller.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un braccialetto ESD o adottare altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.

A proposito di questa attività

Per ciascun controller nel vassoio del disco del controller, procedere come segue

Se si stanno aggiornando i controller in un vassoio del disco del controller duplex, ripetere tutti i passi per rimuovere il secondo contenitore del controller.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al vecchio contenitore del controller. A seconda della configurazione HIC, potrebbe essere possibile ricollegare alcuni cavi dopo aver sostituito il contenitore del controller.
3. Scollegare tutti i cavi di interfaccia ed Ethernet dal vecchio contenitore del controller.

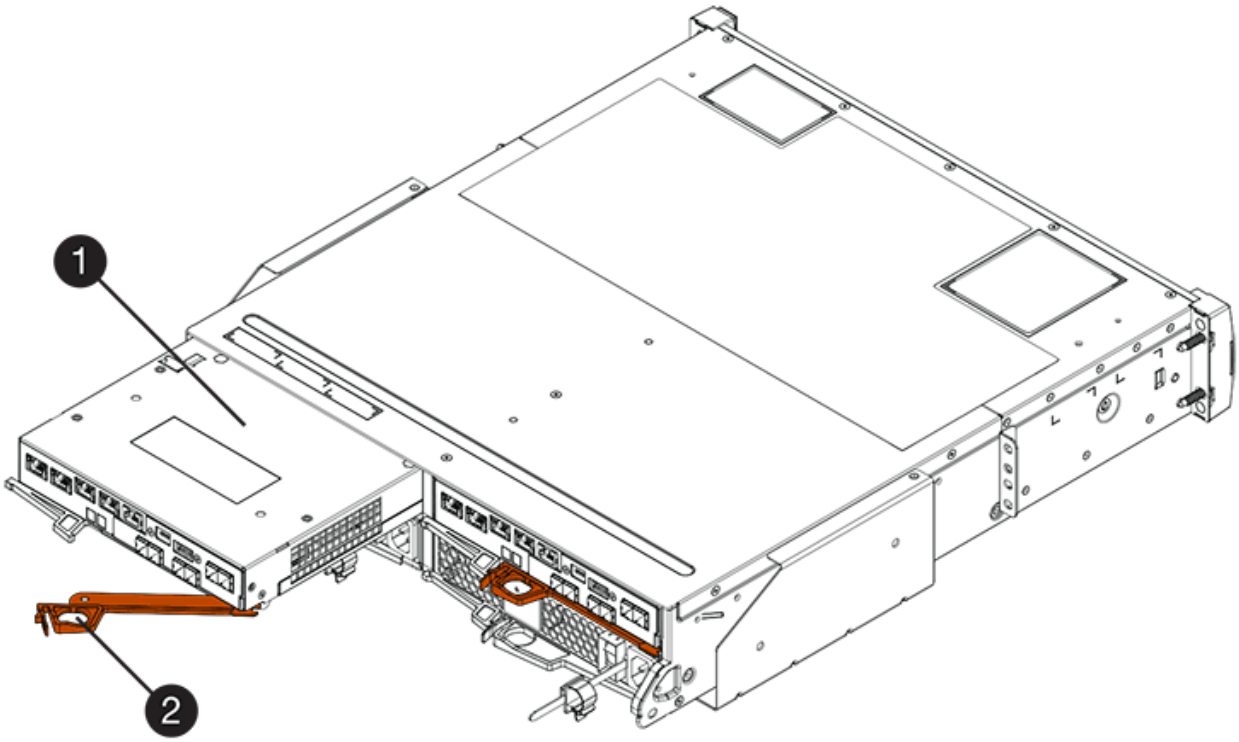
   Se sono presenti cavi in fibra ottica, è possibile utilizzare le due leve di rilascio per rimuovere parzialmente il contenitore del controller. L'apertura di queste leve di rilascio facilita la pressione verso il basso della linguetta di rilascio del cavo in fibra ottica.

   ! Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se il vecchio contenitore del controller contiene un HIC Fibre Channel o un HIC InfiniBand, rimuovere i ricetrasmettitori SFP+ (Small Form-factor Pluggable) (per Fibre Channel) o Quad SFP (QSFP+) (per InfiniBand) dall'HIC e conservarli per un eventuale riutilizzo.
5. Rimuovere il controller A.

   a. Sbloccare e ruotare verso l'esterno le maniglie di rilascio per rilasciare il contenitore del controller.
   b. Utilizzando le maniglie di rilascio e le mani, estrarre il contenitore del controller dal vassoio del disco del controller

      La figura seguente mostra un esempio della posizione generale delle maniglie di rilascio sui modelli di controller. Gli shelf dei controller e i vassoi dei dischi controller hanno una configurazione simile per le maniglie di rilascio.



(1) *contenitore controller*

(2) *maniglia della camma*

6. Posizionare il vecchio contenitore del controller su una superficie piana e priva di elettricità statica vicino al vassoio del disco del controller con le leve di rilascio verso l'alto. Posizionare il contenitore del controller in modo da poter accedere al coperchio superiore.
7. (Condizionale) se si stanno aggiornando i controller in un vassoio del disco del controller duplex, ripetere tutti i passaggi per rimuovere il secondo contenitore del controller.

Se si intende utilizzare la batteria del vecchio controller nel nuovo controller, passare alla parte successiva della sezione; in caso contrario, passare a. "Installare nuovi controller".

Fase 2: Rimuovere la batteria

Rimuovere la batteria solo se si intende utilizzare la batteria dal vecchio contenitore del controller nel nuovo contenitore del controller.

Fasi

1. Premere verso il basso entrambi i pulsanti del dispositivo di chiusura del coperchio superiore sul vecchio contenitore del controller e far scorrere il coperchio superiore verso la parte posteriore del contenitore.
2. Eseguire una delle seguenti opzioni, a seconda del modello di vassoio del controller, per rilasciare la vecchia batteria:
   - Per il controller-drive E2600 o E2700, svitare la vite ad alette che fissa la batteria al contenitore del controller.
   - Per E5400, EF540, E5500, EF550, E5600, O EF600, rilasciare la linguetta che fissa la batteria al contenitore del controller.
3. Rimuovere la batteria facendola scorrere verso la parte posteriore del vecchio contenitore del controller.

Quali sono le prossime novità?

Passare a. "Installare nuovi controller".

Installare nuovi controller

Dopo aver rimosso i vecchi controller, è possibile installare nuovi controller nel vassoio del disco del controller

A proposito di questa attività

Per ciascun controller nel vassoio del disco del controller, procedere come segue Se si stanno aggiornando i controller in un vassoio del controller duplex, ripetere tutti i passi per installare il secondo contenitore del controller.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un braccialetto ESD o adottare altre precauzioni antistatiche.
- Una batteria dal contenitore del controller originale o una nuova batteria ordinata.
- Il nuovo contenitore del controller.

Fase 1: Installare la batteria

Installare la batteria rimossa dal contenitore del controller originale o una nuova batteria ordinata.

Fasi

1. Disimballare il nuovo contenitore del controller e riutilizzarlo su una superficie piana e priva di scariche elettrostatiche, in modo che il coperchio rimovibile sia rivolto verso l'alto.
2. Premere il pulsante del coperchio verso il basso ed estrarre il coperchio.
3. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
4. A seconda del modello di controller in uso, effettuare una delle seguenti operazioni:
   - Per i modelli di controller E2600 o E2700:
     i. Inserire la scheda del circuito della batteria facendola scorrere verso la parte anteriore del nuovo contenitore del controller.
     ii. Serrare la vite a testa zigrinata per fissare la scheda del circuito della batteria nella nuova scheda del contenitore del controller.
     iii. Reinstallare il coperchio superiore sul nuovo contenitore del controller facendolo scorrere in avanti fino a quando i coperchi del dispositivo di chiusura superiore non scattano.

     Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.
   - Per altri modelli di controller:
     i. Inserire la batteria nel nuovo contenitore del controller.

     Far scorrere la batteria nel contenitore, assicurandosi che rimanga sotto i rivetti sulla parete del nuovo contenitore.

     ii. Mantenendo la maniglia di bloccaggio a un angolo di 45 gradi, allineare i connettori sul fondo della batteria con i connettori sul contenitore.
     iii. Spingere la batteria verso il basso fino a udire uno scatto, quindi spostare la maniglia di blocco verso l'alto per fissare la batteria del controller al contenitore del controller.

     > Per assicurarsi che la batteria del controller sia inserita correttamente nel vassoio del controller E5XX, potrebbe essere necessario farla scorrere verso l'esterno e reinserirla. È sicuro quando si sente scattare in posizione e quando la maniglia di blocco non si sposta dalla posizione verticale quando si muove.

     iv. Reinstallare il coperchio superiore sul nuovo contenitore del controller facendolo scorrere in avanti fino a quando i coperchi del dispositivo di chiusura superiore non scattano.

     Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.
5. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

Fase 2: Installare il nuovo contenitore del controller

Installare il nuovo contenitore del controller nello shelf del controller.

Fasi

1. Far scorrere completamente il nuovo contenitore del controller nel vassoio del disco del controller Ruotare le leve di rilascio verso il centro del contenitore del controller per bloccarlo in posizione.
2. Se il nuovo contenitore del controller dispone di un HIC Fibre Channel o di un HIC InfiniBand, installare i

ricetrasmettitori SFP+ (Fibre Channel) o QSFP+ (InfiniBand) nel contenitore del controller e ricollegare i cavi host.

A seconda dell'HICS coinvolto nell'aggiornamento, potrebbe essere possibile riutilizzare il ricetrasmettitore SFP+ o i ricetrasmettitori QSFP+ rimossi dal vecchio contenitore del controller.

3. Ricollegare tutti i cavi tra il vassoio del disco del controller e i vassoi dell'unità.

   Se la configurazione del cablaggio dell'unità è identica a quella dei vecchi controller, utilizzare le etichette collegate ai cavi per ricollegare correttamente i cavi.

   > Se si esegue l'aggiornamento ai controller E2700 da un modello precedente, la configurazione del cablaggio delle unità potrebbe essere diversa da quella utilizzata per i controller precedenti.

Quali sono le prossime novità?

Se si stanno aggiornando i controller E2800 e E5700 e la funzione Drive Security è attivata, visitare il sito Web "Sbloccare i dischi". In caso contrario, passare a. "Aggiornamento completo del controller".

Sbloccare i dischi

Se si aggiornano i controller E2800 e E5700, la funzione Drive Security di questi controller blocca i dischi in parte, esternamente o internamente. Se la funzione Drive Security è attivata, è necessario sbloccare manualmente queste unità.

Seguire la procedura appropriata per:

- Gestione interna delle chiavi
- Gestione esterna delle chiavi

Gestione interna delle chiavi

Seguire questi passaggi per la gestione interna delle chiavi quando tutti i dischi sono bloccati.

A proposito di questa attività

I controller appena scambiati si bloccano con un codice di visualizzazione a sette segmenti **L5**. Questo blocco si verifica quando nessun disco può eseguire la sincronizzazione con codice automatico (ACS). Una volta importata la chiave di sicurezza, ACS riprende e aggiorna i nuovi controller.

> Se non si utilizza la porta di gestione 1, provare con altri indirizzi IP predefiniti: + Ctrl A port 1: 192.168.128.101 + Ctrl A port 2: 192.168.128.102 + Ctrl B port 1: 192.168.129.101 + Ctrl B port 2: 192.168.129.102

Fasi

1. Effettuare una connessione ethernet diretta e privata tra lo storage array e il laptop o PC del client SANtricity. A tale scopo:
   a. Utilizzare un cavo ethernet RJ45 per collegare il laptop alla porta di gestione 1 del controller A.
   b. Per completare la connessione, potrebbe essere necessario assegnare il portatile a un indirizzo IP nella stessa sottorete del controller A. Durante il blocco del controller, il controller A utilizza per impostazione predefinita un indirizzo di gestione 192.168.128.101. In questo modo, è possibile

assegnare il portatile a una subnet come "192.168.128.201".

2. Utilizzando l'indirizzo IP 192.168.128.101 con nome utente **admin** e la password vuota, importare la chiave interna utilizzando `import storageArray securityKey file` Comando CLI, con la chiave di sicurezza salvata da "Preparazione per l'aggiornamento dei controller". Per informazioni sull'utilizzo di questo comando, vedere "Riferimento all'interfaccia della riga di comando".

   Esempio: `SMcli 192.168.128.101 -u admin -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

   In alternativa, è possibile importare la chiave interna tramite l'API REST tramite la seguente chiamata: `/storage-systems/{system-id}/security-key/import`

I controller proseguiranno con il processo di sincronizzazione del codice automatico dai dischi e si riavvieranno. Dopo il riavvio, i controller saranno accessibili attraverso la configurazione IP originale.

Gestione esterna delle chiavi

Seguire questi passaggi per la gestione delle chiavi esterne quando tutti i dischi sono bloccati.

A proposito di questa attività

I controller appena scambiati si bloccano con un codice di visualizzazione a sette segmenti **L5**. Questo blocco si verifica quando nessun disco può eseguire la sincronizzazione con codice automatico (ACS). Una volta importata la chiave di sicurezza, ACS riprende e aggiorna i nuovi controller.

> Lo storage array deve essere in uno stato ottimale per recuperare i certificati client e server. Se i certificati non sono recuperabili, è necessario creare una nuova richiesta di firma del certificato (CSR) e importare il certificato del server dal server di gestione delle chiavi esterno.

Fasi

1. Effettuare una connessione ethernet diretta e privata tra lo storage array e il laptop o PC del client SANtricity. A tale scopo:
   a. Utilizzare un cavo ethernet RJ45 per collegare il laptop alla porta di gestione 1 del controller A.
   b. Per completare la connessione, potrebbe essere necessario assegnare il portatile a un indirizzo IP nella stessa sottorete del controller A. Durante il blocco del controller, il controller A utilizza per impostazione predefinita un indirizzo di gestione 192.168.128.101. In questo modo, è possibile assegnare il portatile a una subnet come "192.168.128.201".
2. Utilizzando l'indirizzo IP predefinito 192.168.128.101 con nome utente **admin** e la password vuota, configurare il server di gestione delle chiavi esterno utilizzando `set storageArray externalKeyManagement` CLI e fornire il comando `serverAddress` e. `serverPort` salvato da "Preparazione per l'aggiornamento dei controller". Per informazioni sull'utilizzo di questo comando, vedere "Riferimento all'interfaccia della riga di comando".

   Esempio: `SMcli 192.168.128.101 -u admin -c "set storageArray externalKeyManagement serverAddress=<ServerIPAddress> serverPort=<serverPort>;"`

   In alternativa, è possibile configurare il server di gestione delle chiavi esterno tramite l'API REST tramite la seguente chiamata: `/storage-systems/{system-id}/external-key-server`

3. Utilizzando l'indirizzo IP predefinito 192.168.128.101 con il nome utente **admin** e la password vuota, importare i certificati utilizzando `storageArray keyManagementCertificate` Comando CLI: Una

volta per il certificato client e una seconda per il certificato server.

Esempio A: `SMcli 192.168.128.101 -u admin -c "download storageArray keyManagementCertificate certificateType=client file=\"Directory&FileName\";"`

Esempio B: `SMcli 192.168.128.101 -u admin -c "download storageArray keyManagementCertificate certificateType=server file=\"Directory&FileName\";"`

In alternativa, è possibile importare il certificato del keyserver tramite l'API REST tramite la seguente chiamata: `/storage-systems/{system-id}/external-key-server/certificate`

4. Utilizzando la chiave di sicurezza salvata da "Preparazione per l'aggiornamento dei controller", Importare la chiave esterna nell'indirizzo IP 192.168.128.101 con il nome utente **admin** e la password che rimane vuota.

   Esempio: `SMcli 192.168.128.101 -u admin -c "import storageArray securityKey file=\"Directory&FileName\" passPhrase=\"passPhraseString\";"`

   In alternativa, è possibile importare la chiave esterna tramite l'API REST tramite la seguente chiamata: `/storage-systems/{system-id}/security-key/import`

I controller proseguiranno con il processo di sincronizzazione del codice automatico dai dischi e si riavvieranno. Dopo il riavvio, i controller saranno accessibili attraverso la configurazione IP originale.

Aggiornamento completo del controller

Completare l'aggiornamento del controller accendendo lo shelf del controller e convalidando la versione del software del controller. Quindi, è possibile raccogliere i dati di supporto e riprendere le operazioni.

Se si stanno aggiornando i controller in un vassoio del disco del controller duplex, ripetere tutti i passi per completare l'aggiornamento del secondo controller.

Fase 1: Accendere il controller

Accendere lo shelf del controller per verificare che funzioni correttamente.

Fasi

1. Accendere l'interruttore di alimentazione situato sul retro di ciascun vassoio dell'unità collegato al vassoio del disco del controller
2. Attendere due minuti per consentire l'accelerazione delle unità.
3. Accendere l'interruttore di alimentazione sul retro del vassoio del disco del controller
4. Attendere tre minuti per il completamento del processo di accensione.
5. Se si sta eseguendo una sostituzione completa del controller per i controller E2800 o E5700, procedere con una delle seguenti procedure in base allo scenario di sicurezza del disco.

Tipo completo di sostituzione del controller	Procedura e prerequisiti
Tutti i dischi non protetti, né la gestione delle chiavi interna o esterna	Passare alla fase successiva.

Tipo completo di sostituzione del controller	Procedura e prerequisiti
Combinazione di dischi protetti e non protetti, gestione interna delle chiavi	Per sbloccare le unità protette, è necessario innanzitutto creare una chiave di sicurezza interna e importarla manualmente. Una volta sbloccati i dischi, è possibile accedervi. a. Creare una chiave di sicurezza interna b. Swap del controller con gestione interna delle chiavi e una o più unità protette c. Eseguire il comando SMclient, `set allDrives nativeState`. d. Attendere il riavvio di entrambi i controller.
Tutti i dischi protetti, gestione interna delle chiavi	Swap del controller con gestione interna delle chiavi e una o più unità protette
Combinazione di dischi protetti e non protetti, External Key Management	Passare alla fase successiva. Dopo aver sostituito il controller, i controller si risincronizzano automaticamente con il server di gestione delle chiavi esterne e i dischi si sbloccano e sono accessibili. Se si riceve un codice di blocco del display a sette segmenti di `L5` dopo aver sostituito un controller di dischi misti protetti con la gestione interna delle chiavi, contattare il supporto tecnico.
Tutti i dischi protetti, Gestione delle chiavi esterne, si è temporaneamente tornati alla gestione delle chiavi interne per la procedura di sostituzione del controller	È necessario prima sbloccare le unità protette utilizzando la procedura di gestione delle chiavi interne. Una volta sbloccati i dischi, si torna alla gestione delle chiavi esterne creando una nuova chiave di sicurezza esterna per lo storage array. a. Swap del controller con gestione interna delle chiavi e una o più unità protette b. Creare una chiave di sicurezza esterna c. Eseguire il comando SMclient, `set allDrives nativeState`. d. Attendere il riavvio di entrambi i controller.
Tutti i dischi protetti, Gestione delle chiavi esterne, non si è temporaneamente passati alla gestione delle chiavi interne per la procedura di sostituzione del controller	Swap del controller con gestione esterna delle chiavi e protezione di tutti i dischi

Fase 2: Controllare lo stato dei controller e dei vassoi

È possibile utilizzare i LED e il software di gestione dello storage per controllare lo stato dei controller e dei vassoi.

Fasi

1. Controllare i LED sul controller A per assicurarsi che sia in fase di avvio corretta.

   I LED host link Service Action Required diventano verdi durante il riavvio. Il display a sette segmenti mostra la sequenza OS+ SD+ vuoto- per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day).

   Una volta completato correttamente il riavvio del controller, il display a sette segmenti mostra l'ID del vassoio corrispondente al display a sette segmenti sul secondo controller. È quindi possibile scoprire il nuovo contenitore del controller utilizzando il software di gestione dello storage.

2. Se uno dei LED Service Action Required (azione di servizio richiesta) del vassoio del disco del controller è *ON*, o se il LED Controller Service Action Required (azione di servizio del controller richiesta) è *ON*:
   a. Verificare che il contenitore del controller sia stato installato correttamente e che tutti i cavi siano inseriti correttamente. Reinstallare il contenitore del controller, se necessario.
   b. Controllare di nuovo i LED Service Action Required (azione di servizio richiesta) del vassoio del controller e il LED Controller Service Action Required (azione di servizio richiesta del controller). Se il problema non viene risolto, contattare il supporto tecnico.
3. Per una configurazione duplex, ripetere i passi da 1 a 2 per il controller B.
4. Utilizzando i LED e il software di gestione dello storage, controllare lo stato di tutti i vassoi dello storage array. Se uno dei componenti ha uno stato di intervento richiesto, utilizzare Recovery Guru per la risoluzione dei problemi. Se il problema non viene risolto, contattare il supporto tecnico.

Fase 3: Convalidare la versione del software del controller

È necessario assicurarsi che i nuovi controller siano in esecuzione con IL sistema operativo (firmware del controller) corretto e CON NVSRAM.

Fasi

1. Effettuare una delle seguenti operazioni:
   - Se si esegue l'aggiornamento a controller che non supportano SANtricity 11.30 e il firmware del controller 8.30, assicurarsi che la versione in esecuzione sui nuovi controller corrisponda alla versione eseguita per ultima sui controller originali. Normalmente, questa sarà la versione più recente supportata dai vecchi controller. Se necessario, installare la versione appropriata sui nuovi controller.
   - Se si esegue l'aggiornamento ai controller che eseguono SANtricity 11.30 e il firmware del controller 8.30, scaricare e installare L'ULTIMA VERSIONE DI NVSRAM dopo l'accensione dei nuovi controller.
2. Se l'aggiornamento del controller comporta una modifica del protocollo (ad esempio, da Fibre Channel a iSCSI) e si dispone già di host definiti per lo storage array, associare le nuove porte host agli host:
   a. Da System Manager, selezionare **Storage › Hosts** (Storage[host]).
   b. Selezionare l'host a cui associare le porte, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

      Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti dell'host.

   c. Fare clic sulla scheda **host Ports** (Porte host).

La finestra di dialogo mostra gli identificatori di porta host correnti.

d. Per aggiornare le informazioni relative all'identificatore della porta host associate a ciascun host, sostituire gli ID della porta host dei vecchi adattatori host con i nuovi ID della porta host per il nuovo adattatore host.

e. Ripetere il passaggio d per ciascun host.

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

Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" e a. "NetApp Hardware Universe".

3. Se la cache write-back è stata disattivata per tutti i volumi thin durante la preparazione per lo scambio di risorse, riattivare la cache write-back.

   a. Da System Manager, selezionare **Storage › Volumes** (Storage[volumi]).

   b. Selezionare un volume qualsiasi, quindi **More › Change cache settings** (Altro[Modifica impostazioni cache]).

      Viene visualizzata la finestra di dialogo Change cache Setting (Modifica impostazioni cache). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

   c. Selezionare la scheda **Basic** e modificare le impostazioni per il caching in lettura e il caching in scrittura.

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

4. Se SAML è stato disattivato durante la preparazione per lo swapping, riattivare SAML.

   a. Da System Manager, selezionare **Impostazioni › Gestione accessi**.

   b. Selezionare la scheda **SAML**, quindi seguire le istruzioni sulla pagina.

5. Raccogliere i dati di supporto relativi allo storage array utilizzando la GUI o la CLI:

   - Utilizzare System Manager o Array Management Window di Storage Manager per raccogliere e salvare un bundle di supporto per lo storage array.

     - Da System Manager, selezionare **Support › Support Center › scheda Diagnostics**. Quindi selezionare **Collect Support Data** e fare clic su **Collect**.

     - Dalla barra degli strumenti della finestra Array Management (Gestione array), selezionare **Monitor › Health › Collect Support Data Manually** (Monitor[Salute > Collect Support Data Manually]). Quindi, immettere un nome e specificare una posizione nel sistema in cui si desidera memorizzare il bundle di supporto.

       Il file viene salvato nella cartella Download del browser con il nome `support-data.7z`.

   Se lo shelf contiene cassetti, i dati di diagnostica per lo shelf vengono archiviati in un file separato con zip denominato `tray-component-state-capture.7z`

   - Utilizzare l'interfaccia CLI per eseguire `save storageArray supportData` per raccogliere dati di supporto completi sull'array di storage.

     > La raccolta dei dati di supporto può influire temporaneamente sulle performance dello storage array.

6. Avvisare il supporto tecnico NetApp delle modifiche apportate alla configurazione dello storage array.

a. Ottenere il numero di serie del vassoio del disco del controller registrato Preparazione per l'aggiornamento dei controller.

b. Accedere al sito di supporto NetApp all'indirizzo "mysupport.netapp.com/eservice/assistant".

c. Selezionare **Product Registration** (registrazione prodotto) dall'elenco a discesa sotto **Category 1** (Categoria 1).

d. Inserire il seguente testo nella casella di testo **commenti**, sostituendo il numero di serie del vassoio del controller con il numero di serie:

```
Please create alert against Serial Number: serial number. The alert name
should be "E-Series Upgrade". The alert text should read as follows:
```

```
"Attention: The controllers in this system have been upgraded from the
original configuration. Verify the controller configuration before ordering
replacement controllers and notify dispatch that the system has been
upgraded."
```

a. Fare clic sul pulsante **Invia** nella parte inferiore del modulo.

Quali sono le prossime novità?

Se l'aggiornamento del controller comporta la modifica dell'ID vendor da LSI a NETAPP, visitare il sito Web "Rimontare i volumi dopo aver cambiato il vendor da LSI a NETAPP"; in caso contrario, l'aggiornamento del controller è completo ed è possibile riprendere le normali operazioni.

Rimontare i volumi dopo aver cambiato il vendor da LSI a NETAPP

Se l'aggiornamento del controller comporta la modifica dell'ID vendor da LSI a NETAPP, seguire la procedura appropriata per il tipo di host:

- Rimontare i volumi su un host AIX
- Rimontare i volumi su un host VMware
- Rimontare i volumi su un host Windows

Rimontare i volumi su un host AIX

Dopo aver sostituito i controller, è possibile osservare che l'host mostra i nuovi volumi sull'array di storage, ma mostra anche i volumi originali come guasti.

Fase

Se vengono visualizzati volumi guasti, eseguire `cfgmgr` comando.

Rimontare i volumi su un host VMware

Dopo aver sostituito i controller, si potrebbero osservare le seguenti condizioni:

- VMware mostra nuovi percorsi per i volumi sull'array di storage, ma mostra anche i percorsi originali come percorsi morti.
- Gli host elencano ancora i volumi sull'array di storage come se disponessi di ID vendor LSI. Questo potrebbe verificarsi quando i volumi sono stati rivendicati dalla regola LSI all'inizio e quindi continuano a utilizzare la stessa regola LSI quando i volumi tornano in linea.

- Il nome visualizzato non riflette la modifica da LSI a NetApp. Questo potrebbe verificarsi perché il nome visualizzato è diventato test libero dopo il rilevamento iniziale. In questo caso, è possibile modificare manualmente il nome visualizzato.

Fasi

1. Eseguire una nuova scansione su ciascun host.
2. Arrestare tutte le operazioni di i/o host per questo sottosistema.
3. Recuperare i volumi in base alla regola NetApp.
   a. Eseguire `esxcli storage core device list` comando. Controllare l'output del comando per identificare i volumi i cui nomi hanno il form `aa.xxxx`.
   b. Eseguire il comando `do esxcli storage core claiming reclaim -d naa.xxxxx` Per modificare l'ID vendor LSI in NetApp.

Rimontare i volumi su un host Windows

Dopo aver sostituito i controller, è necessario eseguire il remount dei volumi su un host Windows per consentire agli host collegati di eseguire operazioni di i/o con i volumi posizionati sull'array di storage aggiornato.

Fasi

1. In **Gestione periferiche**, selezionare **Mostra periferiche nascoste**.
2. Per ogni dispositivo SCSI NETAPP elencato in **Gestione periferiche**, fare clic con il pulsante destro del mouse sulla voce e selezionare **Disinstalla**.

   Se Windows visualizza una finestra di dialogo con un messaggio che indica che è necessario riavviare l'host, completare la disinstallazione di tutti i volumi prima di eseguire la scansione per l'hardware e riavviare.

3. Fare clic con il pulsante destro del mouse in **Gestione periferiche**, quindi selezionare **Cerca modifiche hardware**.
4. Riavviare l'host.

Riconfigurare un sistema SAS-2 dietro un nuovo shelf di controller SAS-3

Se necessario, è possibile riconfigurare il sistema SAS-2 in modo da utilizzarlo dietro un nuovo shelf di controller SAS-3.

Gli array SAS-2 approvati includono E2700, E550/EF5500 e E5600/EF560. Gli shelf di dischi SAS-2 approvati includono DE1600, DE5600 e DE6600. Gli array SAS-3 approvati includono E2800 e E5700/EF570. Gli shelf di dischi SAS-3 approvati includono DE212C, DE224C e DE460C.

A proposito di questa attività

In questa procedura, è possibile convertire lo shelf del controller in un array SAS-2 approvato in uno shelf di dischi, quindi posizionarlo dietro un nuovo array SAS-3 e shelf di dischi approvati, senza preservarne i dati.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

Prima di iniziare

A causa della complessità di questa procedura, è necessario quanto segue:

- È necessario disporre di una funzione FPVR (Feature Product Variance Request). Per archiviare un FPVR, contatta i NetApp Professional Services.

> La mancata acquisizione di un FPVR prima di tentare questa procedura può causare un guasto al disco e il blocco del controller.

- Se sei in grado di eseguire il backup dei dati, puoi eseguire questa procedura senza l'assistenza dei NetApp Professional Services.
- Se non è possibile eseguire il backup dei dati, contattare i NetApp Professional Services per assistenza con questa procedura.
- Assicurarsi che entrambi gli array siano pronti per la procedura:
  - **Array esistente**: Array esistente con sistema operativo SANtricity 8.25 o successivo alimentato.
  - **Nuovo array**: Nuovo array decompresso e spento.
- Annotare il numero di serie dello shelf del controller SAS-2 che si desidera convertire in uno shelf di dischi.

Fase 1: Spegnere i controller (conservazione non dei dati)

Prima di spegnere i controller, è necessario arrestare tutte le operazioni.

Fasi

1. Se l'array SAS-2 esistente è ancora accessibile, eliminare tutti i gruppi di volumi, spegnere entrambi i controller e rimuovere tutti i cavi.
2. Annotare il numero di serie dello shelf del controller SAS-2 che si desidera convertire in uno shelf di dischi.
3. Se la protezione del disco è in uso per l'array esistente, assicurarsi che la chiave di sicurezza sia disponibile.

Fase 2: Installazione dei controller (non conservazione dei dati)

Una volta arrestati correttamente, è possibile sostituire i controller nell'array.

Fasi

1. Sostituire entrambi i controller nell'array esistente con IOM o ESM.
2. Se possibile, utilizzare i cavi host e i cavi di rete dell'array esistente e collegarli ai controller del nuovo array.

   > A seconda delle connessioni host del nuovo array, potrebbero essere necessari cavi diversi.

3. Collegare gli shelf di dischi dietro i controller del nuovo array.

   Il vassoio del controller e gli eventuali vassoi del disco collegati diventano shelf di dischi e possono essere collegati ai controller del nuovo array.

   > Il collegamento di SAS-2 a SAS-3 richiede cavi SAS da HD a mini SAS. Per informazioni più dettagliate sui cavi per la configurazione del controller e dello shelf di espansione, fare riferimento a. "Cablaggio" o il "Guida al cablaggio hardware e-Series".

Fase 3: Accensione dei controller (conservazione non dei dati)

Al termine dell'installazione, accendere i controller e inviare le modifiche di configurazione al supporto tecnico NetApp.

Fasi

1. Accendere il nuovo array, inclusi gli shelf di dischi collegati.
2. Configurare la porta di gestione e gli indirizzi IP installando "Connessione rapida SANtricity" utility.
3. Se la protezione del disco era in uso sull'array esistente, importare la chiave di sicurezza.
4. Se non è stato possibile eliminare i gruppi di volumi dall'array esistente prima di eseguire questa procedura, è necessario impostare tutti i dischi esterni in modo che appaiano come nativi. Per informazioni dettagliate su come impostare i dischi su nativi, consultare la Guida in linea di SANtricity.
5. Inviare le modifiche alla configurazione al supporto tecnico NetApp.
   a. Ottenere il numero di serie del vecchio vassoio del disco del controller registrato nella fase 2.
   b. Accedere a. "Sito di supporto NetApp".
   c. Dall'elenco a discesa sotto **Categoria feedback**, selezionare **prodotti installati > richiesta di rimozione**.
   d. Selezionare **Crea caso**. Inserire il seguente testo nella casella di testo **Comments** (commenti), sostituendo il numero di serie del vassoio del controller con il numero di serie:

      ```
      Please decommission this serial number as the entitlement has been moved to
      another serial number in the system. Please reference this in the SN notes.
      ```

   e. Selezionare **Invia**.

Le modifiche di configurazione da SAS-2 a SAS-3 completate vengono inviate al supporto tecnico di NetApp.

Sistema operativo SANtricity

Panoramica sull'aggiornamento del sistema operativo SANtricity

È possibile aggiornare il sistema operativo e i componenti hardware del sistema alla versione più recente del software e del firmware SANtricity.

Queste procedure di aggiornamento includono istruzioni separate per quanto segue:

- Controller singolo — include procedure per l'aggiornamento del software dello storage array e, facoltativamente, del firmware IOM e della memoria ad accesso casuale statica non volatile (NVSRAM).
- Controller multipli — include procedure per l'aggiornamento del software SANtricity OS su più array di storage dello stesso tipo.
- Drive — include istruzioni per l'aggiornamento del firmware del disco.

Prima di iniziare l'aggiornamento, assicurarsi di esaminare il "Considerazioni sull'upgrade".

Considerazioni sull'upgrade

Per garantire un aggiornamento corretto, fare riferimento alle seguenti considerazioni sull'aggiornamento.

Upgrade del controller (singolo o multiplo)

Esaminare queste considerazioni principali prima di aggiornare i controller.

Versioni correnti

È possibile visualizzare le versioni correnti del software e del firmware, come indicato di seguito:

- Per un singolo controller, utilizzare l'interfaccia Gestore di sistema di SANtricity. Accedere al **Support › Upgrade Center**, quindi fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware).
- Per più controller, utilizzare l'interfaccia di gestione unificata di SANtricity. Accedere alla pagina **Manage** per gli array di storage rilevati. Le versioni sono indicate 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.

Componenti inclusi nell'aggiornamento

I seguenti componenti sono inclusi nel processo di aggiornamento del sistema operativo SANtricity:

- **System Manager** — System Manager è il software che gestisce lo storage array.
- **Controller firmware** — il firmware del controller gestisce l'i/o tra host e volumi.
- **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.

Componenti da aggiornare separatamente

I seguenti componenti devono essere aggiornati separatamente:

- **Controller NVSRAM** — Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller. Le istruzioni per l'aggiornamento DI NVSRAM sono incluse con le istruzioni per l'aggiornamento dei controller.
- **Firmware del disco** — vedere "Aggiornare il firmware del disco" per istruzioni separate.
- **Driver multipath/failover** — come parte del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover dell'host in modo che l'host possa interagire correttamente con i controller. Se gli host che eseguono sistemi operativi diversi da Microsoft Windows dispongono di connessioni i/o al sistema storage, aggiornare i driver multipath per tali host. Per informazioni sulla compatibilità, fare riferimento a. "Matrice di interoperabilità NetApp". Per istruzioni sull'aggiornamento, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".
- **Gestore unificato di SANtricity** — Gestore unificato è il software che gestisce più sistemi storage, inclusi i modelli E2800, E5700, EF300 e EF600. Unified Manager fa parte del proxy dei servizi Web di SANtricity, un server API RESTful installato separatamente su un sistema host per gestire centinaia di sistemi storage NetApp e-Series nuovi e legacy. Per ulteriori informazioni, vedere "Panoramica dei proxy dei servizi web SANtricity".
- **Utility** — altre utility di gestione richiedono aggiornamenti separati, come l'utility host Windows di SANtricity, l'utility host Linux di SANtricity e il DSM Windows di SANtricity. Per ulteriori informazioni su queste utility, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

- **Sistemi legacy** — se il sistema storage fa parte di una rete storage che include sistemi storage meno recenti, potrebbe essere necessario utilizzare la finestra di gestione aziendale (EMW) di SANtricity per fornire una vista aziendale di tutti i sistemi storage. In questo caso, verificare se è disponibile una versione di manutenzione più recente di Gestione storage SANtricity.

Doppi controller ed elaborazione i/O.

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.

Controllo dello stato di salute

Durante il processo di aggiornamento viene eseguito un controllo dello stato di salute. Questo controllo dello stato di salute 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.

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.

Aggiornamento del firmware del disco

Prima di aggiornare il firmware del disco, esaminare queste considerazioni principali.

Compatibilità dei dischi

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.

Metodi di aggiornamento del disco

Esistono due tipi di metodi di aggiornamento del firmware del disco: Online e offline.

Aggiornamento online	Upgrade offline
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.	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

Aggiornamento di software e firmware per un singolo controller

È possibile aggiornare un singolo controller, in modo da disporre di tutte le funzionalità e le correzioni più recenti.

Questo processo comporta l'aggiornamento del software dello storage array e, facoltativamente, del firmware IOM e della memoria ad accesso casuale statica non volatile (NVSRAM).

Prima di iniziare

- Revisione "Considerazioni sull'upgrade".
- Determinare se si desidera aggiornare il file NVSRAM del controller contemporaneamente al firmware del sistema operativo.

  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.

- Determinare 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).

- Decidere se 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.

Fase 1: Scaricare i file software dal sito di supporto

In questa fase, visita il sito del supporto NetApp per salvare i nuovi file software scaricabili del pacchetto (DLP) nel tuo sistema host di gestione.

Il tempo necessario per l'aggiornamento dipende dalla configurazione dello storage array e dai componenti che si stanno aggiornando.

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.

   > Se si esegue l'aggiornamento del sistema operativo SANtricity su un'appliance StorageGRID (ad esempio SG5612 o SG5760), è necessario interrompere l'attività di i/o posizionando l'appliance in modalità di manutenzione prima di continuare con questa procedura, altrimenti i dati potrebbero andare persi. Per informazioni dettagliate, consultare le istruzioni di installazione e manutenzione dell'appliance StorageGRID.

2. Dall'interfaccia di System Manager, selezionare **Support › Upgrade Center**.
3. Nell'area denominata "aggiornamento software del sistema operativo SANtricity", fare clic su **Download del sistema operativo NetApp SANtricity** per aprire il sito del supporto NetApp.

4. Dalla pagina Download, selezionare **Software controller OS SANtricity e-Series**.

> 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. Seguire le istruzioni a schermo per scaricare il software del sistema operativo più recente per il modello di controller in uso. Se si desidera aggiornare ANCHE NVSRAM, scaricare IL file NVSRAM per un singolo controller.

Fase 2: Trasferire i file software ai controller

In questa fase, i file software vengono trasferiti sul controller in modo da poter iniziare il processo di aggiornamento. I componenti vengono copiati dal client di gestione ai controller e collocati in un'area di staging nella memoria flash.

> **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. (Opzionale). Se si prevede di eseguire un aggiornamento durante una finestra di manutenzione specifica, potrebbe essere necessario eseguire un controllo dello stato di salute prima dell'aggiornamento per determinare in anticipo la presenza di problemi principali relativi agli array di storage. In tal caso, selezionare **controllo di stato pre-aggiornamento** dal Centro di aggiornamento in System Manager (**Support › Upgrade Center**) e seguire le istruzioni visualizzate sullo schermo. In caso contrario, è possibile saltare questo passaggio, poiché il processo di aggiornamento prevede un controllo dello stato di salute.
2. Se NON si desidera aggiornare il firmware IOM in questo momento, fare clic su **Sospendi sincronizzazione automatica IOM** e seguire le istruzioni nella finestra di dialogo.

   Se si dispone di uno storage array con un singolo controller, il firmware IOM non viene aggiornato.

3. Dal Centro aggiornamenti di Gestione sistemi, fare clic su **Avvia aggiornamento** da "aggiornamento software SANtricity OS".

   Viene visualizzata la finestra di dialogo Aggiorna software SANtricity OS.

4. 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 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.
5. (Facoltativo) 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).

6. 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.

7. (Facoltativo) per visualizzare un elenco degli aggiornamenti, fare clic su **Save Log** (Salva registro).

   Il file viene salvato nella cartella Download del browser con il nome, `drive_upgrade_log-timestamp.txt`.

Se i file software sono già stati attivati, visitare il sito Web Fase 4: Completare l'aggiornamento del software e del firmware; in caso contrario, passare a. Fase 3: Attivare i file software.

Fase 3: Attivare i file software

Seguire questa procedura solo se si dispone di software o firmware trasferiti ma non attivati. Per verificare questo stato, cercare una notifica nell'area Notifiche della home page di System Manager o nella pagina Upgrade Center.

Quando si esegue l'operazione di attivazione, il software e il firmware correnti vengono sostituiti con il nuovo software e firmware. Non è possibile interrompere il processo di attivazione dopo l'avvio.

Fasi

1. Dall'interfaccia di System Manager, selezionare **Support › Upgrade Center**.
2. Nell'area "aggiornamento software SANtricity OS", fare clic su **attiva** e confermare che si desidera eseguire l'operazione.
3. (Facoltativo) per visualizzare un elenco degli aggiornamenti, fare clic su **Save Log** (Salva registro).

   Il file viene salvato nella cartella Download del browser con il nome, `drive_upgrade_log-timestamp.txt`.

Fase 4: Completare l'aggiornamento del software e del firmware

Completare l'aggiornamento del software e del firmware verificando le versioni nella finestra di dialogo Software and firmware Inventory (inventario software e firmware).

Prima di iniziare

- È necessario aver attivato il software o il firmware.

Fasi

1. In System Manager, verificare che tutti i componenti siano visualizzati nella pagina hardware.
2. 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**).
3. 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.
4. Se durante la procedura di aggiornamento si verifica uno dei seguenti errori, eseguire l'azione consigliata appropriata.

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.

Se si verifica questo errore di download del firmware…	Quindi procedere come segue…
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.
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.
Configuration Database Validation (convalida del database di configurazione) (se supportata dalla versione del controller dello storage array)	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.

Quali sono le prossime novità?

L'aggiornamento del software del controller è stato completato. È possibile riprendere le normali operazioni.

Aggiornamento del software e del firmware per più controller

È possibile aggiornare più controller dello stesso tipo con Gestione unificata di SANtricity.

Prima di iniziare

- Revisione "Considerazioni sull'upgrade".
- Determinare 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.

- Prendere in esame le seguenti precauzioni:

> 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.

> Se si esegue l'aggiornamento del sistema operativo SANtricity su un'appliance StorageGRID (ad esempio SG5612 o SG5760), è necessario interrompere l'attività di i/o posizionando l'appliance in modalità di manutenzione prima di continuare con questa procedura, altrimenti i dati potrebbero andare persi. Per informazioni dettagliate, consultare le istruzioni di installazione e manutenzione dell'appliance StorageGRID.

Fase 1: 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. Aprire Unified Manager.
2. 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.

3. 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.
4. Selezionare le caselle di controllo relative ai sistemi storage che si desidera eseguire attraverso il controllo dello stato di salute.
5. Fare clic su **Start**.

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

6. 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.

Fase 2: Scaricare i file software dal sito di supporto

In questa fase, visita il sito del supporto NetApp per salvare i nuovi file software scaricabili del pacchetto (DLP) nel tuo sistema host di gestione.

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 di Unified Manager, selezionare **Gestisci**, quindi selezionare 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.

Fase 3: Trasferire i file software ai controller

Il file del software del sistema operativo SANtricity e IL file NVSRAM vengono caricati nel repository in modo che sia accessibile al Centro di aggiornamento di Unified Manager.

> 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. Dalla vista principale di Unified Manager, selezionare **Gestisci**, quindi selezionare uno o più array di storage da aggiornare.
2. Selezionare **Centro di aggiornamento › Aggiorna software SANtricity OS**.

   Viene visualizzata la pagina aggiornamento del software SANtricity OS.

3. 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.

4. 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.

5. 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**.
6. (Facoltativo) per trasferire il file software agli array di storage senza attivarli, selezionare la casella di controllo **trasferire il software del sistema operativo agli array di storage, contrassegnarlo come staged e attivarlo in un secondo momento**.
7. Fare clic su **Start**.
8. 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.
9. (Facoltativo) una volta completato l'aggiornamento, è possibile visualizzare un elenco degli aggiornamenti per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

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

Fase 4: Attivazione dei file software in fasi (opzionale)

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.

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

Fasi

1. Dalla vista principale di Unified Manager, selezionare **Gestisci**. Se necessario, fare clic sulla colonna Status (Stato) per ordinare tutti gli array di storage con lo stato "OS Upgrade (waiting activation)" (aggiornamento 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. (Facoltativo) una volta completata l'attivazione, è possibile visualizzare un elenco degli elementi attivati per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

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

Quali sono le prossime novità?

L'aggiornamento del software del controller è stato completato. È possibile riprendere le normali operazioni.

Aggiornare il firmware del disco

Seguire questa procedura per aggiornare il firmware dei dischi, che garantisce di disporre delle ultime funzionalità e correzioni.

Fase 1: Scaricare i file del firmware del disco

In questa fase, accedere al sito del supporto NetApp per scaricare i file del firmware del disco sul client di gestione.

Fasi

1. In Gestore di sistema di SANtricity, selezionare **supporto › Centro di aggiornamento**.
2. In aggiornamento del firmware del disco, fare clic su **NetApp Support** e accedere al sito NetApp Support.

3. Dal sito del supporto tecnico, fare clic sulla scheda **Downloads**, quindi selezionare **Disk Drive & firmware Matrix**.
4. Selezionare **e-Series e EF-Series Disk firmware.**
5. Seguire le istruzioni visualizzate sullo schermo per scaricare i file.

Fase 2: Avviare l'aggiornamento del firmware del disco

In questa fase, si aggiorna il firmware dei dischi.

Prima di iniziare

- 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.
- Assicurarsi che lo stato dello storage array sia ottimale.
- Assicurarsi che tutti i dischi abbiano uno stato ottimale.
- Assicurarsi che non siano 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. Dal System Manager Upgrade Center (**Support › Upgrade Center**), fare clic su **Begin Upgrade** nella sezione "Drive firmware upgrade".

   Viene visualizzata una finestra di dialogo che elenca i file del firmware del disco attualmente in uso.

2. Estrarre (decomprimere) i file scaricati dal sito del supporto.
3. 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.

4. 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 l'unità viene visualizzato nell'area delle informazioni **firmware proposto**. Se è necessario modificare il firmware, fare clic su **Indietro** per tornare alla finestra di dialogo precedente.

5. 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).

6. Nella prima colonna della tabella, selezionare il disco o i dischi che si desidera aggiornare.
7. 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.

8. (Facoltativo) per visualizzare un elenco degli aggiornamenti, fare clic su **Save Log** (Salva registro).

   Il file viene salvato nella cartella Download del browser con il nome `drive_upgrade_log-timestamp.txt`.

9. Se durante la procedura di aggiornamento si verifica uno dei seguenti errori, eseguire l'azione consigliata appropriata.

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.

Se si verifica questo errore di download del firmware…	Quindi procedere come segue…
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.
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.
Configuration Database Validation (convalida del database di configurazione) (se supportata dalla versione del controller dello storage array)	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.

Se si verifica questo errore di download del firmware…	Quindi procedere come segue…
Più di 4 voci MEL critiche negli ultimi 7 giorni	Contattare il supporto tecnico per risolvere il problema.

Quali sono le prossime novità?

L'aggiornamento del firmware del disco è stato completato. È possibile riprendere le normali operazioni.

Manutenzione dei sistemi

EF300 ed EF600

Manutenzione dell’hardware EF300 e EF600

Per i sistemi storage EF300 ed EF600, è possibile eseguire procedure di manutenzione sui seguenti componenti.

Batterie

Una batteria è inclusa in un controller e conserva i dati memorizzati nella cache in caso di interruzione dell’alimentazione CA.

Controller

Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di Gestore di sistema di SANtricity.

DIMM

È necessario sostituire un modulo DIMM (Dual in-line Memory Module) quando è presente una mancata corrispondenza di memoria o se si verifica un guasto al modulo DIMM.

Dischi

Un disco è un dispositivo che fornisce i supporti di storage fisici per i dati.

Ventole

Ogni shelf o shelf di controller EF300 o EF600 include cinque ventole per il raffreddamento del controller.

HICS (host Interface Card)

Una scheda di interfaccia host (HIC) deve essere installata all’interno di un contenitore del controller. Il controller EF600 include porte host sull’HIC opzionale. Le porte host integrate nell’HIC sono chiamate porte HIC.

Protocollo della porta host

È possibile convertire il protocollo di un host in un protocollo diverso in modo da stabilire compatibilità e comunicazione.

Alimentatori

Un alimentatore fornisce una fonte di alimentazione ridondante in uno shelf di controller.

Schede di espansione SAS

È possibile installare una scheda di espansione SAS all’interno di un contenitore di controller. Il controller EF300 supporta l’espansione SAS.

Batterie

Requisiti per la sostituzione della batteria EF300 o EF600

Prima di sostituire una batteria EF300 o EF600, esaminare i requisiti e le considerazioni.

Una batteria è inclusa in un controller e conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA.

Recovery Guru

Se il guru del ripristino in Gestione sistema di SANtricity riporta uno dei seguenti stati, è necessario sostituire la batteria interessata:

- Guasto alla batteria
- Sostituzione della batteria necessaria

Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.

Panoramica della procedura

Per proteggere i dati, è necessario sostituire una batteria guasta il prima possibile.

Di seguito è riportata una panoramica dei passaggi per la sostituzione di una batteria nei controller EF300 o EF600:

1. Portare il controller offline.
2. Rimuovere il contenitore del controller.
3. Sostituire la batteria.
4. Sostituire il contenitore del controller.
5. Portare il controller online.

Requisiti

Se si intende sostituire una batteria, è necessario disporre di:

- Una batteria sostitutiva.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

  In alternativa, è possibile utilizzare l'interfaccia della riga di comando (CLI) per eseguire alcune procedure. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:

  - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema

operativo, ad esempio il prompt di DOS C:.

- **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Sostituire la batteria EF300 o EF600

È possibile sostituire una batteria in un sistema storage EF300 o EF600.

A proposito di questa attività

Ogni contenitore del controller include una batteria che conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA. Se il guru del ripristino in Gestione sistema di SANtricity segnala lo stato di batteria guasta o lo stato Sostituzione batteria richiesta, è necessario sostituire la batteria interessata.

Prima di iniziare

- Verificare che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Esaminare "Requisiti per la sostituzione della batteria EF300 o EF600".
- Assicurarsi di disporre di quanto segue:
  - La batteria sostitutiva.
  - Un braccialetto ESD o altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare il controller offline

Eseguire il backup dei dati e posizionare il controller interessato offline.

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.
2. Dall'area Details (Dettagli) del Recovery Guru, determinare quale batteria sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.
   a. Selezionare **hardware**.
   b. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
   c. Selezionare il controller che si desidera mettere offline.
   d. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

   Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

6. Selezionare **ricontrollare** dal Recovery Guru e confermare che il campo OK per rimuovere nell'area Dettagli visualizza Sì, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimuovere il contenitore del controller

Sostituire la batteria guasta con una nuova.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere la batteria guasta

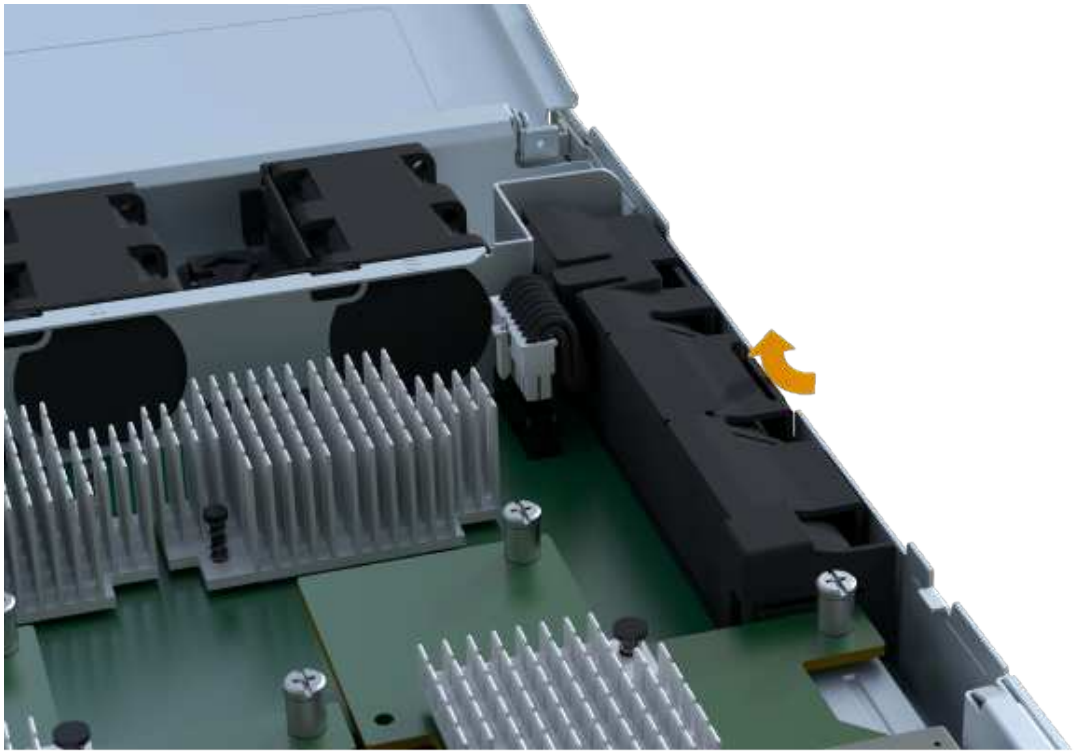
Estrarre la batteria guasta dal controller.

Fasi

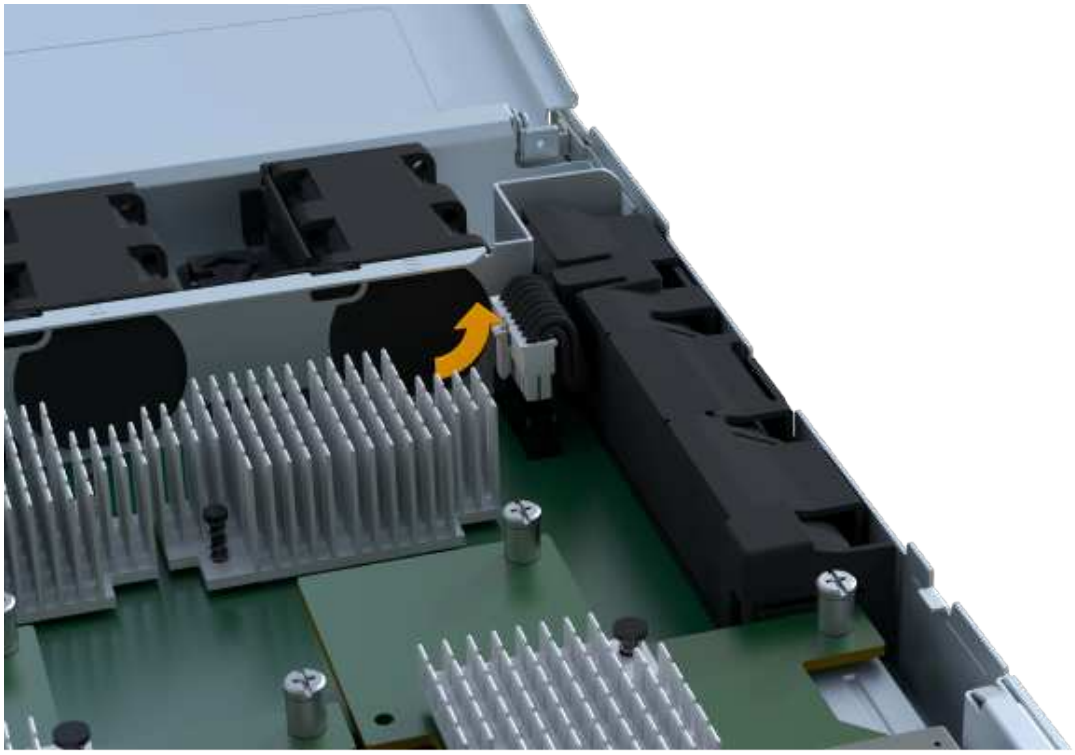
1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

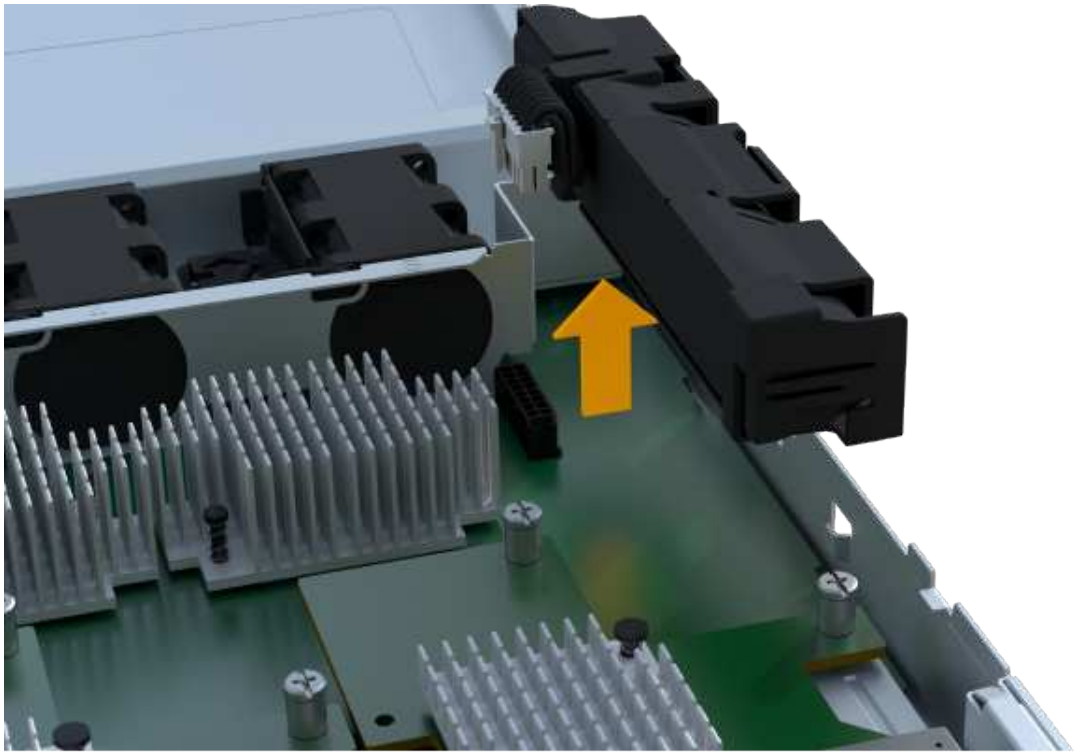
3. Individuare la scheda 'PRESS' sul lato del controller.
4. Sganciare la batteria premendo la linguetta e premendo l'alloggiamento della batteria.



5. Premere delicatamente il connettore che ospita il cablaggio della batteria. Tirare verso l'alto, scollegando la batteria dalla scheda.



6. Estrarre la batteria dal controller e posizionarla su una superficie piana e priva di scariche elettrostatiche.



7. Seguire le procedure appropriate per il riciclaggio o lo smaltimento della batteria guasta.

> Per rispettare le normative IATA (International Air Transport Association), non spedire mai una batteria al litio via etere se non è installata nello shelf del controller.

Fase 4: Installare una nuova batteria

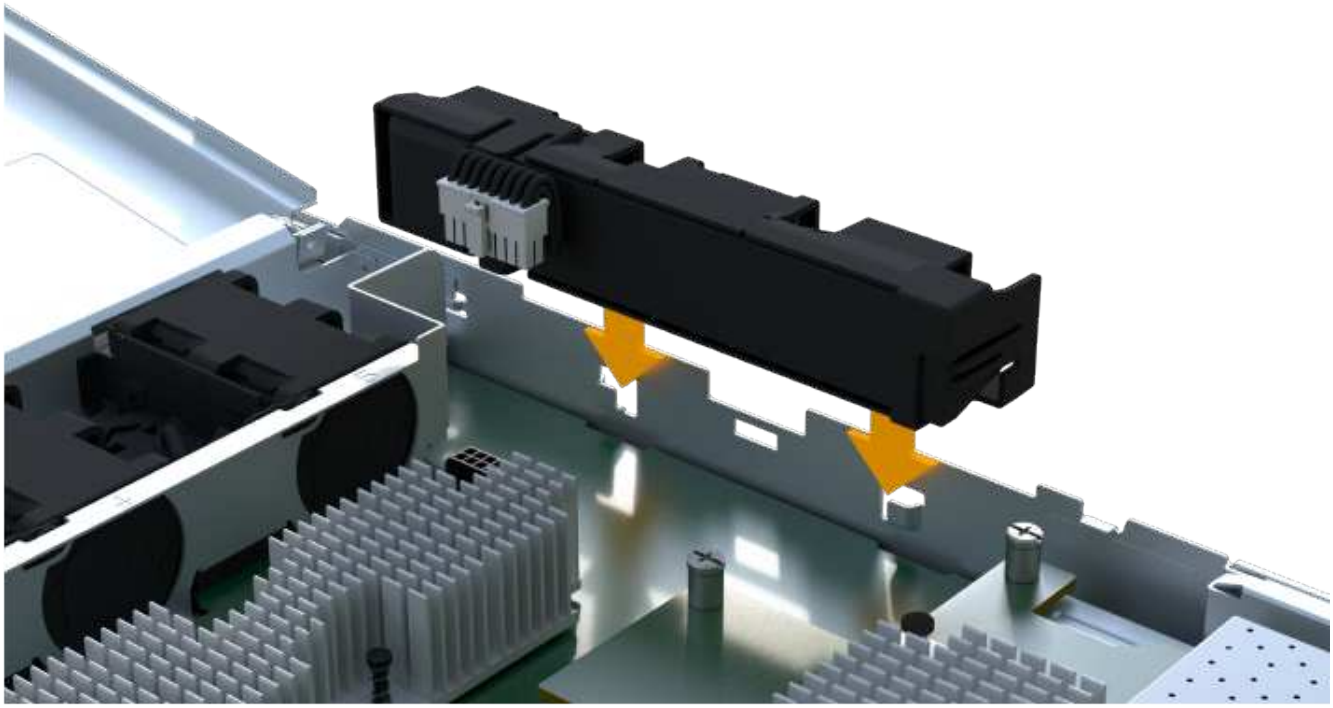
Dopo aver rimosso la batteria guasta dal contenitore del controller, seguire questa procedura per installare la nuova batteria.

Fasi

1. Disimballare la nuova batteria e riutilizzarla su una superficie piana e priva di scariche elettrostatiche.

> Per rispettare le normative IATA in materia di sicurezza, le batterie sostitutive vengono spedite con uno stato di carica (SoC) pari o inferiore al 30%. Quando si riattiva l'alimentazione, tenere presente che il caching in scrittura non viene ripristinato fino a quando la batteria sostitutiva non viene completamente caricata e non viene completato il ciclo di apprendimento iniziale.

2. Inserire la batteria nel controller allineando l'alloggiamento della batteria con i fermi metallici sul lato del controller.



   La batteria scatta in posizione.

3. Ricollegare il connettore della batteria alla scheda.

Fase 5: Reinstallare il contenitore del controller

Reinstallare il controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

Fase 6: Sostituzione completa della batteria

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Posizionare il controller online.
   a. In System Manager, accedere alla pagina hardware.
   b. Selezionare **Mostra retro del controller**.
   c. Selezionare il controller con la batteria sostituita.
   d. Selezionare **Place online** dall'elenco a discesa.
2. All'avvio del controller, controllare i LED del controller.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **supporto › Centro aggiornamento** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della batteria è completata. È possibile riprendere le normali operazioni.

Controller

Requisiti per la sostituzione del controller EF300 o EF600

Prima di sostituire un controller EF300 o EF600, esaminare i requisiti e le considerazioni.

Un controller è costituito da una scheda, firmware e software. Controlla i dischi e implementa le funzioni di Gestore di sistema di SANtricity.

Requisiti per la sostituzione del controller

Prima di sostituire un controller, è necessario disporre di:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Un cacciavite Phillips n. 1.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del

controller.

Sostituzione all'accensione

È possibile sostituire un contenitore di controller mentre lo storage array è acceso ed esegue operazioni di i/o host, se sono soddisfatte le seguenti condizioni:

- Il secondo contenitore del controller nello shelf ha uno stato ottimale.
- Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Sostituire il controller EF300 o EF600

È possibile sostituire un singolo controller nello shelf di controller EF300 o EF600.

A proposito di questa attività

Quando si sostituisce un contenitore del controller guasto, è necessario rimuovere la batteria, l'alimentatore, i moduli DIMM, le ventole e la scheda di interfaccia host (HIC) dal contenitore del controller originale, quindi installarli nel contenitore del controller sostitutivo.

Prima di iniziare

- Revisione "Requisiti per la sostituzione del controller EF300 o EF600".
- Determinare se il contenitore del controller è guasto in due modi:
  - Il guru del ripristino in Gestione di sistema di SANtricity richiede la sostituzione del contenitore del controller.
  - Il LED di attenzione ambra sul contenitore del controller è acceso, a indicare che il controller è guasto.
- Assicurarsi di disporre di quanto segue:
  - Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Un cacciavite Phillips n. 1
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del controller

Preparare la sostituzione di un contenitore del controller guasto verificando che il contenitore del controller sostitutivo disponga del codice FRU corretto, eseguendo il backup della configurazione e raccogliendo i dati di supporto.

Fasi

1. Disimballare il nuovo contenitore del controller e riutilizzarlo su una superficie piana e priva di elettricità statica.

   Conservare il materiale di imballaggio da utilizzare per la spedizione del contenitore del controller guasto.

2. Individuare le etichette dell'indirizzo MAC e del numero di parte della FRU sul retro del contenitore del controller.
3. Da Gestore di sistema di SANtricity, individuare il numero di parte di ricambio del contenitore del controller che si sta sostituendo.

   Quando un controller presenta un guasto e deve essere sostituito, il codice del ricambio viene visualizzato nell'area Details (Dettagli) del Recovery Guru. Se è necessario trovare questo numero manualmente, attenersi alla seguente procedura:

   a. Selezionare **hardware**.
   b. Individuare lo shelf del controller, contrassegnato dall'icona del controller .
   c. Fare clic sull'icona del controller.
   d. Selezionare il controller e fare clic su **Avanti**.
   e. Nella scheda **base**, annotare il **numero di parte di ricambio** del controller.
4. Verificare che il numero di parte sostitutivo del controller guasto sia lo stesso del numero di parte FRU del controller sostitutivo.

   > **Possibile perdita di accesso ai dati** — se i numeri di due parti non sono gli stessi, non tentare questa procedura. Inoltre, se il contenitore del controller guasto include una scheda di interfaccia host (HIC), è necessario installare tale HIC nel nuovo contenitore del controller. La presenza di controller non corrispondenti o HICS causa il blocco del nuovo controller quando lo si porta online.

5. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

6. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   a. Selezionare **hardware**.
   b. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
   c. Selezionare il controller che si desidera mettere offline.
   d. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

> Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

7. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

8. Selezionare **ricontrollare** dal Recovery Guru e confermare che nel campo **OK per rimuovere** nell'area Dettagli sia visualizzato **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimuovere il controller guasto

Rimuovere un contenitore del controller per sostituire il contenitore guasto con uno nuovo.

Si tratta di una procedura in più fasi che richiede la rimozione dei seguenti componenti: Batteria, scheda di interfaccia host, alimentatore, DIMM e ventole.

Fase 2a: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller guasto in modo da poterlo sostituire con uno nuovo.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   > Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se il contenitore del controller dispone di un HIC che utilizza ricetrasmettitori SFP+, rimuovere gli SFP.

   Poiché è necessario rimuovere l'HIC dal contenitore del controller guasto, è necessario rimuovere eventuali SFP dalle porte HIC. Quando si ricollegano i cavi, è possibile spostare questi SFP nel nuovo contenitore del controller.

5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
6. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

7. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

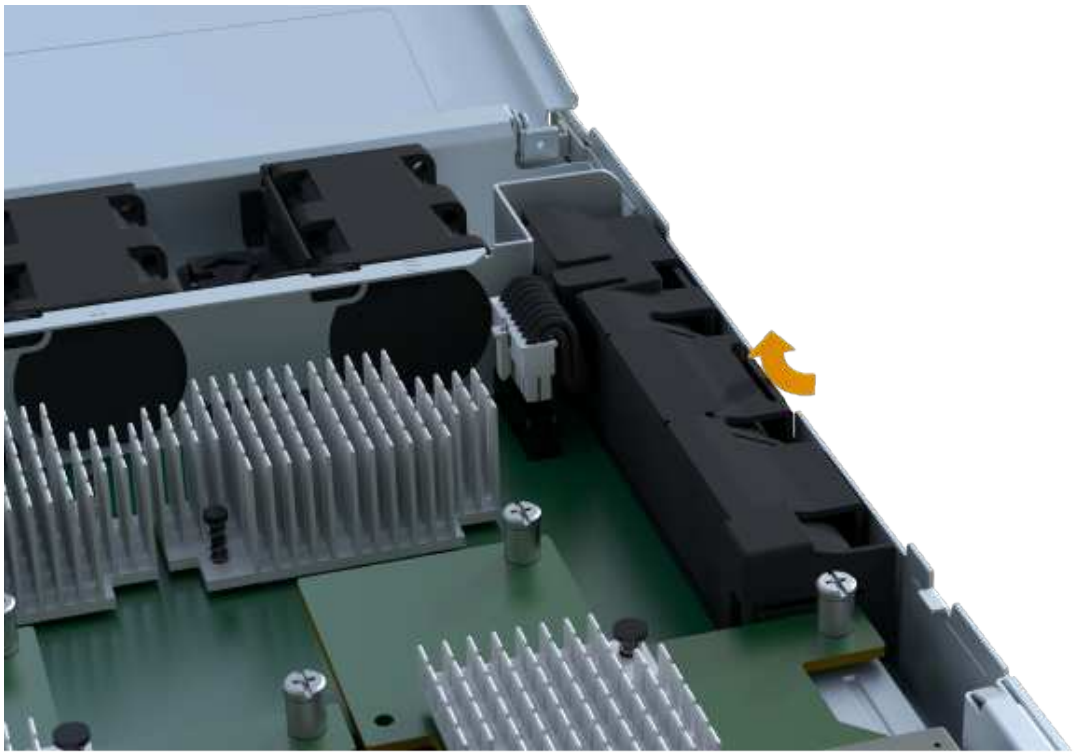
8. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 2b: Rimuovere la batteria

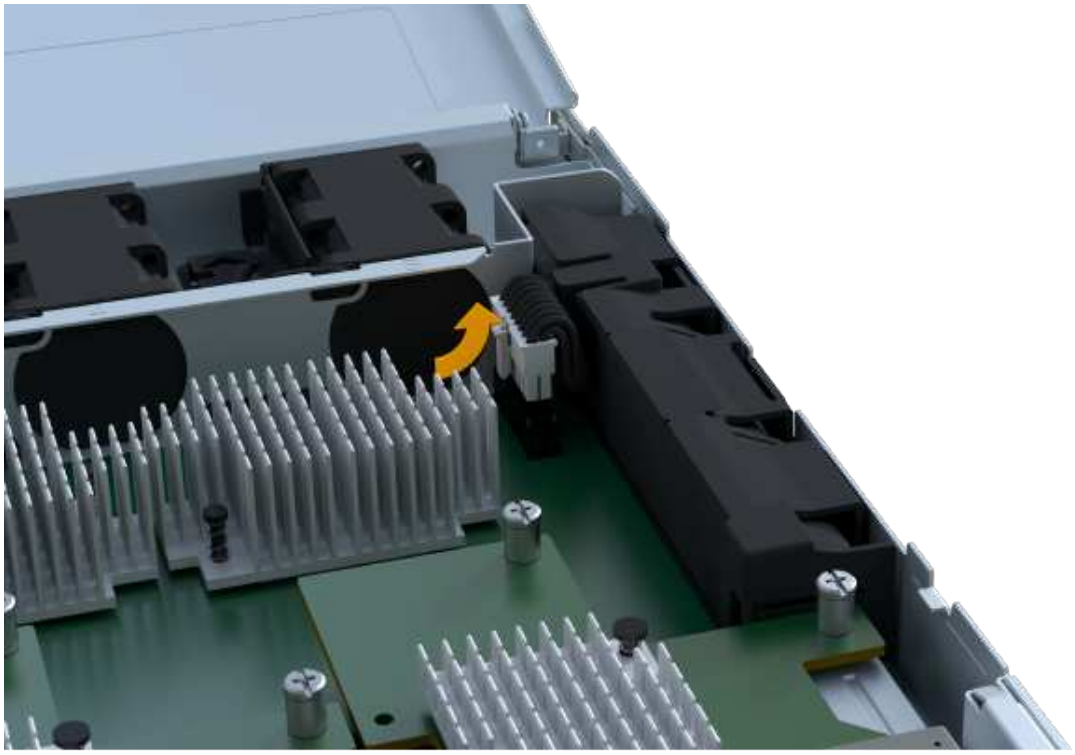
Rimuovere la batteria dal contenitore del controller guasto in modo da poterla installare nel nuovo contenitore del controller.

Fasi

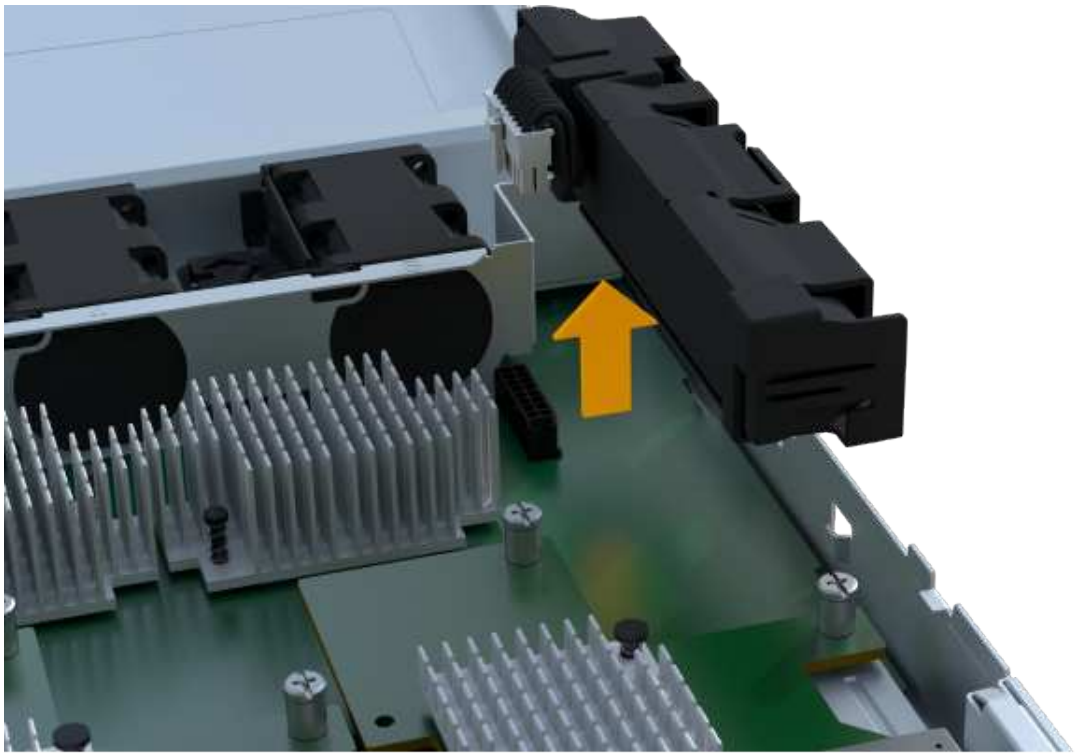
1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Individuare la scheda 'PRESS' sul lato del controller.
3. Sganciare la batteria premendo la linguetta e premendo l'alloggiamento della batteria.



4. Premere delicatamente il connettore che ospita il cablaggio della batteria. Tirare verso l'alto, scollegando la batteria dalla
scheda.



5. Estrarre la batteria dal controller e posizionarla su una superficie piana e priva di scariche elettrostatiche.



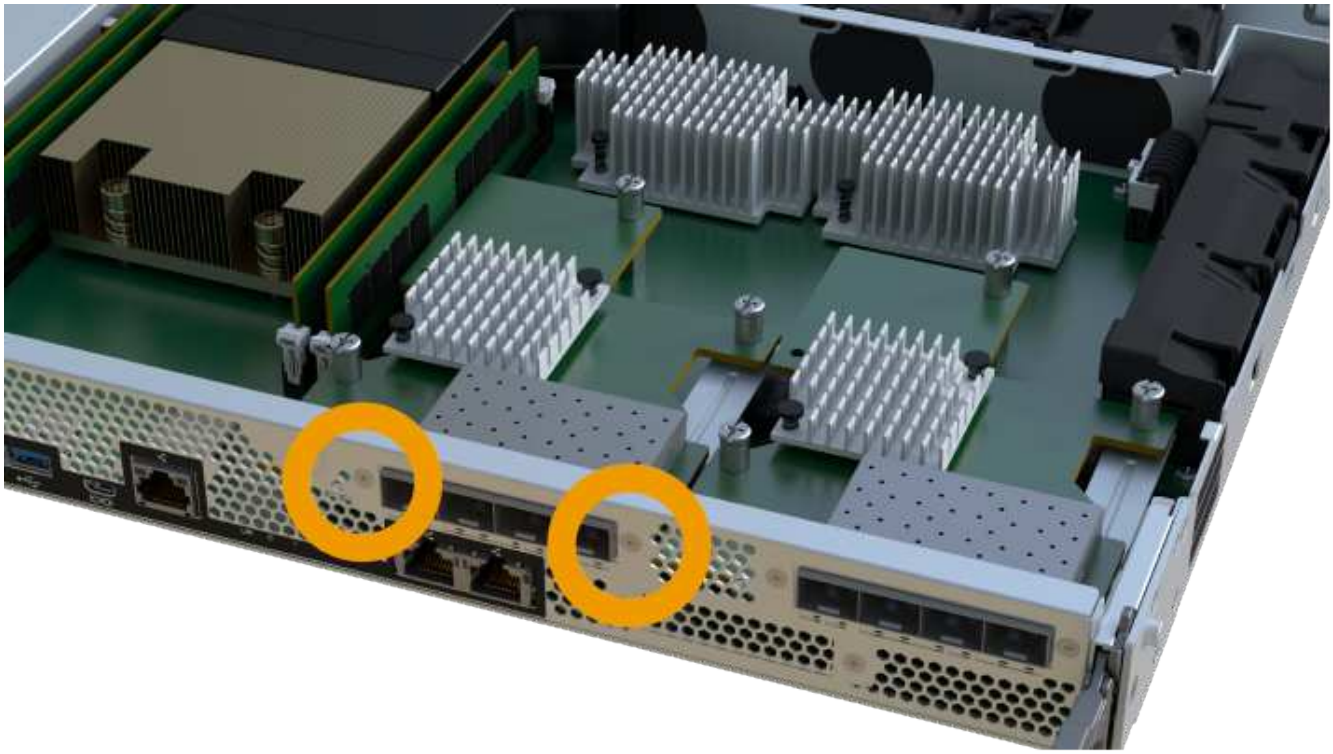
Fase 2c: Rimuovere l'HIC

Se il contenitore del controller include un HIC, è necessario rimuovere l'HIC dal contenitore del controller originale. In caso contrario, è possibile saltare questo passaggio.

Fasi

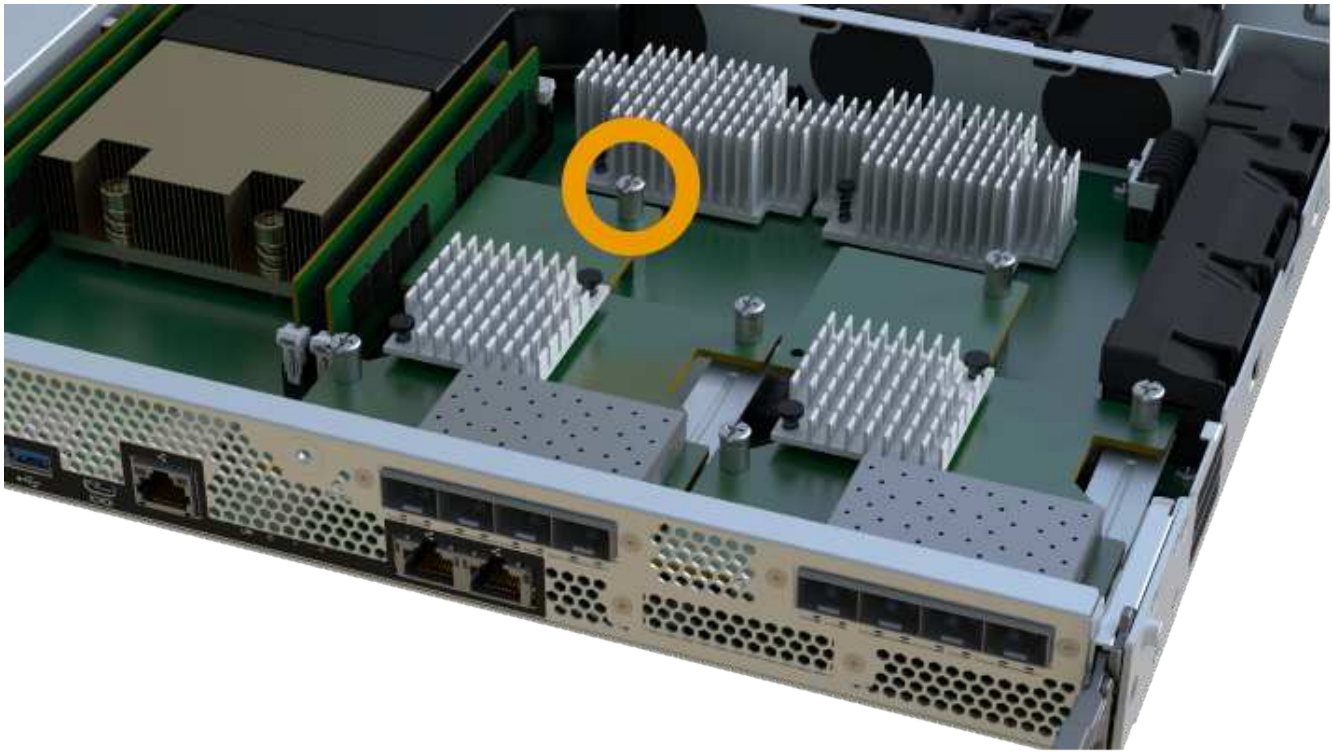
1. Utilizzando un cacciavite Phillips, rimuovere le due viti che fissano la mascherina HIC al contenitore del

controller.



L'immagine riportata sopra è un esempio, l'aspetto dell'HIC potrebbe differire.

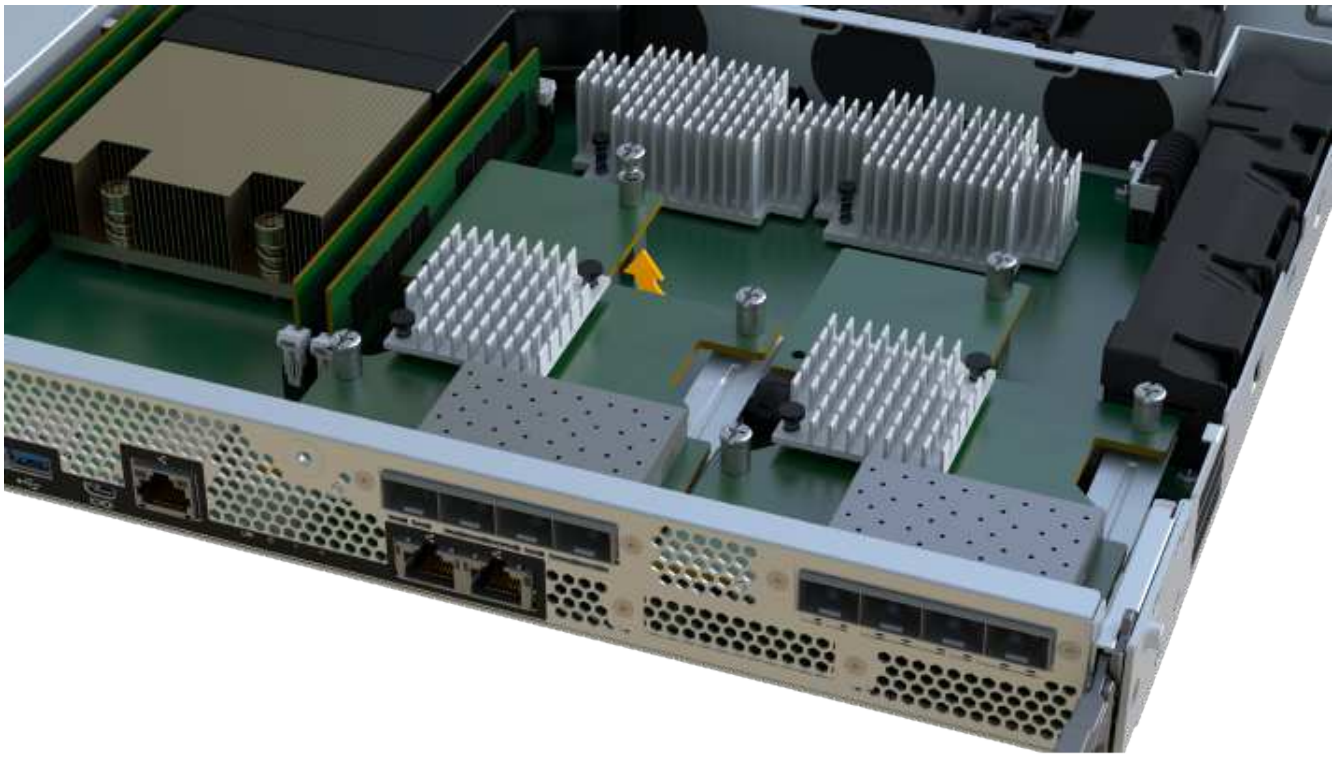
2. Rimuovere la piastra anteriore dell'HIC.
3. Utilizzando le dita o un cacciavite Phillips, allentare la singola vite a testa zigrinata che fissa l'HIC alla scheda del controller.



L'HIC viene fornito con tre posizioni delle viti sulla parte superiore, ma è fissato con una sola.

4. Scollegare con cautela l'HIC dalla scheda del controller sollevando la scheda e sollevandola dal controller.

Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



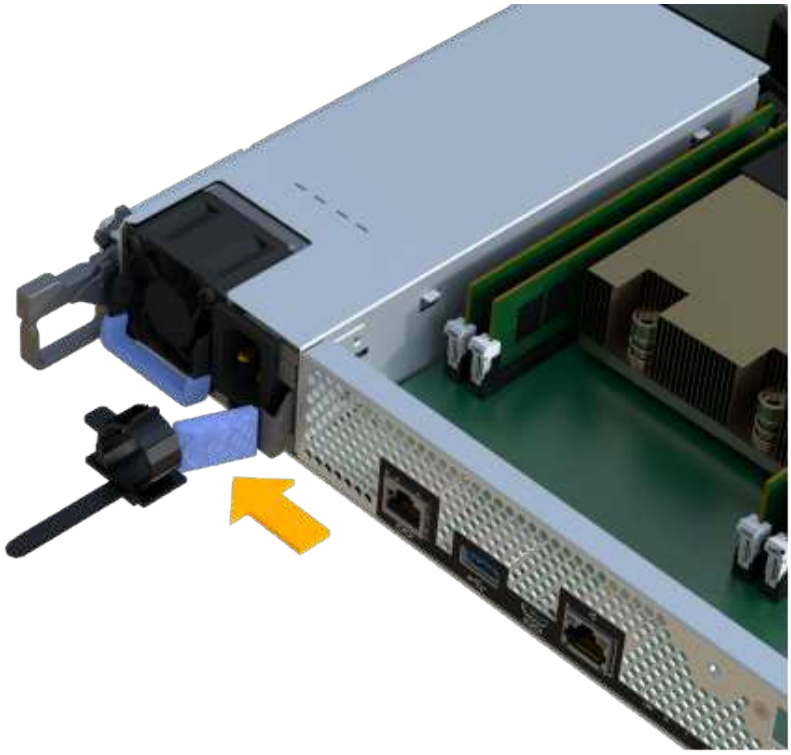
5. Posizionare l'HIC su una superficie piana e priva di scariche elettrostatiche.

Fase 2d: Rimuovere l'alimentatore

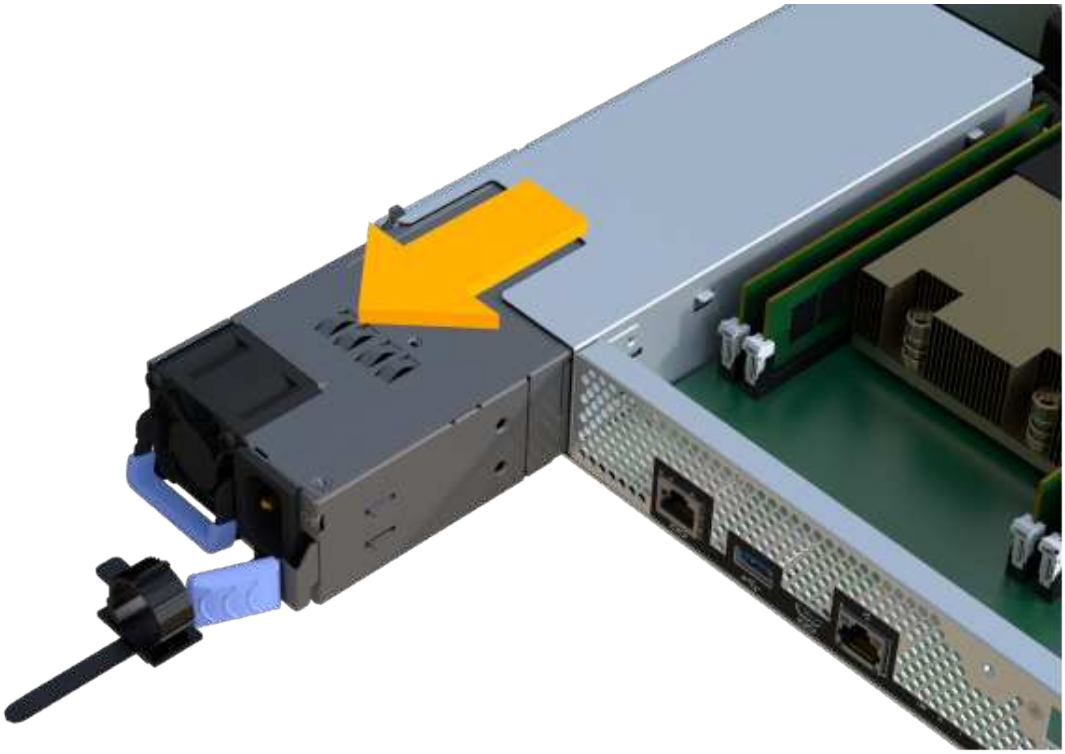
Rimuovere l'alimentatore per installarlo nel nuovo controller.

Fasi

1. Scollegare i cavi di alimentazione:
   a. Aprire il fermo del cavo di alimentazione, quindi scollegare il cavo di alimentazione dall'alimentatore.
   b. Scollegare il cavo di alimentazione dalla presa di corrente.
2. Individuare la linguetta a destra dell'alimentatore e spingerla verso l'alimentatore.



3. Individuare la maniglia sulla parte anteriore dell'alimentatore.
4. Utilizzare la maniglia per estrarre l'alimentatore dal sistema.



Quando si rimuove un alimentatore, utilizzare sempre due mani per sostenerne il peso.

Fase 2e: Rimuovere i DIMM

Rimuovere i DIMM in modo da poterli installare nel nuovo controller.

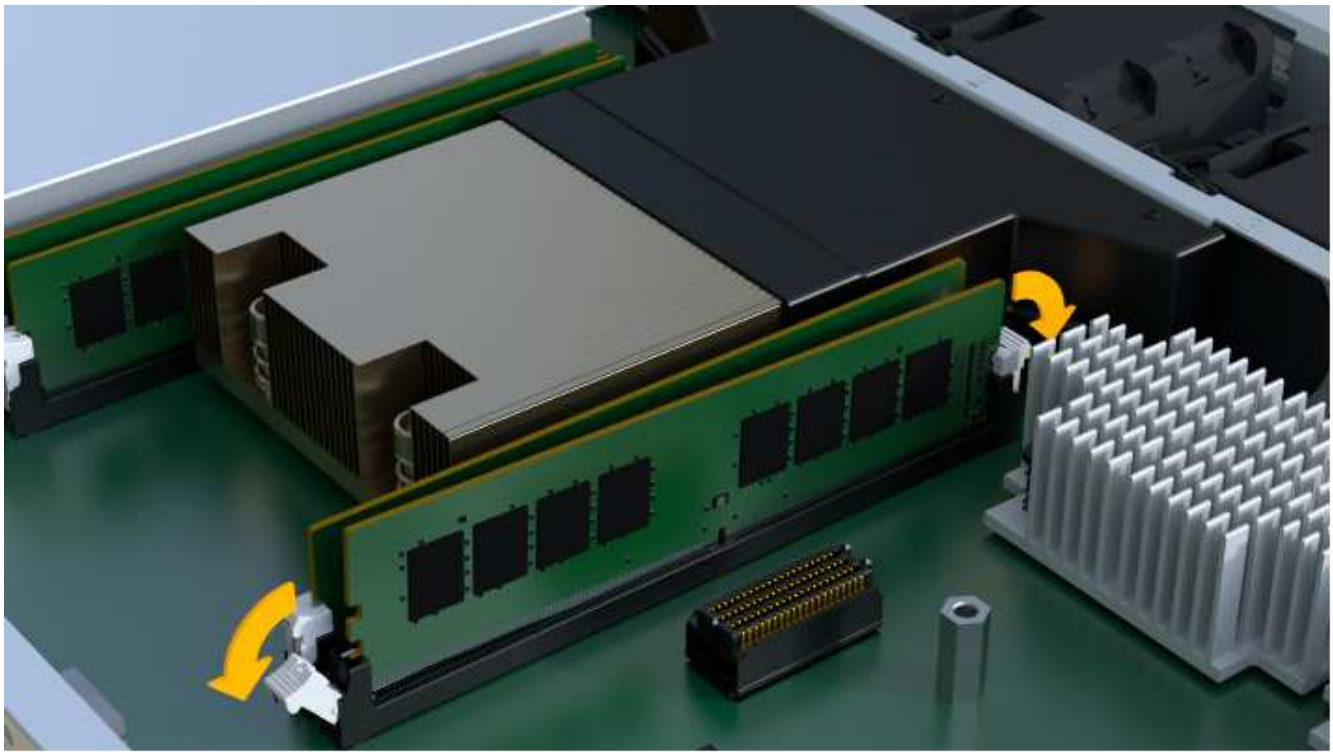
Fasi

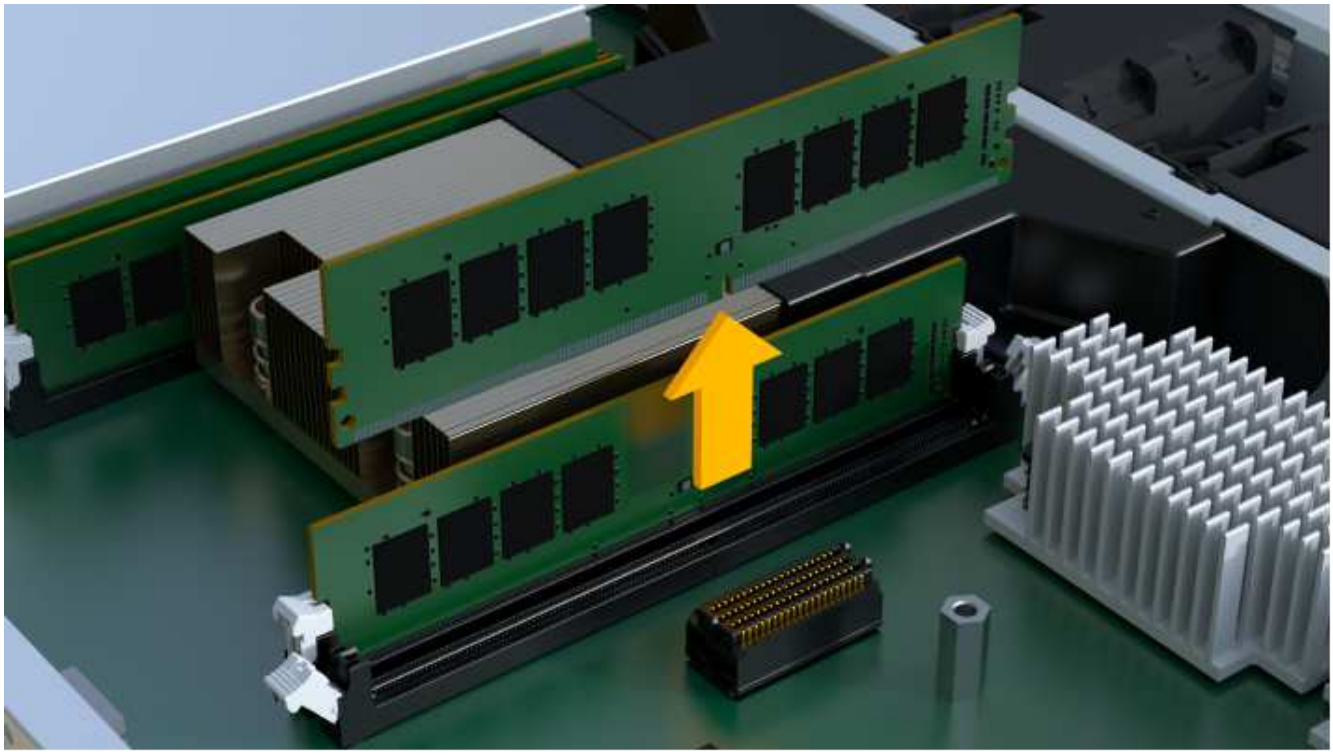
1. Individuare i DIMM sul controller.
2. Prendere nota dell'orientamento del DIMM nello zoccolo in modo da poter inserire il DIMM sostitutivo nell'orientamento corretto.

> Una tacca nella parte inferiore del DIMM consente di allineare il DIMM durante l'installazione.

3. Spingere lentamente verso l'esterno le due linguette di espulsione dei moduli DIMM su entrambi i lati del modulo DIMM per estrarlo dal relativo slot, quindi farlo scorrere verso l'esterno.

> Tenere il modulo DIMM per i bordi in modo da evitare di esercitare pressione sui componenti della scheda a circuiti stampati del modulo DIMM.



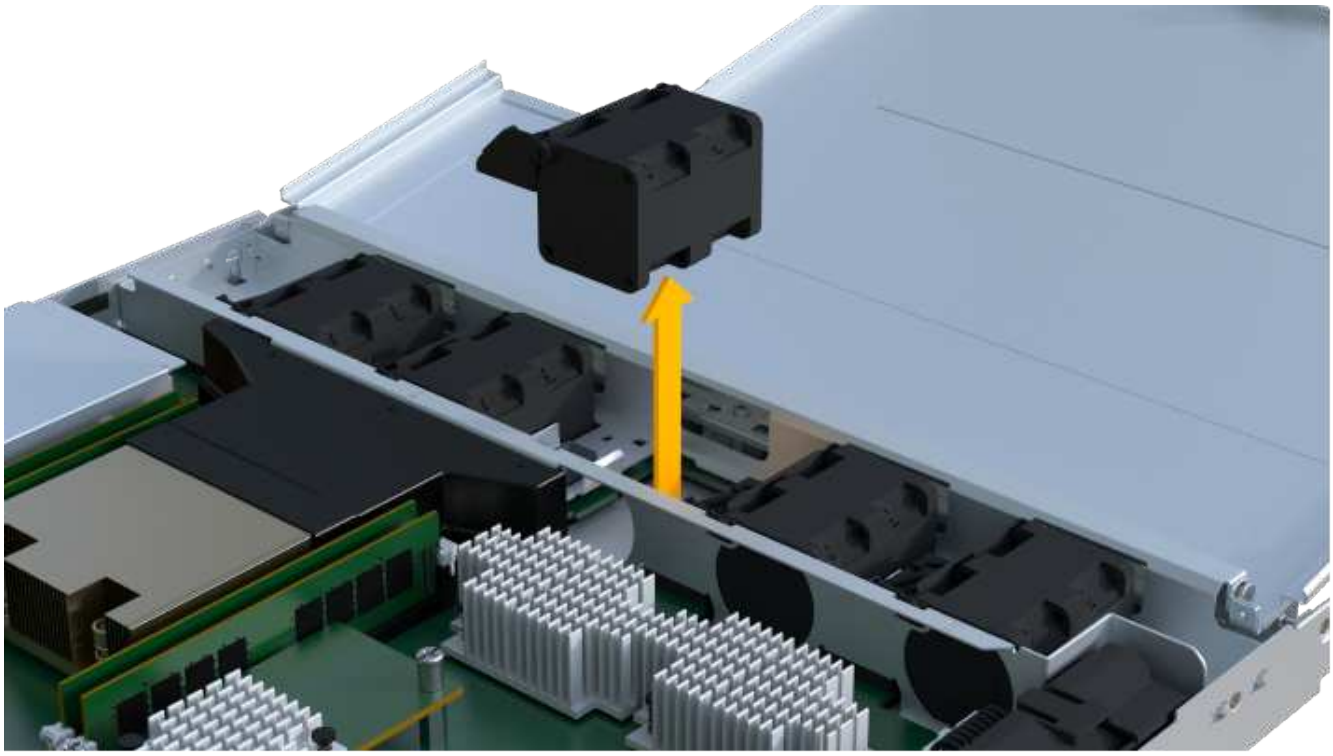


Fase 2f: Rimuovere le ventole

Rimuovere le ventole in modo da poterle installare nel nuovo controller.

Fasi

1. Sollevare delicatamente la ventola dal controller.



2. Ripetere l’operazione fino a rimuovere tutte le ventole.

Fase 3: Installare un nuovo controller

Installare un nuovo elemento filtrante del controller per sostituire quello guasto.

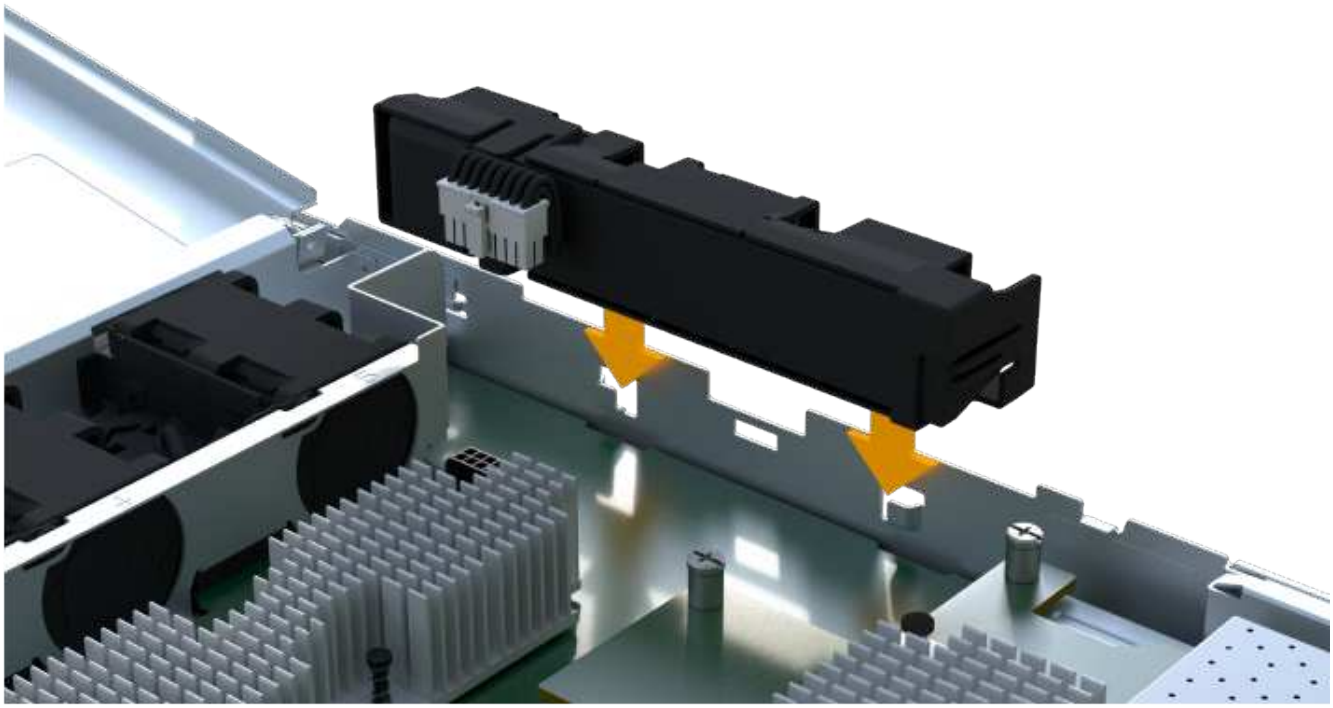
Si tratta di una procedura in più fasi che richiede l'installazione dei seguenti componenti dal controller originale: Batteria, scheda di interfaccia host, alimentatore, DIMM e ventole.

Fase 3a: Installare la batteria

Installare la batteria nel contenitore del controller di ricambio.

Fasi

1. Assicurarsi di disporre di:
    - La batteria dal contenitore del controller originale o una nuova batteria ordinata.
    - Il contenitore del controller di ricambio.
2. Inserire la batteria nel controller allineando l'alloggiamento della batteria con i fermi metallici sul lato del controller.



   La batteria scatta in posizione.

3. Ricollegare il connettore della batteria alla scheda.

Fase 3b: Installare l'HIC

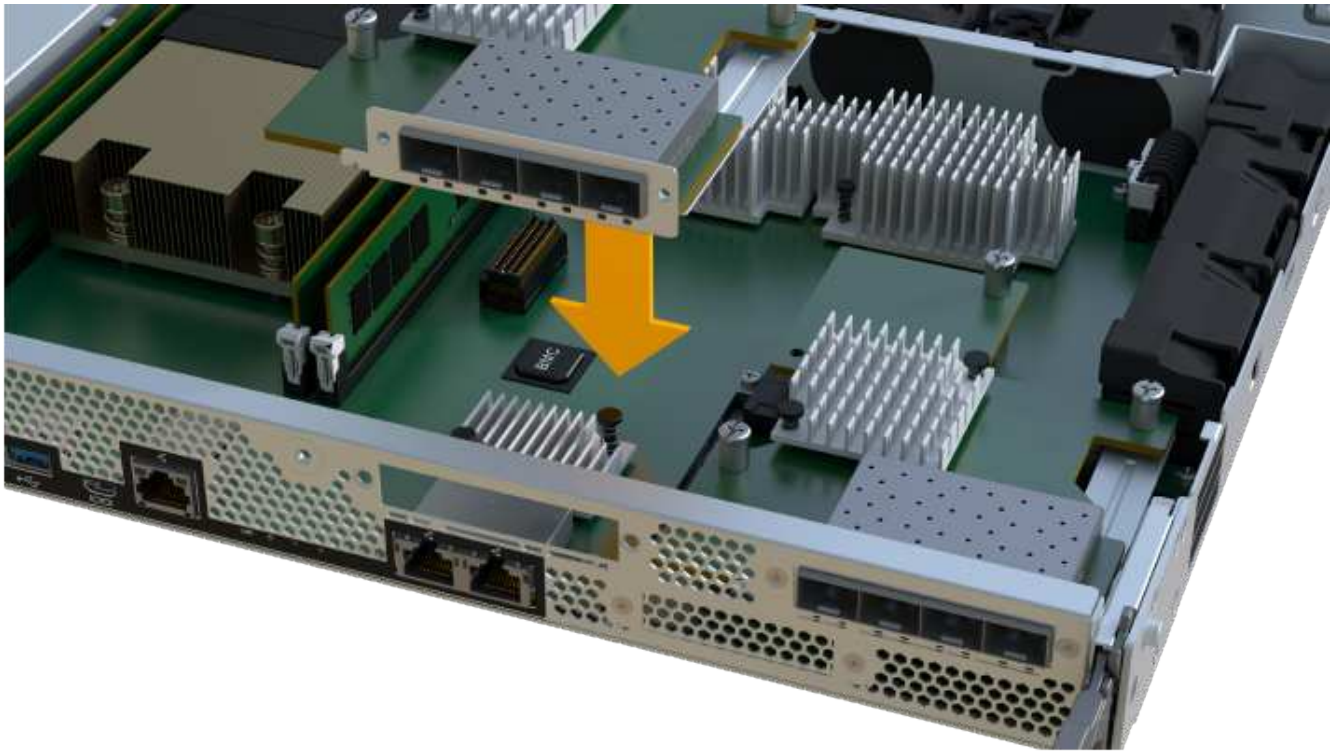
Se è stato rimosso un HIC dal contenitore del controller originale, è necessario installarlo nel nuovo contenitore del controller. In caso contrario, è possibile saltare questo passaggio.

Fasi

1. Utilizzando un cacciavite Phillips n. 1, rimuovere le due viti che fissano la mascherina vuota al contenitore del controller sostitutivo, quindi rimuovere la piastra frontale.

2. Allineare la singola vite a testa zigrinata sull'HIC con il foro corrispondente sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



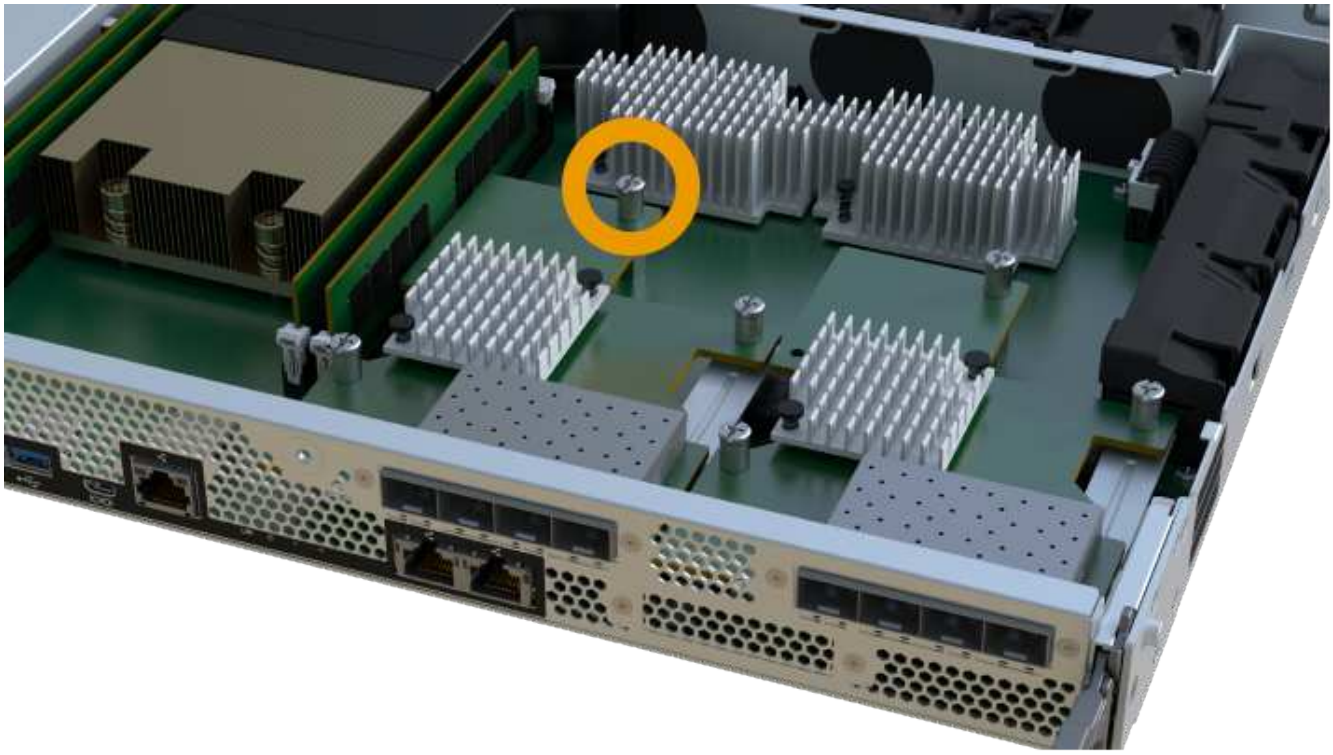
L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e la vite a testa zigrinata.

4. Serrare manualmente la vite a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente la vite.



L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dal contenitore del controller originale al nuovo contenitore del controller con le due viti.

Fase 3c: Installare l'alimentatore

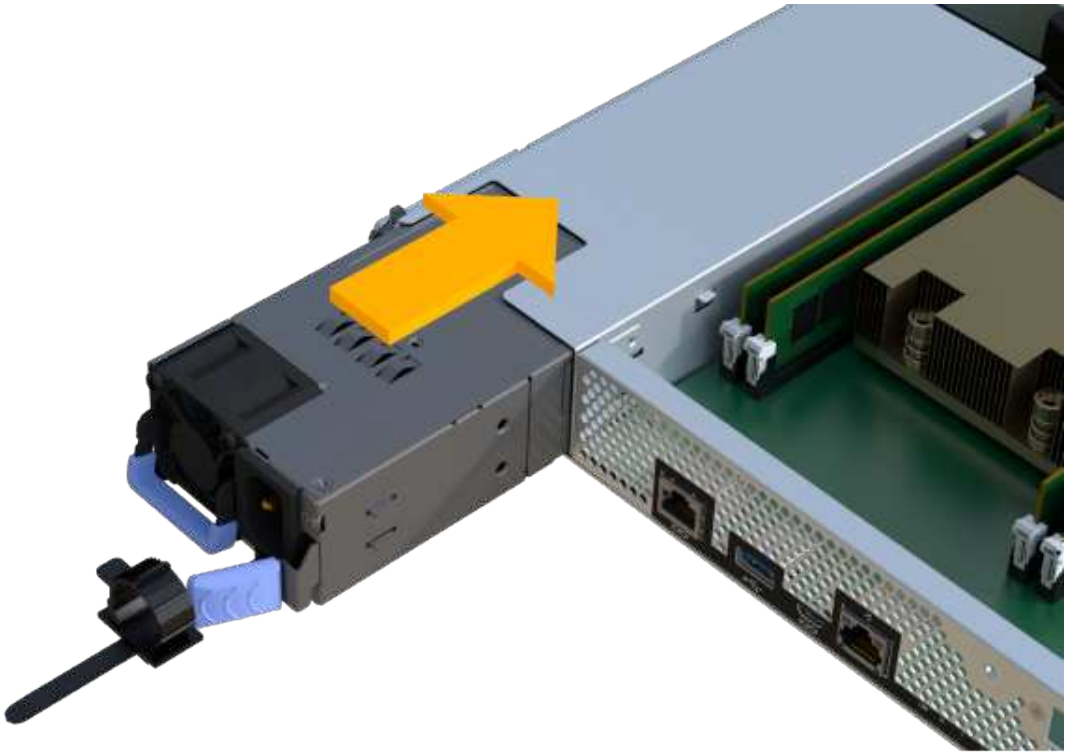
Installare l'alimentatore nel contenitore del controller sostitutivo.

Fasi

1. Con entrambe le mani, sostenere e allineare i bordi dell'alimentatore con l'apertura nello chassis del sistema, quindi spingere delicatamente l'alimentatore nello chassis utilizzando la maniglia della camma.

   Gli alimentatori sono dotati di chiavi e possono essere installati in un solo modo.

   Non esercitare una forza eccessiva quando si inserisce l'alimentatore nel sistema, poiché si potrebbe danneggiare il connettore.



Fase 3d: Installare i DIMM

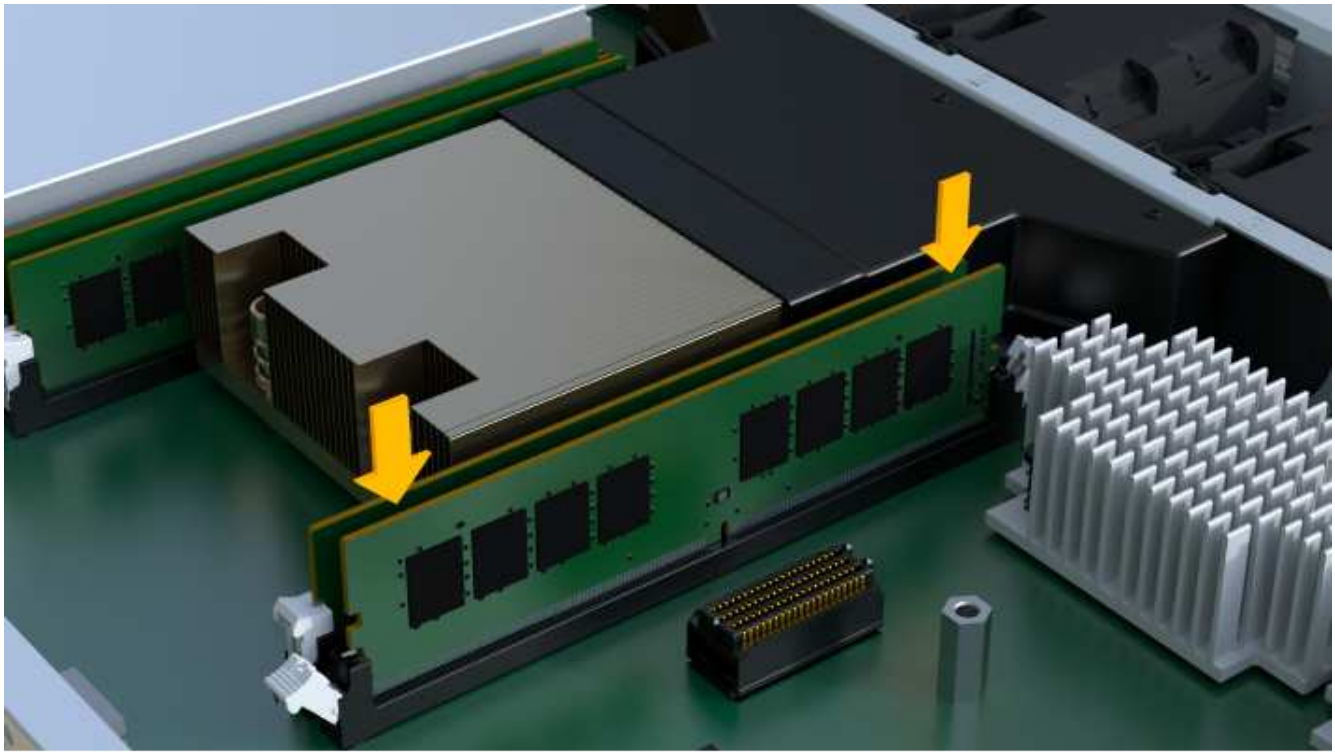
Installare i DIMM nel nuovo contenitore del controller.

Fasi

1. Tenere il modulo DIMM per gli angoli e allinearlo allo slot.

   La tacca tra i pin del DIMM deve allinearsi con la linguetta dello zoccolo.

2. Inserire il DIMM nello slot.

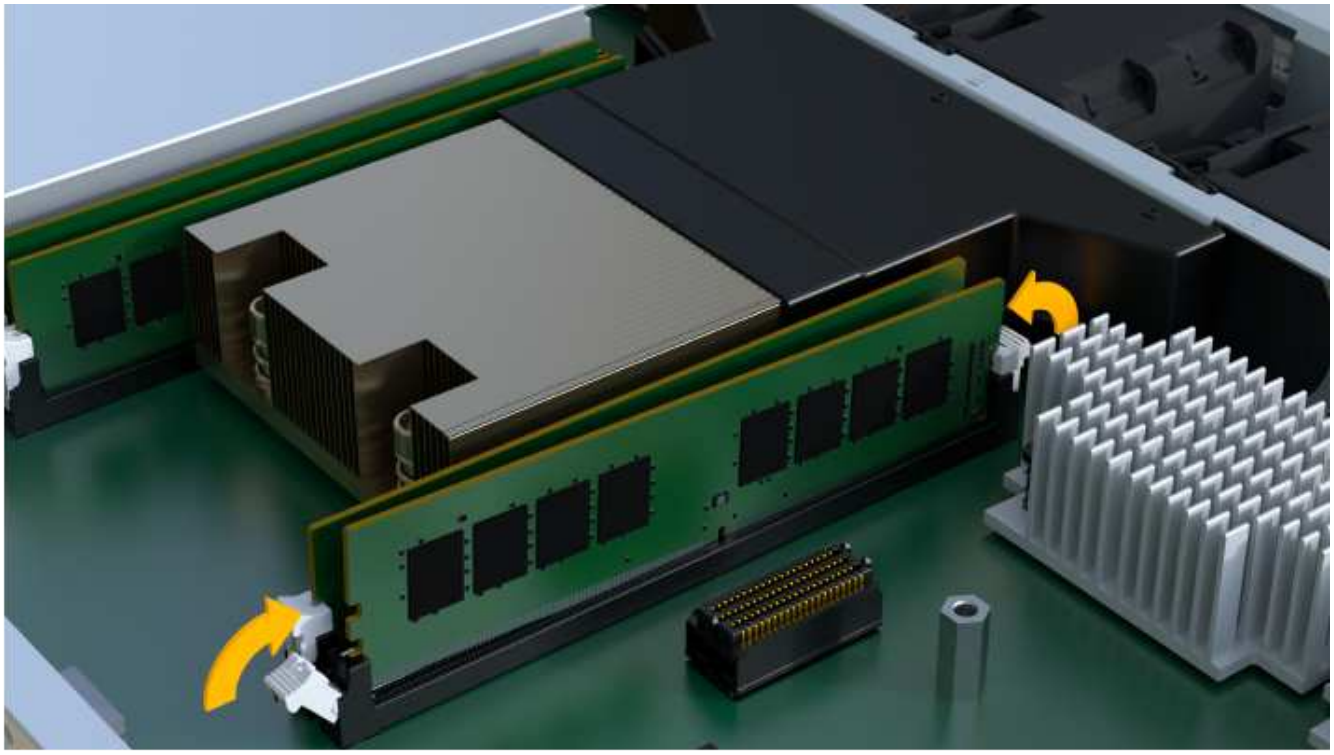


Il DIMM si inserisce saldamente nello slot, ma dovrebbe essere inserito facilmente. In caso contrario, riallineare il DIMM con lo slot e reinserirlo.

> Esaminare visivamente il DIMM per verificare che sia allineato in modo uniforme e inserito completamente nello slot.

3. Spingere con cautela, ma con decisione, sul bordo superiore del DIMM fino a quando i fermi non scattano in posizione sulle tacche alle estremità del DIMM.

> I DIMM si inseriscono saldamente. Potrebbe essere necessario premere delicatamente su un lato alla volta e fissare ciascuna linguetta singolarmente.

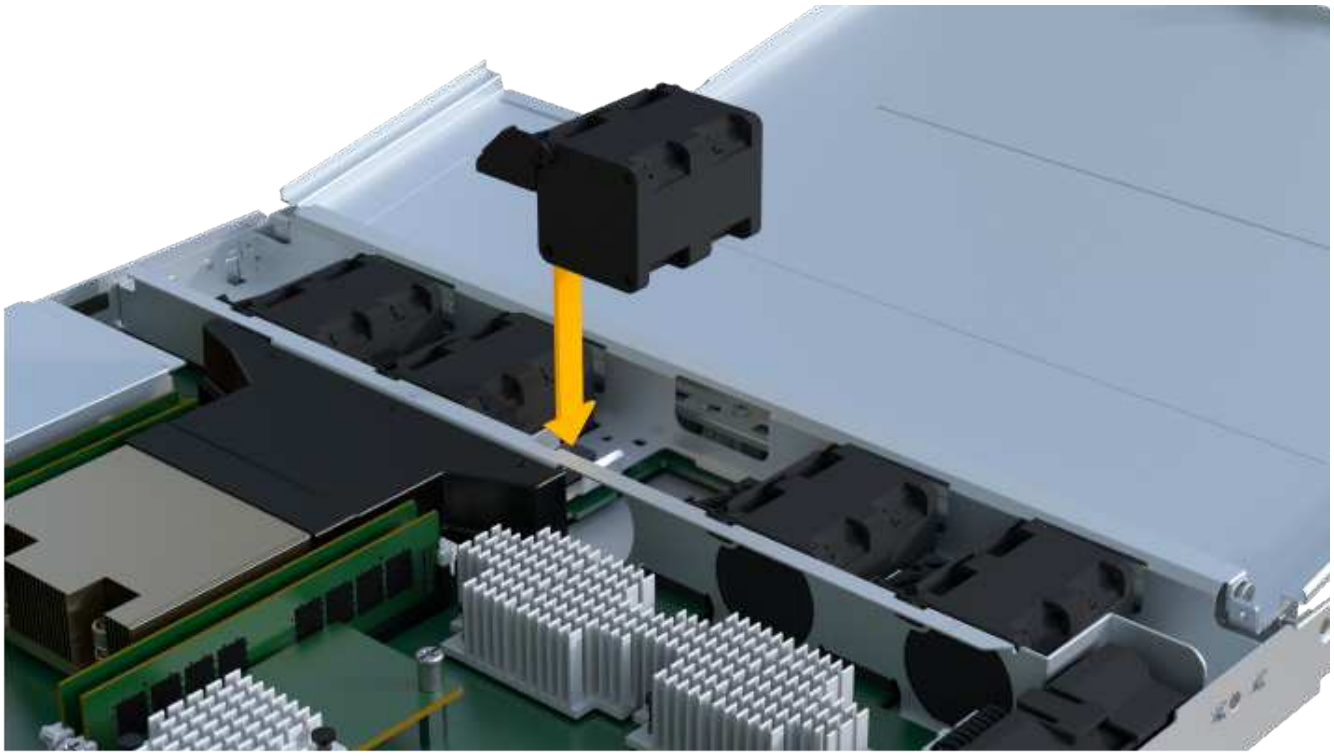


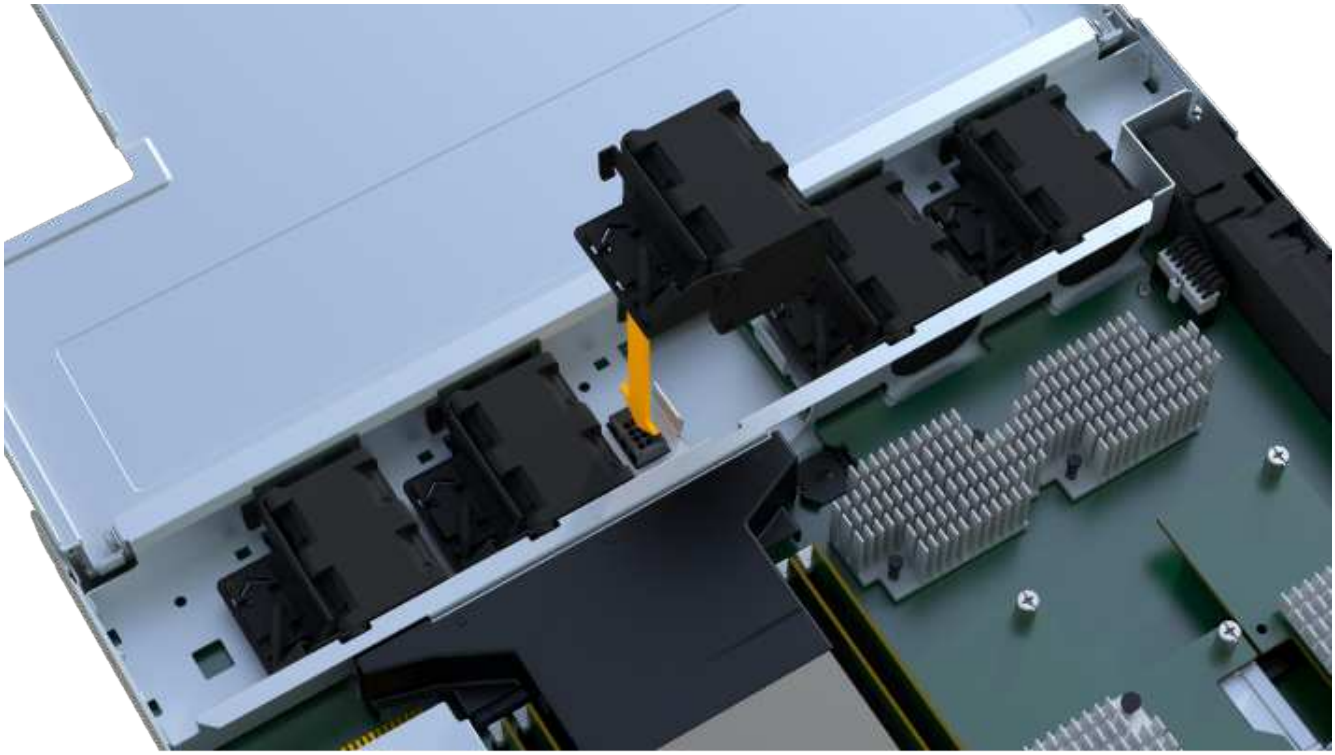
Fase 3e: Installare le ventole

Installare le ventole nel contenitore del controller sostitutivo.

Fasi

1. Far scorrere la ventola fino in fondo nel controller sostitutivo.





2. Ripetere l’operazione fino a installare tutte le ventole.

Fase 3f: Installare il nuovo contenitore del controller

Infine, installare il nuovo contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

> Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

3. Installare gli SFP dal controller originale nelle porte host del nuovo controller, se installati nel controller originale, e ricollegare tutti i cavi.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

4. Se il controller originale utilizzava DHCP per l'indirizzo IP, individuare l'indirizzo MAC sull'etichetta sul retro del controller sostitutivo. Chiedere all'amministratore di rete di associare il DNS/rete e l'indirizzo IP del controller rimosso con l'indirizzo MAC del controller sostitutivo.

   > Se il controller originale non ha utilizzato DHCP per l'indirizzo IP, il nuovo controller adotta l'indirizzo IP del controller rimosso.

Fase 4: Sostituzione completa del controller

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Posizionare il controller online.
   a. In System Manager, accedere alla pagina hardware.
   b. Selezionare **Mostra retro del controller**.
   c. Selezionare il controller sostituito.
   d. Selezionare **Place online** dall'elenco a discesa.
2. All'avvio del controller, controllare i LED del controller.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda

dell'interfaccia host.

3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione del controller è completata. È possibile riprendere le normali operazioni.

DIMM

Requisiti per la sostituzione di un modulo DIMM EF300 o EF600

Prima di sostituire un DIMM in un array di storage EF300 o EF600, esaminare i requisiti e le considerazioni.

È necessario sostituire un modulo DIMM in caso di mancata corrispondenza della memoria o di un modulo DIMM guasto. Verificare la configurazione del controller EF300 o EF600 per assicurarsi che vengano sostituite le dimensioni DIMM corrette.

Tenere presente che i DIMM dell'array di storage sono fragili; una gestione errata può causare danni.

Attenersi alle seguenti regole per evitare di danneggiare i DIMM dell'array di storage:

- Prevenzione delle scariche elettrostatiche (ESD):
  - Conservare il modulo DIMM nel sacchetto ESD fino a quando non si è pronti per l'installazione.
  - Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici. Non inserire utensili metallici o coltelli nel sacchetto ESD.
  - Conservare il sacchetto ESD e il materiale di imballaggio nel caso in cui sia necessario restituire un modulo DIMM in un secondo momento.

    Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis dell'enclosure di storage.

- Gestire con attenzione i DIMM:
  - Utilizzare sempre due mani per rimuovere, installare o trasportare un modulo DIMM.
  - Non forzare mai un modulo DIMM in uno shelf e esercitare una pressione leggera e decisa per inserire completamente il dispositivo di chiusura.
  - Per la spedizione dei moduli DIMM, utilizzare sempre confezioni approvate.
- Evitare i campi magnetici. Tenere i DIMM lontani dai dispositivi magnetici.

Sostituire i DIMM in EF300 o EF600

È possibile sostituire un DIMM in un array EF300 o EF600.

A proposito di questa attività

Per sostituire un DIMM, verificare le dimensioni della cache del controller, posizionare il controller offline, rimuovere il controller, rimuovere i DIMM e installare i nuovi DIMM nel controller. Quindi, è possibile riportare il controller online e verificare che lo storage array funzioni correttamente.

Prima di iniziare

- Revisione "Requisiti per la sostituzione di un modulo DIMM EF300 o EF600".
- Assicurarsi che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Assicurarsi di disporre di quanto segue:
  - Un DIMM sostitutivo.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Determinare se è necessario sostituire un DIMM

Verificare le dimensioni della cache del controller prima di sostituire i DIMM.

Fasi

1. Accedere al profilo Storage Array per il controller. Da Gestore di sistema di SANtricity, andare al **supporto › Centro di supporto**. Dalla pagina Support Resources (risorse di supporto), selezionare **Storage Array Profile** (Profilo array di storage).
2. Scorrere verso il basso o utilizzare il campo Search (Cerca) per individuare le informazioni **Data cache Module** (modulo cache dati).
3. Se è presente una delle seguenti opzioni, prendere nota della posizione del DIMM e continuare con le altre procedure descritte in questa sezione per sostituire i DIMM sul controller:
   - Un modulo DIMM guasto o un modulo DIMM che segnala **Data cache Module** come non ottimale.
   - Un DIMM con capacità **Data cache Module** non corrispondente.

Fase 2: Posizionare il controller offline

Posizionare il controller offline in modo da poter rimuovere e sostituire i DIMM in modo sicuro.

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una memoria non corrispondente e per assicurarsi che non siano prima necessari altri elementi.
2. Nell'area Details (Dettagli) del Recovery Guru, determinare quale DIMM sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.
   a. Selezionare **hardware**.
   b. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
   c. Selezionare il controller che si desidera mettere offline.
   d. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

6. Selezionare **ricontrollare** dal Recovery Guru e confermare che il campo OK per rimuovere nell'area Dettagli visualizza Sì, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 3: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller guasto in modo da poter sostituire i DIMM con altri nuovi.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte

anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

> Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 4: Rimuovere i DIMM

Se la memoria non corrisponde, sostituire i DIMM nel controller.

Fasi

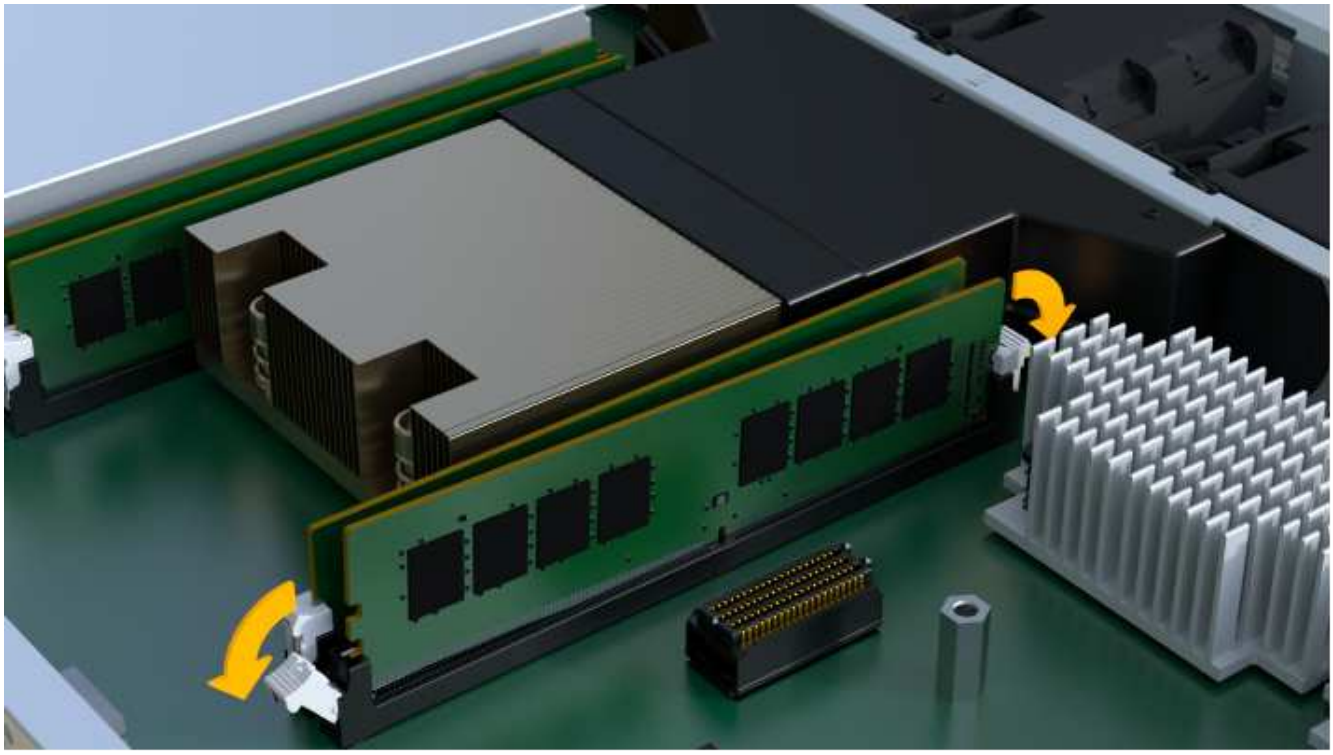
1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

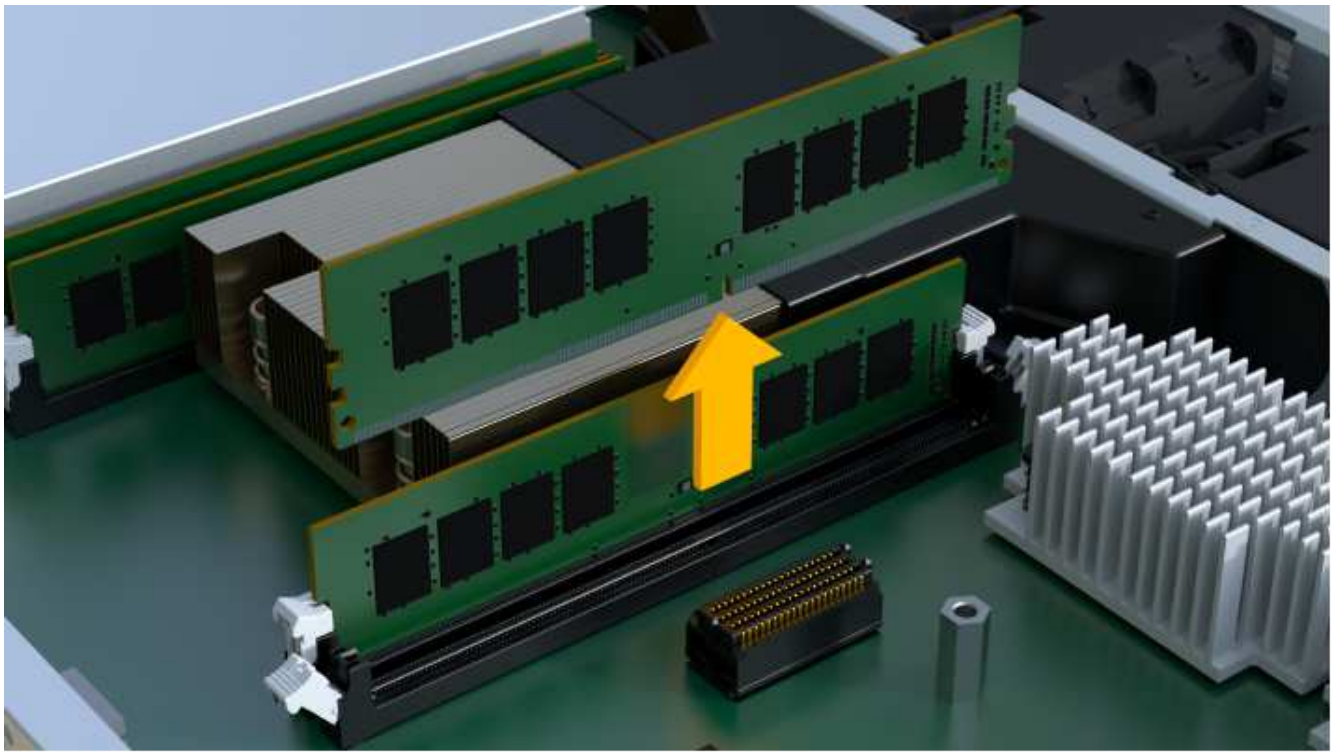
   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

3. Individuare i DIMM sul controller.
4. Prendere nota dell'orientamento del DIMM nello zoccolo in modo da poter inserire il DIMM sostitutivo nell'orientamento corretto.

   > Una tacca nella parte inferiore del DIMM consente di allineare il DIMM durante l'installazione.

5. Spingere lentamente verso l'esterno le due linguette di espulsione dei moduli DIMM su entrambi i lati del modulo DIMM per estrarlo dal relativo slot, quindi farlo scorrere verso l'esterno.





Tenere il modulo DIMM per i bordi in modo da evitare di esercitare pressione sui componenti della scheda a circuiti stampati del modulo DIMM.

Il numero e la posizione dei DIMM di sistema dipendono dal modello del sistema.

Fase 5: Installare nuovi DIMM

Installare un nuovo DIMM per sostituire quello vecchio.

Fasi

1. Tenere il modulo DIMM per gli angoli e allinearlo allo slot.

   La tacca tra i pin del DIMM deve allinearsi con la linguetta dello zoccolo.

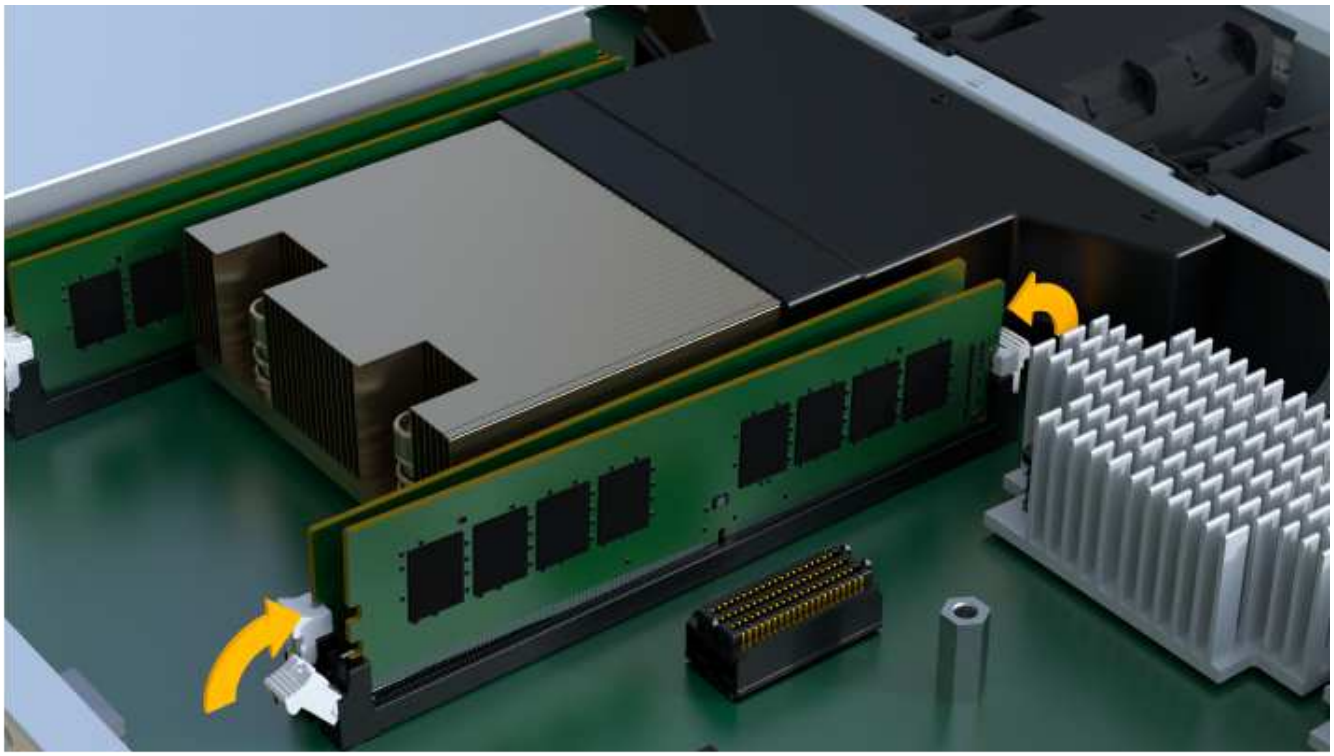
2. Inserire il DIMM nello slot.

   Il DIMM si inserisce saldamente nello slot, ma dovrebbe essere inserito facilmente. In caso contrario, riallineare il DIMM con lo slot e reinserirlo.

   > Esaminare visivamente il DIMM per verificare che sia allineato in modo uniforme e inserito completamente nello slot.

3. Spingere con cautela, ma con decisione, sul bordo superiore del DIMM fino a quando i fermi non scattano in posizione sulle tacche alle estremità del DIMM.

   > I DIMM si inseriscono saldamente. Potrebbe essere necessario premere delicatamente su un lato alla volta e fissare ciascuna linguetta singolarmente.



Fase 6: Reinstallare il contenitore del controller

Dopo aver installato i nuovi DIMM, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

   > Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

3. Ricollegare tutti i cavi.

Fase 7: Completare la sostituzione dei moduli DIMM

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Posizionare il controller online.
   a. In System Manager, accedere alla pagina hardware.
   b. Selezionare **Mostra retro del controller**.
   c. Selezionare il controller con i DIMM sostituiti.
   d. Selezionare **Place online** dall'elenco a discesa.
2. All'avvio del controller, controllare i LED del controller.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se non è presente un Recovery Guru o se si seguono le fasi del Recovery Guru, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione del modulo DIMM è completata. È possibile riprendere le normali operazioni.

Dischi

Requisiti per la sostituzione del disco EF300 o EF600

Prima di sostituire un disco in un array EF300 o EF600, esaminare i requisiti e le considerazioni.

> Tenere presente che i dischi dell'array di storage sono fragili; una gestione errata dei dischi è la causa principale del guasto dei dischi.

Requisiti per la sostituzione del disco

Attenersi alle seguenti regole per evitare di danneggiare le unità dello storage array:

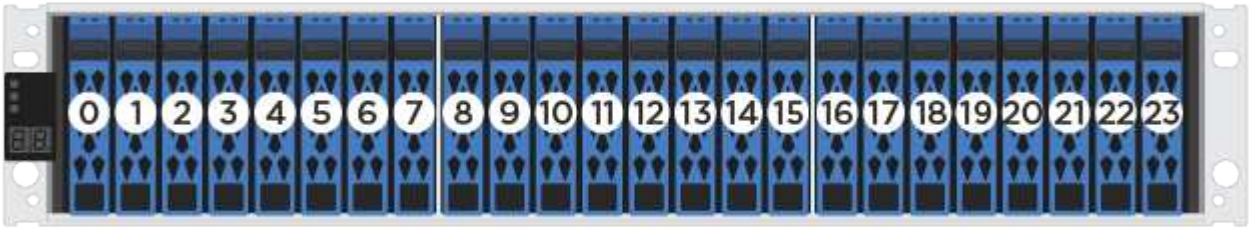
- Prevenzione delle scariche elettrostatiche (ESD):
  - Tenere l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
  - Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici. Non inserire utensili metallici o coltelli nel sacchetto ESD.
  - Conservare il sacchetto ESD e il materiale di imballaggio nel caso in cui sia necessario restituire un'unità in un secondo momento.
  - Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis dell'enclosure di storage. Se non è disponibile un braccialetto, toccare una superficie non verniciata sullo chassis del cabinet di storage prima di maneggiare il disco.

- Gestire i dischi con attenzione:
  - Utilizzare sempre due mani per rimuovere, installare o trasportare un disco.
  - Non forzare mai un'unità in uno shelf e esercitare una pressione leggera e decisa per inserire completamente il dispositivo di chiusura dell'unità.
  - Posizionare i dischi su superfici imbottite e non impilare mai i dischi uno sopra l'altro.
  - Non urtare i dischi contro altre superfici.
  - Prima di rimuovere un'unità da uno shelf, sganciare la maniglia e attendere 30 secondi affinché l'unità si spenda.
  - Utilizzare sempre imballaggi approvati per la spedizione delle unità.
- Evitare i campi magnetici. Tenere le unità lontano da dispositivi magnetici.

  I campi magnetici possono distruggere tutti i dati presenti sul disco e causare danni irreparabili ai circuiti del disco.

Unità sbalorditive nello shelf di controller da 24 dischi

Gli shelf standard da 24 dischi richiedono uno scaglionamento delle unità. La figura seguente mostra come i dischi sono numerati in ogni shelf (il pannello anteriore dello shelf è stato rimosso).



Quando si inseriscono meno di 24 dischi in un controller EF300 o EF600, è necessario alternare le due metà del controller. Partendo dall'estrema sinistra e spostandosi verso destra, posizionare i dischi in uno alla volta.

La figura seguente mostra come eseguire lo sfalsamento dei dischi tra le due metà.

Sostituire il disco in un array EF300

È possibile sostituire un disco in un array EF300.

EF300 supporta l'espansione SAS con shelf da 24 e 60 dischi. La procedura da seguire dipende dal fatto che si disponga di uno shelf da 24 dischi o di uno shelf da 60 dischi:

- Sostituire l’unità in un EF300 (shelf da 24 dischi)
- Sostituire l’unità in un EF300 (shelf da 60 dischi)

Sostituire l’unità in un EF300 (shelf da 24 dischi)

Seguire questa procedura per sostituire un disco in uno shelf da 24 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell’array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array riceve i/O.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco EF300 o EF600".
- Assicurarsi di disporre di quanto segue:
  - Un’unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Una superficie di lavoro piana e priva di elettricità statica.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l’interfaccia di System Manager, puntare il browser sul nome di dominio o sull’indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco (24 dischi)

Preparare la sostituzione di un disco controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un’unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull’unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l’unità sostitutiva abbia una capacità uguale o superiore a quella dell’unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema SANtricity per individuare l’unità all’interno dell’array di storage: Dal menu di scelta rapida dell’unità, selezionare **attiva indicatore localizzatore**.

   Il LED di attenzione del disco (ambra) lampeggia per identificare il disco da sostituire.

Se si sostituisce un'unità in uno shelf dotato di pannello, rimuovere il pannello per visualizzare i LED dell'unità.

Fase 2: Rimozione del disco guasto (24 dischi)

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

   Conservare tutti i materiali di imballaggio.

2. Premere il pulsante di rilascio sul disco guasto.

   - Per i dischi negli shelf di controller E5724 o negli shelf di dischi DE224C, il pulsante di rilascio si trova nella parte superiore dell'unità. La maniglia della camma sulle molle del disco si apre parzialmente e il disco si disinnesta dalla scheda intermedia.

3. Aprire la maniglia della camma ed estrarre leggermente l'unità.
4. Attendere 30 secondi.
5. Rimuovere l'unità dallo shelf con entrambe le mani.
6. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
7. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

Fase 3: Installazione di un nuovo disco (24 dischi)

Viene installata una nuova unità per sostituire quella guasta. Installare l'unità sostitutiva il prima possibile dopo aver rimosso l'unità guasta. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

Fasi

1. Aprire la maniglia della camma.
2. Con due mani, inserire l'unità sostitutiva nell'alloggiamento aperto, spingendo con decisione fino a quando non si arresta.
3. Chiudere lentamente la maniglia della camma fino a quando l'unità non è completamente inserita nel piano intermedio e la maniglia non scatta in posizione.

Il LED verde sull'unità si accende quando l'unità è inserita correttamente.

> A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco (24 dischi)

Verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita.

   Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.

   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   > Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.
4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire l'unità in un EF300 (shelf da 60 dischi)

Seguire questa procedura per sostituire un disco in uno shelf da 60 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare

un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array sta ricevendo le operazioni di i/O.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco EF300 o EF600".
- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco (60 dischi)

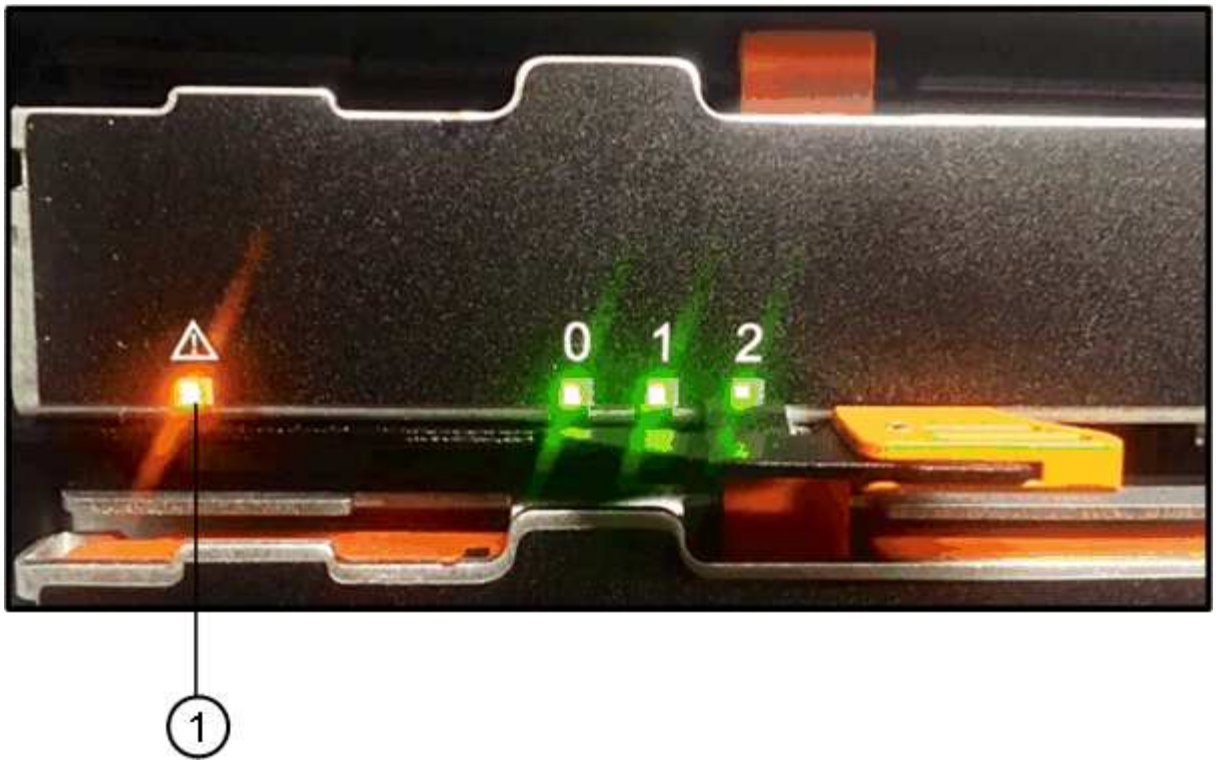
Preparare la sostituzione di un disco controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema di SANtricity per individuare il disco all'interno dello storage array.
   a. Se lo shelf è dotato di una cornice, rimuovetela per vedere i LED.
   b. Dal menu di scelta rapida del disco, selezionare **attiva indicatore di posizione**.

      Il LED di attenzione del cassetto dell'unità (ambra) lampeggia per consentire l'apertura del cassetto dell'unità corretto e identificare l'unità da sostituire.



(1) *LED attenzione*

c. Sganciare il cassetto dell'unità tirando entrambe le leve.

d. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta.

e. Controllare la parte superiore del cassetto dell'unità per individuare il LED di attenzione davanti a ciascun disco.

(1) *LED attenzione acceso per l'unità in alto a destra*

I LED attenzione cassetto unità si trovano sul lato sinistro davanti a ciascun disco, con un'icona di attenzione sulla maniglia del disco appena dietro il LED.

(1) *icona attenzione*

(2) *LED attenzione*

Fase 2: Rimozione del disco guasto (60 dischi)

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

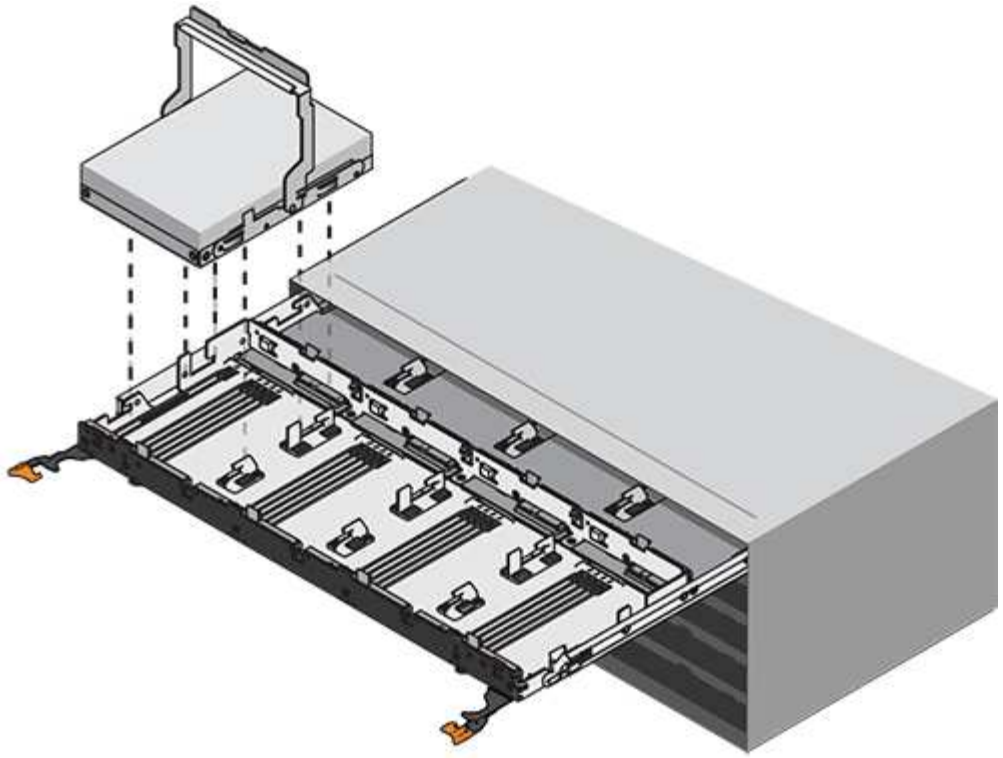
   Conservare tutti i materiali di imballaggio per la prossima volta che sarà necessario restituire un disco.

2. Rilasciare le leve del cassetto dell'unità dal centro del cassetto dell'unità appropriato, tirandole verso i lati del cassetto.
3. Tirare con cautela le leve del cassetto dell'unità esteso per estrarre il cassetto dell'unità fino alla sua estensione completa senza rimuoverlo dal contenitore.
4. Tirare delicatamente indietro il dispositivo di chiusura arancione che si trova davanti all'unità che si desidera rimuovere.

   La maniglia della camma sulle molle di azionamento si apre parzialmente e l'unità viene rilasciata dal cassetto.

(1) *dispositivo di chiusura arancione*

5. Aprire la maniglia della camma ed estrarre leggermente l’unità.
6. Attendere 30 secondi.
7. Utilizzare la maniglia della camma per sollevare l’unità dallo scaffale.



8. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
9. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

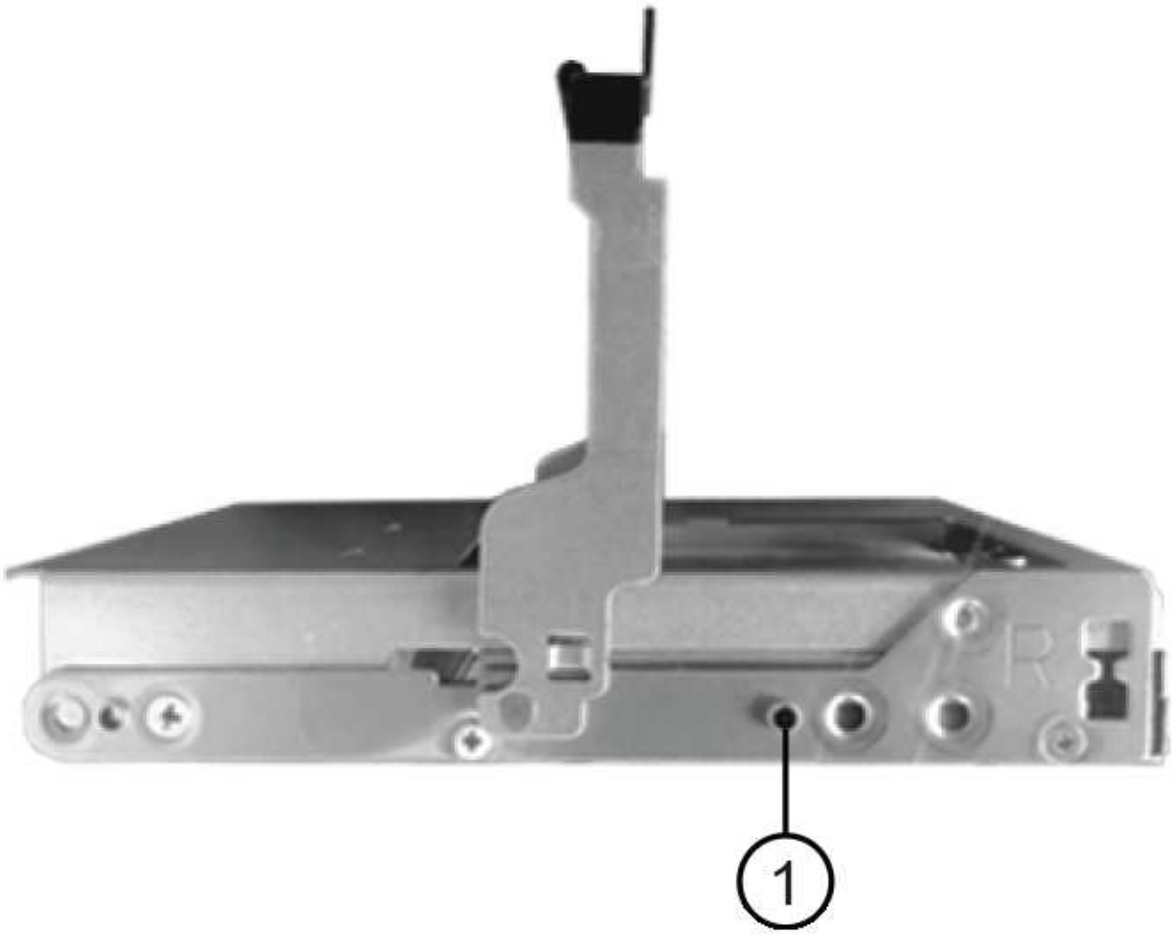
Fase 3: Installazione di un nuovo disco (60 dischi)

Installare un nuovo disco per sostituire quello guasto.

> **Possibile perdita di accesso ai dati** — quando si reinserisce il cassetto del disco nel contenitore, non chiudere mai il cassetto. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.

Fasi

1. Sollevare la maniglia della camma sul nuovo disco in verticale.
2. Allineare i due pulsanti rialzati su ciascun lato del supporto dell'unità con lo spazio corrispondente nel canale dell'unità sul cassetto dell'unità.



(1) *pulsante sollevato sul lato destro del supporto del disco*

3. Abbassare l'unità, quindi ruotare la maniglia della camma verso il basso fino a quando non scatta in posizione sotto il dispositivo di chiusura arancione.
4. Spingere con cautela il cassetto dell'unità all'interno del contenitore. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.
5. Chiudere il cassetto dell'unità spingendo entrambe le leve verso il centro.

   Il LED di attività verde per l'unità sostituita nella parte anteriore del cassetto si accende quando l'unità è inserita correttamente.

   A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco (60 dischi)

Verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita. (Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.
   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.
4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire il disco in un array EF600

È possibile sostituire un disco in un array EF600.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array riceve i/O.

Prima di iniziare

- Revisione "Requisiti per la sostituzione del disco EF300 o EF600".
- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Una superficie di lavoro piana e priva di elettricità statica.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o

sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco

Preparare la sostituzione del disco controllando il guru del ripristino in Gestione sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema SANtricity per individuare l'unità all'interno dell'array di storage: Dal menu di scelta rapida dell'unità, selezionare **attiva indicatore localizzatore**.

   Il LED di attenzione del disco (ambra) lampeggia per identificare il disco da sostituire.

   > Se si sostituisce un'unità in uno shelf dotato di pannello, rimuovere il pannello per visualizzare i LED dell'unità.

Fase 2: Rimuovere l'unità

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

   Conservare tutti i materiali di imballaggio.
2. Premere il pulsante di rilascio nero sul disco guasto.

   Il fermo sulle molle dell'unità si apre parzialmente, quindi l'unità si sgancia dal controller.
3. Aprire la maniglia della camma ed estrarre leggermente l'unità.
4. Attendere 30 secondi.
5. Rimuovere l'unità dallo shelf con entrambe le mani.

6. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
7. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

Fase 3: Installare un nuovo disco

Installare un nuovo disco per sostituire quello guasto. Installare l'unità sostitutiva il prima possibile dopo aver rimosso l'unità guasta.

Fasi

1. Aprire la maniglia della camma.
2. Con due mani, inserire l'unità sostitutiva nell'alloggiamento aperto, spingendo con decisione fino a quando non si arresta.
3. Chiudere lentamente la maniglia della camma fino a quando l'unità non è completamente inserita nel piano intermedio e la maniglia non scatta in posizione.

   Il LED verde sull'unità si accende quando l'unità è inserita correttamente.

> A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco

Completare la sostituzione del disco per verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita. (Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.
   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.

- LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
- LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.

2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.

4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Aggiunta a caldo di uno shelf di dischi

È possibile aggiungere un nuovo shelf di dischi mentre gli altri componenti del sistema di storage sono ancora in funzione. È possibile configurare, riconfigurare, aggiungere o spostare la capacità del sistema storage senza interrompere l'accesso degli utenti ai dati.

Prima di iniziare

A causa della complessità di questa procedura, si consiglia quanto segue:

- Leggere tutti i passaggi prima di iniziare la procedura.
- Assicurarsi che l'aggiunta a caldo di uno shelf di dischi sia la procedura necessaria.

A proposito di questa attività

Questa procedura si applica all'aggiunta a caldo di uno shelf di dischi DE212C, DE224C o DE460C a E2800, E2800, EF280, E5700, E5700B, Shelf di controller EF570, EF300 o EF600.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

> Per mantenere l'integrità del sistema, seguire la procedura esattamente nell'ordine suggerito.

Fase 1: Preparazione all'aggiunta dello shelf di dischi

Per prepararsi all'aggiunta a caldo di uno shelf di dischi, è necessario verificare la presenza di eventi critici e lo stato degli IOM.

Prima di iniziare

- La fonte di alimentazione del sistema storage deve essere in grado di soddisfare i requisiti di alimentazione del nuovo shelf di dischi. Per le specifiche di alimentazione dello shelf di dischi, consultare "Hardware Universe".
- Lo schema di cablaggio per il sistema storage esistente deve corrispondere a uno degli schemi applicabili illustrati in questa procedura.

Fasi

1. In Gestore di sistema di SANtricity, selezionare **supporto** > **Centro di supporto** > **Diagnostica**.
2. Selezionare **Collect Support Data**.

   Viene visualizzata la finestra di dialogo Collect Support Data (raccolta dati di supporto).

3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome support-data.7z. I dati non vengono inviati automaticamente al supporto tecnico.

4. Selezionare **supporto** > **Registro eventi**.

   La pagina Registro eventi visualizza i dati dell'evento.

5. Selezionare l'intestazione della colonna **priorità** per ordinare gli eventi critici all'inizio dell'elenco.
6. Esaminare gli eventi critici di sistema per gli eventi che si sono verificati nelle ultime due o tre settimane e verificare che gli eventi critici recenti siano stati risolti o altrimenti risolti.

   > Se si sono verificati eventi critici non risolti nelle due o tre settimane precedenti, interrompere la procedura e contattare il supporto tecnico. Continuare la procedura solo dopo aver risolto il problema.

7. Selezionare **hardware**.
8. Selezionare l'icona **IOM (ESM)**.

   Viene visualizzata la finestra di dialogo Shelf Component Settings (Impostazioni componenti shelf) con la scheda **IOM (ESM)** selezionata.

9. Assicurarsi che lo stato visualizzato per ogni IOM/ESM sia *ottimale*.
10. Fare clic su **Mostra altre impostazioni**.
11. Verificare che sussistano le seguenti condizioni:
    - Il numero di ESM/IOM rilevati corrisponde al numero di ESM/IOM installati nel sistema e a quello di ogni shelf di dischi.
    - Entrambi gli ESM/IOM mostrano che la comunicazione è corretta.
    - La velocità di trasferimento dati è di 12 GB/s per gli shelf di dischi DE212C, DE224C e DE460C o di 6 GB/s per gli altri tray di dischi.

Fase 2: Installare lo shelf di dischi e alimentare

Si installa un nuovo shelf di dischi o uno shelf di dischi precedentemente installato, si accende l'alimentazione e si verifica la presenza di eventuali LED che richiedono attenzione.

Fasi

1. Se si sta installando uno shelf di dischi precedentemente installato in un sistema storage, rimuovere i dischi. I dischi devono essere installati uno alla volta più avanti in questa procedura.

   Se la cronologia di installazione dello shelf di dischi che si sta installando non è nota, si deve presumere che sia stato precedentemente installato in un sistema storage.

2. Installare lo shelf di dischi nel rack che contiene i componenti del sistema di storage.

   > Consultare le istruzioni di installazione del modello in uso per la procedura completa per l'installazione fisica e il cablaggio di alimentazione. Le istruzioni di installazione del modello in uso includono note e avvisi da tenere in considerazione per installare in sicurezza uno shelf di dischi.

3. Accendere il nuovo shelf di dischi e verificare che sullo shelf non siano accesi LED di attenzione color ambra. Se possibile, risolvere eventuali condizioni di guasto prima di continuare con questa procedura.

Fase 3: Collegare il sistema via cavo

Selezionare una delle seguenti opzioni:

- Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700
- Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

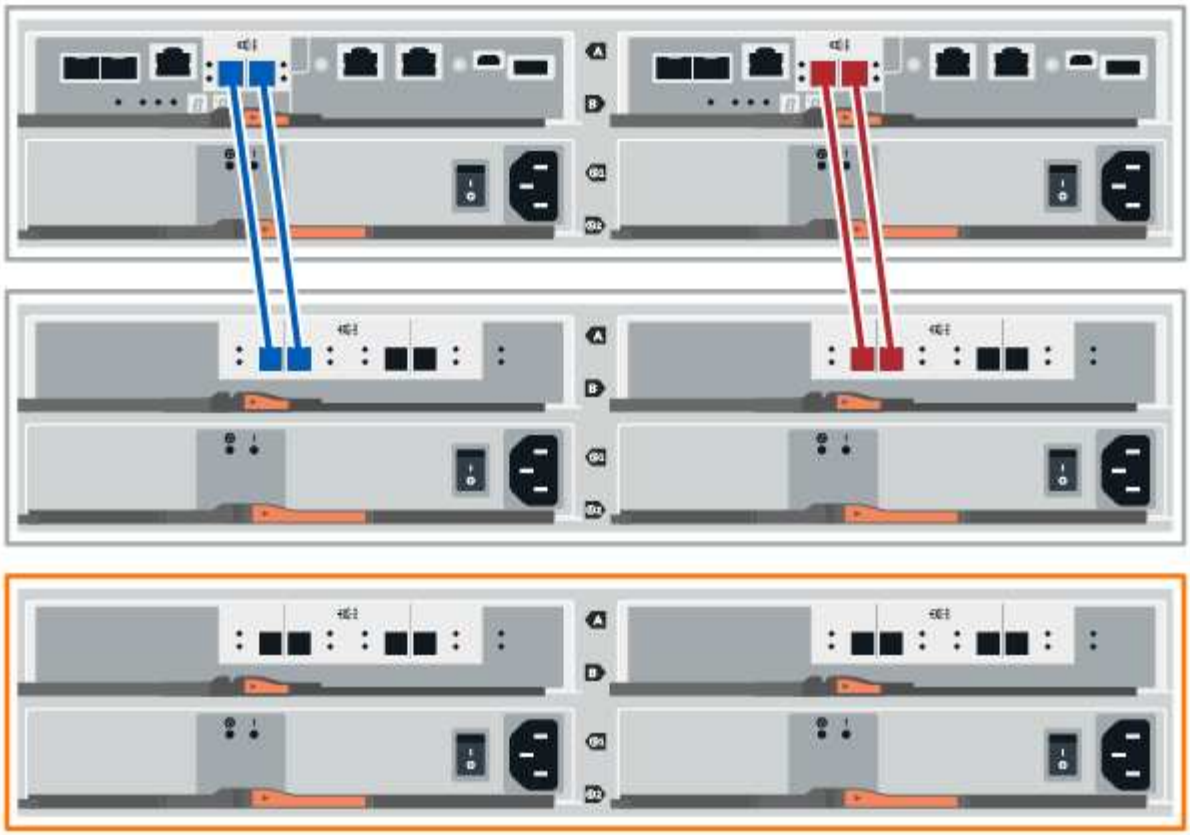
Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700

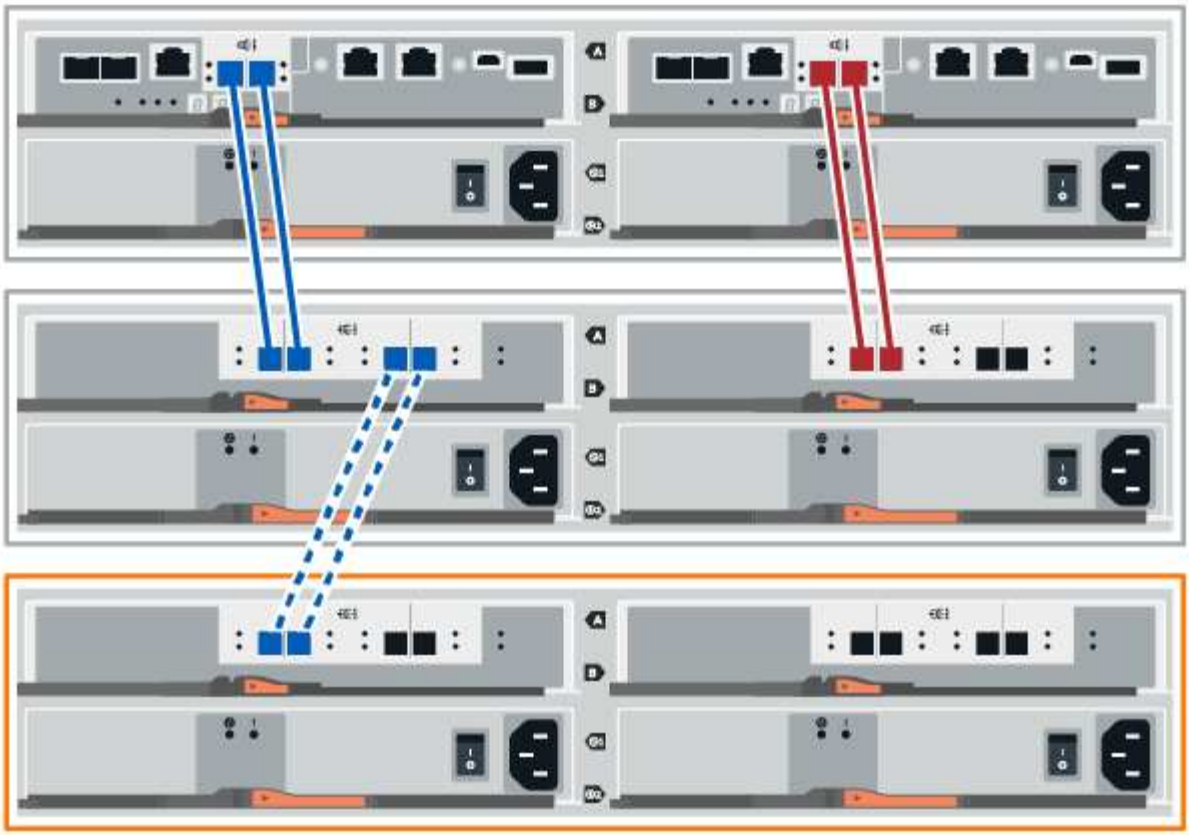
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Fasi

1. Collegare lo shelf di dischi al controller A.

   La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller A. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".





2. In Gestione sistema di SANtricity, fare clic su **hardware**.

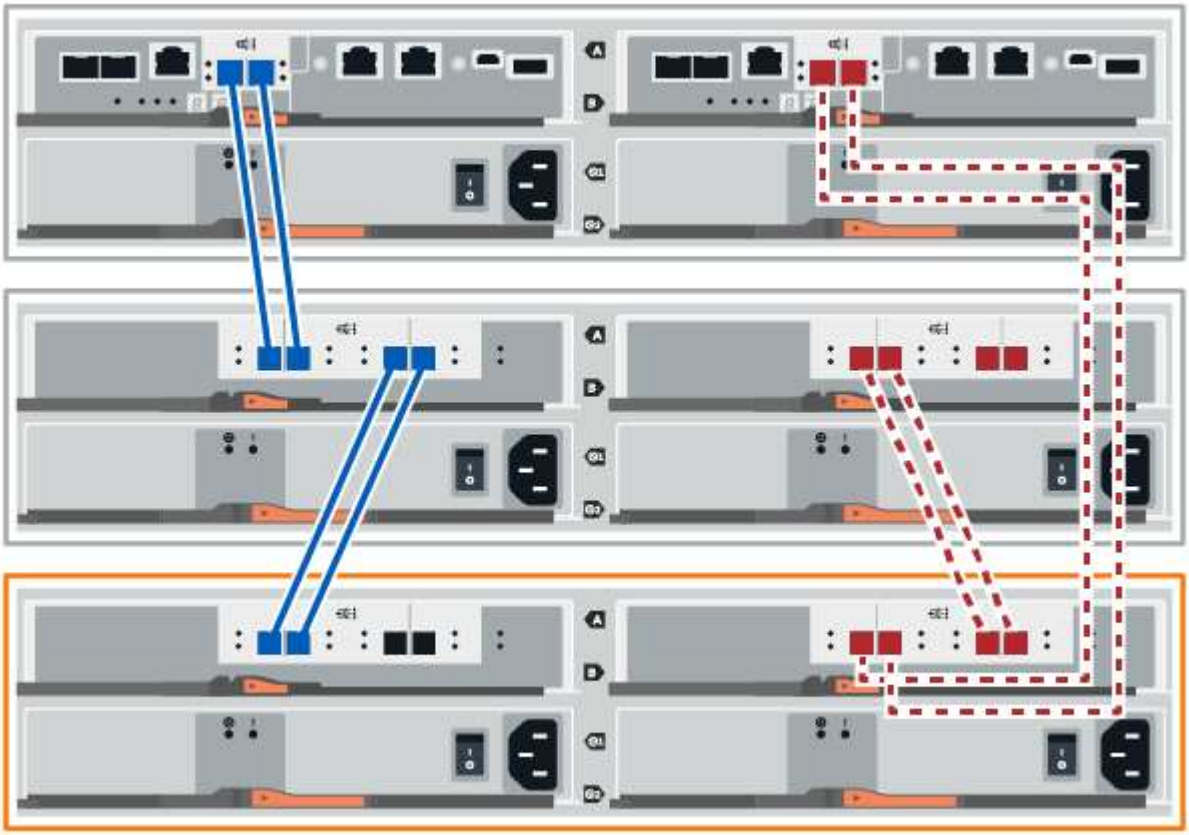
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

3. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
4. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

   Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

5. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
6. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
7. Scollegare tutti i cavi di espansione dal controller B.
8. Collegare lo shelf di dischi al controller B.

La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller B. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



9. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

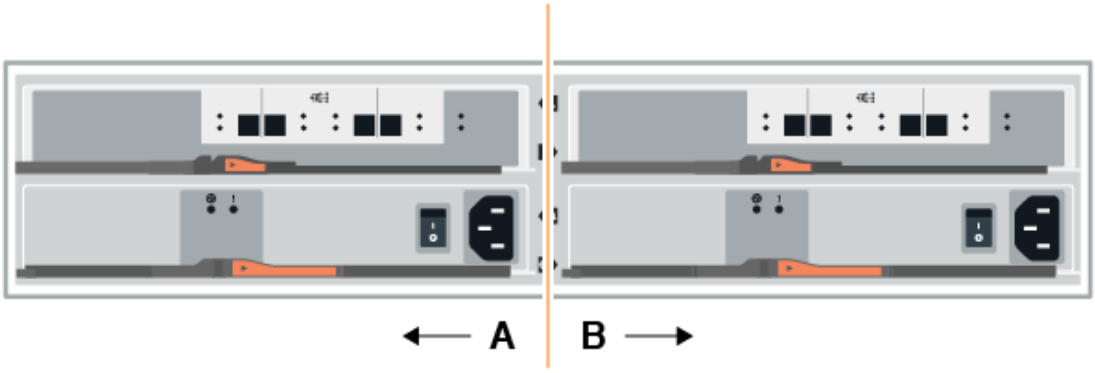
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Prima di iniziare

- Il firmware è stato aggiornato alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".

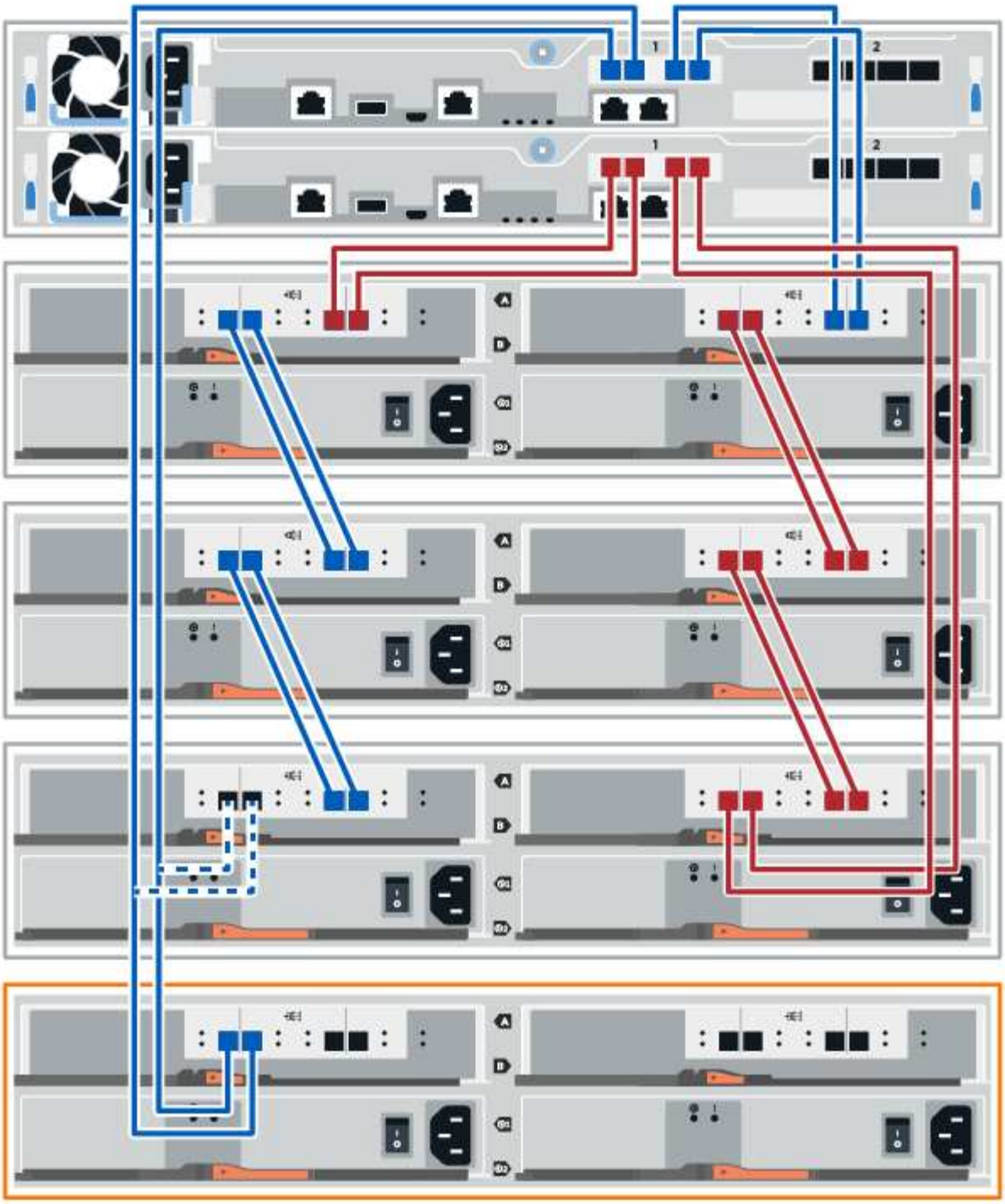
Fasi

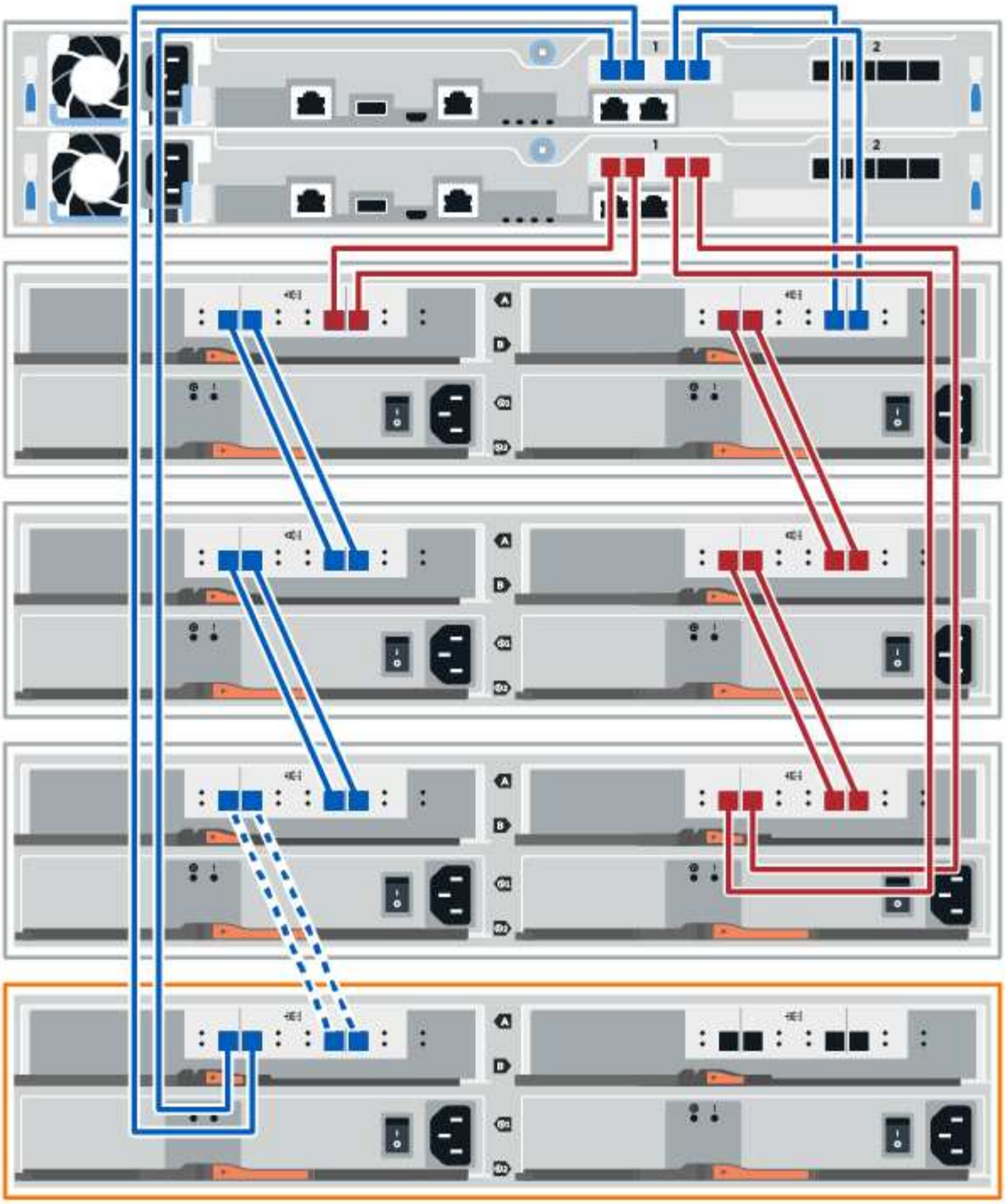
1. Scollegare entrambi i cavi del controller Lato A dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.



2. Collegare i cavi alle porte IOM12 lato A tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di connessione per un lato tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".


1
2
1
2
A
B



3. In Gestione sistema di SANtricity, fare clic su **hardware**.

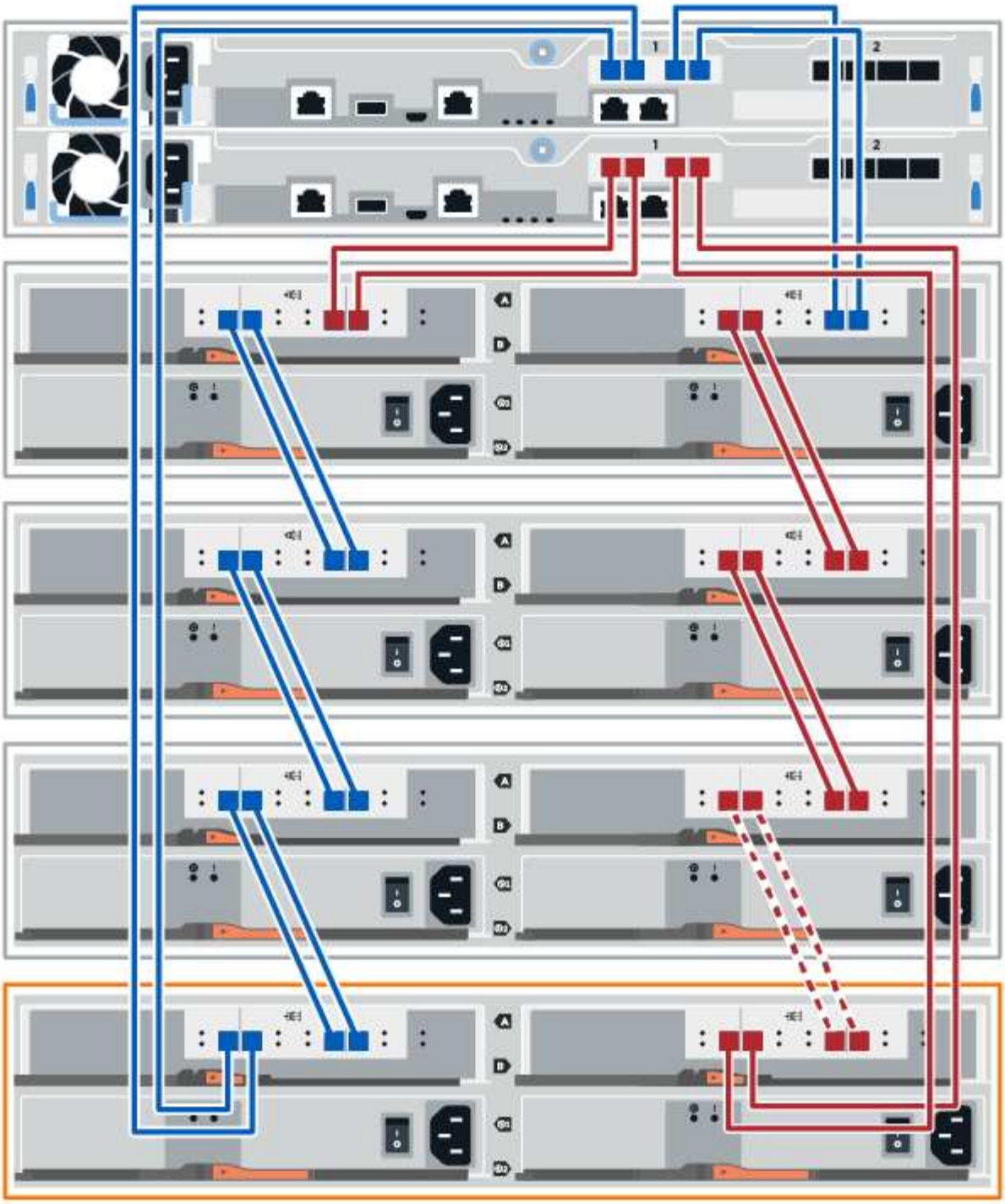
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

4. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
5. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

6. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
7. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
8. Scollegare entrambi i cavi del controller lato B dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.
9. Collegare i cavi alle porte IOM12 lato B tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di collegamento per il lato B tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



10. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Fase 4: Completare l'aggiunta a caldo

Per completare l'aggiunta a caldo, verificare la presenza di eventuali errori e confermare che lo shelf di dischi appena aggiunto utilizzi il firmware più recente.

Fasi

1. In Gestore di sistema di SANtricity, fare clic su **Home**.
2. Se il collegamento **Recover from Problems** (Ripristina da problemi) viene visualizzato al centro della pagina, fare clic sul collegamento e risolvere eventuali problemi indicati nel Recovery Guru.
3. In Gestione sistema di SANtricity, fare clic su **hardware** e scorrere verso il basso, se necessario, per visualizzare lo shelf di dischi appena aggiunto.
4. Per i dischi precedentemente installati in un sistema storage diverso, aggiungere un disco alla volta allo shelf di dischi appena installato. Attendere che ogni disco venga riconosciuto prima di inserire il disco successivo.

   Quando un disco viene riconosciuto dal sistema di storage, la rappresentazione dello slot nella pagina **hardware** viene visualizzata come un rettangolo blu.

5. Selezionare la scheda **Support** > **Support Center** > **Support Resources**.
6. Fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware) e verificare quali versioni del firmware IOM/ESM e del firmware del disco sono installate sul nuovo shelf di dischi.

   > Potrebbe essere necessario scorrere la pagina verso il basso per individuare questo collegamento.

7. Se necessario, aggiornare il firmware del disco.

   Il firmware IOM/ESM viene aggiornato automaticamente alla versione più recente, a meno che non sia stata disattivata la funzione di aggiornamento.

La procedura di aggiunta a caldo è stata completata. È possibile riprendere le normali operazioni.

Ventole

Requisiti per la sostituzione delle ventole EF300 o EF600

Prima di sostituire una ventola guasta in un array EF300 o EF600, esaminare i seguenti requisiti.

- Si dispone di una ventola sostitutiva supportata per il modello di shelf di controller o di dischi.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.

> Se il Recovery Guru indica che non è possibile rimuovere la ventola, contattare il supporto tecnico.

Sostituire una ventola EF300 o EF600

È possibile sostituire una ventola in un array EF300 o EF600.

A proposito di questa attività

Ogni shelf o shelf di controller EF300 e EF600 include cinque ventole. In caso di guasto di una ventola, è necessario sostituirla il prima possibile per assicurarsi che lo shelf abbia un raffreddamento adeguato.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Una ventola sostitutiva.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Un'area di lavoro piana e priva di elettricità statica.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare il controller offline

Posizionare il contenitore del controller offline in modo da poter sostituire in sicurezza la ventola guasta.

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una ventola e per assicurarsi che non siano prima necessari altri elementi da risolvere.
2. Dall'area Details (Dettagli) del Recovery Guru, determinare quale ventola sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   a. Selezionare **hardware**.
   b. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
   c. Selezionare il controller che si desidera mettere offline.
   d. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

6. Selezionare **ricontrollare** dal Recovery Guru e confermare che il campo **OK per rimuovere** nell'area Dettagli sia Sì, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter sostituire la ventola guasta con una nuova.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere la ventola guasta

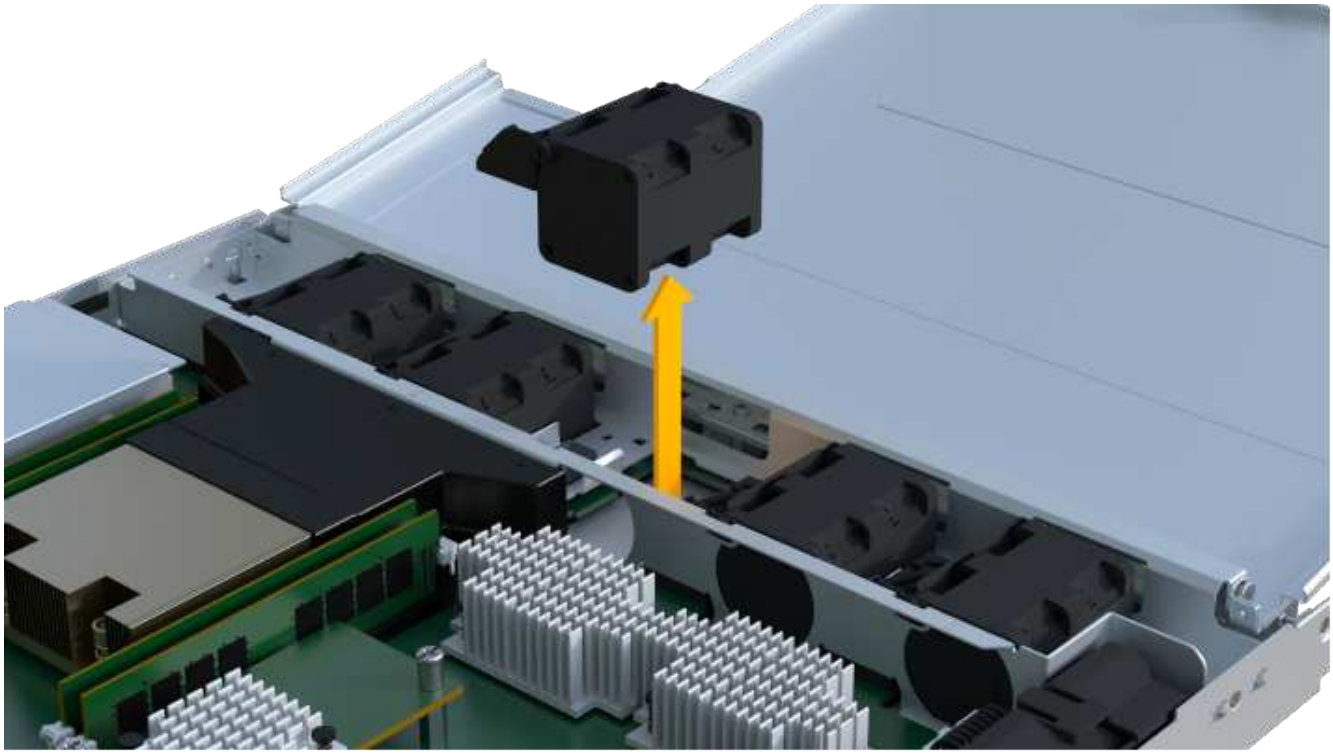
Rimuovere una ventola guasta per poterla sostituire con una nuova.

Fasi

1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

3. Sollevare delicatamente la ventola guasta dal controller.

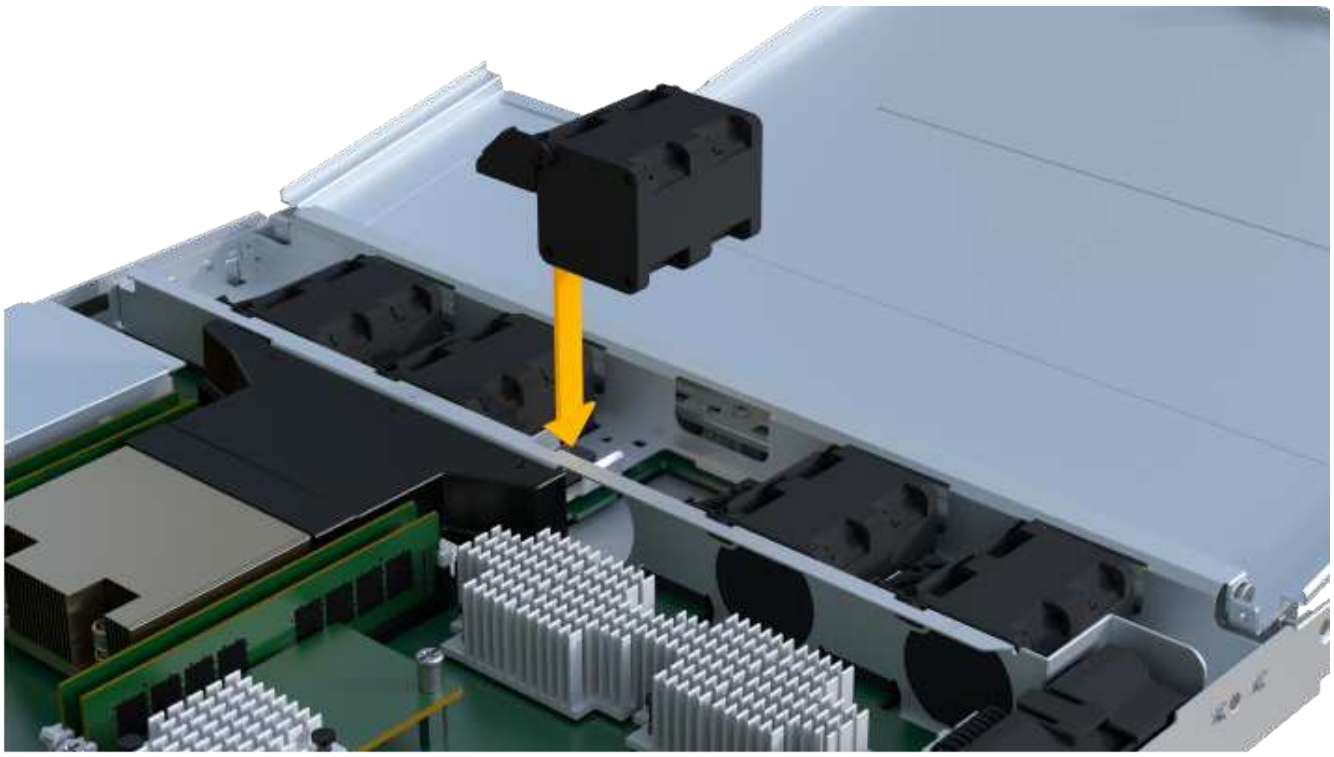


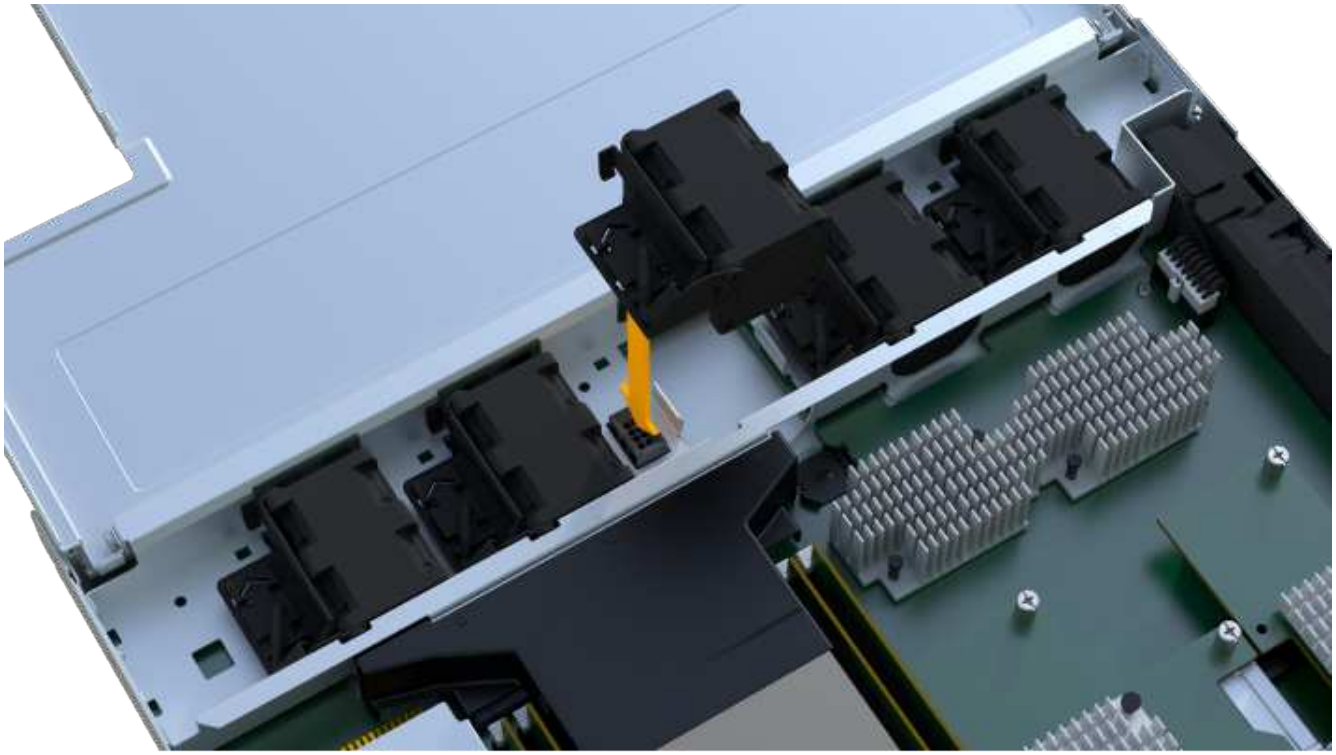
Fase 4: Installare una nuova ventola

Installare una nuova ventola per sostituire quella guasta.

Fasi

1. Far scorrere la ventola di ricambio fino in fondo nello scaffale.





Fase 5: Reinstallare il contenitore del controller

Dopo aver installato la nuova ventola, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

> Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

Fase 6: Sostituzione completa della ventola

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

1. Posizionare il controller online.
   a. In System Manager, accedere alla pagina hardware.
   b. Selezionare **Mostra retro del controller**.
   c. Selezionare il controller con la ventola sostituita.
   d. Selezionare **Place online** dall'elenco a discesa.
2. All'avvio del controller, controllare i LED del controller.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della ventola è completata. È possibile riprendere le normali operazioni.

Schede di interfaccia host

Requisiti per gli aggiornamenti HIC EF300 o EF600

Prima di aggiornare o sostituire una scheda di interfaccia host (HIC) in un array EF300 o EF600, esaminare i seguenti requisiti.

- È stata pianificata una finestra di manutenzione dei downtime per questa procedura. Non è possibile accedere ai dati sull'array di storage fino a quando la procedura non è stata completata correttamente. Poiché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi, l'alimentazione deve essere disattivata quando si modifica la configurazione HIC. La presenza di HICS non corrispondenti causa il blocco del controller con l'HIC sostitutivo quando lo si porta online.
- Sono disponibili tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host Bus Adapter) necessari per collegare le nuove porte host.

  Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Hai un cacciavite Phillips n. 1.
- Sono presenti etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del

controller.

- Alcuni aggiornamenti o sostituzioni HIC potrebbero richiedere una conversione del protocollo della porta host. Seguire le istruzioni in Modificare il protocollo host per EF300 o EF600 per questo requisito.
- I controller EF300 devono avere la porta HIC 2 piena di un HIC per la connettività host.

Upgrade della scheda di interfaccia host (HIC) EF300 o EF600

È possibile aggiornare le schede di interfaccia host (HICS) per aumentare il numero di porte host o modificare i protocolli host.

A proposito di questa attività

- Quando si aggiorna HICS, è necessario spegnere lo storage array, aggiornare l'HICS e riapplicare l'alimentazione.
- Quando si aggiorna HICS in un controller EF300 o EF600, ripetere tutti i passaggi per rimuovere il secondo controller, aggiornare l'HICS del secondo controller e reinstallare il secondo controller prima di riapplicare l'alimentazione allo shelf del controller.

Prima di iniziare

- Revisione "Requisiti per gli aggiornamenti HIC EF300 o EF600".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Non è possibile accedere ai dati sull'array di storage fino a quando la procedura non è stata completata correttamente. Poiché entrambi i controller devono avere la stessa configurazione HIC quando sono accesi, l'alimentazione deve essere disattivata quando si installa HICS.
- Assicurarsi di disporre di quanto segue:
  - Due HICS compatibili con i controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Un cacciavite Phillips n. 1.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

> **Possibile perdita di accesso ai dati** — non installare mai un HIC in un contenitore di controller EF300 o EF600 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fase 1: Posizionare lo shelf del controller offline

Posiziona lo shelf del controller offline in modo da poter aggiornare l'HICS in tutta sicurezza.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

3. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

4. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

5. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
6. Spegnere lo shelf del controller.
   a. Etichettare e scollegare entrambi i cavi di alimentazione dallo shelf del controller.
   b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller per aggiornare il nuovo HIC.

Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.

2. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Se le porte HIC utilizzano ricetrasmettitori SFP+, rimuoverli.

   A seconda del tipo di HIC a cui si esegue l'aggiornamento, potrebbe essere possibile riutilizzare questi SFP.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere l'HIC

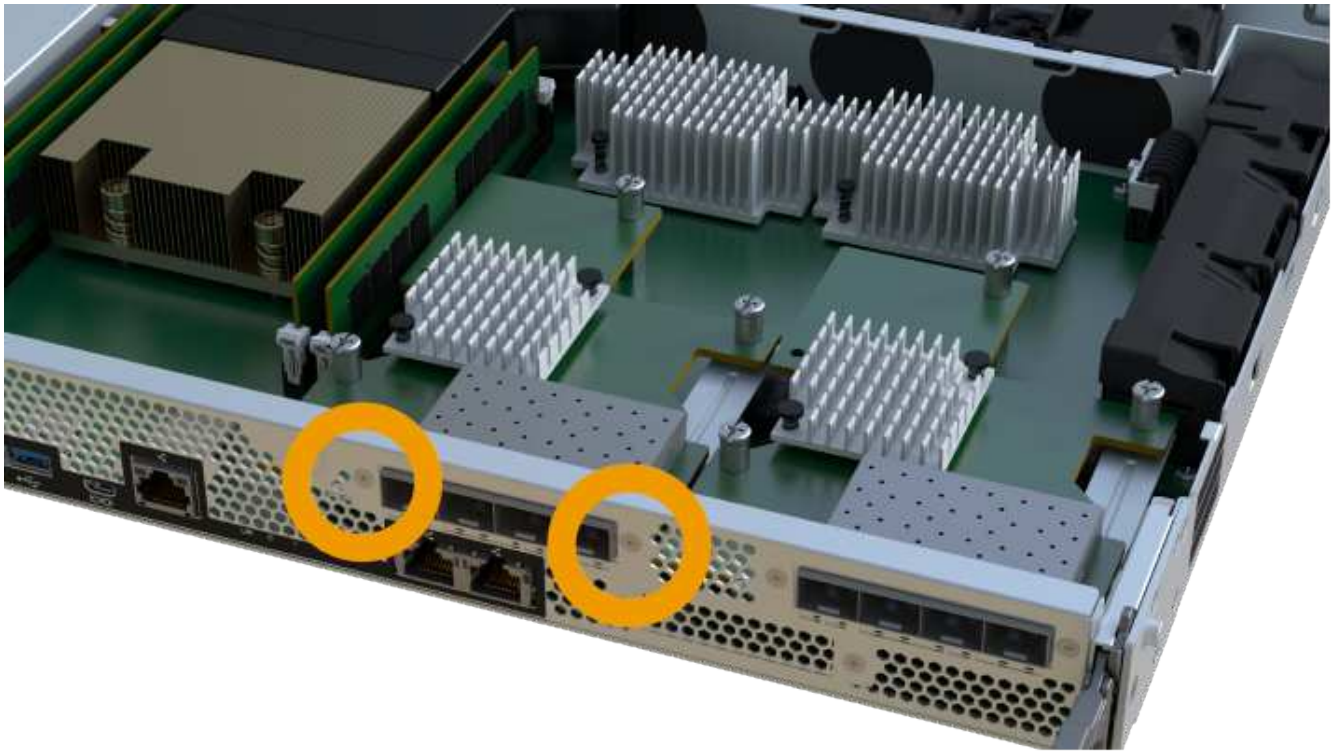
Rimuovere l'HIC originale in modo da poterlo sostituire con uno aggiornato.

Fasi

1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

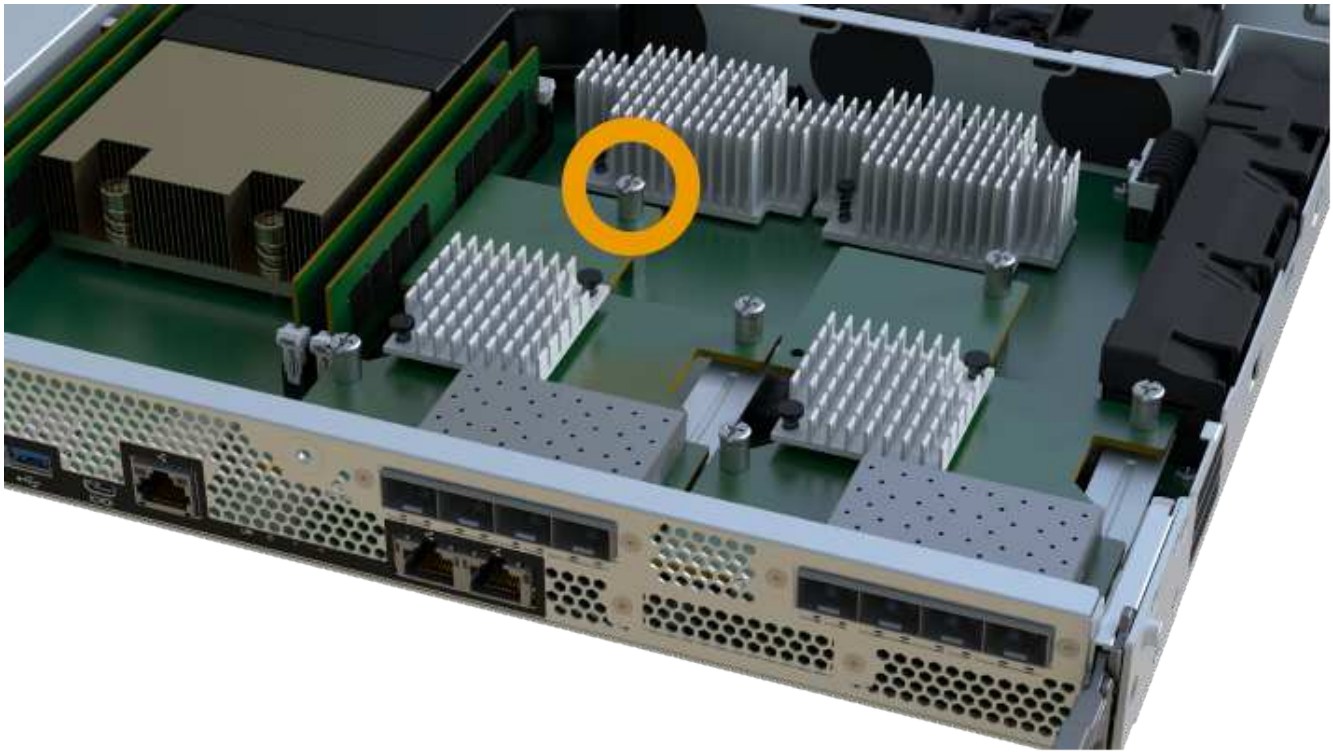
   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

3. Utilizzando un cacciavite Phillips, rimuovere le due viti che fissano la mascherina HIC al contenitore del controller.



L'immagine riportata sopra è un esempio, l'aspetto dell'HIC potrebbe differire.

4. Rimuovere la piastra anteriore dell'HIC.
5. Utilizzando le dita o un cacciavite Phillips, allentare la singola vite a testa zigrinata che fissa l'HIC alla scheda del controller.

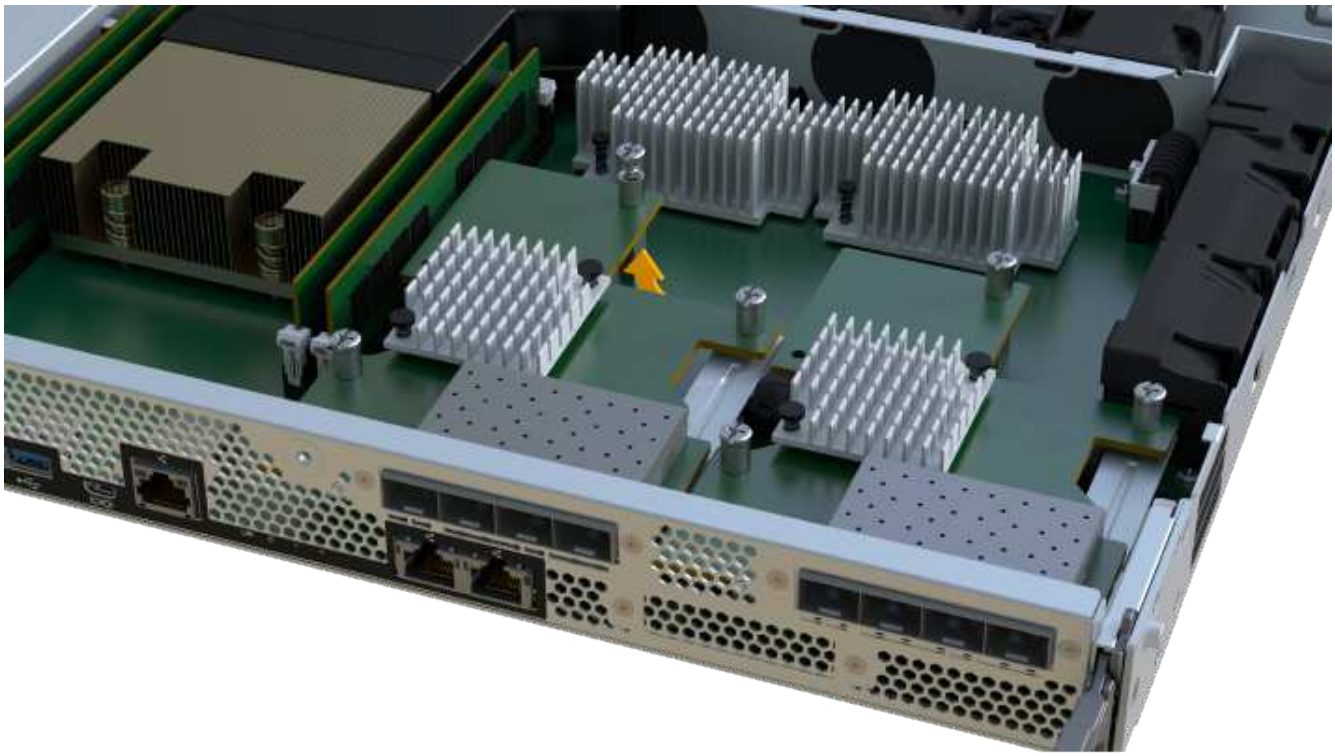


L'HIC viene fornito con tre posizioni delle viti sulla parte superiore, ma è fissato con una sola.

L'immagine riportata sopra è un esempio, l'aspetto dell'HIC potrebbe differire.

6. Scollegare con cautela l'HIC dalla scheda del controller sollevando la scheda e sollevandola dal controller.

Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



L'immagine riportata sopra è un esempio, l'aspetto dell'HIC potrebbe differire.

7. Posizionare l'HIC su una superficie piana e priva di scariche elettrostatiche.

Fase 4: Aggiornare l'HIC

Dopo aver rimosso il vecchio HIC, installare il nuovo HIC.

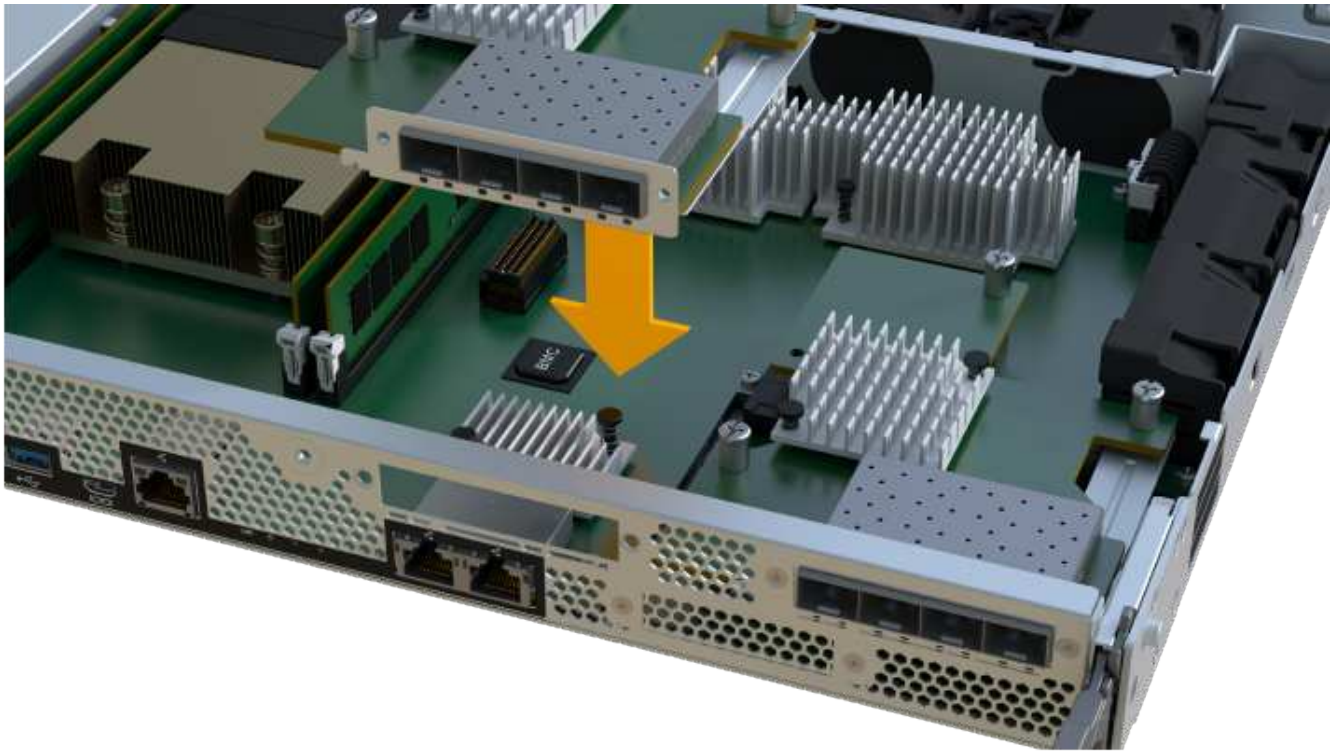
Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore di controller EF300 o EF600 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Allineare la singola vite a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della

scheda del controller.

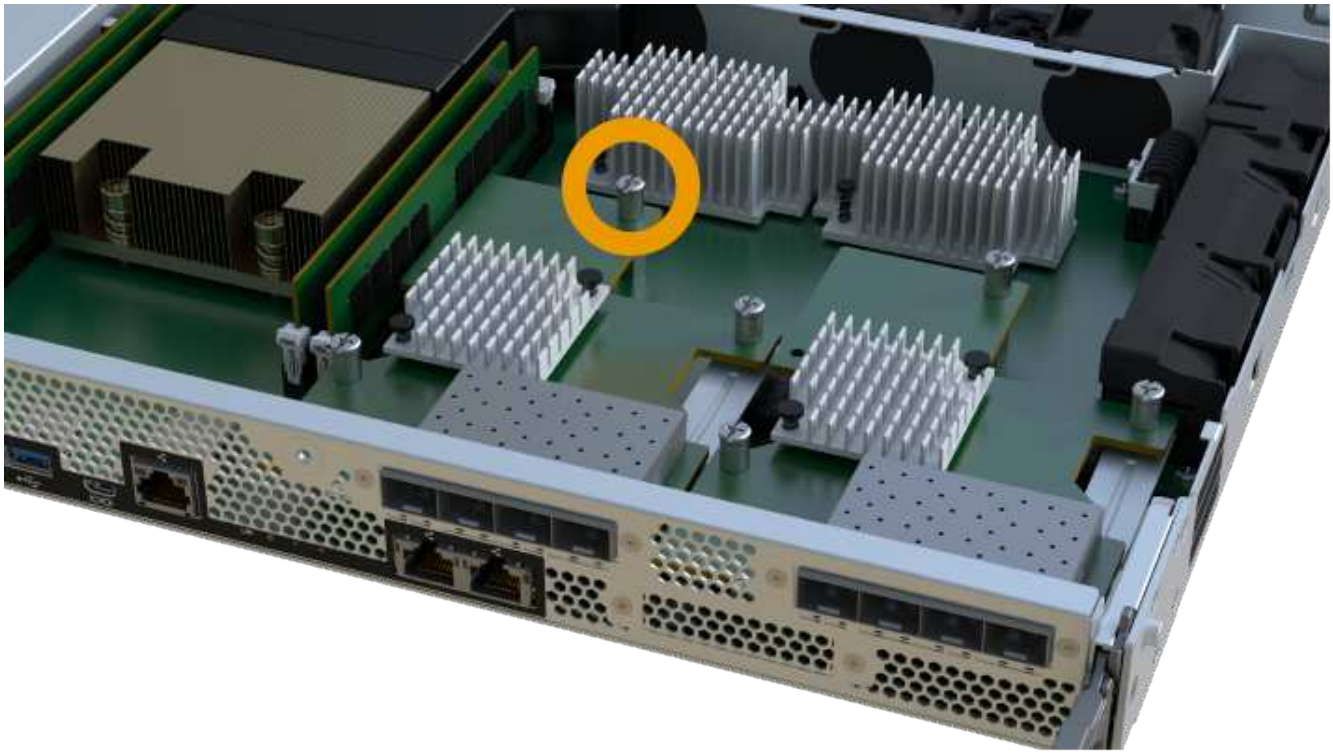


L'immagine riportata sopra è un esempio, l'aspetto dell'HIC potrebbe differire.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e la vite a testa zigrinata.

4. Serrare manualmente la vite a testa zigrinata HIC.



L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dall'HIC originale con le tre viti.

Fase 5: Reinstallare il contenitore del controller

Dopo aver aggiornato l'HIC, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

   Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

3. Se rimossi, installare gli SFP nel nuovo HIC e ricollegare tutti i cavi. Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

Fase 6: Completare l'aggiornamento HIC

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Posizionare il controller online.
   a. Collegare i cavi di alimentazione.
2. All'avvio del controller, controllare i LED del controller.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

Il processo di aggiornamento di una scheda di interfaccia host nell'array di storage è completo. È possibile riprendere le normali operazioni.

Sostituire la scheda di interfaccia host (HIC) guasta in EF300 o EF600

Seguire questa procedura per sostituire una scheda di interfaccia host (HIC) guasta in un array EF300 o EF600.

A proposito di questa attività

Quando si sostituisce un HIC guasto, è necessario spegnere lo storage array, sostituire l'HIC e riapplicare l'alimentazione.

Prima di iniziare

- Revisione "Requisiti per gli aggiornamenti HIC EF300 o EF600".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Non è possibile accedere ai dati sull'array di storage fino a quando la procedura non è stata completata correttamente. Poiché entrambi i controller devono avere la stessa configurazione HIC quando sono accesi, l'alimentazione deve essere disattivata quando si installa HICS.
- Assicurarsi di disporre di quanto segue:
  - HICS compatibili con i controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Un cacciavite Phillips n. 1.

- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

> **Possibile perdita di accesso ai dati** — non installare mai un HIC in un contenitore di controller EF300 o EF600 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fase 1: Posizionare il controller offline

Posizionare il controller interessato offline in modo da poter sostituire l'HICS in modo sicuro.

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.
2. Dall'area Details (Dettagli) del Recovery Guru, determinare quale batteria sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.
   a. Selezionare **hardware**.
   b. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
   c. Selezionare il controller che si desidera mettere offline.
   d. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

   > Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

6. Selezionare **ricontrollare** dal Recovery Guru e confermare che il campo OK per rimuovere nell'area Dettagli visualizza Sì, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter sostituire la scheda di interfaccia host guasta.

Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Se le porte HIC utilizzano ricetrasmettitori SFP+, rimuoverli.

   A seconda del tipo di HIC a cui si esegue l'aggiornamento, potrebbe essere possibile riutilizzare questi SFP.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere l'HIC

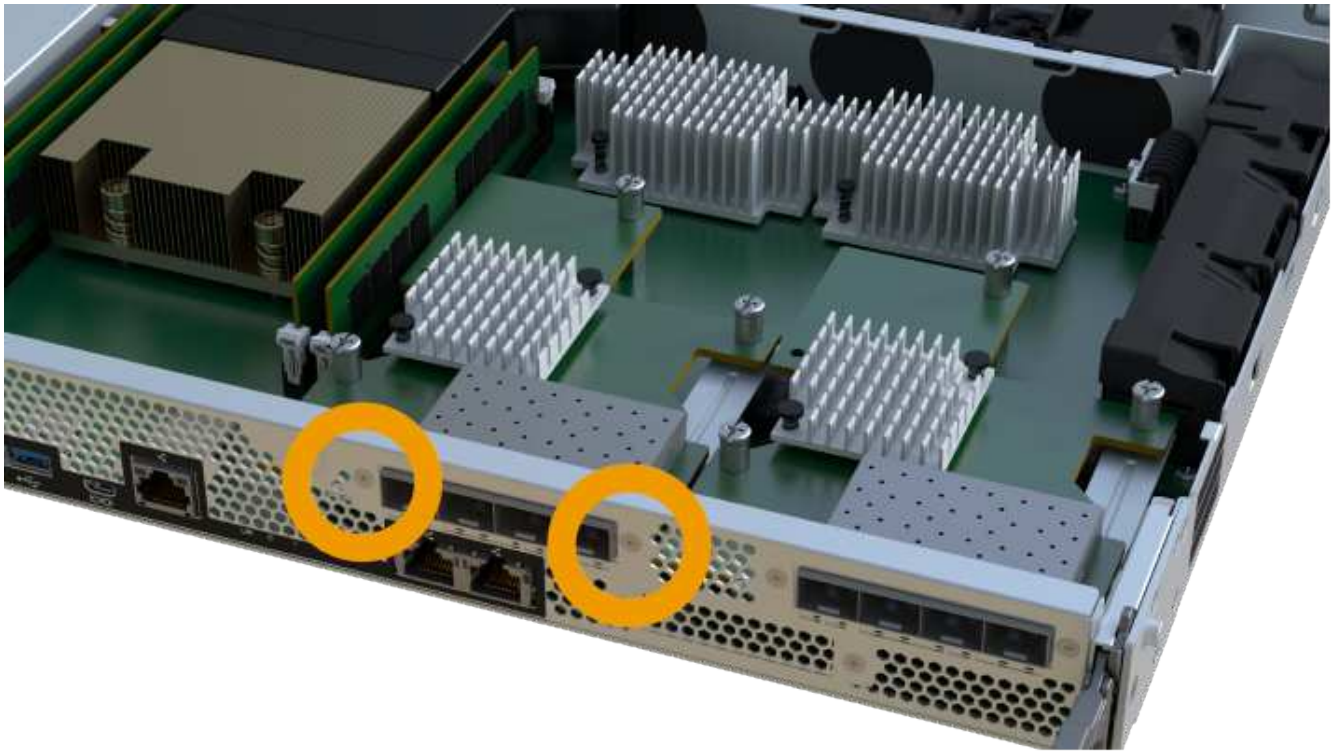
Rimuovere l'HIC originale in modo da poterlo sostituire con uno aggiornato.

Fasi

1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

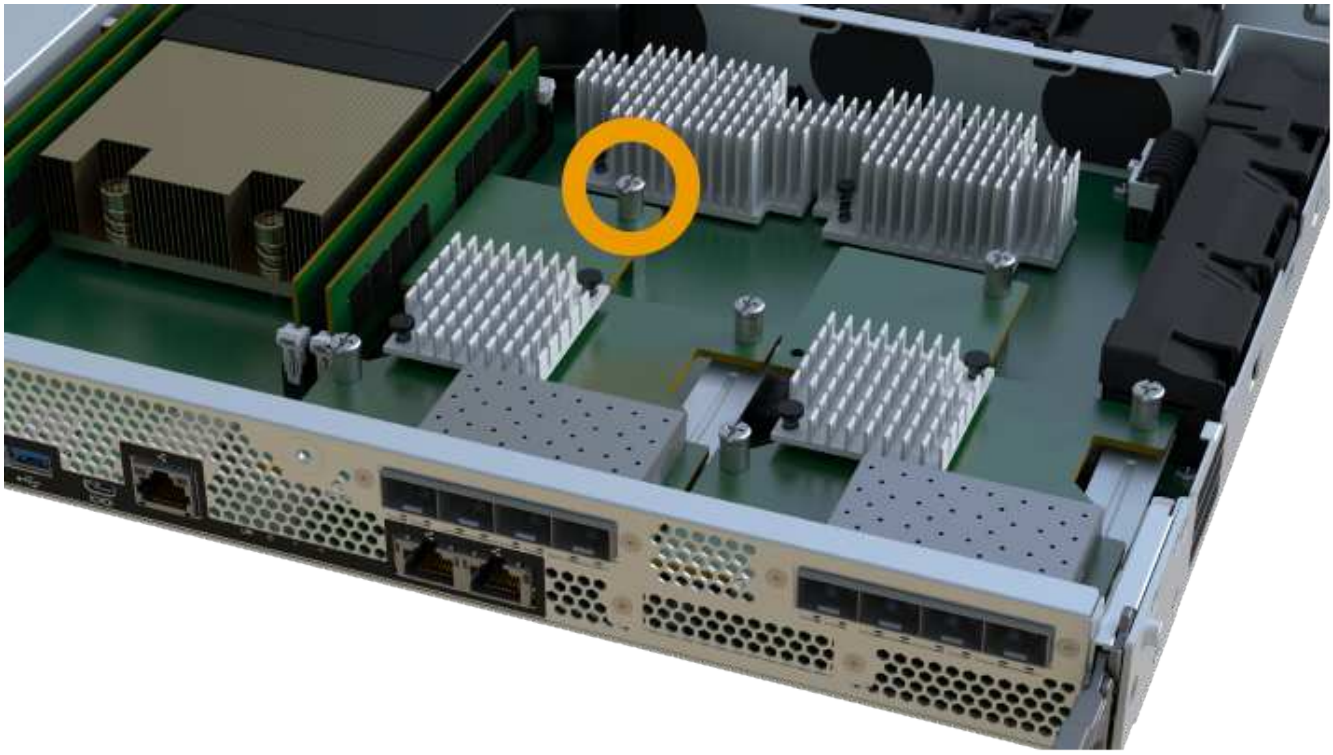
   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

3. Utilizzando un cacciavite Phillips, rimuovere le due viti che fissano la mascherina HIC al contenitore del controller.



L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

4. Rimuovere la piastra anteriore dell'HIC.
5. Utilizzando le dita o un cacciavite Phillips, allentare la singola vite a testa zigrinata che fissa l'HIC alla scheda del controller.

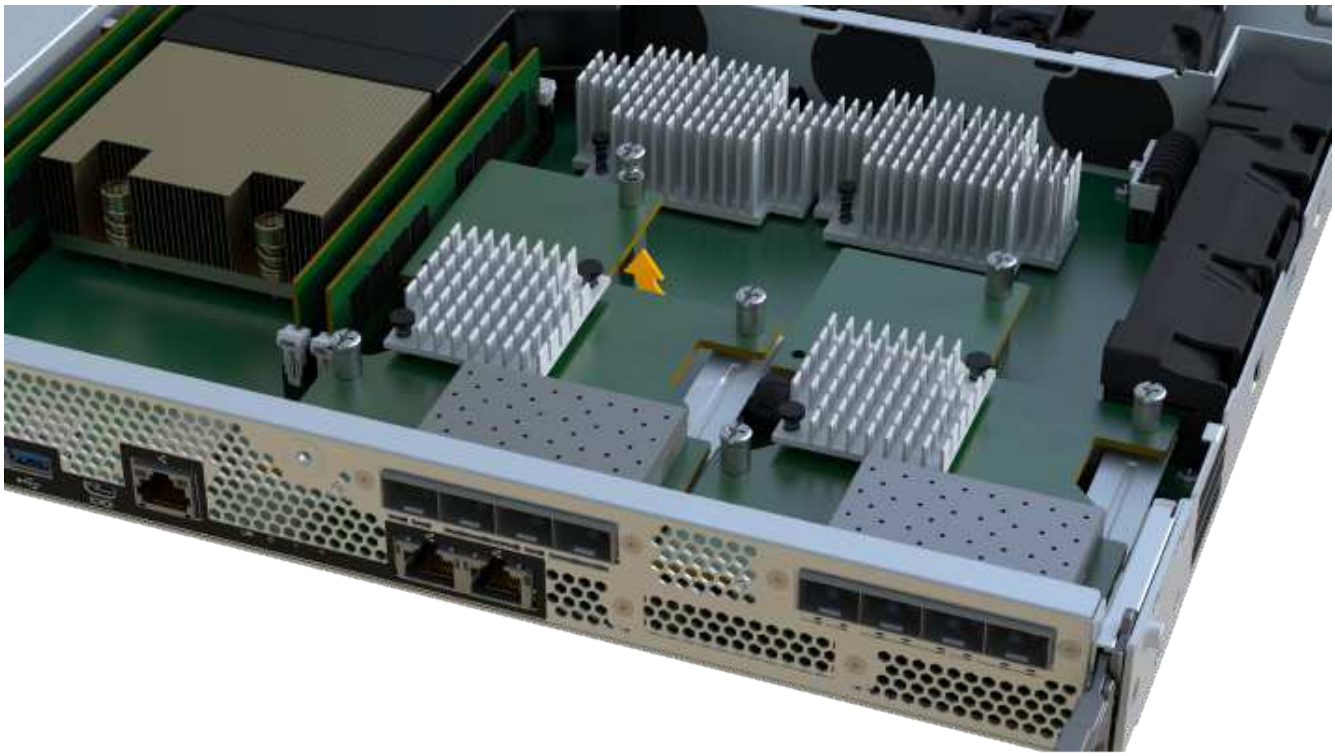


L'HIC viene fornito con tre posizioni delle viti sulla parte superiore, ma è fissato con una sola.

L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

6. Scollegare con cautela l'HIC dalla scheda del controller sollevando la scheda e sollevandola dal controller.

Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

7. Posizionare l'HIC su una superficie piana e priva di scariche elettrostatiche.

Fase 4: Sostituire l'HIC

Dopo aver rimosso il vecchio HIC, installare un nuovo HIC.

Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore di controller EF300 o EF600 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

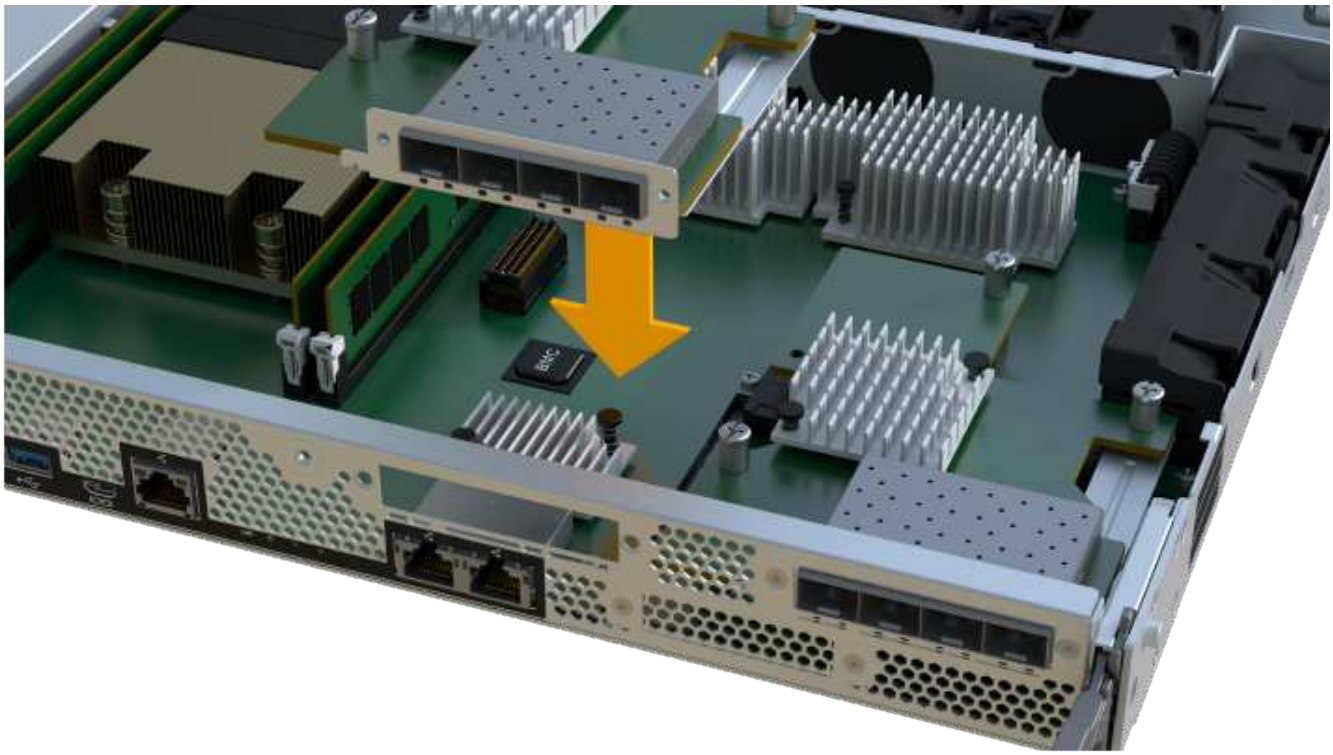
Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Allineare la singola vite a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato per i LED del controller tra l'HIC e la vite a testa zigrinata.



L'immagine riportata sopra è un esempio; l'aspetto dell'HIC potrebbe differire.

4. Serrare manualmente la vite a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dall'HIC originale con le tre viti.

Fase 5: Reinstallare il contenitore del controller

Dopo aver sostituito l'HIC, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

   Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

3. Installare gli SFP nel nuovo HIC e ricollegare tutti i cavi.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

Fase 6: Completare la sostituzione dell'HIC

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Posizionare il controller online.
   a. In System Manager, accedere alla pagina hardware.
   b. Selezionare **Mostra retro del controller**.
   c. Selezionare il controller con la scheda di interfaccia host sostituita.
   d. Selezionare **Place online** dall'elenco a discesa.
2. All'avvio del controller, controllare i LED del controller.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della scheda di interfaccia host è completata. È possibile riprendere le normali operazioni.

Conversione del protocollo della porta host

Requisiti per la conversione del protocollo host EF300 o EF600

Prima di convertire il protocollo host per un array EF300 o EF600, esaminare i seguenti requisiti.

- È stata pianificata una finestra di manutenzione dei downtime per questa procedura.
- È necessario interrompere le operazioni di i/o host quando si esegue la conversione. Non è possibile accedere ai dati sull'array di storage fino a quando la conversione non è stata completata correttamente.
- Stai utilizzando la gestione fuori banda. Non è possibile utilizzare la gestione in-band per completare questa procedura.
- Hai ottenuto l'hardware necessario per la conversione, che potrebbe includere un nuovo set di HICS e/o SFP. Il tuo rappresentante commerciale NetApp può aiutarti a determinare l'hardware di cui hai bisogno e a ordinare le parti corrette.
- I ricetrasmettitori SFP a doppio protocollo supportano FC da 16 GB e 8 GB, oltre a iSCSI da 10 GB. Pertanto, potrebbe non essere necessario modificare gli SFP se si dispone del protocollo doppio e si sta

semplicemente passando da FC a iSCSI o viceversa.

- Alcune conversioni del protocollo della porta host potrebbero richiedere l'aggiunta o l'aggiornamento di una scheda di interfaccia host.

Modificare il protocollo host per EF300 o EF600

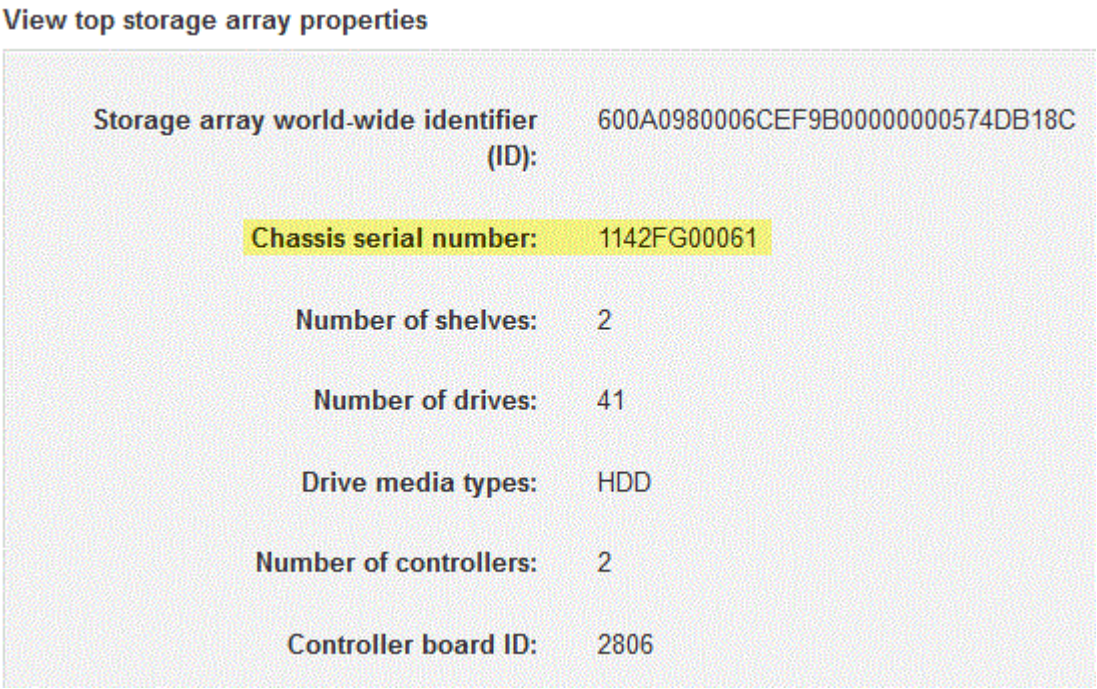
Seguire questa procedura per modificare il protocollo della porta host in un array EF300 o EF600. Questa procedura si applica solo alle schede di interfaccia host (HICS) che utilizzano Infiniband (IB) o Fibre Channel (FC).

Fase 1: Ottenere la chiave del Feature Pack

Per ottenere la chiave del Feature Pack, è necessario il numero di serie dallo shelf del controller, un codice di attivazione della funzione e l'identificatore di abilitazione della funzione per lo storage array.

Fasi

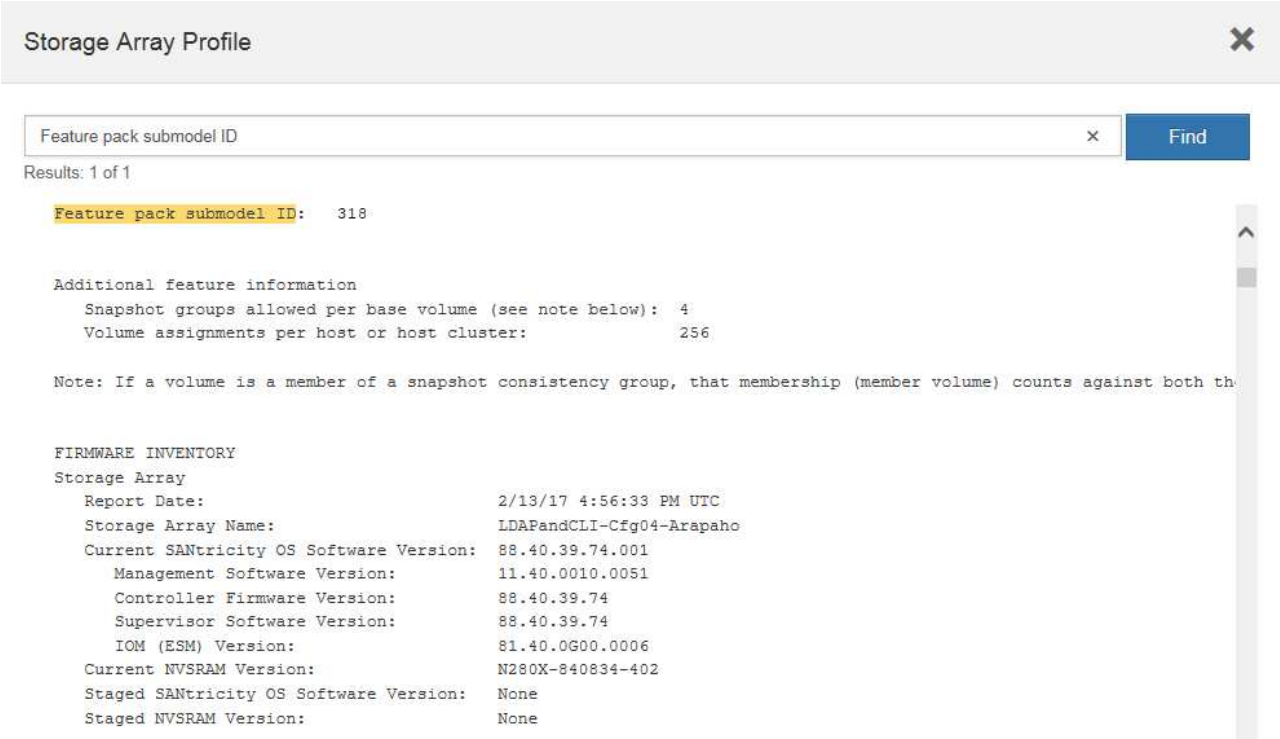
1. Individuare il numero di serie.
   a. Da Gestore di sistema di SANtricity, selezionare **supporto › Centro di supporto**.
   b. Con la scheda **Support Resources** (risorse di supporto) selezionata, scorrere fino alla sezione **View top storage array properties** (Visualizza proprietà principali storage array).
   c. Individuare **chassis Serial Number** (numero di serie chassis) e copiare questo valore in un file di testo.



2. Individuare l'ID del sottomodello **Feature Pack**.
   a. In Gestione sistema di SANtricity, selezionare **supporto**.
   b. Selezionare il riquadro **Support Center**.
   c. Nella scheda Support Resources (risorse di supporto), individuare e selezionare il collegamento **Storage Array Profile** (Profilo array di storage).

d. Digitare **Feature Pack submodel ID** nella casella di testo e fare clic su **Find** (trova).

e. Individuare l'ID del sottomodello del Feature Pack per la configurazione iniziale.



3. Utilizzando l'ID del sottomodello del Feature Pack, individuare l'ID del sottomodello del controller corrispondente per la configurazione iniziale e individuare il codice di attivazione della funzione per la configurazione finale desiderata all'interno della seguente tabella. Quindi, copiare il codice di attivazione della funzione in un file di testo.

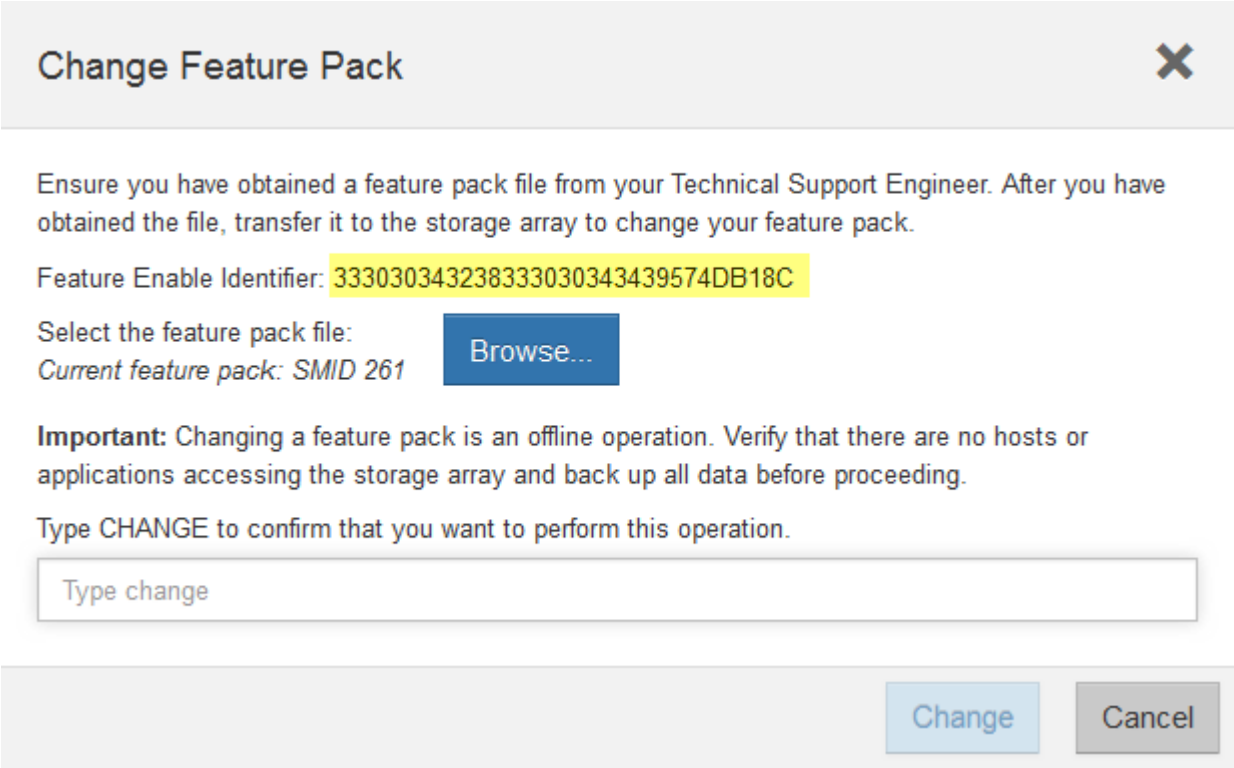
Avvio della configurazione		**Fine della configurazione**		**Codice di attivazione della funzione**
ID del sottomodello del controller	Porte HIC	ID del sottomodello del controller	Porte HIC	
443	NVMe/FC, NVMe/RoCE o iSCSI	444	NVME/FC o NVMe/IB	DH5-HB4-ZK9QH
448	FC	JHX-UB4-ZGTP1	491	Er/IB
0H1-675-Z5SII	492	SRP/IB	NHD-V75-ZB6ZX	444
NVMe/FC o NVMe/IB	443	NVMe/FC, NVMe/RoCE o iSCSI	YH3-XB4-ZJRIZ	448
FC	2HU-BB4-ZFCG5	491	Er/IB	2H3-P75-Z6AQG

Avvio della configurazione		Fine della configurazione		Codice di attivazione della funzione
492	SRP/IB	5HG-G75-ZDNEZ	448	FC
443	NVMe/FC, NVMe/RoCE o iSCSI	7 HZ-EB4-ZHAYW	444	NVMe/FC o NVMe/IB
LHS-RB4-ZDV29	491	Er/IB	FH6-975-Z7Q7H	492
SRP/IB	0HI-Z75-ZE4L5	491	Er/IB	443
NVMe/FC, NVMe/RoCE o iSCSI	MHQ-M85-ZIJNT	444	NVMe/FC o NVMe/IB	4HS-685-ZJZ1U
448	FC	YHU-P85-ZLHCX	465	FC/PTL
AHX-985-ZMXMI	492	SRP/IB	ZHZ-S85-ZNF4J	492
SRP/IB	443	NVMe/FC, NVMe/RoCE o iSCSI	EH3-C85-Z0V93	444
NVMe/FC o NVMe/IB	BH5-V85-ZQDQJ	448	FC	1H8-F85-ZRT1V
465	FC/PTL	1HA-Y85-ZSB7S	491	Er/IB
KHD-I85-ZUSMI	465	FC/PTL	491	Er
6H8-S75-Z98FH	492	SRP	NHL-J75-ZFL3W	516
NVMe/FC, NVMe/RoCE o iSCSI	517	NVMe/IB o NVMe/FC	LHF-285-ZV9YZ	518
FC	IHI-L85-ZXQEP	519	Er/IB	RHK-585-ZY7P5
520	FC-PTL	NHN-095-ZZ0XF	521	SRP/IB
GHP-895-Z25BD	517	NVMe/IB o NVMe/FC	516	NVMe/FC, NVMe/RoCE o iSCSI

Avvio della configurazione		Fine della configurazione		Codice di attivazione della funzione
7HS-R95-Z3M06	518	FC	UHU-B95-Z43X2	519
FC-PTL	8HX-U95-Z5K6F	520	Er/IB	UHZ-E95-Z71LH
521	SRP/IB	SH2-X95-Z8IVS	518	FC
516	NVMe/FC, NVMe/RoCE o iSCSI	UH5-H95-Z9Z58	517	NVMe/FC o NVMe/IB
XH7-195-ZBGJC	519	FC-PTL	FHA-K95-ZCXX0	520
Er/IB	JHC-595-ZDE3X	521	SRP/IB	0HF-095-ZFVFN
519	FC-PTL	516	NVMe/FC, NVMe/RoCE o iSCSI	YHH-895-ZGCXS
517	NVMe/FC o NVMe/IB	2HK-R95-ZHT83	518	FC
1HM-BA5-ZJALA	520	Er/IB	YHP-UA5-ZKRXA	521
SRP/IB	MHR-EA5-ZL83V	520	Er/IB	516
NVMe/FC, NVMe/RoCE o iSCSI	HHU-XA5-ZNPLT	517	NVMe/FC o NVMe/IB	YHW-HA5-Z07QK
518	FC	WHZ-1A5-ZPN4U	519	FC/PTL
7H2-KA5-ZR5C3	521	SRP	3H5-4A5-ZSLVX	521
SRP/IB	516	NVMe/FC, NVMe/RoCE o iSCSI	1H7-NA5-ZT31W	517
NVMe/FC o NVMe/IB	XHA-7A5-ZVJGC	518	FC	KHC-QA5-ZW1P3
519	FC/PTL	CHE-AA5-ZXH2F	520	Er/IB

Se l'ID del sottomodello del controller non è presente nell'elenco, contattare "Supporto NetApp".

4. In System Manager, individuare Feature Enable Identifier.
   a. Accedere al **Impostazioni › sistema**.
   b. Scorrere verso il basso fino a **componenti aggiuntivi**.
   c. In **Change Feature Pack**, individuare **Feature Enable Identifier**.
   d. Copiare e incollare questo numero di 32 cifre in un file di testo.



5. Passare a. "Attivazione della licenza NetApp: Attivazione della funzionalità Premium dello storage Array"e immettere le informazioni necessarie per ottenere il feature pack.
   - Numero di serie dello chassis
   - Codice di attivazione della funzione
   - Feature Enable Identifier NOTA: Il sito Web Premium Feature Activation include un collegamento a "Premium Feature Activation Instructions". Non tentare di seguire queste istruzioni per questa procedura.
6. Scegliere se ricevere il file delle chiavi per il Feature Pack in un'e-mail o scaricarlo direttamente dal sito.

Fase 2: Arrestare l'i/o host

Interrompere tutte le operazioni di i/o dall'host prima di convertire il protocollo delle porte host.

Non è possibile accedere ai dati sull'array di storage fino a quando la conversione non viene completata correttamente.

Fasi

1. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio,

è possibile eseguire le seguenti operazioni:

- Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
- Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
- Smontare tutti i file system associati ai volumi sull'array.

> I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

> **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

2. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

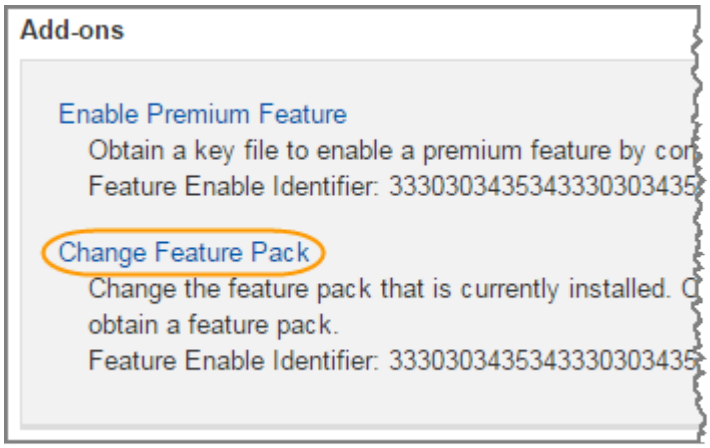
3. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
4. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.

Fase 3: Modificare il Feature Pack

Modificare il Feature Pack per convertire il protocollo host delle porte host.

Fasi

1. Da Gestore di sistema di SANtricity, selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **Cambia Feature Pack**.



3. Fare clic su **Sfoglia**, quindi selezionare il Feature Pack che si desidera applicare.
4. Digitare **CHANGE** nel campo.
5. Fare clic su **Cambia**.

   Viene avviata la migrazione dei Feature Pack. Entrambi i controller si riavviano automaticamente due volte per rendere effettivo il nuovo Feature Pack. Una volta completato il riavvio, lo storage array torna allo stato

di risposta.

6. Verificare che le porte host dispongano del protocollo previsto.
   a. Da Gestione sistema di SANtricity, selezionare **hardware**.
   b. Fare clic su **Mostra retro dello shelf**.
   c. Selezionare l'immagine per Controller A o Controller B.
   d. Selezionare **Visualizza impostazioni** dal menu di scelta rapida.
   e. Selezionare la scheda **interfacce host**.
   f. Fare clic su **Mostra altre impostazioni**.

Quali sono le prossime novità?

Passare a. "Completa la conversione del protocollo host".

Conversione completa del protocollo host per EF300 o EF600

Dopo aver applicato la chiave Feature Pack per convertire il protocollo, è necessario configurare l'host in modo che utilizzi il protocollo appropriato.

Per istruzioni dettagliate, consultare la guida appropriata per il sistema in uso:

- "Configurazione di Linux Express"
- "Configurazione di VMware Express"
- "Configurazione di Windows Express"

  Impostazioni specifiche potrebbero variare. Controllare "Matrice di interoperabilità NetApp" per istruzioni specifiche e impostazioni aggiuntive consigliate per la soluzione.

Alimentatori

Requisiti per la sostituzione dell'alimentatore EF300 o EF600

Prima di sostituire un alimentatore in un array EF300 o EF600, esaminare i seguenti requisiti.

- È necessario disporre di un alimentatore sostitutivo supportato per il modello di shelf di controller o di dischi.

  Non mischiare alimentatori di diversi tipi di tensione. Sostituire sempre come per come.

- È necessario disporre di un braccialetto antistatico o adottare altre precauzioni antistatiche.

Sostituire un alimentatore EF300 o EF600

È possibile sostituire un alimentatore in caso di guasto nel controller EF300 o EF600.

In caso di guasto a un alimentatore, è necessario sostituirlo il prima possibile, in modo che lo shelf del controller disponga di una fonte di alimentazione ridondante.

Prima di iniziare

- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con l'alimentatore. Selezionare **ricontrollare** dal Recovery Guru per assicurarsi che nessun altro elemento debba essere affrontato per primo.
- Verificare che il LED di attenzione ambra sull'alimentatore sia acceso, a indicare che l'alimentatore o la ventola integrata sono guasti.
- Assicurarsi di disporre di quanto segue:
  - Un alimentatore sostitutivo supportato per lo shelf del controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Rimuovere l'alimentatore guasto

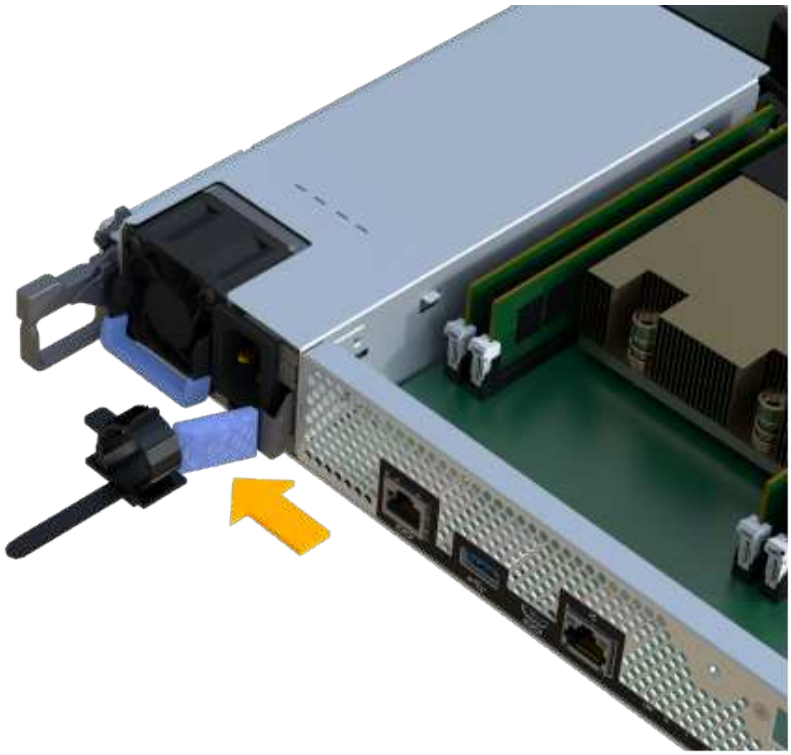
Rimuovere un alimentatore guasto per poterlo sostituire con uno nuovo.

Fasi

1. Disimballare il nuovo alimentatore e posizionare il nuovo alimentatore su una superficie piana vicino allo shelf del disco.

   Conservare tutti i materiali di imballaggio per l'utilizzo quando si restituisce l'alimentatore guasto.

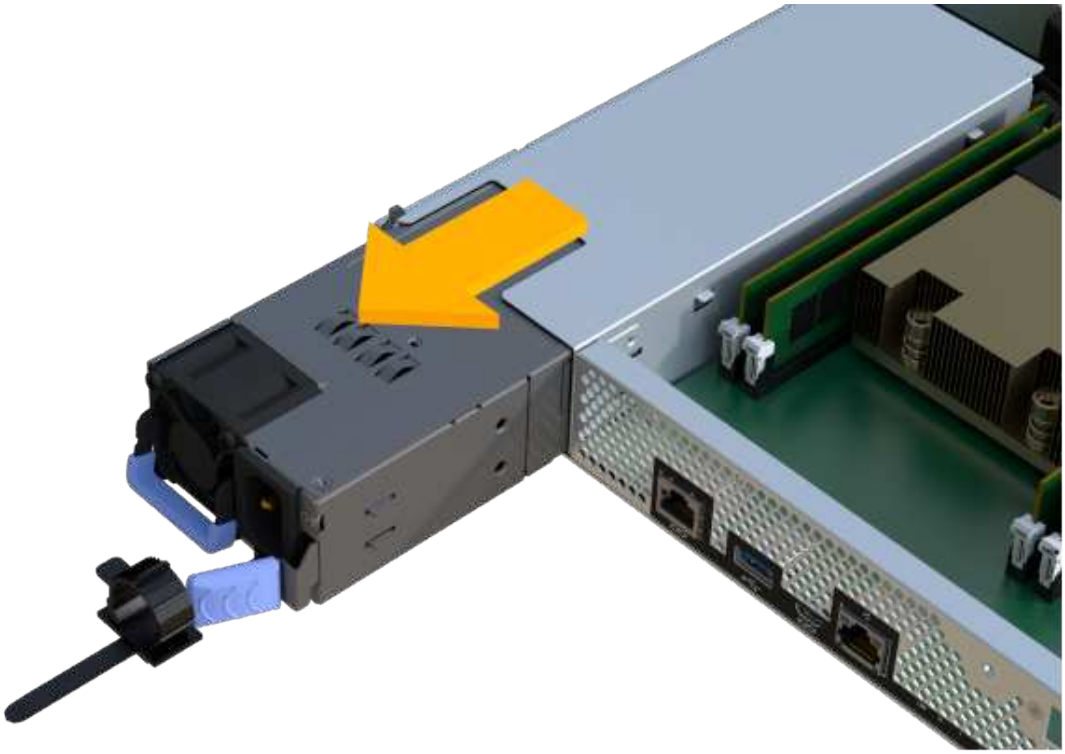
2. Scollegare i cavi di alimentazione:
   a. Aprire il fermo del cavo di alimentazione, quindi scollegare il cavo di alimentazione dall'alimentatore.
   b. Scollegare il cavo di alimentazione dalla presa di corrente.
3. Individuare la linguetta a destra dell'alimentatore e spingerla verso l'alimentatore.



4. Individuare la maniglia sulla parte anteriore dell'alimentatore.

5. Utilizzare la maniglia per estrarre l'alimentatore dal sistema.

> Quando si rimuove un alimentatore, utilizzare sempre due mani per sostenerne il peso.



Fase 2: Installare un nuovo alimentatore e completare la sostituzione

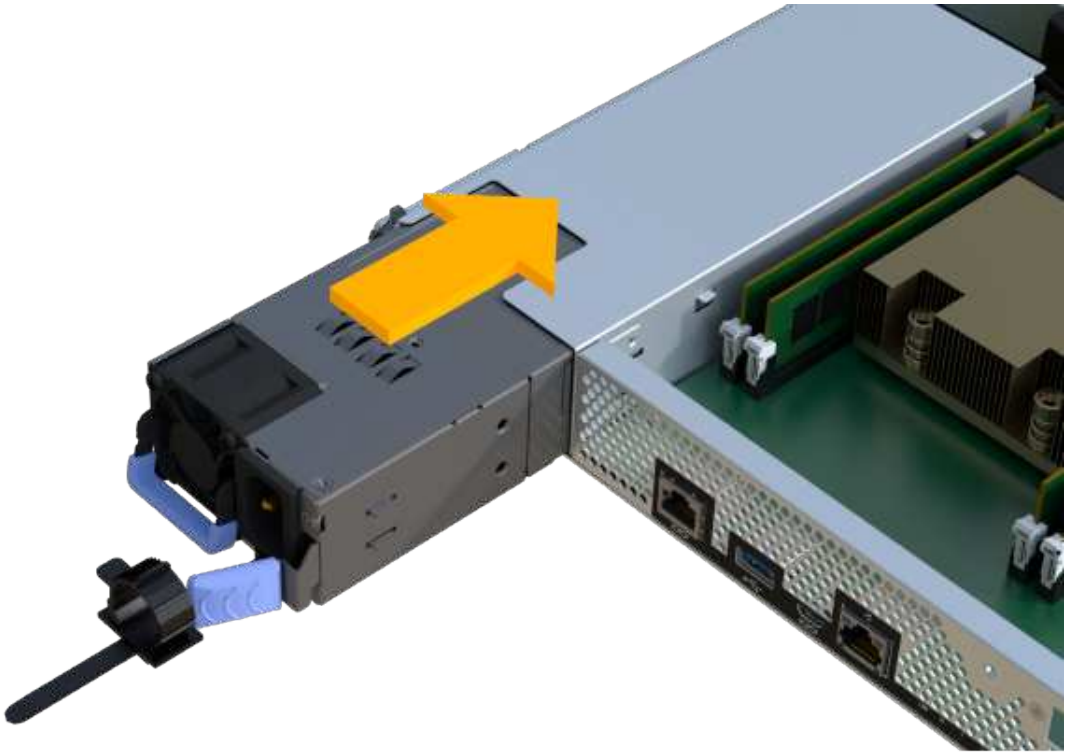
Dopo aver rimosso l'alimentatore guasto, installarne uno nuovo.

Fasi

1. Con entrambe le mani, sostenere e allineare i bordi dell'alimentatore con l'apertura nello chassis del sistema, quindi spingere delicatamente l'alimentatore nello chassis utilizzando la maniglia della camma.

   Gli alimentatori sono dotati di chiavi e possono essere installati in un solo modo.

   > Non esercitare una forza eccessiva quando si inserisce l'alimentatore nel sistema, poiché si potrebbe danneggiare il connettore.



2. Verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

3. Da Gestione sistemi SANtricity, fare clic su **supporto › Centro aggiornamento** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

Quali sono le prossime novità?

La sostituzione dell'alimentatore è completata. È possibile riprendere le normali operazioni.

Schede di espansione SAS

Requisiti per la sostituzione delle schede di espansione SAS EF300 e EF600

Se si intende aggiungere una scheda di espansione SAS a un sistema EF300 o EF600, esaminare i seguenti requisiti.

- Seguire la "Installare e configurare i sistemi storage EF300 e EF600" per configurare il controller.
- È necessario aggiornare il firmware alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".
- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Non è possibile accedere ai dati sull'array di storage fino a quando la procedura non è stata completata correttamente.

- È necessario eseguire questa attività con entrambi i canister del controller.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Hai un cacciavite Phillips n. 1.
- Sono presenti etichette per identificare ciascun cavo collegato al contenitore del controller.
- Si dispone di una stazione di gestione con un browser in grado di accedere a Gestore di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.
- Nei controller EF300 potrebbe essere installata una scheda di espansione SAS nella porta 1 per consentire l'espansione del vassoio dell'unità.
- Per collegare l'espansione SAS, vedere "Cablaggio dell'hardware e-Series" per istruzioni.

Aggiunta di una scheda di espansione SAS a EF300 e EF600

È possibile aggiungere una scheda di espansione SAS a un controller EF300 o EF600 per consentire l'espansione del vassoio dell'unità.

A proposito di questa attività

Quando si aggiunge una scheda di espansione SAS, è necessario spegnere lo storage array, installare la nuova scheda di espansione SAS e rialimentare.

Prima di iniziare

- Revisione "Requisiti per la sostituzione delle schede di espansione SAS EF300 e EF600".
- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Non è possibile accedere ai dati sull'array di storage fino a quando la procedura non è stata completata correttamente.

> Questa procedura deve essere eseguita con entrambi i contenitori del controller. Le configurazioni HIC del controller devono corrispondere esattamente.

- Assicurarsi di disporre di quanto segue:
  - Una scheda di espansione SAS compatibile con il controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un'area di lavoro piana e priva di elettricità statica.
  - Un cacciavite Phillips n. 1.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare lo shelf del controller offline

Posizionare lo shelf del controller offline in modo da poter aggiungere la scheda di espansione SAS in tutta sicurezza.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

3. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

4. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

5. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
6. Spegnere lo shelf del controller.
   a. Etichettare e scollegare entrambi i cavi di alimentazione dallo shelf del controller.
   b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller per aggiungere la nuova scheda di espansione SAS.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
5. Premere le maniglie su entrambi i lati del controller e tirare indietro fino a quando non si sgancia dallo shelf.

6. Utilizzando due mani e le maniglie, estrarre il contenitore del controller dallo scaffale. Quando la parte anteriore del controller è libera dal contenitore, estrarlo completamente con due mani.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Aggiungere la nuova scheda di espansione SAS

Installare la scheda di espansione SAS per consentire l'espansione del vassoio dell'unità.

Fasi

1. Rimuovere il coperchio del contenitore del controller svitando la singola vite a testa zigrinata e sollevando il coperchio.
2. Verificare che il LED verde all'interno del controller sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

3. Utilizzando un cacciavite Phillips n. 1, rimuovere le due viti che fissano la piastra anteriore al contenitore del controller, quindi rimuovere la piastra anteriore.
4. Allineare la singola vite a testa zigrinata sulla scheda di espansione SAS con il foro corrispondente sul controller, quindi allineare il connettore sul fondo della scheda di espansione con il connettore di interfaccia della scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo della scheda di espansione SAS o sulla parte superiore della scheda del controller.

5. Abbassare con cautela la scheda di espansione SAS in posizione e inserire il connettore della scheda di espansione premendo delicatamente sulla scheda di espansione.
6. Serrare manualmente la vite a testa zigrinata della scheda di espansione SAS.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

7. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore rimossa dal contenitore del controller originale al nuovo contenitore del controller con le due viti.

Fase 4: Reinstallare il contenitore del controller

Dopo aver installato la nuova scheda di espansione SAS, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Abbassare il coperchio sul contenitore del controller e fissare la vite a testa zigrinata.
2. Mentre si stringono le maniglie del controller, far scorrere delicatamente il contenitore del controller fino in fondo nello shelf del controller.

   Il controller scatta in maniera udibile quando viene installato correttamente nello shelf.

Fase 5: Completare l'aggiunta della scheda di espansione SAS

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Collegare i cavi di alimentazione per posizionare il controller online.
2. All'avvio del controller, controllare i LED del controller.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia host.
3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente di SANtricity OS.

   Se necessario, installare la versione più recente.

5. Verificare che tutti i volumi siano stati restituiti al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]). Dalla pagina **tutti i volumi**, verificare che i volumi siano distribuiti ai proprietari preferiti. Selezionare **More › Change ownership** (Altro[Cambia proprietà]) per visualizzare i proprietari dei volumi.
   b. Se tutti i volumi sono di proprietà del proprietario preferito, passare alla fase 6.
   c. Se nessuno dei volumi viene restituito, è necessario restituire manualmente i volumi. Vai al **More › redistribuisci volumi**.
   d. Se solo alcuni dei volumi vengono restituiti ai proprietari preferiti dopo la distribuzione automatica o manuale, è necessario controllare il Recovery Guru per verificare la presenza di problemi di connettività host.
   e. Se non è presente un Recovery Guru o se si seguono le fasi del guru del recovery, i volumi non vengono ancora restituiti ai proprietari preferiti, contattare il supporto.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

7. Ripetere questa operazione con il secondo contenitore del controller.

Per collegare l'espansione SAS, vedere "Cablaggio dell'hardware e-Series" per istruzioni.

Quali sono le prossime novità?

Il processo di aggiunta di una scheda di espansione SAS nell'array di storage è completo. È possibile riprendere le normali operazioni.

E2800

Manutenzione dell'hardware E2800

Per il sistema storage E2800, è possibile eseguire le procedure di manutenzione dei seguenti componenti.

Batterie

Ogni contenitore del controller include una batteria che conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA.

Controller

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

Canister

I contenitori sono costituiti da tre tipi diversi: Contenitori per ventole di alimentazione (alimentatori) che forniscono una fonte di alimentazione ridondante e un raffreddamento adeguato in uno shelf o uno shelf di controller da 12 o 24 dischi; contenitori di alimentazione utilizzati per la ridondanza dell'alimentazione in uno shelf di controller da 60 dischi o in uno shelf di dischi; e i contenitori per ventole utilizzati per il raffreddamento dello shelf di controller da 60 dischi o dello shelf di dischi.

Dischi

Un'unità è un dispositivo elettromeccanico che fornisce i supporti di storage fisici per i dati.

HICS (host Interface Card)

È possibile installare una scheda di interfaccia host (HIC) all'interno di un contenitore di controller. Il controller E2800 include porte host integrate sulla scheda controller stessa, nonché porte host sull'HIC opzionale. Le porte host integrate nel controller sono chiamate porte host baseboard. Le porte host integrate nell'HIC sono chiamate porte HIC.

Protocollo della porta host

È possibile convertire il protocollo di un host in un protocollo diverso in modo da stabilire compatibilità e comunicazione.

Batterie

Requisiti per la sostituzione della batteria E2800

Prima di sostituire una batteria E2800, esaminare i requisiti e le considerazioni.

Ogni contenitore del controller include una batteria che conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA.

Recovery Guru

Se il guru del ripristino in Gestione sistema di SANtricity riporta uno dei seguenti stati, è necessario sostituire la batteria interessata:

- Guasto alla batteria
- Sostituzione della batteria necessaria

Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.

Panoramica della procedura

Per proteggere i dati, è necessario sostituire una batteria guasta il prima possibile.

Di seguito è riportata una panoramica dei passaggi necessari per sostituire una batteria in un controller E2800:

1. Preparare la sostituzione seguendo la procedura appropriata per una configurazione duplex o simplex.
2. Rimuovere il contenitore del controller.
3. Rimuovere la batteria guasta.
4. Installare la nuova batteria.
5. Reinstallare il contenitore del controller.
6. Completare la sostituzione seguendo la procedura appropriata per una configurazione duplex o simplex.

Configurazione duplex o simplex

La procedura per sostituire una batteria dipende dal fatto che si disponga di uno o due controller, come segue:

Se lo storage array dispone di…	Devi…
Due controller (duplex)	1. Portare il controller offline. 2. Rimuovere il contenitore del controller. 3. Sostituire la batteria. 4. Sostituire il contenitore del controller. 5. Portare il controller online.
Un controller (simplex)	1. Interrompere le operazioni di i/o dell'host. 2. Spegnere lo shelf del controller. 3. Rimuovere il contenitore del controller. 4. Sostituire la batteria. 5. Sostituire il contenitore del controller. 6. Alimentare lo shelf del controller.

Requisiti per la sostituzione di una batteria

Se si intende sostituire una batteria guasta, è necessario disporre di:

- Una batteria sostitutiva.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Preparare la sostituzione della batteria E2800

La procedura da seguire per la sostituzione della batteria dipende dalla configurazione duplex (due controller) o simplex (un controller).

- Per le configurazioni duplex, vedere Posiziona il controller offline (duplex).

- Per le configurazioni simplex, vedere Spegnere lo shelf del controller (simplex).

Prima di iniziare

- Verificare che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Esaminare "Requisiti per la sostituzione della batteria E2800".

Posiziona il controller offline (duplex)

Se si dispone di una configurazione duplex, è necessario posizionare il controller interessato offline in modo da poter rimuovere in sicurezza la batteria guasta. Il controller che non si sta mettendo offline deve essere in linea (nello stato ottimale).

> Eseguire questa operazione solo se lo storage array dispone di due controller (configurazione duplex).

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.
2. Dall'area Details (Dettagli) del Recovery Guru, determinare quale batteria sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.
   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

4. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.

c. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

5. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
     iii. Selezionare il controller che si desidera mettere offline.
     iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

     > Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

   - In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=offline`

   Per il controller B: `set controller [b] availability=offline`

6. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.
7. Passare a. "Rimuovere il contenitore del controller E2800".

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

Spegnere lo shelf del controller (simplex)

Se si dispone di una configurazione simplex, spegnere lo shelf del controller in modo da poter rimuovere in sicurezza la batteria guasta.

> Eseguire questa attività solo se lo storage array dispone di un controller (configurazione simplex).

Fasi

1. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).

iii. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

- In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

2. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

3. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

   a. Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   b. Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   c. Smontare tutti i file system associati ai volumi sull'array.

   I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

4. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

5. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
6. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
7. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
8. Attendere che tutti i LED sullo shelf del controller si spenga.
9. Passare a. "Rimuovere il contenitore del controller E2800".

Rimuovere il contenitore del controller E2800

È necessario rimuovere il contenitore del controller dallo shelf del controller, in modo da poter rimuovere la batteria.

Quando si rimuove un contenitore del controller, scollegare tutti i cavi. Quindi, far scorrere il contenitore del controller fuori dallo shelf del controller.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.

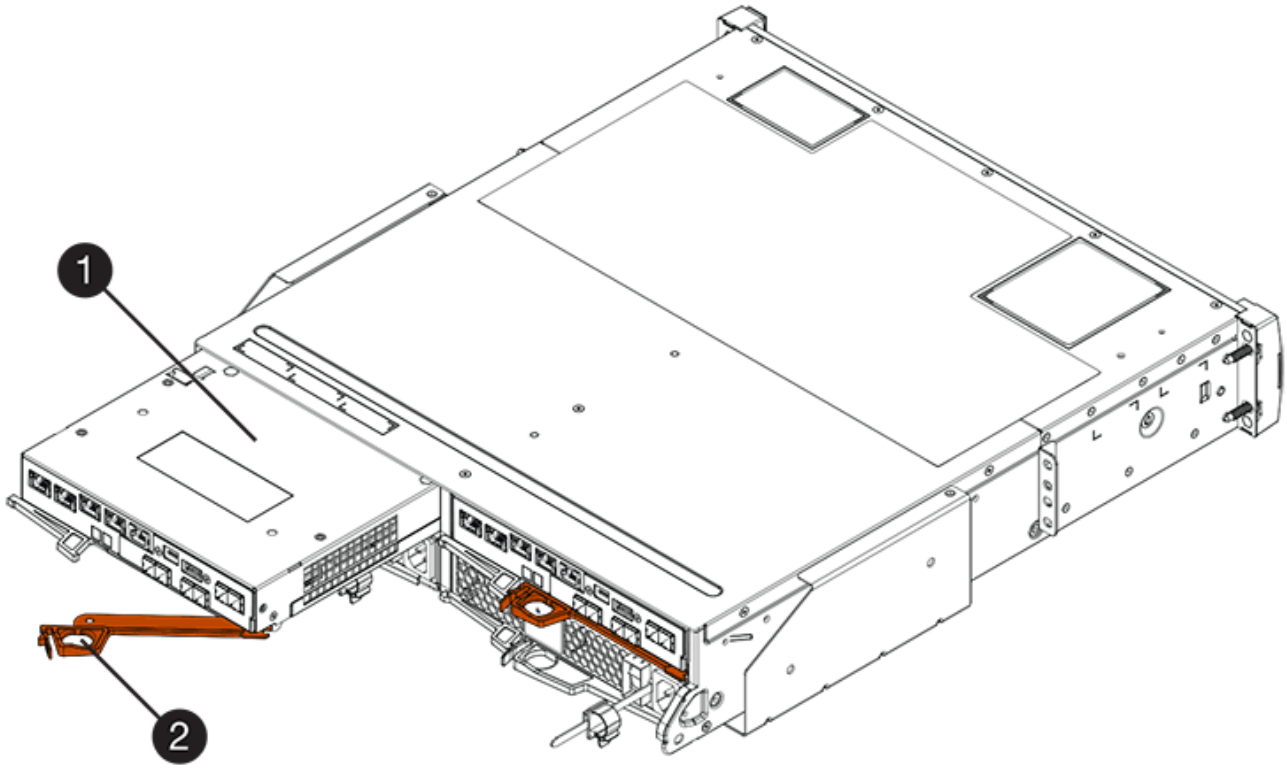
Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se le porte host sul contenitore del controller utilizzano ricetrasmettitori SFP+, lasciarli installati.
5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
6. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

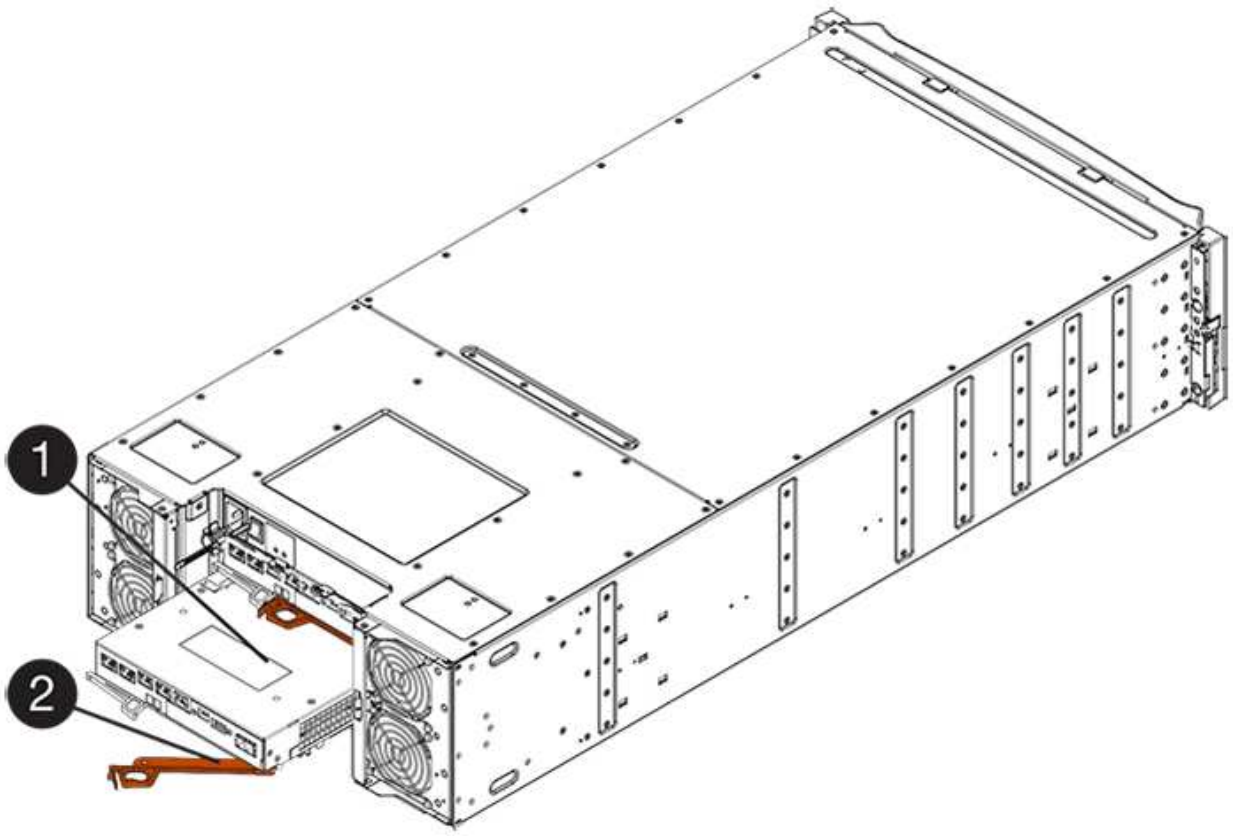
   La figura seguente è un esempio di shelf di controller E2812, shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

7. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

8. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
9. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.
10. Passare a. "Rimuovere la batteria E2800 guasta".

Rimuovere la batteria E2800 guasta

Dopo aver rimosso il contenitore del controller dallo shelf del controller, è possibile rimuovere la batteria.

Fasi

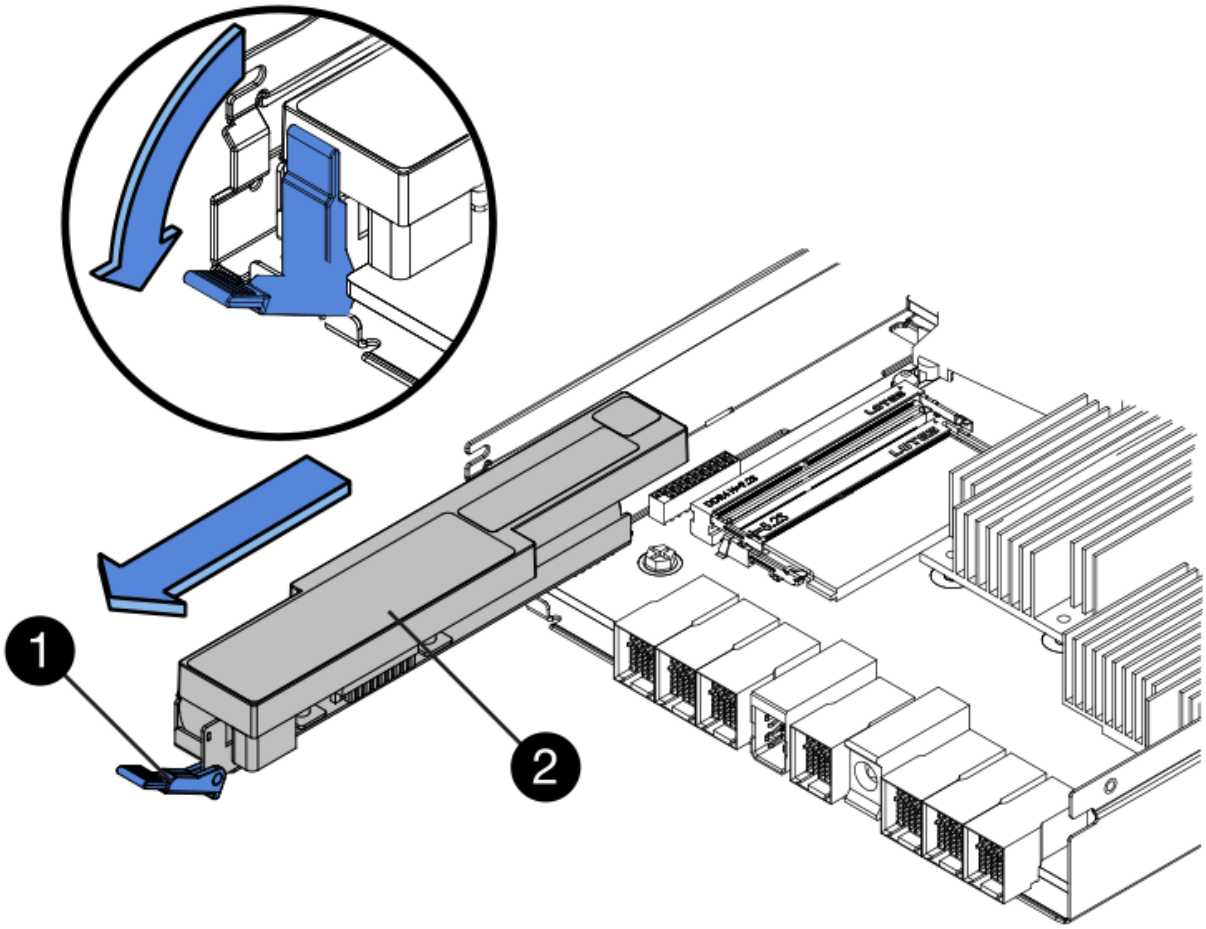
1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *cache interna attiva*

(2) *batteria*

3. Individuare il dispositivo di chiusura blu della batteria.
4. Sbloccare la batteria spingendo il dispositivo di chiusura verso il basso e lontano dal contenitore del controller.



(1) *dispositivo di chiusura a scatto della batteria*

(2) *batteria*

5. Sollevare la batteria ed estrarla dal contenitore del controller.
6. Seguire le procedure appropriate per il riciclaggio o lo smaltimento della batteria guasta.

> Per rispettare le normative IATA (International Air Transport Association), non spedire mai una batteria al litio via etere se non è installata nello shelf del controller.

7. Passare a. "Installare una nuova batteria".

Installare una nuova batteria E2800

Dopo aver rimosso la batteria guasta, è possibile installarne una nuova.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- La batteria sostitutiva.
- Una superficie piana e priva di cariche elettrostatiche.

Fasi

1. Disimballare la nuova batteria e riutilizzarla su una superficie piana e priva di scariche elettrostatiche.

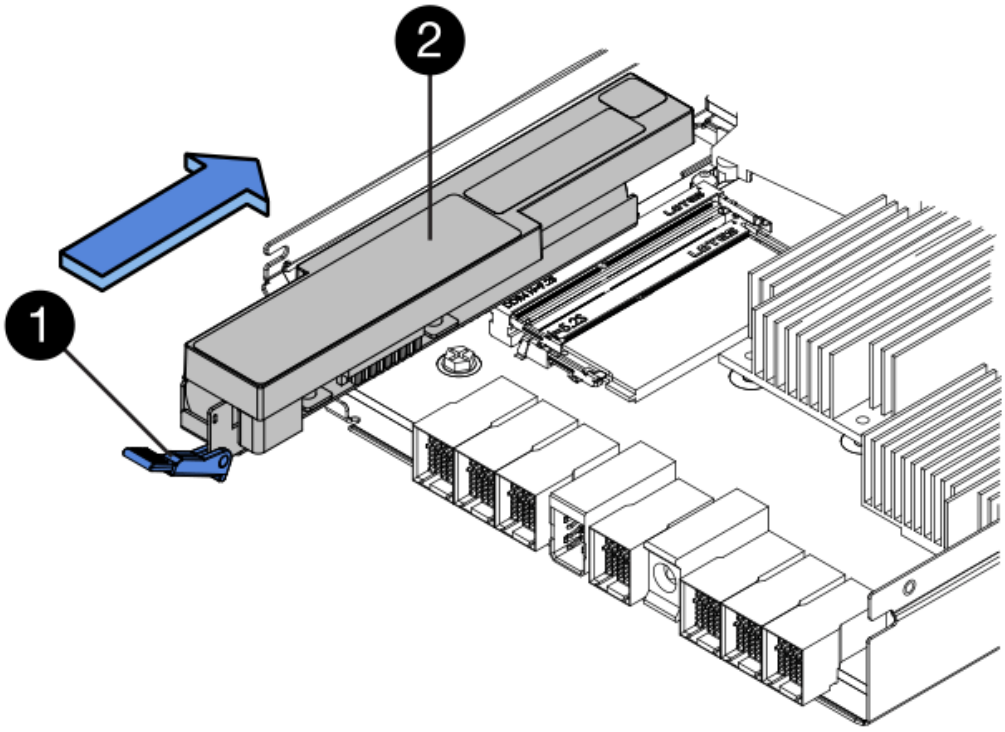
> Per rispettare le normative IATA in materia di sicurezza, le batterie sostitutive vengono spedite con uno stato di carica (SoC) pari o inferiore al 30%. Quando si riattiva l'alimentazione, tenere presente che il caching in scrittura non viene ripristinato fino a quando la batteria sostitutiva non viene completamente caricata e non viene completato il ciclo di apprendimento iniziale.

2. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
3. Inserire la batteria nel contenitore del controller inclinandola leggermente verso il basso.

   Inserire la flangia metallica nella parte anteriore della batteria nello slot sul fondo del contenitore del controller e far scorrere la parte superiore della batteria sotto il piccolo perno di allineamento sul lato sinistro del contenitore.

4. Spostare il dispositivo di chiusura della batteria verso l'alto per fissare la batteria.

   Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.



   (1) *dispositivo di chiusura a scatto della batteria*

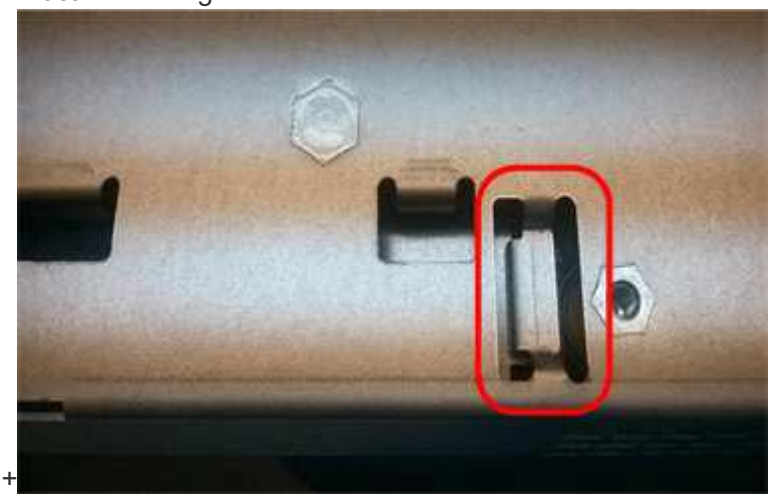
   (2) *batteria*

5. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

Possibili danni all'hardware — la flangia metallica sulla parte anteriore della batteria deve essere inserita completamente nello slot sul contenitore del controller (come mostrato nella prima figura). Se la batteria non è installata correttamente (come mostrato nella seconda figura), la flangia metallica potrebbe entrare in contatto con la scheda del controller, danneggiando il controller quando si applica l'alimentazione.

- **Corretto** — la flangia metallica della batteria è completamente inserita nello slot del controller:

- **Errato** — la flangia metallica della batteria non è inserita nello slot del controller:



+

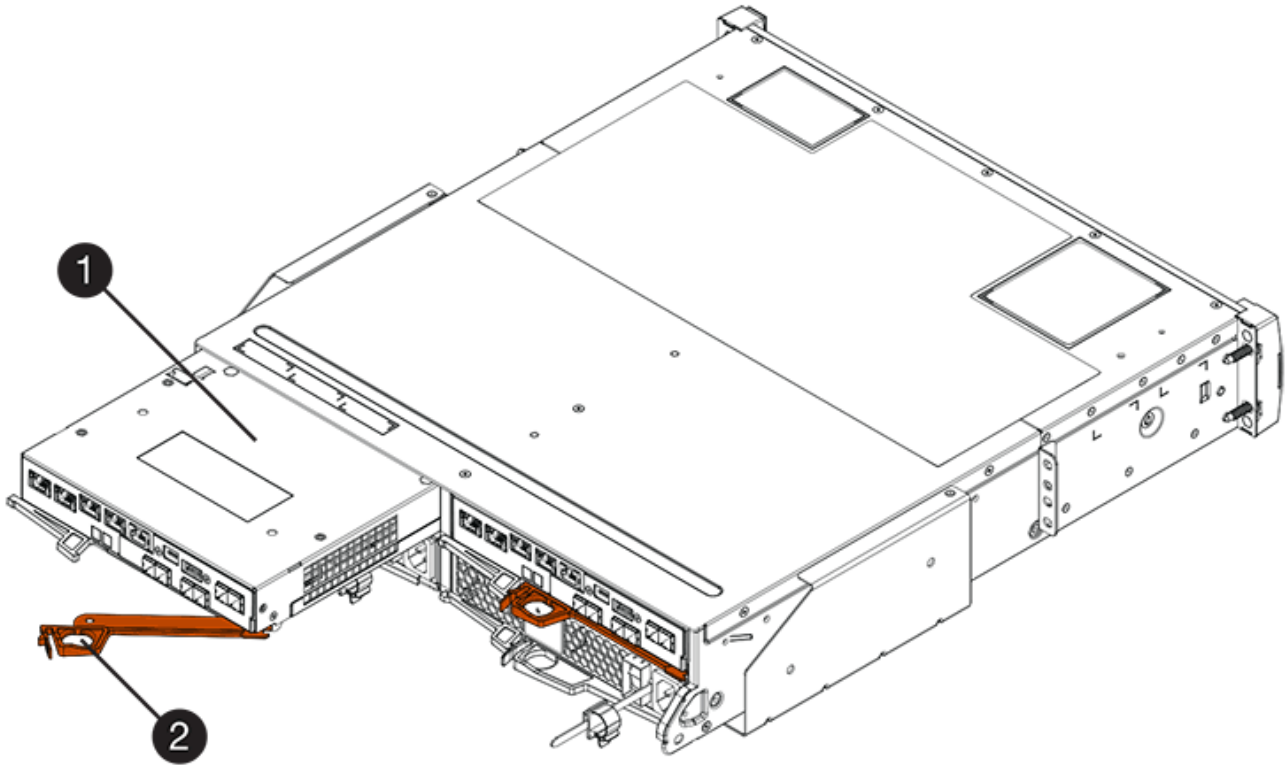
6. Passare a. "Reinstallare il contenitore del controller E2800".

Reinstallare il contenitore del controller E2800

Dopo aver installato la nuova batteria, reinstallare il contenitore del controller nello shelf del controller.

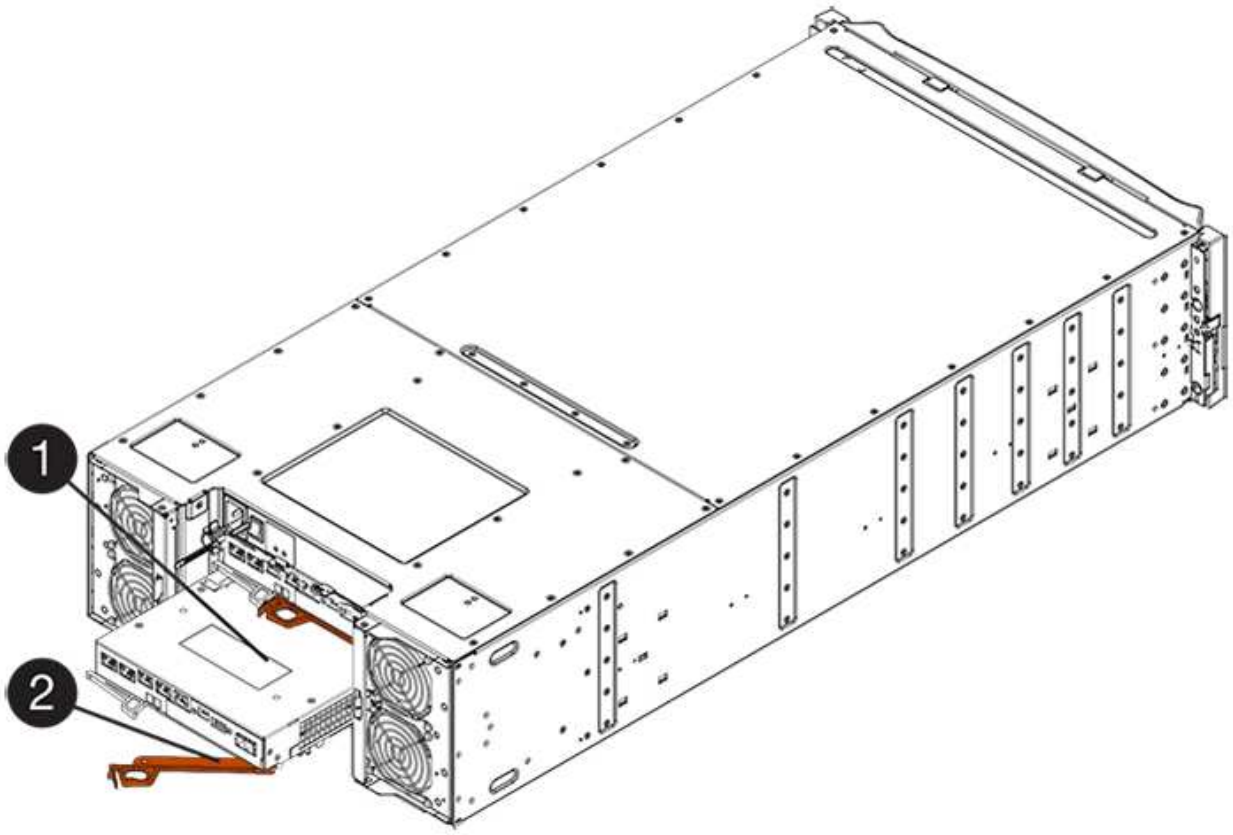
Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Ricollegare tutti i cavi.
6. Passare a. "Sostituzione completa della batteria E2800".

Sostituzione completa della batteria E2800

La procedura per completare la sostituzione della batteria dipende dalla configurazione duplex (due controller) o simplex (un controller).

- Per le configurazioni duplex, vedere Posizionare il controller online (duplex).
- Per le configurazioni simplex, vedere Controller di accensione (simplex).

Posizionare il controller online (duplex)

Posizionare il controller online per verificare che lo storage array funzioni correttamente. Quindi, è possibile raccogliere i dati di supporto e riprendere le operazioni.

> Eseguire questa operazione solo se lo storage array dispone di due controller.

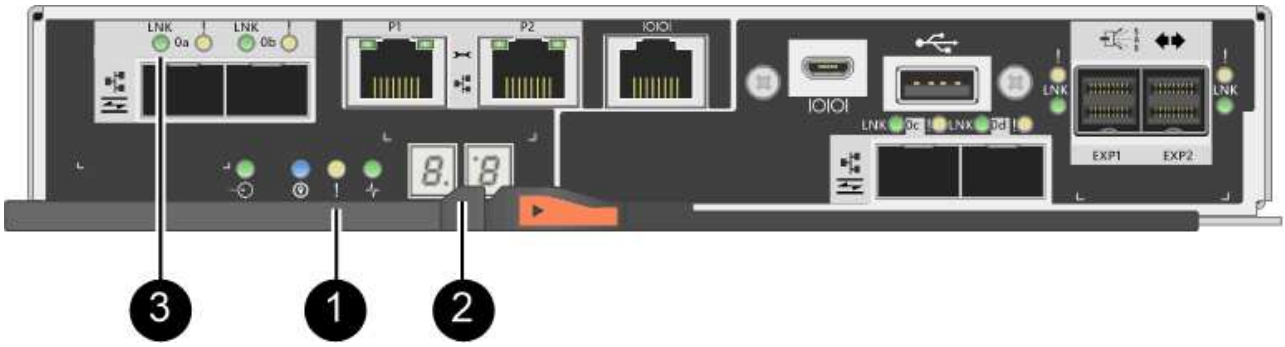
Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   > La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
     host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

2. Portare il controller online utilizzando Gestione di sistema di SANtricity.
   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf**.
     iii. Selezionare il controller che si desidera mettere in linea.
     iv. Selezionare **Place Online** (Esegui online) dal menu di scelta rapida e confermare che si desidera eseguire l'operazione.

     Il sistema mette il controller in linea.
   - In alternativa, è possibile ripristinare il controller online utilizzando i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=online;`

   Per il controller B: `set controller [b] availability=online;`

3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che la batteria e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e la batteria.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se necessario, raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della batteria è completata. È possibile riprendere le normali operazioni.

Controller di accensione (simplex)

Accendere lo shelf del controller per verificare che funzioni correttamente. Quindi, è possibile raccogliere i dati di supporto e riprendere le operazioni.

Eseguire questa attività solo se lo storage array dispone di un controller.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede

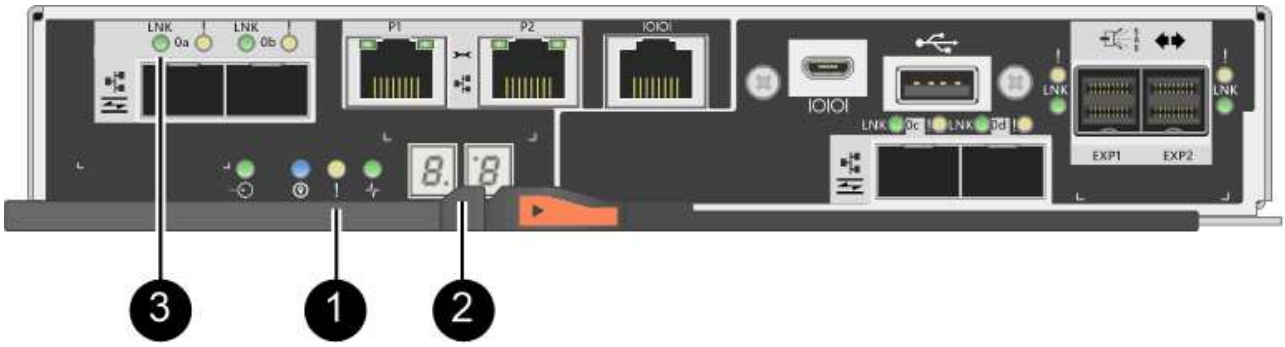
90 secondi o meno.

- Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.

2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a sette segmenti dovrebbe visualizzare l'ID del vassoio.
   - Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
   - I LED verdi del collegamento host si accendono.

   La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



   (1) *LED di attenzione (ambra)*

   (2) *Display a sette segmenti*

   (3) *LED collegamento host*

3. Verificare che lo stato del controller sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che la batteria e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e la batteria.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se necessario, raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della batteria è completata. È possibile riprendere le normali operazioni.

Controller

Requisiti per la sostituzione del controller E2800

Prima di sostituire o aggiungere un controller E2800, esaminare i requisiti e le considerazioni.

Ogni contenitore di controller contiene una scheda controller, una batteria e una scheda di interfaccia host (HIC) opzionale. È possibile aggiungere un secondo controller a una configurazione simplex o sostituire un controller guasto.

Queste procedure si applicano agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Queste procedure si riferiscono a sostituzioni o sostituzioni IOM simili a quelle degli shelf. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Requisiti per l'aggiunta di un secondo controller

È possibile aggiungere un secondo contenitore di controller alla versione simplex dei seguenti shelf di controller:

- Shelf di controller E2812
- Shelf di controller E2824
- Flash array EF280

Le figure mostrano un esempio di shelf di controller prima di aggiungere un secondo controller (un contenitore di controller e un bianco di controller) e dopo aver aggiunto un secondo controller (due contenitori di controller).

Le figure mostrano esempi di canister dei controller; le porte host sui canister dei controller potrebbero essere diverse.

Prima di aggiungere un secondo controller, è necessario disporre di:

- Un nuovo contenitore del controller con lo stesso numero di parte del contenitore del controller attualmente installato.
- Un nuovo HIC identico all'HIC nel contenitore del controller attualmente installato (necessario solo se il contenitore del controller attualmente installato include una scheda di interfaccia host).
- Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte del controller.

  Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

- Driver multipath installato sull'host in modo da poter utilizzare entrambi i controller. Fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express" per istruzioni.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Un cacciavite Phillips n. 1.
- Etichette per identificare i nuovi cavi.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

  In alternativa, è possibile utilizzare l'interfaccia della riga di comando (CLI) per eseguire alcune procedure. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:

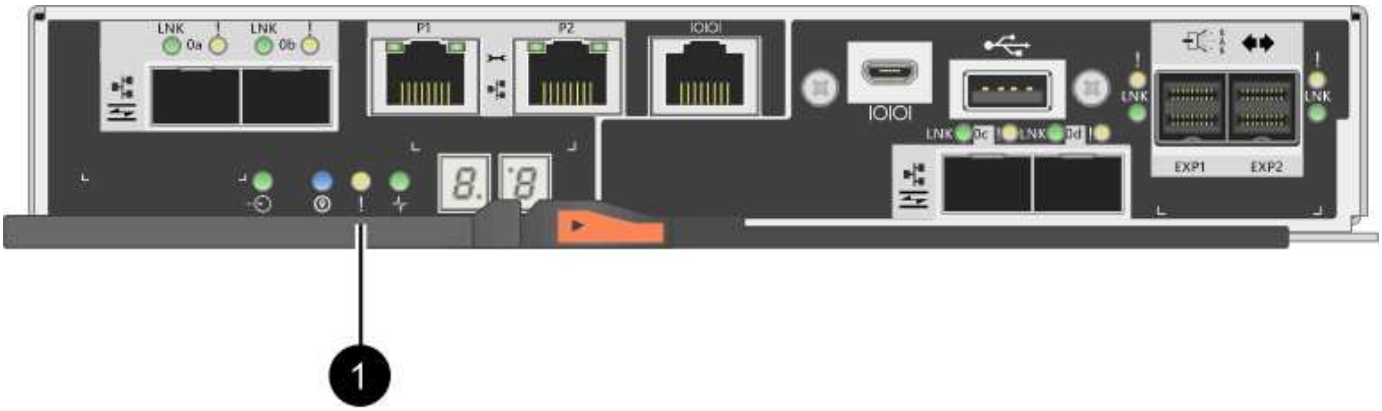
  - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
  - **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Requisiti per la sostituzione del controller

Quando si sostituisce un contenitore del controller guasto, rimuovere la batteria e l'HIC, se installato, dal contenitore del controller originale e installarli nel contenitore del controller sostitutivo.

È possibile determinare se si dispone di un contenitore del controller guasto in due modi:

- Il guru del ripristino in Gestione di sistema di SANtricity richiede la sostituzione del contenitore del controller.
- Il LED di attenzione ambra sul contenitore del controller è acceso, a indicare che il controller è guasto.



(1) *LED attenzione*

> La figura mostra un esempio di contenitore del controller; le porte host sul contenitore del controller potrebbero essere diverse.

Prima di sostituire un controller, è necessario disporre di:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Cacciavite Phillips n. 1.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

  In alternativa, è possibile utilizzare l'interfaccia della riga di comando (CLI) per eseguire alcune procedure. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:

  - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
  - **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Requisiti di configurazione duplex

Se lo shelf di controller dispone di due controller (configurazione duplex), è possibile sostituire un contenitore di controller mentre lo storage array è acceso ed esegue le operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:

- Il secondo contenitore del controller nello shelf ha uno stato ottimale.
- Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Requisiti di configurazione simplex

Se si dispone di un solo contenitore di controller (configurazione simplex), i dati sull'array di storage non saranno accessibili fino a quando non si sostituisce il contenitore di controller. È necessario interrompere le operazioni di i/o dell'host e spegnere lo storage array.

Aggiungere il secondo contenitore del controller in E2800

È possibile aggiungere un secondo contenitore di controller nell'array E2800.

A proposito di questa attività

Questa attività descrive come aggiungere un secondo contenitore di controller alla versione simplex di uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280. Questa procedura viene anche chiamata conversione simplex-to-duplex, che è una procedura online. È possibile accedere ai dati sull'array di storage durante l'esecuzione di questa procedura.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

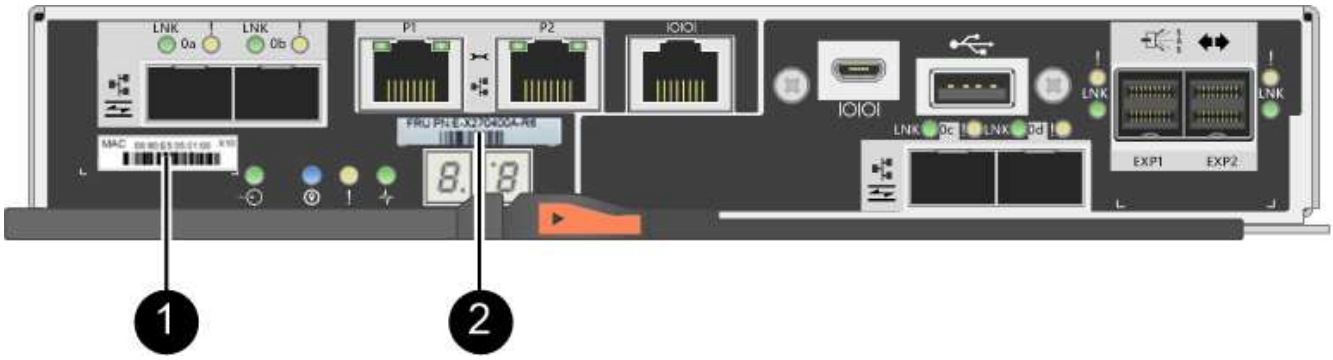
- Un nuovo contenitore del controller con lo stesso numero di parte del contenitore del controller attualmente installato. (Vedere il passaggio 1 per verificare il codice del ricambio).
- Un nuovo HIC identico all'HIC nel contenitore del controller attualmente installato (necessario solo se il contenitore del controller attualmente installato include una scheda di interfaccia host).
- Un braccialetto ESD o adottare altre precauzioni antistatiche.
- Un cacciavite Phillips n. 1.
- Etichette per identificare i nuovi cavi. Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".
- Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Verificare il codice del nuovo controller

Verificare che il nuovo controller abbia lo stesso numero di parte del controller attualmente installato.

Fasi

1. Disimballare il nuovo contenitore del controller e riutilizzarlo su una superficie piana e priva di elettricità statica.
2. Individuare le etichette dell'indirizzo MAC e del numero di parte della FRU sul retro del contenitore del controller.



(1) *MAC address:* Indirizzo MAC per la porta di gestione 1 (“P1”). Se si è utilizzato DHCP per ottenere l’indirizzo IP del controller originale, sarà necessario questo indirizzo per connettersi al nuovo controller.

(2) *numero di parte FRU:* questo numero deve corrispondere al numero di parte di ricambio per il controller attualmente installato.

3. Da Gestore di sistema di SANtricity, individuare il numero di parte di ricambio per il contenitore del controller installato.
   a. Selezionare **hardware**.
   b. Individuare lo shelf del controller, contrassegnato dall’icona del controller .
   c. Fare clic sull’icona del controller.
   d. Selezionare il controller e fare clic su **Avanti**.
   e. Nella scheda **base**, annotare il **numero di parte di ricambio** del controller.
4. Verificare che il numero di parte di ricambio per il controller installato sia lo stesso del numero di parte FRU per il nuovo controller.

> **Possibile perdita di accesso ai dati** — se i due numeri di parte non sono gli stessi, non tentare questa procedura. Inoltre, se il contenitore del controller originale include una scheda di interfaccia host (HIC), è necessario installare un HIC identico nel nuovo contenitore del controller. La presenza di controller non corrispondenti o HICS causerà il blocco del nuovo controller quando lo si porta online.

Fase 2: Installare la scheda di interfaccia host

Se il controller attualmente installato include un HIC, è necessario installare lo stesso modello di scheda di interfaccia host (HIC) nel secondo contenitore del controller.

Fasi

1. Disimballare il nuovo HIC e verificare che sia identico all’HIC esistente.

> **Possibile perdita di accesso ai dati** — l’HICS installato nei due contenitori del controller deve essere identico. Se l’HIC di ricambio non è identico all’HIC che si sta sostituendo, non tentare questa procedura. La presenza di HICS non corrispondenti causerà il blocco del nuovo controller quando viene online.

2. Capovolgere il nuovo contenitore del controller, in modo che il coperchio sia rivolto verso l’alto.
3. Premere il pulsante sul coperchio ed estrarre il coperchio.
4. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al

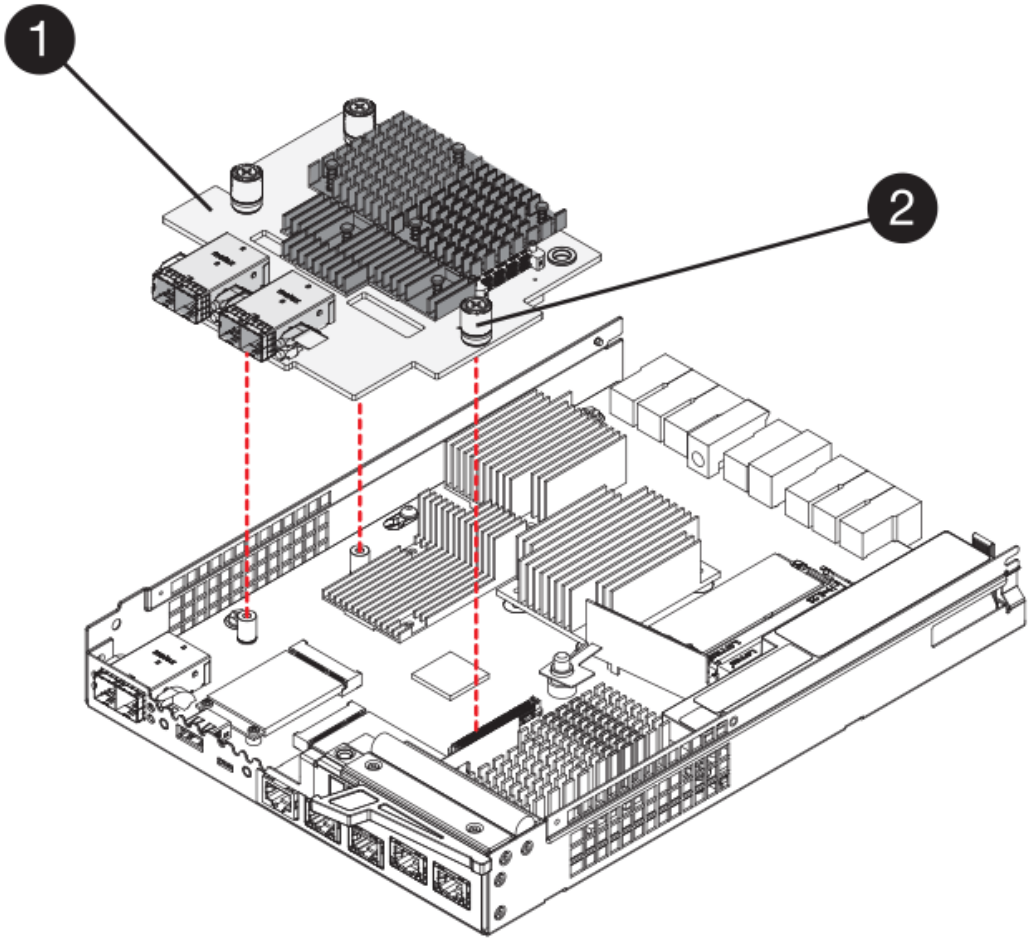
contenitore del controller, quindi rimuovere la piastra frontale.

5. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

6. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



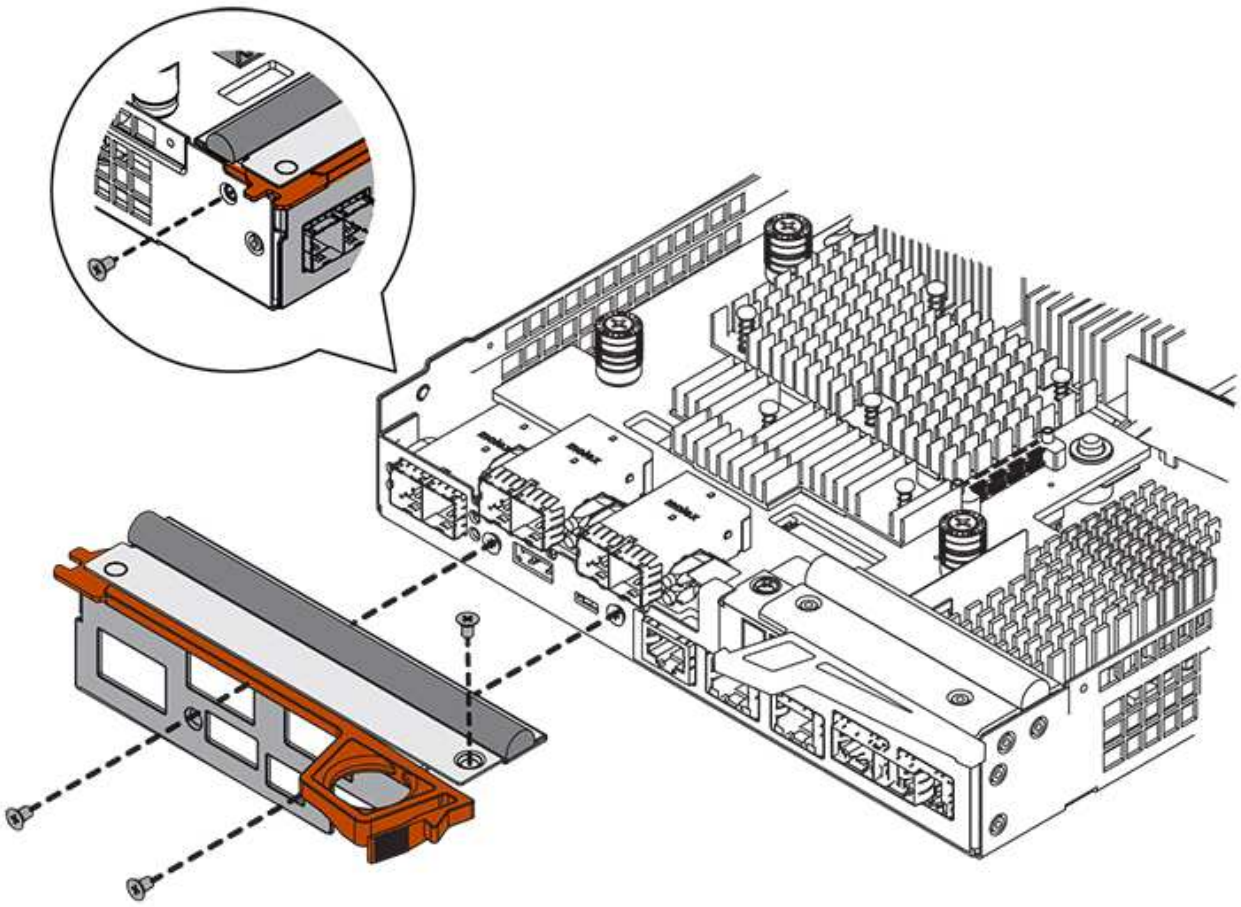
   (1) *scheda di interfaccia host*

   (2) *viti a testa zigrinata*

7. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

8. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.



9. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
10. Mettere da parte il contenitore del controller fino a quando non si è pronti per installarlo.

Fase 3: Raccolta dei dati di supporto

Raccogliere i dati di supporto prima e dopo la sostituzione di un componente per assicurarsi di poter inviare un set completo di registri al supporto tecnico nel caso in cui la sostituzione non risolva il problema.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

3. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio,

è possibile eseguire le seguenti operazioni:

- Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
- Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
- Smontare tutti i file system associati ai volumi sull'array.

> I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

> **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

Fase 4: Modificare la configurazione in duplex

Prima di aggiungere un secondo controller allo shelf di controller, è necessario modificare la configurazione in duplex installando un nuovo file NVSRAM e utilizzando l'interfaccia della riga di comando per impostare lo storage array su duplex. La versione duplex del file NVSRAM è inclusa nel file di download per il software SANtricity OS (firmware del controller).

Fasi

1. Scaricare il file NVSRAM più recente dal sito del supporto NetApp sul client di gestione.
   a. Da Gestore di sistema di SANtricity, selezionare **supporto › Centro di aggiornamento**. Nell'area denominata "aggiornamento software del sistema operativo SANtricity", fare clic su **Download del sistema operativo NetApp SANtricity**.
   b. Dal sito del supporto NetApp, selezionare **Software del controller del sistema operativo SANtricity e-Series**.
   c. Seguire le istruzioni online per selezionare la versione DI NVSRAM che si desidera installare, quindi completare il download del file. Assicurarsi di selezionare la versione duplex DI NVSRAM (il file ha "D" vicino alla fine del nome).

      Il nome del file sarà simile a: **N290X-830834-D01.dlp**

2. Aggiornare i file utilizzando Gestione di sistema di SANtricity.

   > **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.

   È possibile annullare l'operazione durante il controllo dello stato di salute prima dell'aggiornamento, ma non durante il trasferimento o l'attivazione.

   - Da Gestore di sistema di SANtricity:
     i. Nella sezione **aggiornamento del software del sistema operativo SANtricity**, fare clic su **Avvia aggiornamento**.
     ii. Accanto a **Select Controller NVSRAM file**, fare clic su **Browse**, quindi selezionare il file NVSRAM scaricato.

iii. Fare clic su **Start**, quindi confermare che si desidera eseguire l'operazione.

L'aggiornamento ha inizio e si verifica quanto segue:

- Viene avviato il controllo dello stato di salute prima dell'aggiornamento. Se il controllo dello stato di salute prima dell'aggiornamento non riesce, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema.
- I file del controller vengono trasferiti e attivati. Il tempo necessario dipende dalla configurazione dello storage array.
- Il controller si riavvia automaticamente per applicare le nuove impostazioni.

◦ In alternativa, è possibile utilizzare il seguente comando CLI per eseguire l'aggiornamento:

```
download storageArray NVSRAM file="filename"
healthCheckMelOverride=FALSE;
```

In questo comando, `filename` È il percorso del file e il nome del file per la versione duplex del file NVSRAM del controller (il file con "D" nel nome). Racchiudere il percorso del file e il nome del file tra virgolette doppie (" "). Ad esempio:

```
file="C:\downloads\N290X-830834-D01.dlp"
```

3. (Facoltativo) per visualizzare un elenco degli aggiornamenti, fare clic su **Save Log** (Salva registro).

Il file viene salvato nella cartella Download del browser con il nome **latest-upgrade-log-timestamp.txt**.

◦ Dopo aver aggiornato IL controller NVSRAM, verificare quanto segue in Gestione sistema di SANtricity:
  - Accedere alla pagina hardware e verificare che tutti i componenti siano visualizzati.
  - Accedere alla finestra di dialogo Software and firmware Inventory (inventario software e firmware) (andare al **Support › Upgrade Center**, quindi fare clic sul collegamento **Software and firmware Inventory**). Verificare le nuove versioni del software e del firmware.

◦ Quando si aggiorna IL controller NVSRAM, tutte le impostazioni personalizzate applicate all'NVSRAM esistente vengono perse durante il processo di attivazione. Al termine del processo di attivazione, è necessario applicare nuovamente le impostazioni personalizzate A NVSRAM.

4. Modificare l'impostazione dello storage array su duplex utilizzando i comandi CLI. Per utilizzare CLI, è possibile aprire un prompt dei comandi se il pacchetto CLI è stato scaricato oppure aprire Enterprise Management Window (EMW) se Storage Manager è installato.

◦ Da un prompt dei comandi:

i. Utilizzare il seguente comando per passare dalla modalità simplex alla modalità duplex:

```
set storageArray redundancyMode=duplex;
```

ii. Utilizzare il seguente comando per ripristinare il controller.

```
reset controller [a];
```

- Dall'interfaccia EMW:
  i. Selezionare l'array di storage.
  ii. Selezionare **Strumenti › Esegui script**.
  iii. Digitare il seguente comando nella casella di testo.

```
set storageArray redundancyMode=duplex;
```

  iv. Selezionare **Strumenti › Verify and Execute** (verifica ed esegui).
  v. Digitare il seguente comando nella casella di testo.

```
reset controller [a];
```

  vi. Selezionare **Strumenti › Verify and Execute** (verifica ed esegui).

Dopo il riavvio del controller, viene visualizzato il messaggio di errore "Alternate controller missing" (Controller alternativo mancante). Questo messaggio indica che il controller A è stato convertito correttamente in modalità duplex. Questo messaggio persiste fino a quando non si installa il secondo controller e si collegano i cavi host.

Fase 5: Rimuovere la protezione del controller

Rimuovere la protezione del controller prima di installare il secondo controller. Un controller vuoto viene installato negli shelf di controller che hanno un solo controller.

Fasi

1. Premere il fermo sull'impugnatura della camma per il pannello di controllo finché non viene rilasciato, quindi aprire l'impugnatura della camma a destra.
2. Estrarre il contenitore del controller vuoto dallo scaffale e metterlo da parte.

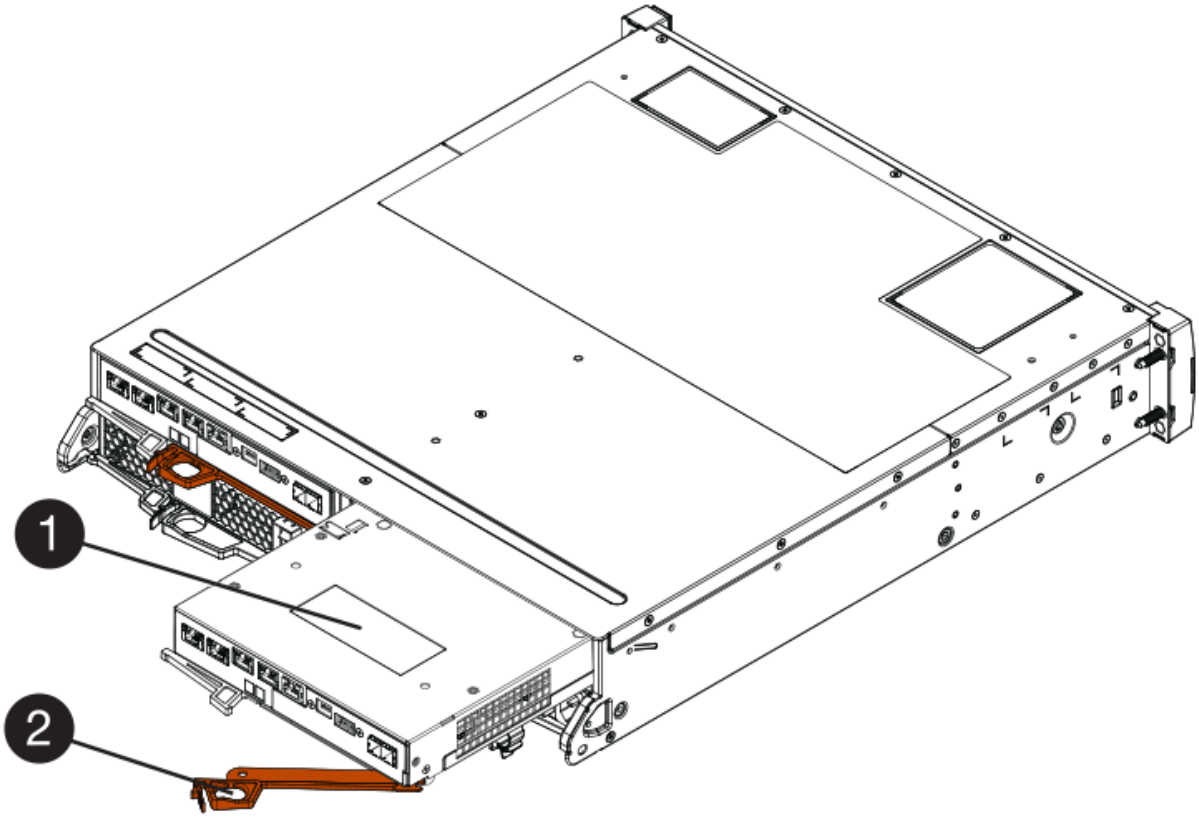
   Quando si rimuove la protezione del controller, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto.

Fase 6: Installare il secondo contenitore del controller

Installare un secondo contenitore del controller per modificare una configurazione simplex in una configurazione duplex.

Fasi

1. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
2. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*

3. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
4. Inserire i ricetrasmettitori SFP+ e collegare i cavi al nuovo controller.

Fase 7: Completare l'aggiunta di un secondo controller

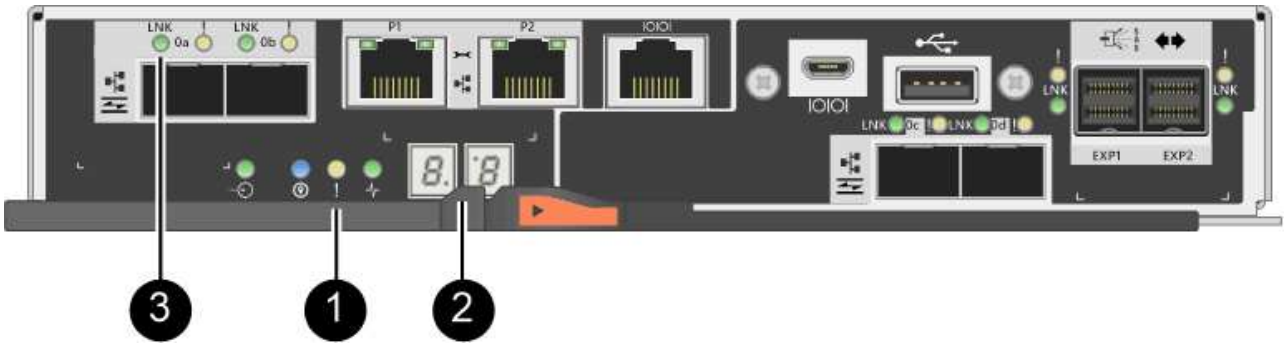
Completare il processo di aggiunta di un secondo controller confermando che funziona correttamente, reinstallare il file NVSRAM duplex, distribuire i volumi tra i controller e raccogliere i dati di supporto.

Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
     host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

2. Controllare i codici sul display a sette segmenti del controller non appena viene online. Se sul display viene visualizzata una delle seguenti sequenze di ripetizione, rimuovere immediatamente il controller.
   - **OE**, **L0**, ***blank*** (controller non corrispondenti)
   - **OE**, **L6**, ***blank*** (HIC non supportato)

> **Possibile perdita di accesso ai dati** — se il controller appena installato mostra uno di questi codici e l'altro controller viene resettato per qualsiasi motivo, anche il secondo controller potrebbe bloccarsi.

3. Aggiornare le impostazioni dell'array da simplex a duplex con il seguente comando CLI:

```
set storageArray redundancyMode=duplex;
```

4. Da Gestore di sistema di SANtricity, verificare che lo stato del controller sia ottimale.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

> Se non si riesce a risolvere il problema, contattare il supporto tecnico.

5. Reinstallare la versione duplex del file NVSRAM utilizzando Gestione di sistema di SANtricity.

   Questo passaggio garantisce che entrambi i controller dispongano di una versione identica di questo file.

> **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.

> È necessario installare il software SANtricity OS quando si installa un nuovo file NVSRAM utilizzando Gestione di sistema di SANtricity. Se si dispone già della versione più recente del software SANtricity OS, è necessario reinstallarla.

   a. Se necessario, scaricare la versione più recente del software SANtricity OS dal sito del supporto NetApp.

b. In System Manager, accedere al Centro aggiornamenti.

c. Nella sezione **aggiornamento del software del sistema operativo SANtricity**, fare clic su **Avvia aggiornamento**.

d. Fare clic su **Sfoglia** e selezionare il file del software SANtricity OS.

e. Fare clic su **Browse** (Sfoglia) e selezionare il file NVSRAM del controller.

f. Fare clic su **Start** e confermare che si desidera eseguire l'operazione.

   Viene avviato il trasferimento dell'operazione di controllo.

6. Dopo il riavvio dei controller, è possibile distribuire i volumi tra il controller A e il nuovo controller B.

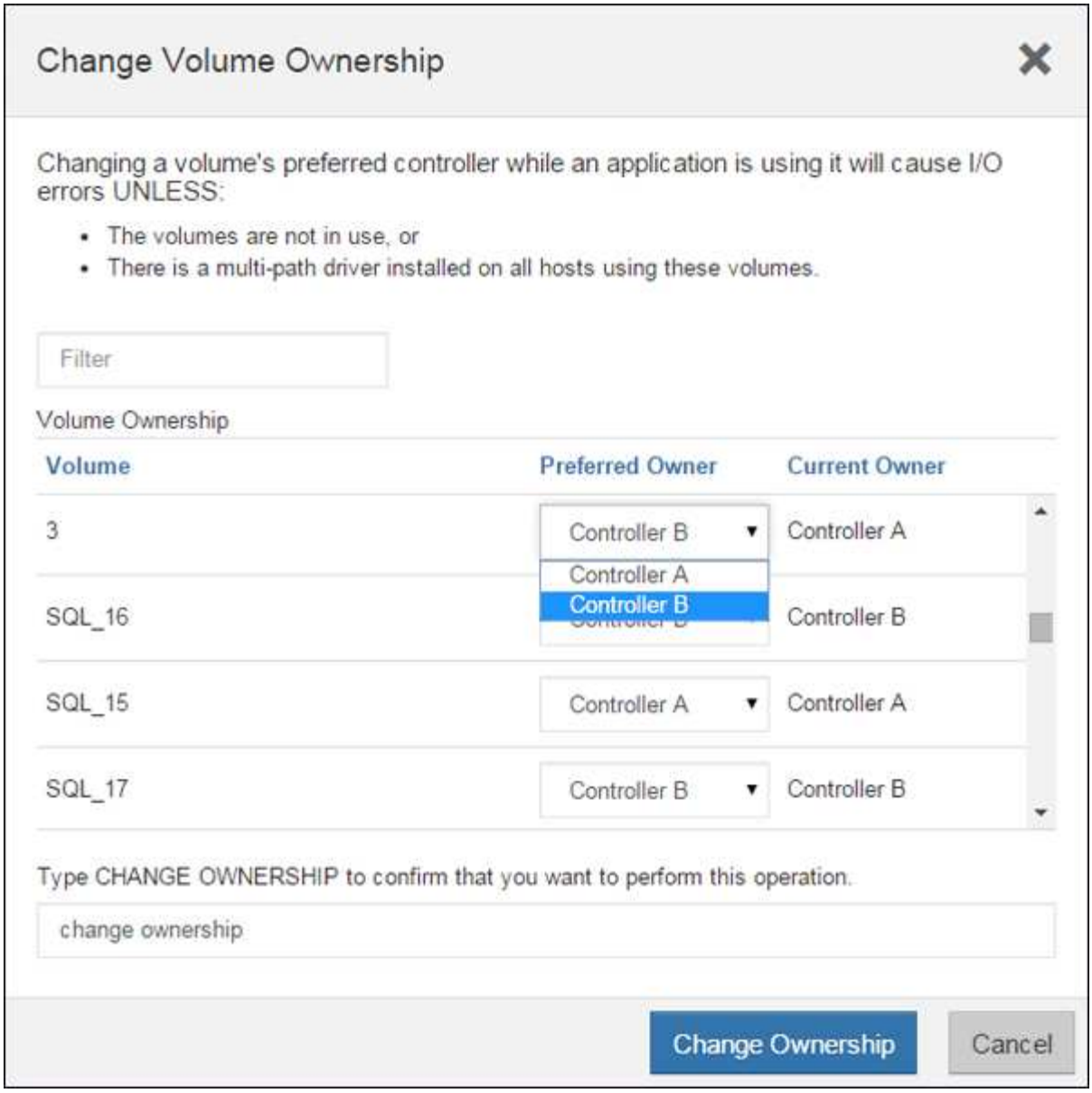
   a. Selezionare **Storage › Volumes** (Storage[volumi]).

   b. Dalla scheda All Volumes (tutti i volumi), selezionare **More › Change Ownership** (Altro[Modifica proprietà]).

   c. Digitare il seguente comando nella casella di testo: `change ownership`

      Il pulsante Change Ownership (Cambia proprietà) è attivato.

   d. Per ciascun volume che si desidera ridistribuire, selezionare **Controller B** dall'elenco **Preferred Owner** (Proprietario preferito).



e. Fare clic su **Cambia proprietà**.

   Al termine del processo, la finestra di dialogo Change Volume Ownership (Modifica proprietà volume) mostra i nuovi valori per **Preferred Owner** (Proprietario preferito) e **Current Owner** (Proprietario attuale).

7. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

Il processo di aggiunta di un secondo controller è completo. È possibile riprendere le normali operazioni.

Sostituire il controller nella configurazione duplex E2800

È possibile sostituire un contenitore di controller in una configurazione duplex (a due controller) per i seguenti shelf di controller:

- Shelf di controller E2812
- Shelf di controller E2824
- Shelf di controller E2860
- Flash array EF280

A proposito di questa attività

Ogni contenitore di controller contiene una scheda controller, una batteria e una scheda di interfaccia host (HIC) opzionale. Quando si sostituisce un contenitore del controller, è necessario rimuovere la batteria e l'HIC, se installato, dal contenitore del controller originale e installarli nel contenitore del controller sostitutivo.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo. (Vedere il passaggio 1 per verificare il codice del ricambio).
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Cacciavite Phillips n. 1.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del controller (duplex)

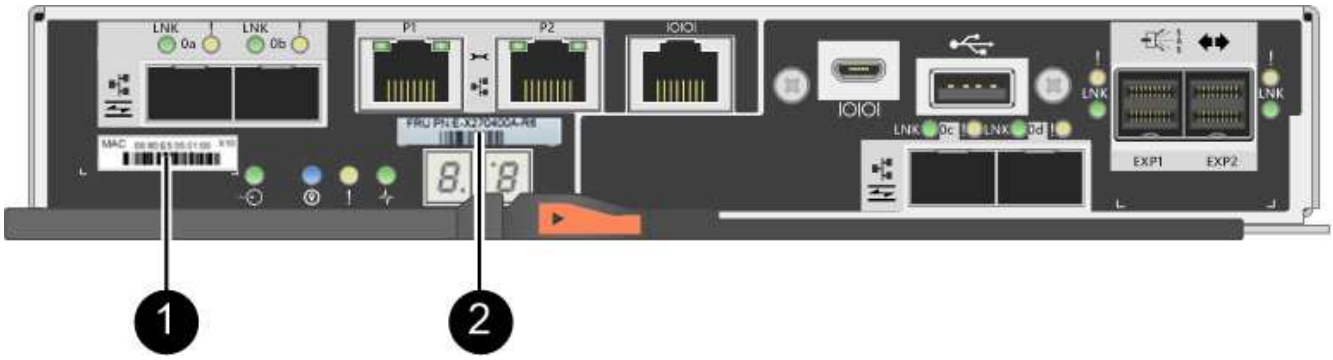
Preparare la sostituzione del controller verificando che il contenitore del controller sostitutivo disponga del codice FRU corretto, eseguendo il backup della configurazione e raccogliendo i dati di supporto. Se il controller è ancora online, è necessario portarlo offline.

Fasi

1. Disimballare il nuovo contenitore del controller e riutilizzarlo su una superficie piana e priva di elettricità statica.

   Conservare il materiale di imballaggio da utilizzare per la spedizione del contenitore del controller guasto.

2. Individuare le etichette dell'indirizzo MAC e del numero di parte della FRU sul retro del contenitore del controller.



(1) *MAC address:* Indirizzo MAC per la porta di gestione 1 (“P1”). Se si è utilizzato DHCP per ottenere l’indirizzo IP del controller originale, è necessario questo indirizzo per connettersi al nuovo controller.

(2) *numero di parte FRU:* questo numero deve corrispondere al numero di parte di ricambio per il controller attualmente installato.

3. Da Gestore di sistema di SANtricity, individuare il numero di parte di ricambio del contenitore del controller che si sta sostituendo.

   Quando un controller presenta un guasto e deve essere sostituito, il codice del ricambio viene visualizzato nell’area Details (Dettagli) del Recovery Guru. Se è necessario trovare questo numero manualmente, attenersi alla seguente procedura:

   a. Selezionare **hardware**.
   b. Individuare lo shelf del controller, contrassegnato dall’icona del controller .
   c. Fare clic sull’icona del controller.
   d. Selezionare il controller e fare clic su **Avanti**.
   e. Nella scheda **base**, annotare il **numero di parte di ricambio** del controller.

4. Verificare che il numero di parte sostitutivo del controller guasto sia lo stesso del numero di parte FRU del controller sostitutivo.

   > **Possibile perdita di accesso ai dati** — se i due numeri di parte non sono gli stessi, non tentare questa procedura. Inoltre, se il contenitore del controller guasto include una scheda di interfaccia host (HIC), è necessario installare tale HIC nel nuovo contenitore del controller. La presenza di controller non corrispondenti o HICS causerà il blocco del nuovo controller quando lo si porta online.

5. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

- In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

7. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
     iii. Selezionare il controller che si desidera mettere offline.
     iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

     > Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

   - In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=offline`

   Per il controller B: `set controller [b] availability=offline`

8. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

9. Selezionare **ricontrollare** dal Recovery Guru e confermare che nel campo **OK per rimuovere** nell'area Dettagli sia visualizzato **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimozione del controller guasto (duplex)

Sostituire il filtro a carboni attivi guasto con uno nuovo.

Fase 2a: Rimozione del contenitore del controller (duplex)

Rimuovere il contenitore del controller guasto in modo da poterlo sostituire con uno nuovo.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

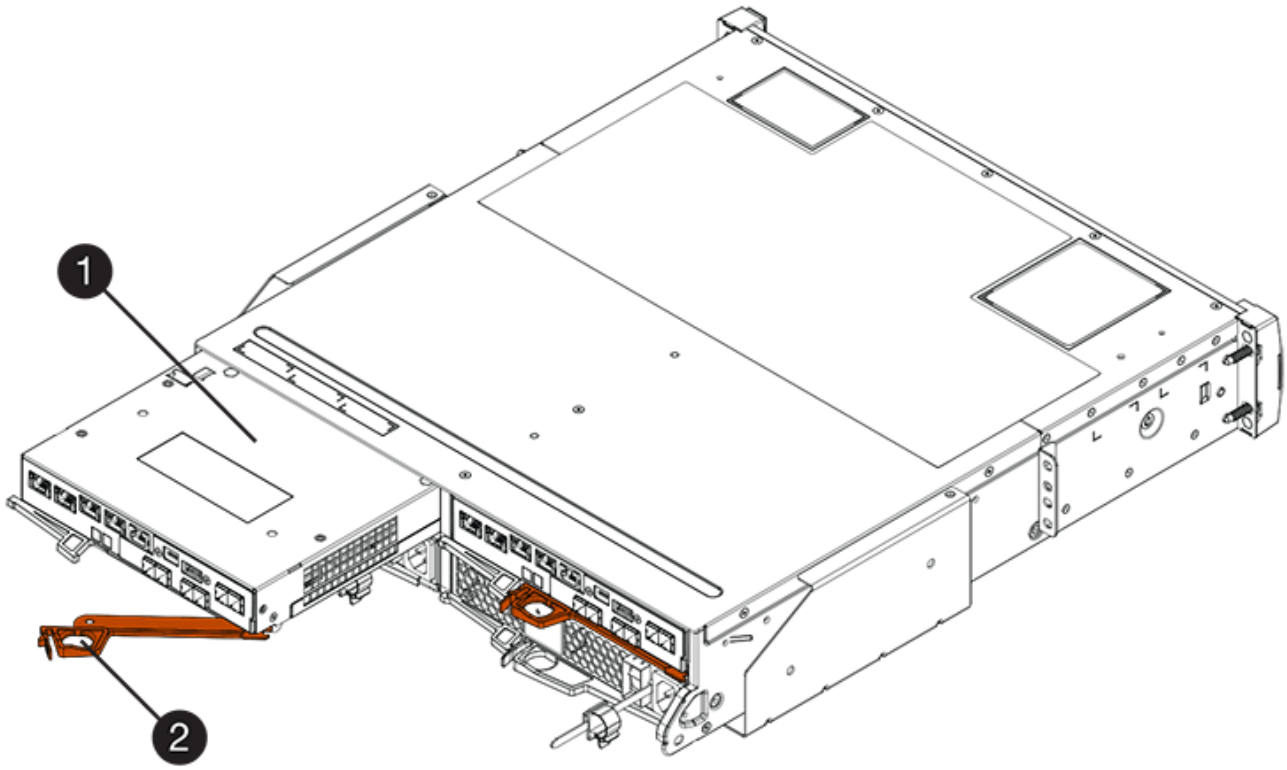
   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se il contenitore del controller dispone di un HIC che utilizza ricetrasmettitori SFP+, rimuovere gli SFP.

   Poiché è necessario rimuovere l'HIC dal contenitore del controller guasto, è necessario rimuovere eventuali SFP dalle porte HIC. Tuttavia, è possibile lasciare qualsiasi SFP installato nelle porte host della scheda base. Quando si ricollegano i cavi, è possibile spostare questi SFP nel nuovo contenitore del controller.

5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
6. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

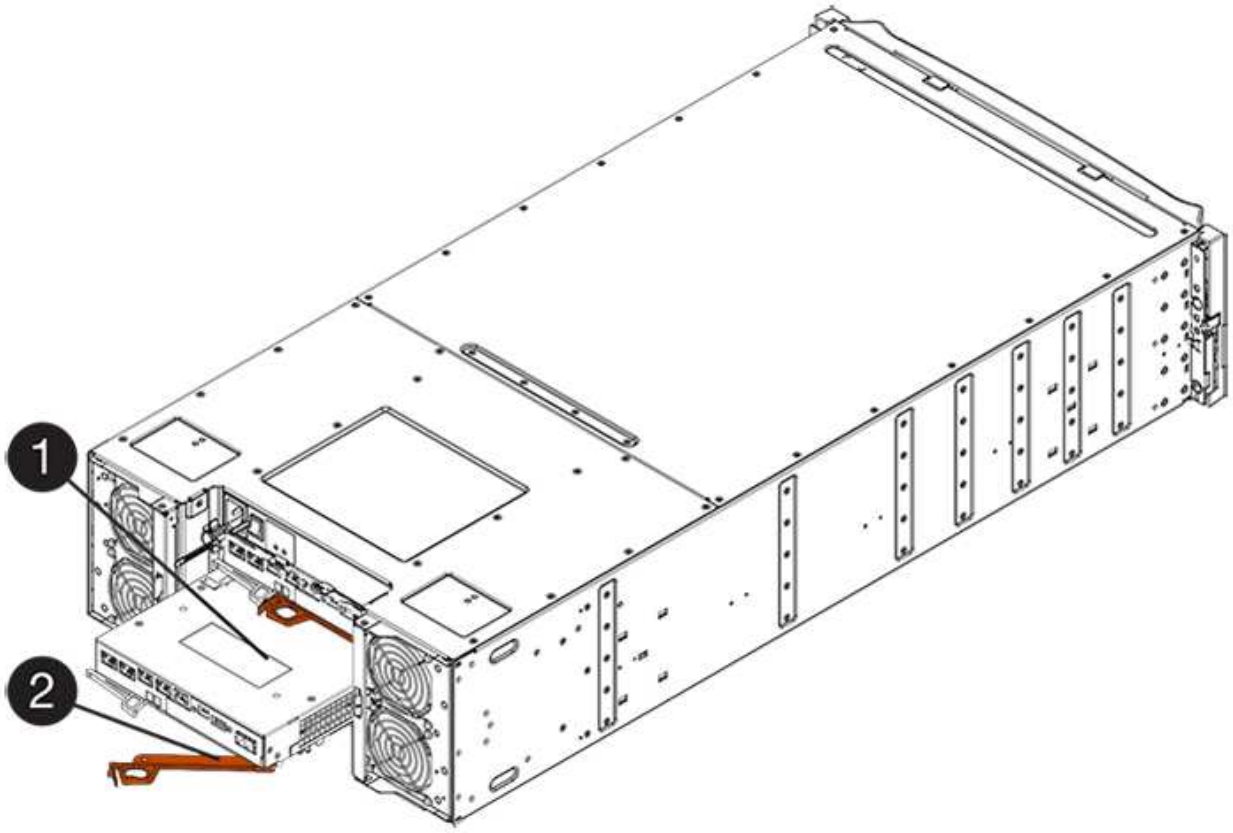
   La figura seguente è un esempio di shelf di controller E2812, shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

7. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

8. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
9. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 2b: Rimozione della batteria (duplex)

Rimuovere la batteria per installare il nuovo controller.

Fasi

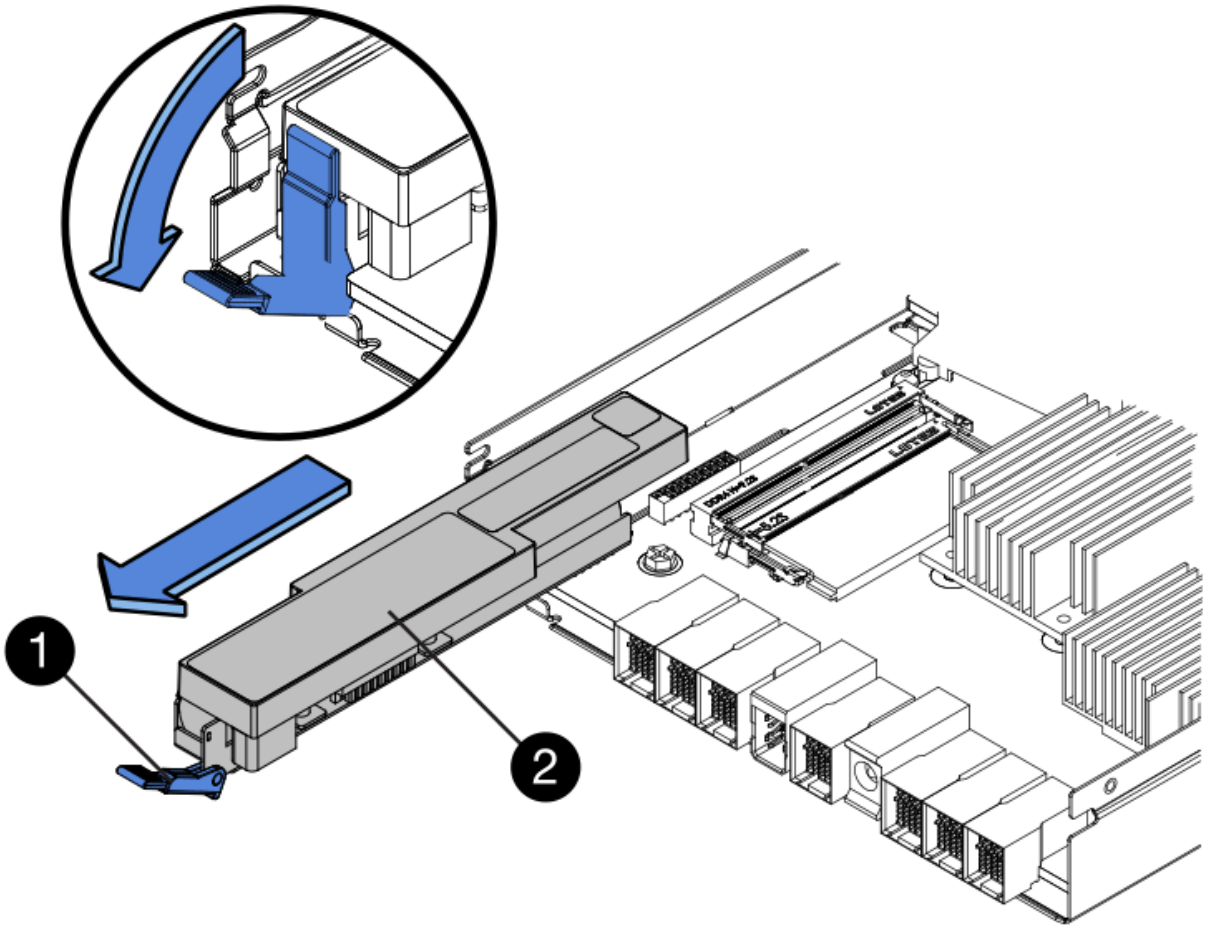
1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *LED cache interna attiva*

(2) *batteria*

3. Individuare il dispositivo di chiusura blu della batteria.
4. Sbloccare la batteria spingendo il dispositivo di chiusura verso il basso e lontano dal contenitore del controller.



(1) *dispositivo di chiusura a scatto della batteria*

(2) *batteria*

5. Sollevare la batteria ed estrarla dal contenitore del controller.

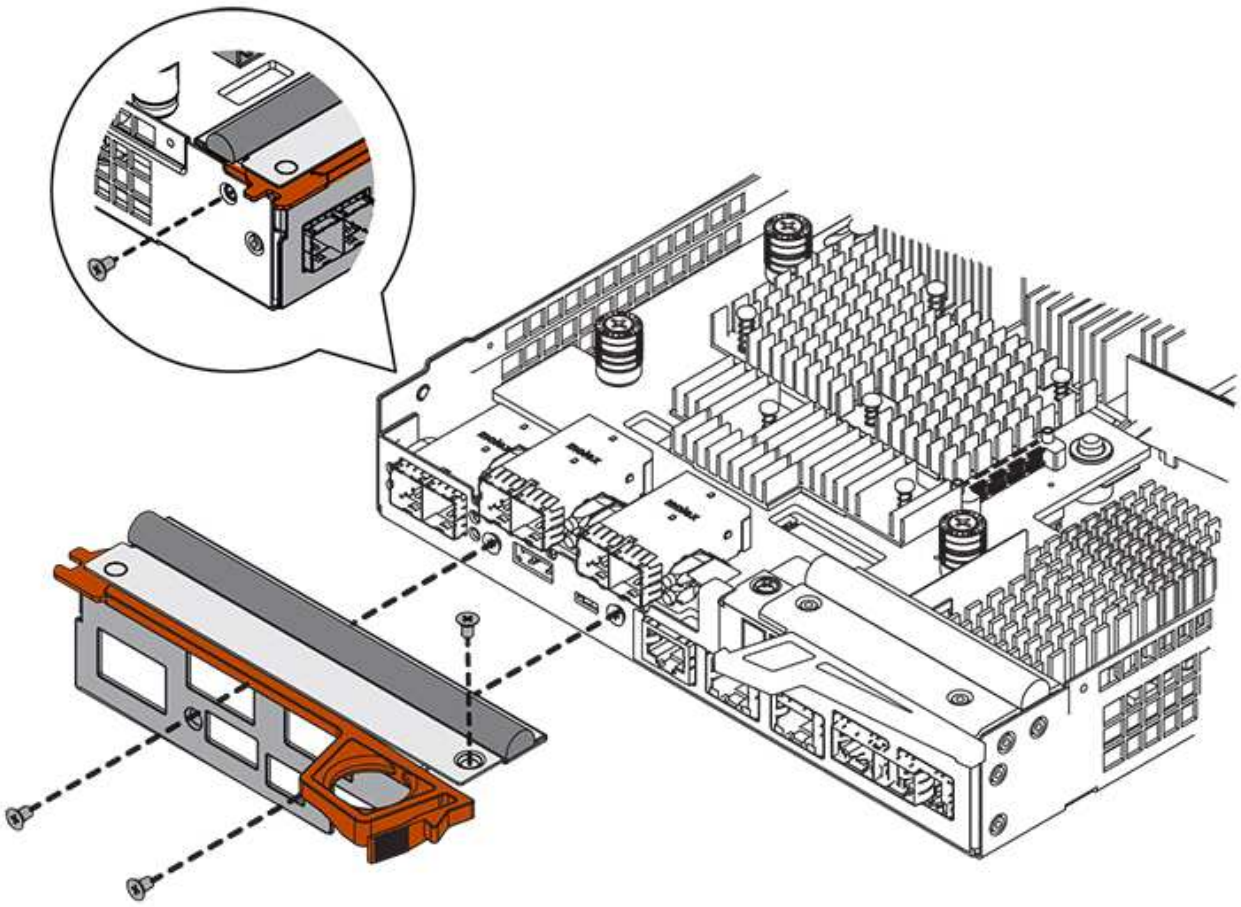
Fase 2c: Rimozione della scheda di interfaccia host (duplex)

Se il contenitore del controller include una scheda di interfaccia host (HIC), è necessario rimuovere l'HIC dal contenitore del controller originale, in modo da poterlo riutilizzare nel nuovo contenitore del controller.

Fasi

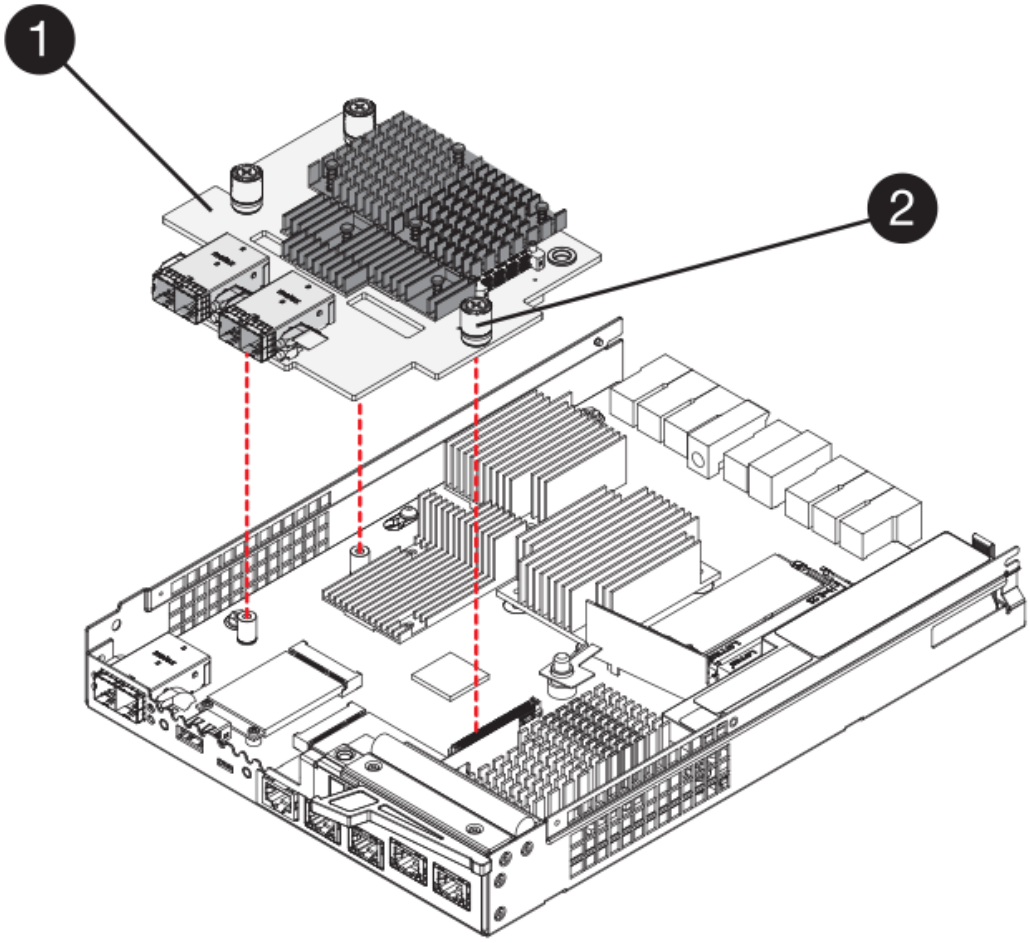
1. Utilizzando un cacciavite Phillips n. 1, rimuovere le viti che fissano la mascherina HIC al contenitore del controller.

   Sono presenti quattro viti: Una sulla parte superiore, una laterale e due sulla parte anteriore.



2. Rimuovere la piastra anteriore dell'HIC.
3. Utilizzando le dita o un cacciavite Phillips, allentare le tre viti a testa zigrinata che fissano l'HIC alla scheda del controller.
4. Scollegare con cautela l'HIC dalla scheda del controller sollevandola e facendola scorrere all'indietro.

> Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

5. Posizionare l'HIC su una superficie priva di elettricità statica.

Fase 3: Installazione di un nuovo controller (duplex)

Installare un nuovo elemento filtrante del controller per sostituire quello guasto. Eseguire questa operazione solo se lo storage array dispone di due controller (configurazione duplex).

Fase 3a: Installazione della batteria (duplex)

È necessario installare la batteria nel contenitore del controller sostitutivo. È possibile installare la batteria rimossa dal contenitore del controller originale o installare una nuova batteria ordinata.

Fasi

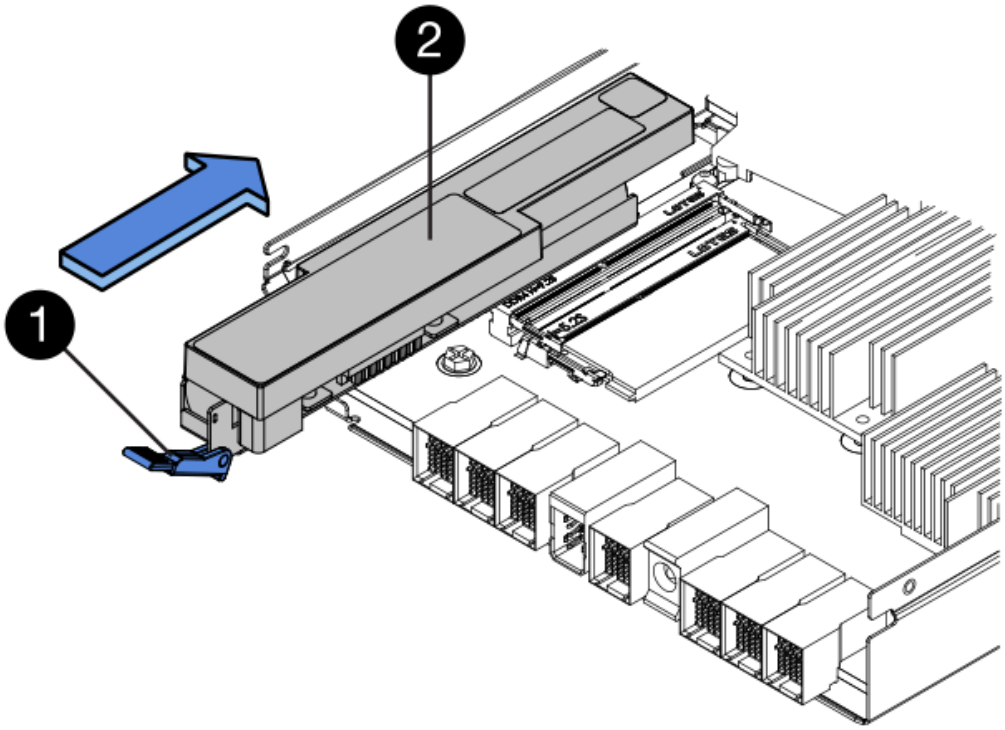
1. Capovolgere il contenitore del controller sostitutivo, in modo che il coperchio rimovibile sia rivolto verso l'alto.
2. Premere il pulsante del coperchio verso il basso ed estrarre il coperchio.
3. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
4. Inserire la batteria nel contenitore del controller inclinandola leggermente verso il basso.

   Inserire la flangia metallica nella parte anteriore della batteria nello slot sul fondo del contenitore del

controller e far scorrere la parte superiore della batteria sotto il piccolo perno di allineamento sul lato sinistro del contenitore.

5. Spostare il dispositivo di chiusura della batteria verso l'alto per fissare la batteria.

   Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.



   (1) *dispositivo di chiusura a scatto della batteria*

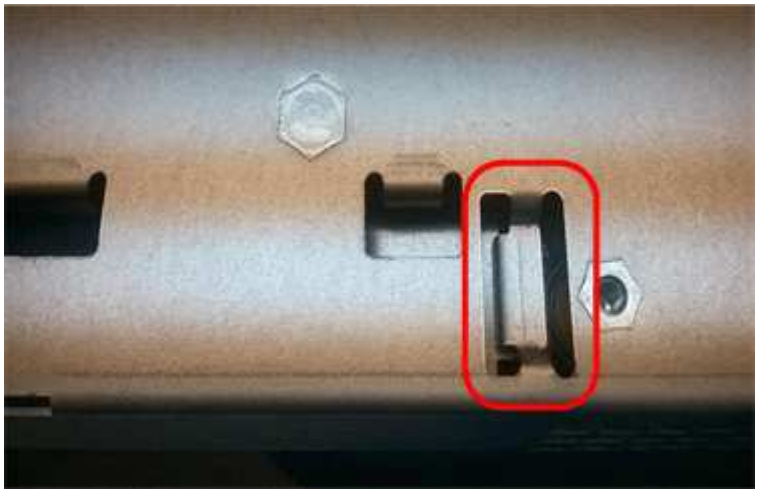
   (2) *batteria*

6. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

   > **Possibili danni all'hardware** — la flangia metallica sulla parte anteriore della batteria deve essere inserita completamente nello slot sul contenitore del controller (come mostrato nella prima figura). Se la batteria non è installata correttamente (come mostrato nella seconda figura), la flangia metallica potrebbe entrare in contatto con la scheda del controller, danneggiando il controller quando si applica l'alimentazione.

   - **Corretto** — la flangia metallica della batteria è completamente inserita nello slot del controller:

- **Errato** — la flangia metallica della batteria non è inserita nello slot del controller:



Fase 3b: Installazione della scheda di interfaccia host (duplex)

Se è stato rimosso un HIC dal contenitore del controller originale, è necessario installarlo nel nuovo contenitore del controller.

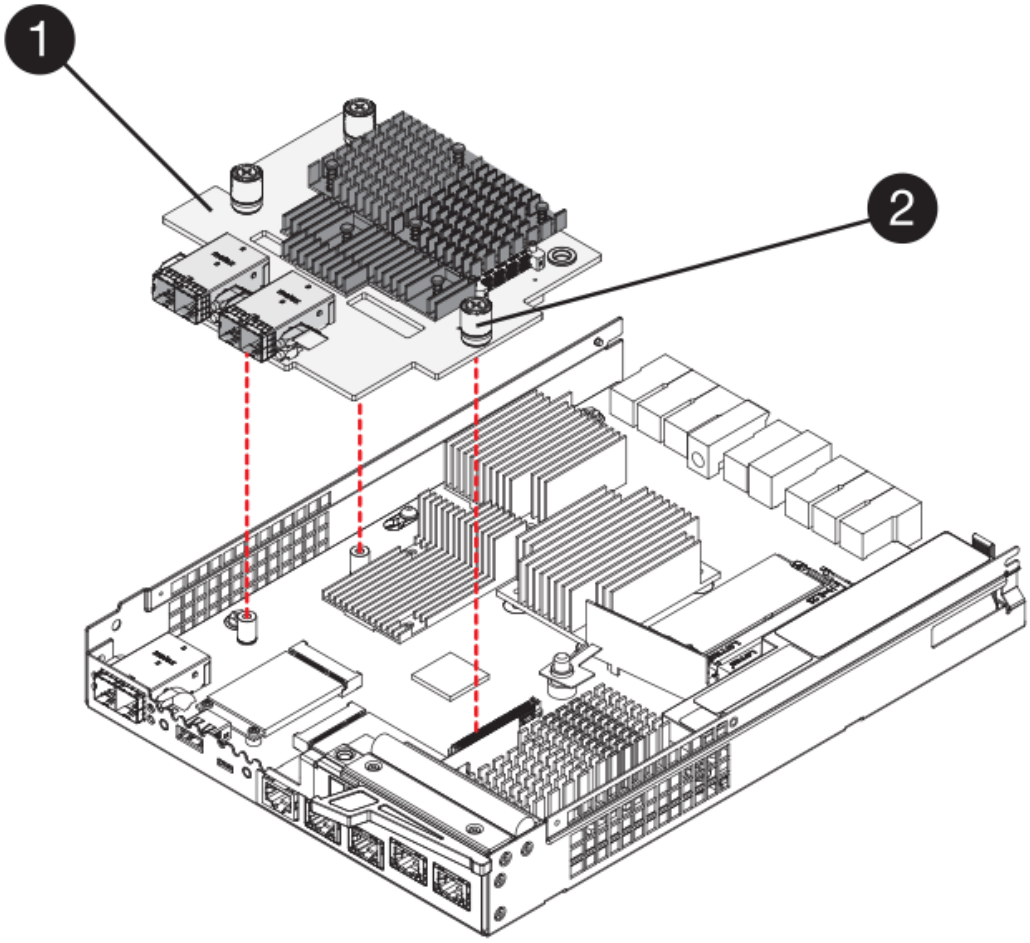
Fasi

1. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller sostitutivo, quindi rimuovere la piastra frontale.
2. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



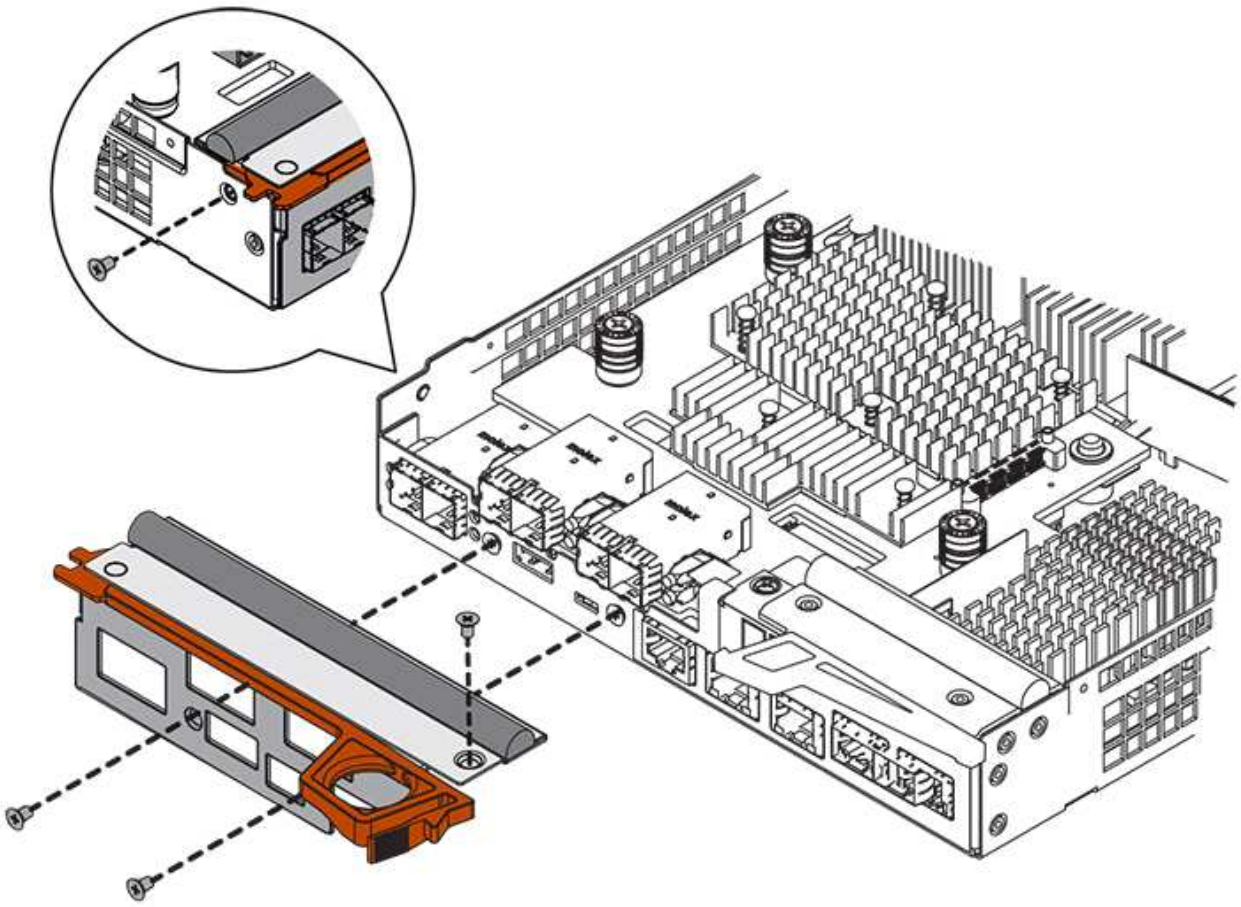
(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

4. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dal contenitore del controller originale al nuovo contenitore del controller con quattro viti.

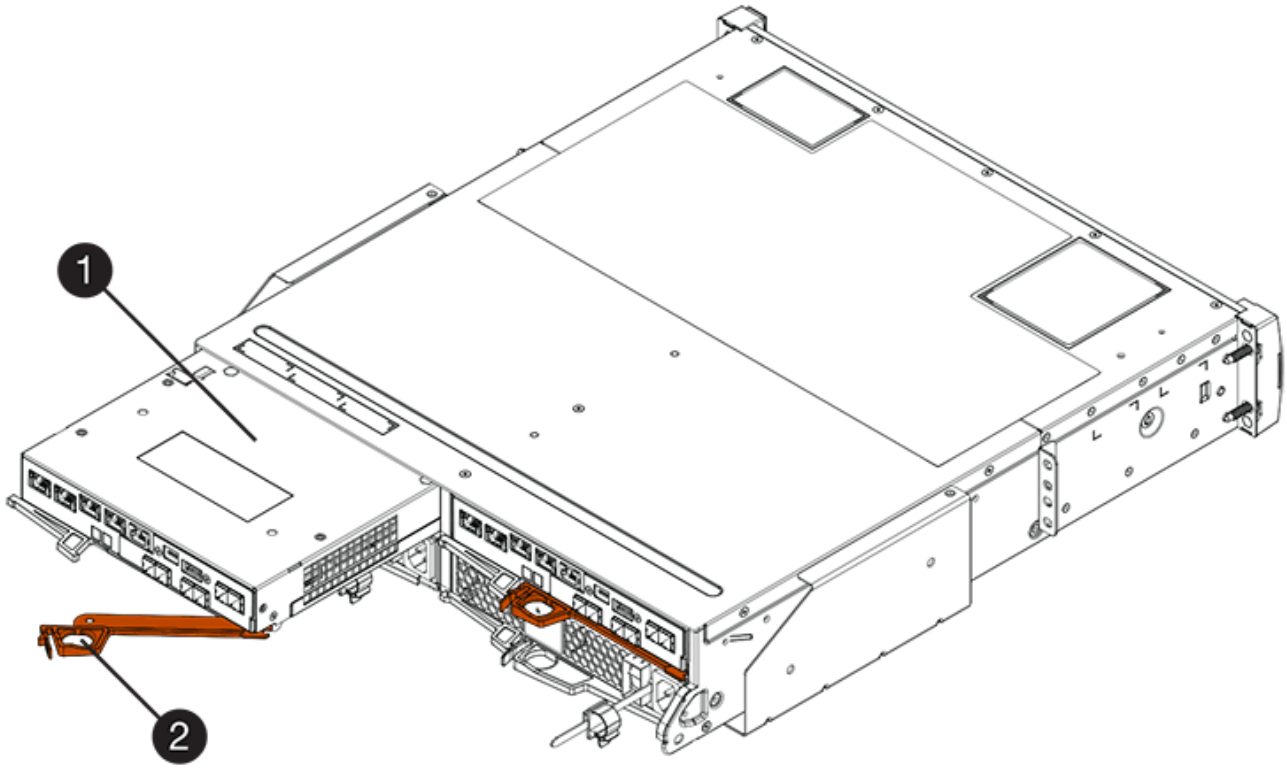


Fase 3c: Installare il nuovo contenitore del controller (duplex)

Dopo aver installato la batteria e la scheda di interfaccia host (HIC), se inizialmente installata, è possibile installare il nuovo contenitore del controller nello shelf del controller.

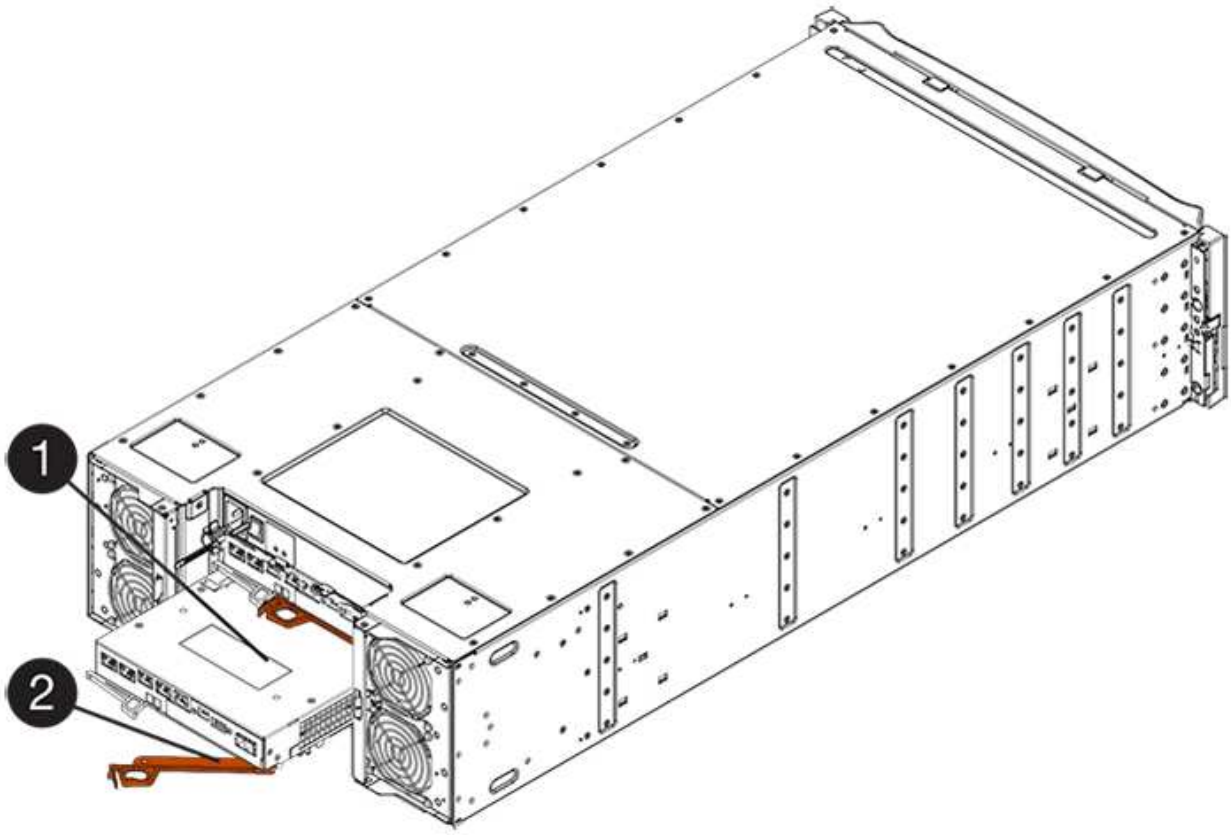
Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Installare gli SFP dal controller originale nelle porte host del nuovo controller e ricollegare tutti i cavi.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

6. Se il controller originale utilizzava DHCP per l'indirizzo IP, individuare l'indirizzo MAC sull'etichetta sul retro del controller sostitutivo. Chiedere all'amministratore di rete di associare il DNS/rete e l'indirizzo IP del controller rimosso con l'indirizzo MAC del controller sostitutivo.

   Se il controller originale non ha utilizzato DHCP per l'indirizzo IP, il nuovo controller adotterà l'indirizzo IP del controller rimosso.

Fase 4: Sostituzione completa del controller (duplex)

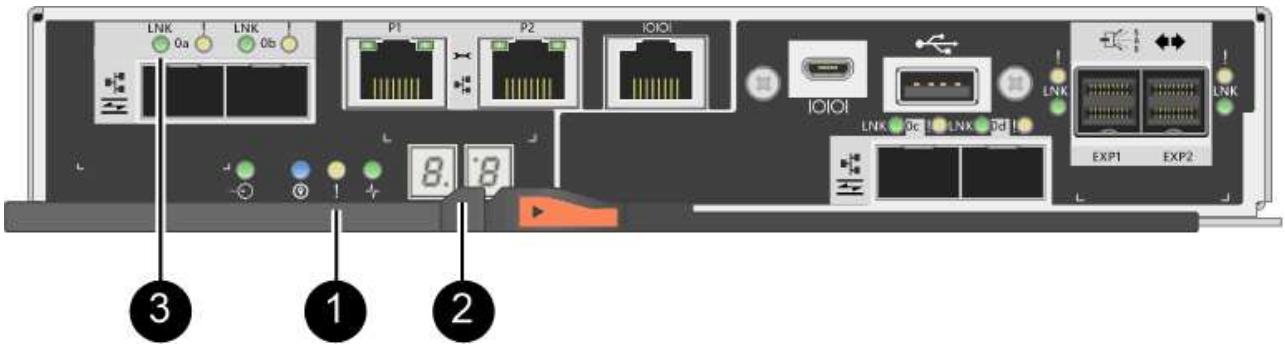
Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
     host.



   (1) *LED di attenzione (ambra)*

   (2) *Display a sette segmenti*

   (3) *LED collegamento host*

2. Controllare i codici sul display a sette segmenti del controller quando torna online. Se sul display viene visualizzata una delle seguenti sequenze di ripetizione, rimuovere immediatamente il controller.
   - **OE**, **L0**, ***blank*** (controller non corrispondenti)
   - **OE**, **L6**, ***blank*** (HIC non supportato)

Possibile perdita di accesso ai dati — se il controller appena installato mostra uno di questi codici e l'altro controller viene resettato per qualsiasi motivo, anche il secondo controller potrebbe bloccarsi.

3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se necessario, ridistribuire tutti i volumi al proprietario preferito utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Storage › Volumes** (Storage[volumi]).
   b. Selezionare il **More › redistribuisci volumi**.
5. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente del software SANtricity OS (firmware del controller).

   Se necessario, installare la versione più recente.

6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione del controller è completata. È possibile riprendere le normali operazioni.

Sostituire il controller nella configurazione simplex E2800

È possibile sostituire un contenitore di controller guasto in una configurazione simplex (controller singolo) per i seguenti shelf di controller:

- Shelf di controller E2812
- Shelf di controller E2824

A proposito di questa attività

Il contenitore del controller contiene una scheda controller, una batteria e una scheda di interfaccia host (HIC) opzionale. Quando si sostituisce un contenitore del controller guasto, rimuovere la batteria e l'HIC, se installato, dal contenitore del controller originale e installarli nel contenitore del controller sostitutivo.

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Cacciavite Phillips n. 1.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del controller (simplex)

Preparare la sostituzione di un contenitore di controller salvando la chiave di sicurezza del disco, eseguendo il backup della configurazione e raccogliendo i dati di supporto. Quindi, è possibile interrompere le operazioni di i/o dell'host e spegnere lo shelf del controller.

Fasi

1. Se possibile, prendere nota della versione del software SANtricity OS attualmente installata sul controller. Aprire Gestione sistemi SANtricity e selezionare **supporto › Centro aggiornamento › Visualizza inventario software e firmware**.
2. Se la funzione Drive Security è attivata, assicurarsi che esista una chiave salvata e di conoscere la password richiesta per l'installazione.

   > **Possibile perdita di accesso ai dati** — se tutte le unità dello storage array sono abilitate per la sicurezza, il nuovo controller non sarà in grado di accedere allo storage array fino a quando non si sbloccano le unità protette utilizzando la finestra di gestione aziendale in Gestione storage di SANtricity.

   Per salvare la chiave (potrebbe non essere possibile, a seconda dello stato del controller):

   a. Da Gestore di sistema di SANtricity, selezionare **Impostazioni › sistema**.
   b. In **Drive Security key management** (Gestione chiavi di sicurezza unità), selezionare **Backup Key** (chiave di backup).
   c. Nei campi **Definisci password/Inserisci nuova password**, immettere e confermare una password per questa copia di backup.
   d. Fare clic su **Backup**.
   e. Registrare le informazioni sulla chiave in una posizione sicura, quindi fare clic su **Chiudi**.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

- In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

4. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

5. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
8. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
9. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
10. Attendere che tutti i LED sullo shelf del controller si spenga.
11. Selezionare **ricontrollare** dal Recovery Guru e confermare che nel campo **OK per rimuovere** nell'area Dettagli sia visualizzato **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

    I dati sullo storage array non saranno accessibili fino a quando non si sostituisce il contenitore del

controller.

Fase 2: Rimozione del controller guasto (simplex)

Sostituire il filtro a carboni attivi guasto con uno nuovo.

Fase 2a: Rimozione del contenitore del controller (simplex)

Rimuovere un contenitore del controller.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

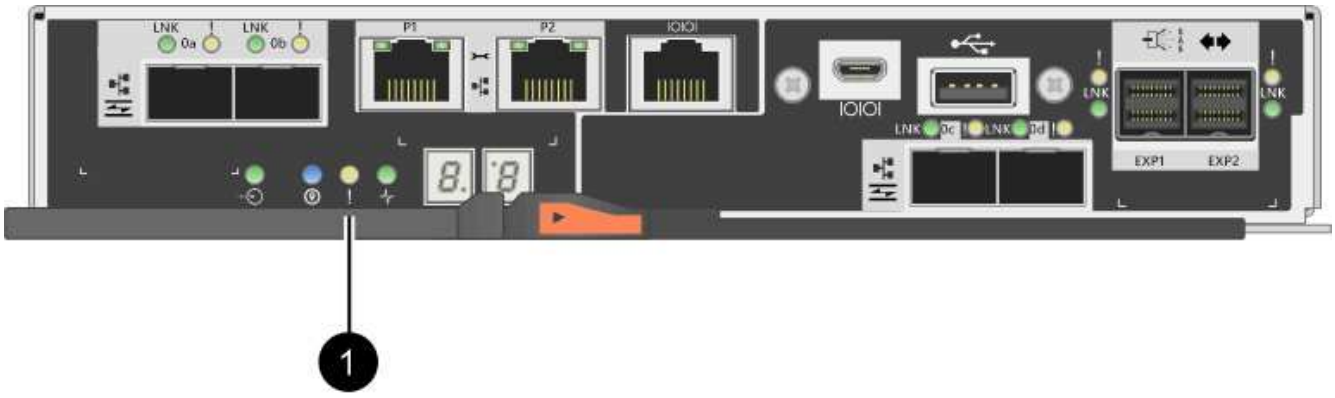
4. Se le porte HIC sul contenitore del controller utilizzano ricetrasmettitori SFP+, rimuovere gli SFP.

   Poiché è necessario rimuovere l'HIC dal contenitore del controller guasto, è necessario rimuovere eventuali SFP dalle porte HIC. Tuttavia, è possibile lasciare qualsiasi SFP installato nelle porte host della scheda base. Quando si è pronti a collegare il nuovo controller, è sufficiente spostare questi SFP nel nuovo contenitore del controller. Questo approccio è particolarmente utile se si dispone di più tipi di SFP.

5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

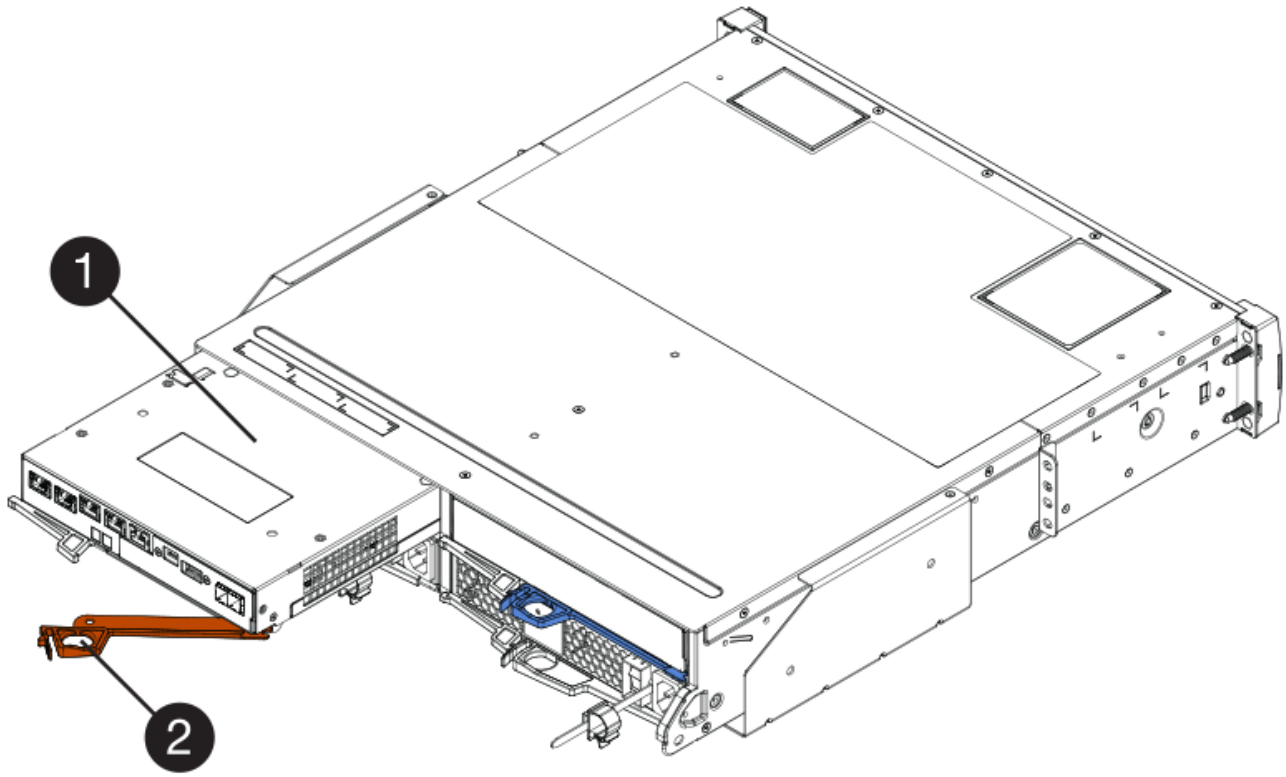
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.

   La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



(1) *LED cache attiva*

6. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dalla scheda intermedia.



(1) *contenitore controller*

(2) *maniglia della camma*

7. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Quando si rimuove il contenitore del controller, un'aletta oscilla in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

8. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
9. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 2b: Rimuovere la batteria (simplex)

Dopo aver rimosso il contenitore del controller dallo shelf del controller, rimuovere la batteria.

Fasi

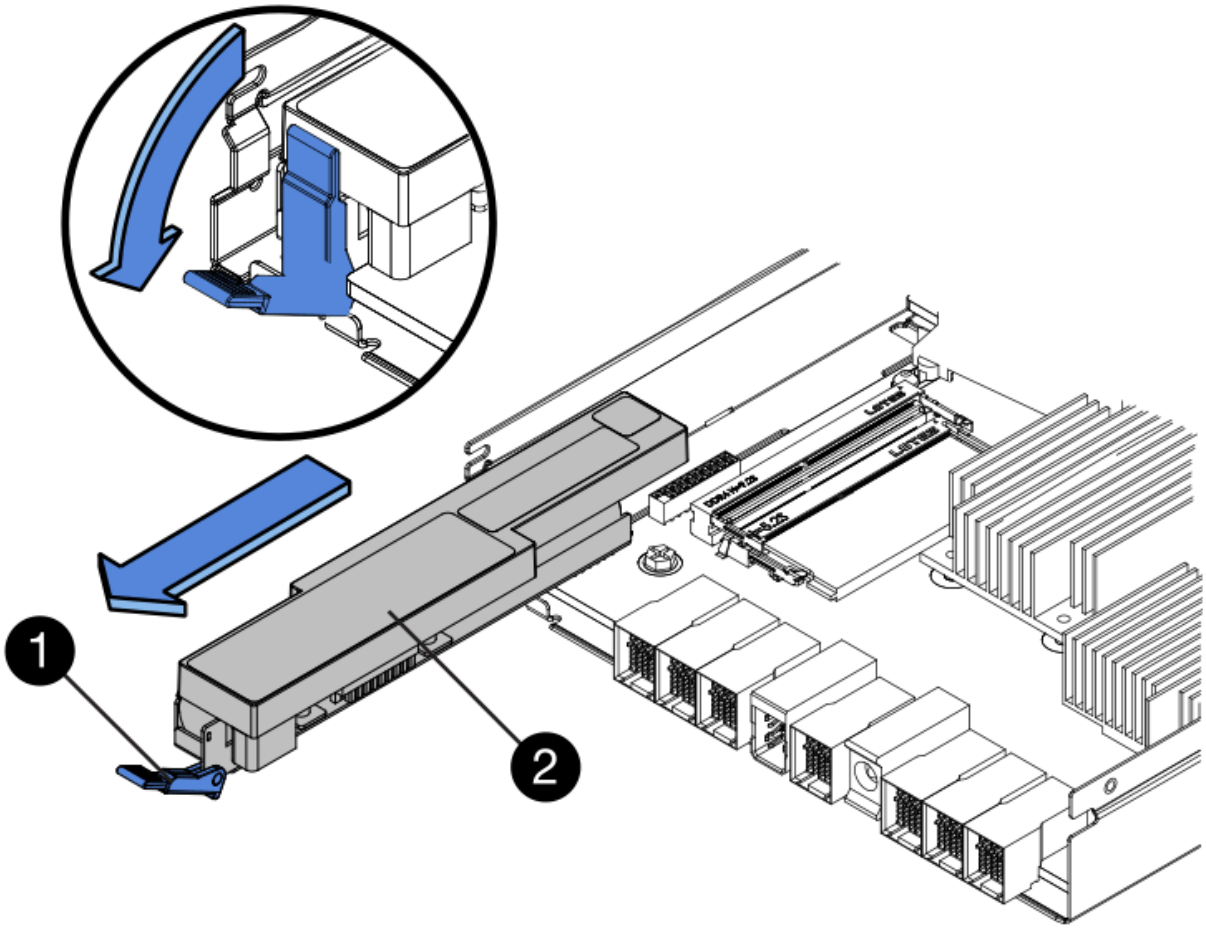
1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *cache interna attiva*

(2) *batteria*

3. Individuare il dispositivo di chiusura blu della batteria.
4. Sbloccare la batteria spingendo il dispositivo di chiusura verso il basso e lontano dal contenitore del controller.



(1) *dispositivo di chiusura a scatto della batteria*

(2) *batteria*

5. Sollevare la batteria ed estrarla dal contenitore del controller.

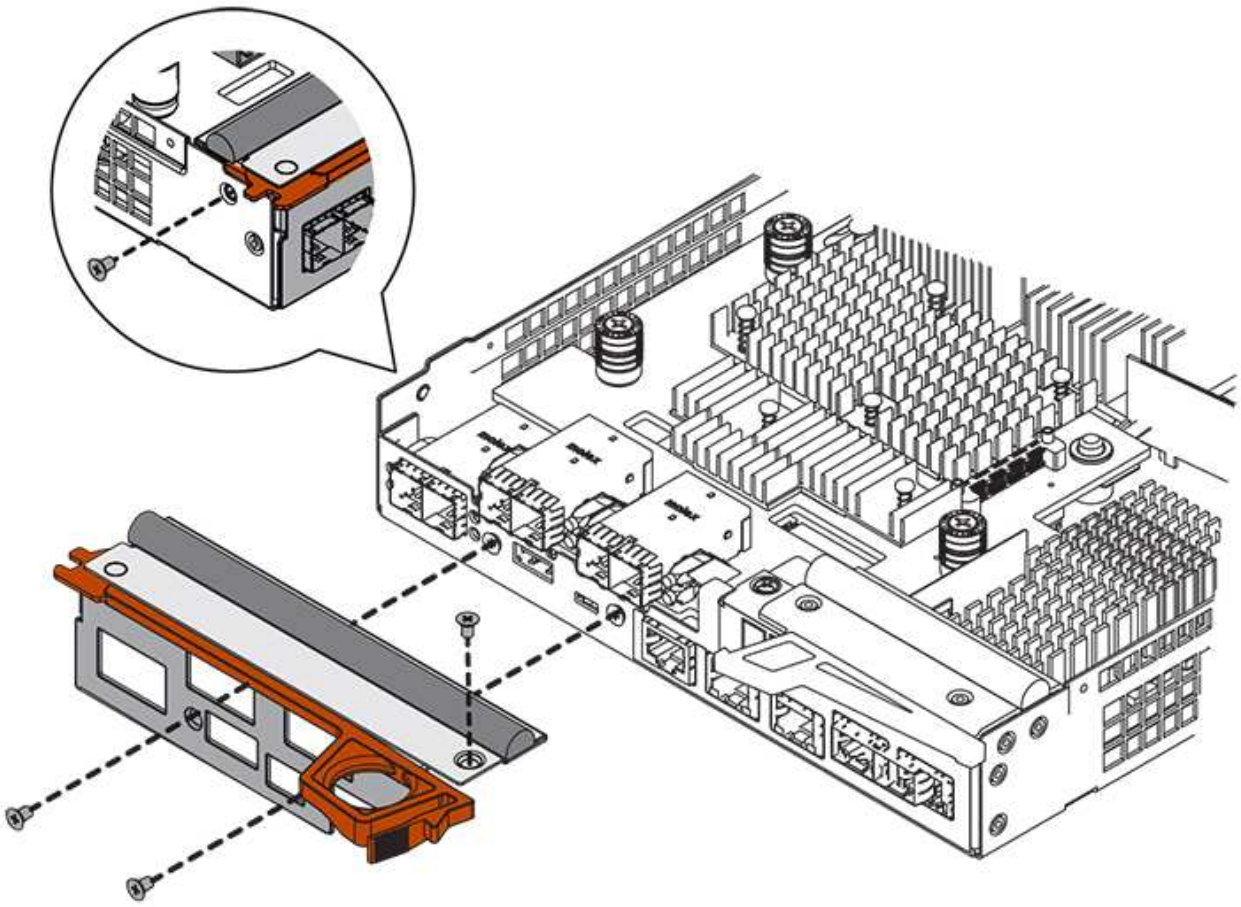
Fase 2c: Rimozione della scheda di interfaccia host (simplex)

Se il contenitore del controller include una scheda di interfaccia host (HIC), rimuovere l'HIC dal contenitore del controller originale in modo da poterlo riutilizzare nel nuovo contenitore del controller.

Fasi

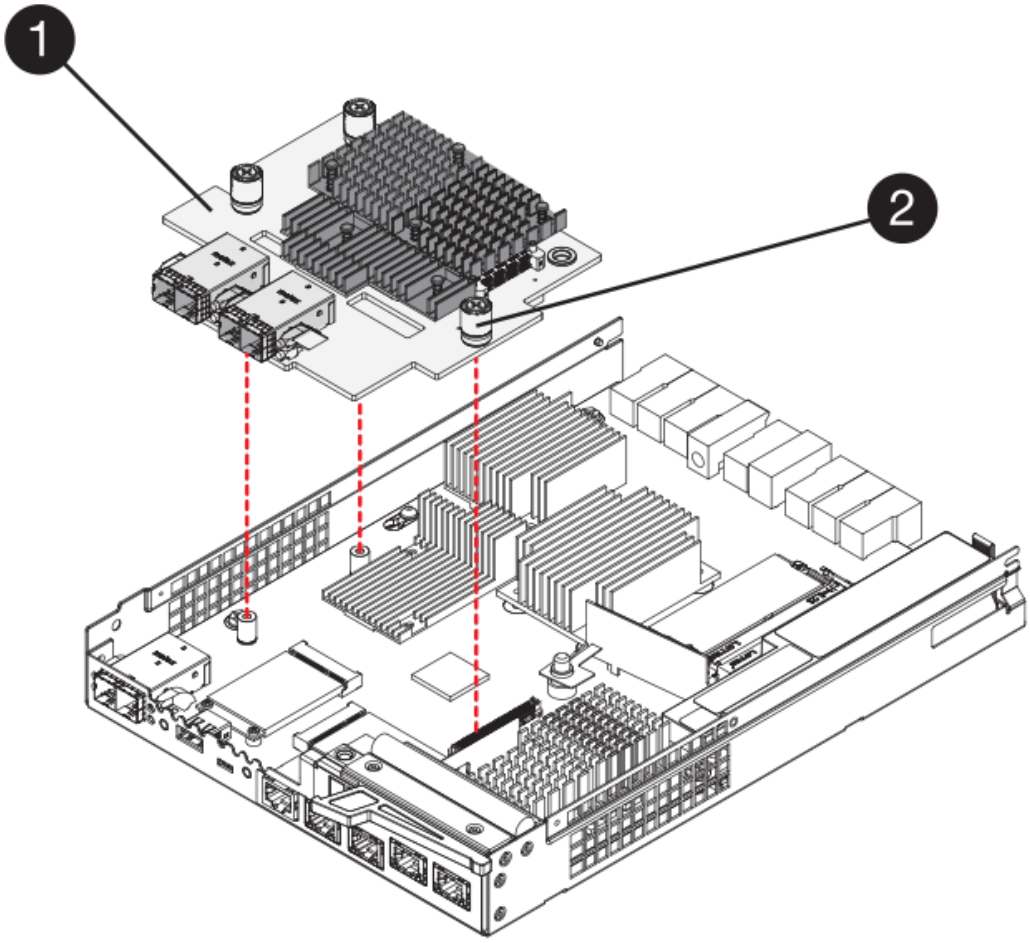
1. Utilizzando un cacciavite Phillips n. 1, rimuovere le viti che fissano la mascherina HIC al contenitore del controller.

   Sono presenti quattro viti: Una sulla parte superiore, una laterale e due sulla parte anteriore.



2. Rimuovere la piastra anteriore dell'HIC.
3. Utilizzando le dita o un cacciavite Phillips, allentare le tre viti a testa zigrinata che fissano l'HIC alla scheda del controller.
4. Scollegare con cautela l'HIC dalla scheda del controller sollevandola e facendola scorrere all'indietro.

> Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



(1) *scheda di interfaccia host*

(2) *viti a testa zigrinata*

5. Posizionare l'HIC su una superficie priva di elettricità statica.

Fase 3: Installazione di un nuovo controller (simplex)

Installare un nuovo elemento filtrante del controller per sostituire quello guasto.

Fase 3a: Installazione della batteria (simplex)

Installare la batteria nel contenitore del controller di ricambio. È possibile installare la batteria rimossa dal contenitore del controller originale o installare una nuova batteria ordinata.

Fasi

1. Disimballare il contenitore del controller di ricambio e riutilizzarlo su una superficie piana e priva di cariche elettrostatiche, in modo che il coperchio rimovibile sia rivolto verso l'alto.

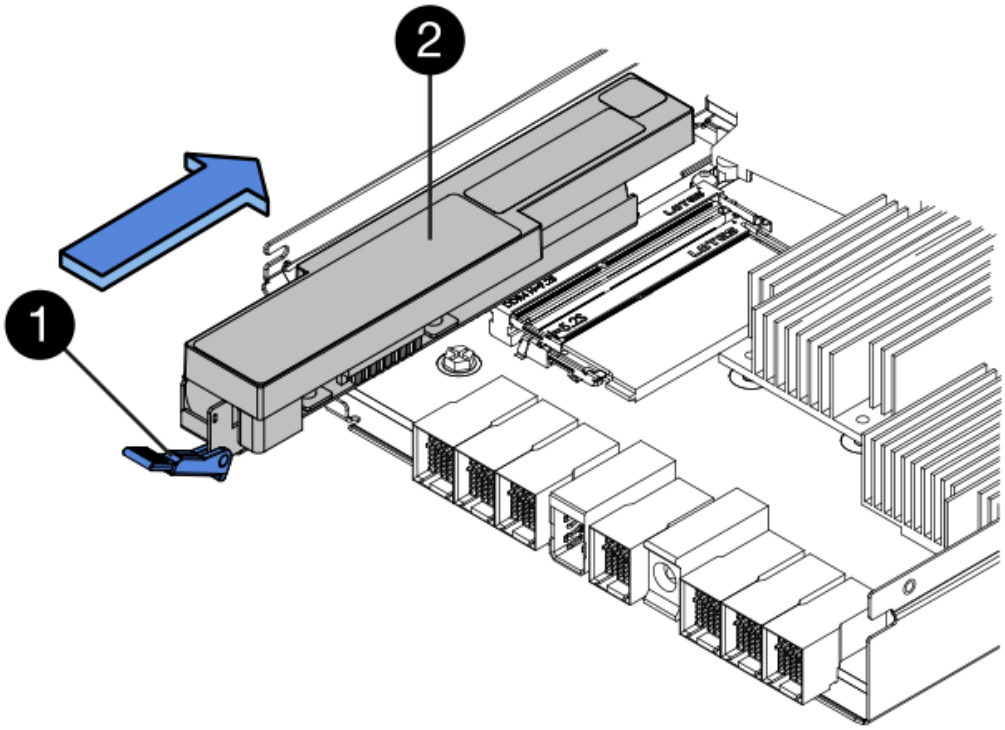
   Conservare il materiale di imballaggio da utilizzare per la spedizione del contenitore del controller guasto.

2. Premere il pulsante del coperchio verso il basso ed estrarre il coperchio.
3. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
4. Inserire la batteria nel contenitore del controller inclinandola leggermente verso il basso.

Inserire la flangia metallica nella parte anteriore della batteria nello slot sul fondo del contenitore del controller e far scorrere la parte superiore della batteria sotto il piccolo perno di allineamento sul lato sinistro del contenitore.

5. Spostare il dispositivo di chiusura della batteria verso l'alto per fissare la batteria.

   Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.



   (1) *dispositivo di chiusura a scatto della batteria*

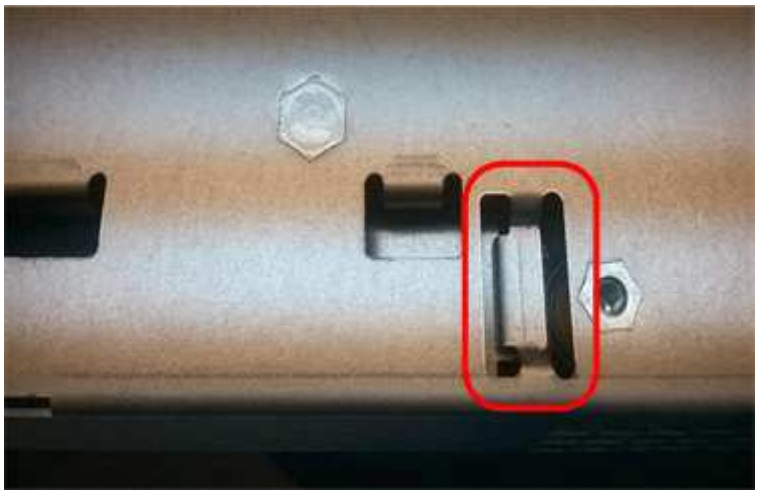
   (2) *batteria*

6. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

   > **Possibili danni all'hardware** — la flangia metallica sulla parte anteriore della batteria deve essere inserita completamente nello slot sul contenitore del controller (come mostrato nella prima figura). Se la batteria non è installata correttamente (come mostrato nella seconda figura), la flangia metallica potrebbe entrare in contatto con la scheda del controller, danneggiando il controller quando si applica l'alimentazione.

   - **Corretto** — la flangia metallica della batteria è completamente inserita nello slot del controller:

- **Errato** — la flangia metallica della batteria non è inserita nello slot del controller:



Fase 3b: Installazione della scheda di interfaccia host (simplex)

Se è stata rimossa una scheda di interfaccia host (HIC) dal contenitore del controller originale, installarla nel nuovo contenitore del controller.

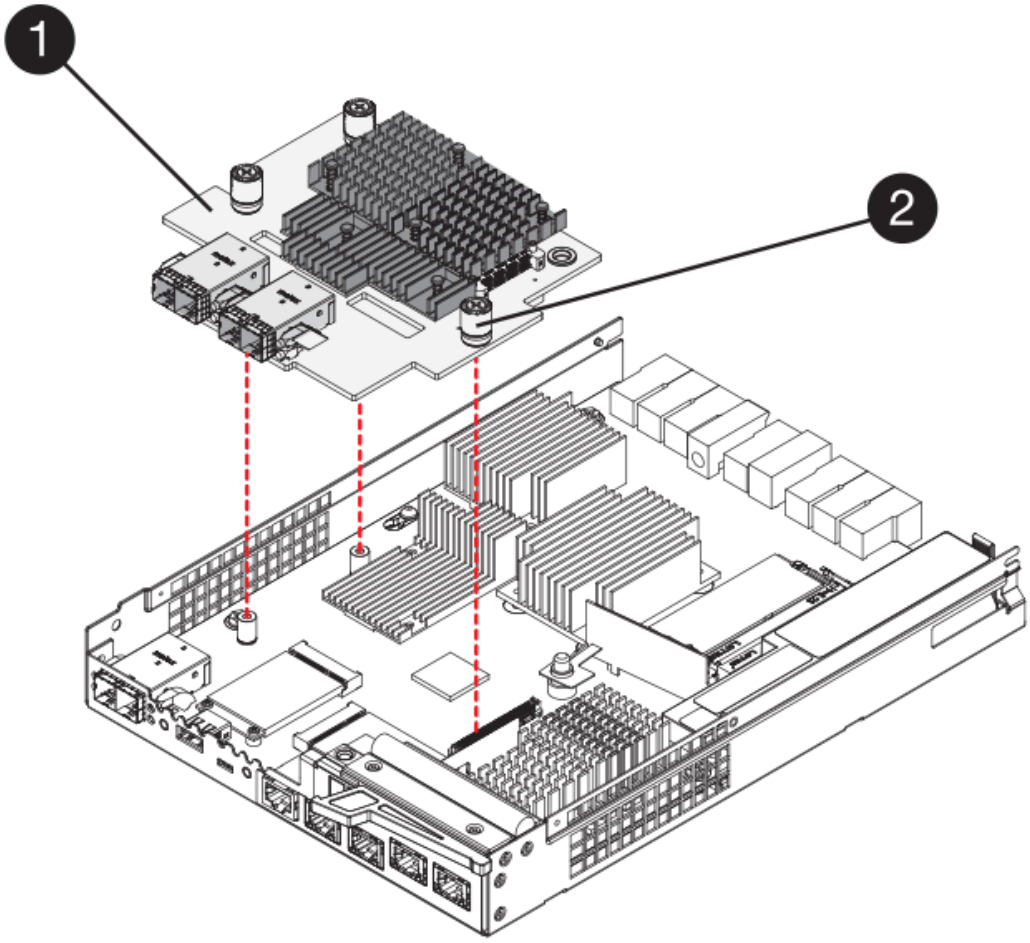
Fasi

1. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller sostitutivo, quindi rimuovere la piastra frontale.
2. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



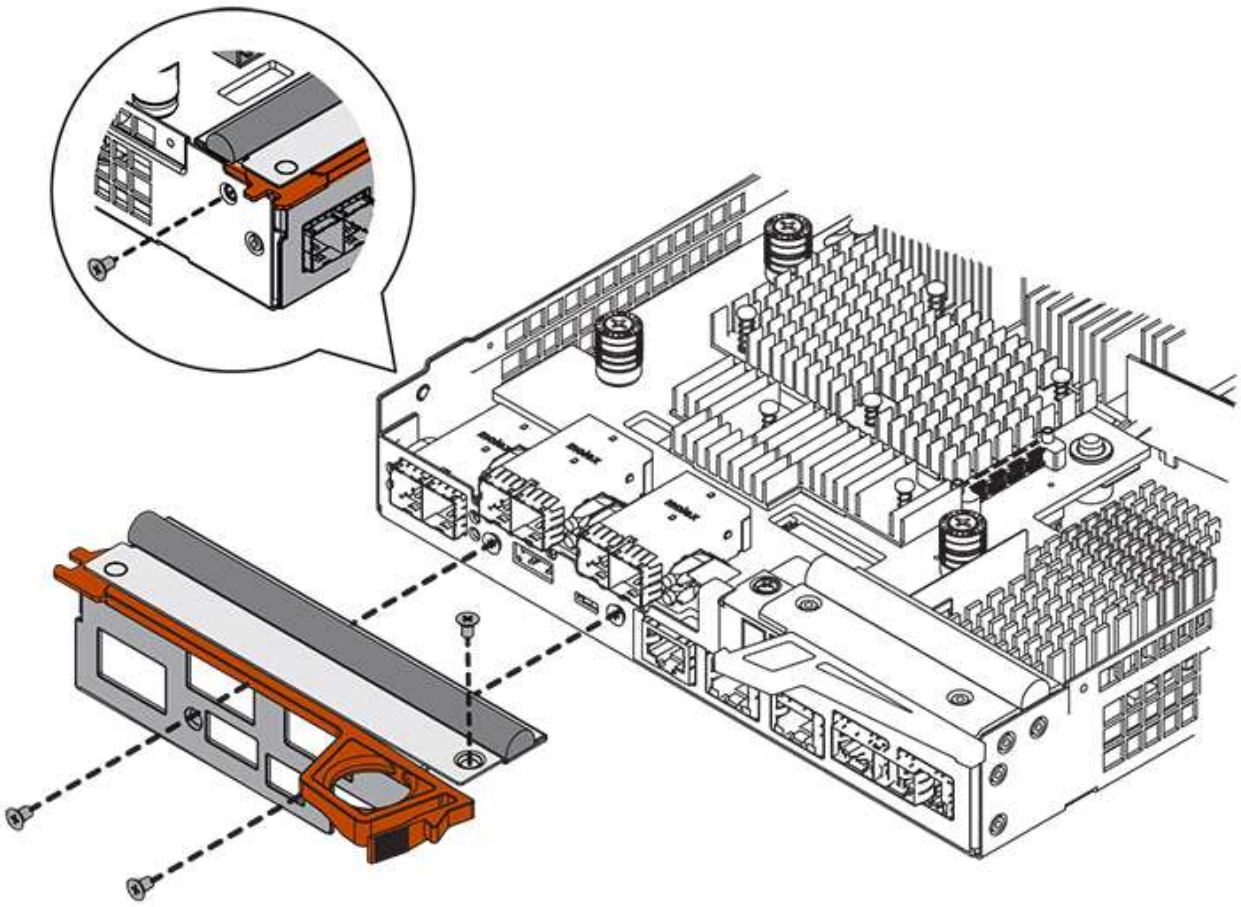
(1) *scheda di interfaccia host*

(2) *viti a testa zigrinata*

4. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dal contenitore del controller originale al nuovo contenitore del controller con quattro viti.

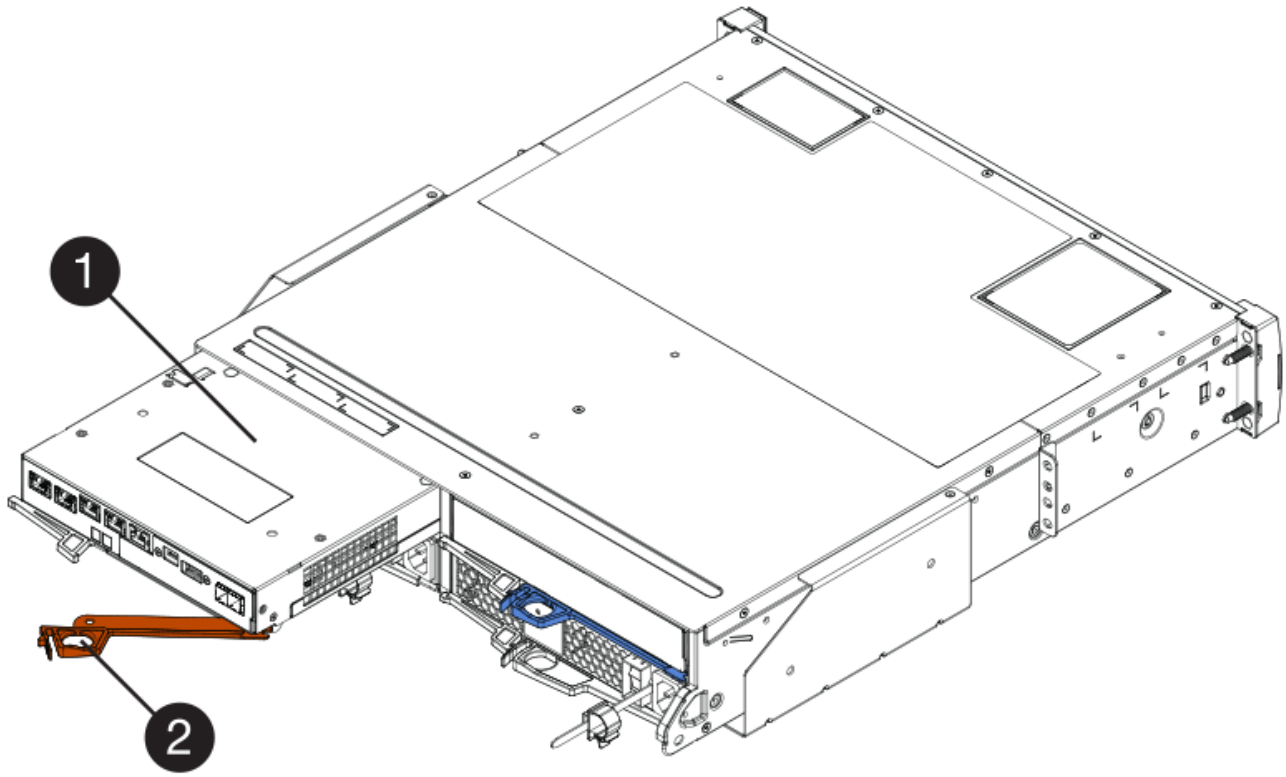


Fase 3c: Installare il nuovo contenitore del controller (simplex)

Dopo aver installato la batteria e l'HIC, se ne è stata inizialmente installata una, è possibile installare il nuovo contenitore del controller nello shelf del controller.

Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Installare gli SFP dal controller originale nelle porte host del nuovo controller e ricollegare tutti i cavi.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

6. Determinare come assegnare un indirizzo IP al controller sostitutivo, in base al fatto che la porta Ethernet 1 (indicata con P1) sia collegata a una rete con un server DHCP e che tutti i dischi siano protetti.

Utilizzo del server DHCP	Tutti i dischi sono protetti?	Fasi
Sì	No	Il nuovo controller ottiene l'indirizzo IP dal server DHCP. Questo valore potrebbe essere diverso dall'indirizzo IP del controller originale. Individuare l'indirizzo MAC sull'etichetta sul retro del controller sostitutivo e contattare l'amministratore di rete per ottenere l'indirizzo IP assegnato dal server DHCP.

Utilizzo del server DHCP	Tutti i dischi sono protetti?	Fasi
Sì	Sì	Il nuovo controller ottiene l'indirizzo IP dal server DHCP. Questo valore potrebbe essere diverso dall'indirizzo IP del controller originale. Individuare l'indirizzo MAC sull'etichetta sul retro del controller sostitutivo e contattare l'amministratore di rete per ottenere l'indirizzo IP assegnato dal server DHCP. È quindi possibile sbloccare i dischi utilizzando l'interfaccia della riga di comando.
No	No	Il nuovo controller adotta l'indirizzo IP del controller rimosso.
No	Sì	È necessario impostare manualmente l'indirizzo IP del nuovo controller. È possibile riutilizzare l'indirizzo IP del vecchio controller o utilizzare un nuovo indirizzo IP. Quando il controller dispone di un indirizzo IP, è possibile sbloccare i dischi utilizzando l'interfaccia della riga di comando. Una volta sbloccati i dischi, il nuovo controller riutilizza automaticamente l'indirizzo IP del controller originale.

Fase 4: Sostituzione completa del controller (simplex)

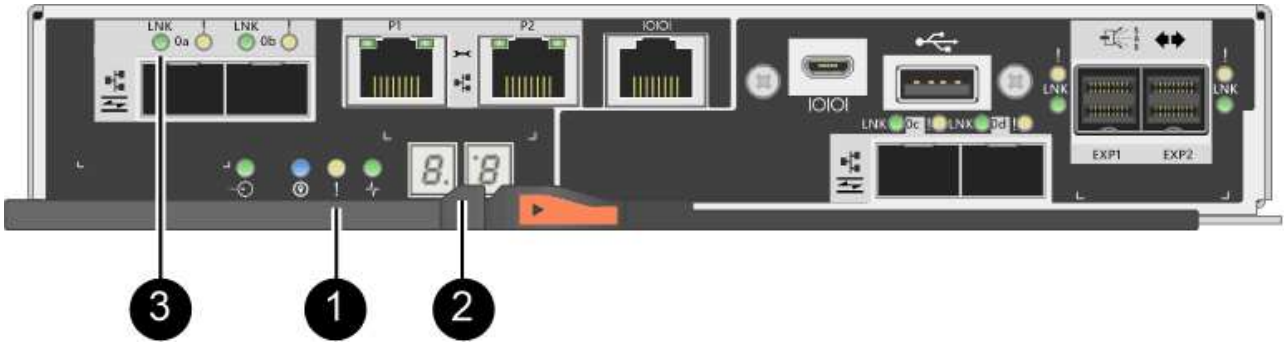
Accendere lo shelf del controller, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a sette segmenti dovrebbe visualizzare l'ID del vassoio.
   - Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.

- I LED verdi del collegamento host si accendono.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

3. Se uno dei LED attenzione dello shelf di controller rimane acceso, verificare che il contenitore del controller sia stato installato correttamente e che tutti i cavi siano inseriti correttamente. Reinstallare il contenitore del controller, se necessario.

> Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se lo storage array dispone di dischi sicuri, importare la chiave di sicurezza del disco; in caso contrario, passare alla fase successiva. Seguire la procedura appropriata riportata di seguito per un array di storage con tutti i dischi sicuri o una combinazione di dischi sicuri e non sicuri.

> *Dischi non sicuri* sono dischi non assegnati, dischi hot spare globali o dischi che fanno parte di un gruppo di volumi o di un pool non protetti dalla funzione Drive Security. *Dischi sicuri* sono dischi assegnati che fanno parte di un gruppo di volumi o di un pool di dischi protetti mediante Drive Security.

- **Solo dischi protetti (non dischi non sicuri)**:
  i. Accedere all'interfaccia a riga di comando (CLI) dello storage array.
  ii. Immettere il seguente comando per importare la chiave di sicurezza:

```
import storageArray securityKey file="C:/file.slk"
passPhrase="passPhrase";
```

dove:

- `C:/file.slk` rappresenta il percorso della directory e il nome della chiave di sicurezza del disco
- `passPhrase` È la password necessaria per sbloccare il file dopo l'importazione della chiave di sicurezza, il controller si riavvia e il nuovo controller adotta le impostazioni salvate per l'array di

storage.

iii. Passare alla fase successiva per verificare che il nuovo controller sia ottimale.

- **Combinazione di dischi sicuri e non sicuri**:
  i. Raccogliere il bundle di supporto e aprire il profilo dello storage array.
  ii. Individuare e registrare tutte le posizioni delle unità non sicure, che si trovano nel pacchetto di supporto.
  iii. Spegnere il sistema.
  iv. Rimuovere le unità non sicure.
  v. Sostituire il controller.
  vi. Accendere il sistema e attendere che il display a sette segmenti visualizzi il numero del vassoio.
  vii. Da Gestore di sistema di SANtricity, selezionare **Impostazioni › sistema**.
  viii. Nella sezione Security Key Management (Gestione chiave di sicurezza), selezionare **Create/Change Key** (Crea/Cambia chiave) per creare una nuova chiave di sicurezza.
  ix. Selezionare **Unlock Secure Drives** per importare la chiave di sicurezza salvata.
  x. Eseguire `set allDrives nativeState` Comando CLI.

     Il controller si riavvia automaticamente.

  xi. Attendere che il controller si avvii e che il display a sette segmenti visualizzi il numero del vassoio o un L5 lampeggiante.
  xii. Spegnere il sistema.
  xiii. Reinstallare le unità non sicure.
  xiv. Ripristinare il controller utilizzando Gestione di sistema di SANtricity.
  xv. Accendere il sistema e attendere che il display a sette segmenti visualizzi il numero del vassoio.
  xvi. Passare alla fase successiva per verificare che il nuovo controller sia ottimale.

5. Da Gestore di sistema di SANtricity, verificare che il nuovo controller sia ottimale.
   a. Selezionare **hardware**.
   b. Per lo shelf del controller, selezionare **Mostra retro dello shelf**.
   c. Selezionare il contenitore del controller sostituito.
   d. Selezionare **Visualizza impostazioni**.
   e. Verificare che lo stato * del controller sia ottimale.
   f. Se lo stato non è ottimale, evidenziare il controller e selezionare **posiziona online**.
6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › *Diagnostics**.
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione del controller è completata. È possibile riprendere le normali operazioni.

Canister

Requisiti per la sostituzione del filtro E2800

Prima di sostituire un contenitore in un array E2800, esaminare i tipi e i requisiti del contenitore.

I tipi di taniche includono alimentatori, taniche di alimentazione e taniche per ventole.

Alimentatore

> La procedura di sostituzione dell'alimentatore è applicabile per le sostituzioni IOM. Per sostituire il modulo IOM, eseguire la procedura di sostituzione dell'alimentatore.

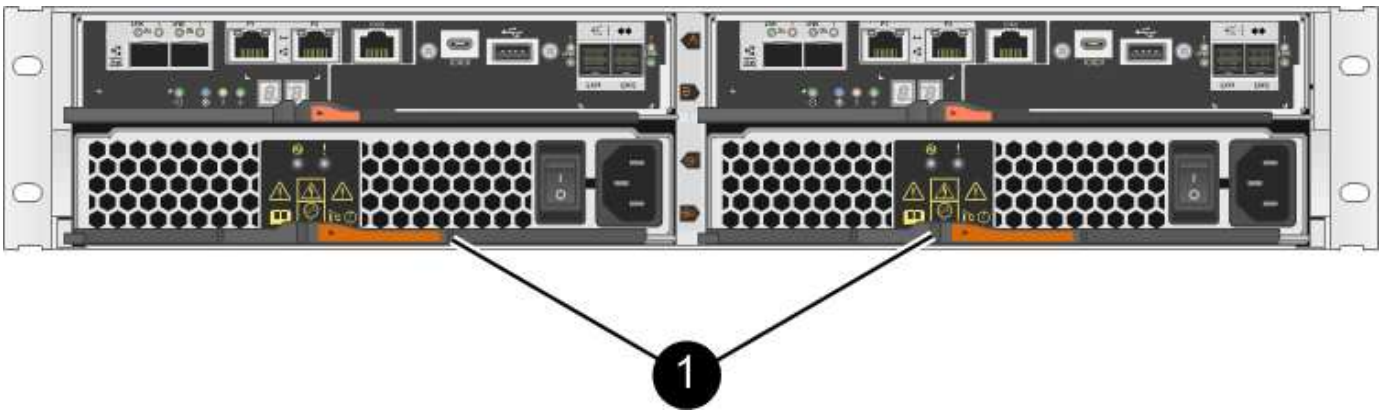
Ogni shelf o shelf di controller da 12 o 24 dischi include due alimentatori con ventole integrate. In Gestione sistema di SANtricity, questi sono denominati *canister per ventole di alimentazione*. In caso di guasto di un contenitore della ventola di alimentazione, è necessario sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante e di un raffreddamento adeguato.

Tipi di shelf per un alimentatore

È possibile sostituire un alimentatore nei seguenti shelf:

- Shelf di controller E2812
- Shelf di controller E2824
- Flash array EF280
- Shelf di dischi DE212C
- Shelf di dischi DE224C

La figura seguente mostra un esempio di shelf di controller E2812, shelf di controller E2824 e flash array EF280 con due alimentatori (contenitori per ventole di alimentazione). Gli shelf di dischi DE212C e DE224C sono identici, ma includono i moduli i/o (IOM) invece dei controller canister.



(1) *Shelf del controller con due alimentatori (contenitori per ventole di alimentazione) sotto i contenitori del controller*

La procedura per la sostituzione di un alimentatore non descrive come sostituire un contenitore della ventola di alimentazione guasto in un vassoio dell'unità DE1600 o DE5600, che potrebbe essere collegato agli shelf dei controller E5700 o E2800. Per istruzioni su questi modelli di tray di dischi, fare riferimento a. "Ricollocamento

di un contenitore della ventola di alimentazione nel vassoio dell'unità DE1600 o nel vassoio dell'unità DE5600".

Requisiti per la sostituzione di un alimentatore

Se si prevede di sostituire un alimentatore, tenere presenti i seguenti requisiti.

- È necessario disporre di un alimentatore sostitutivo (contenitore della ventola di alimentazione) supportato per il modello di shelf di controller o di unità.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- È possibile sostituire un alimentatore (contenitore della ventola di alimentazione) mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:
  - Il secondo alimentatore (contenitore della ventola di alimentazione) nello shelf ha uno stato ottimale.
  - Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

> Se il secondo alimentatore (contenitore della ventola di alimentazione) nello shelf non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore della ventola di alimentazione, contattare il supporto tecnico.

Filtro a carboni attivi

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori di alimentazione per la ridondanza dell'alimentazione.

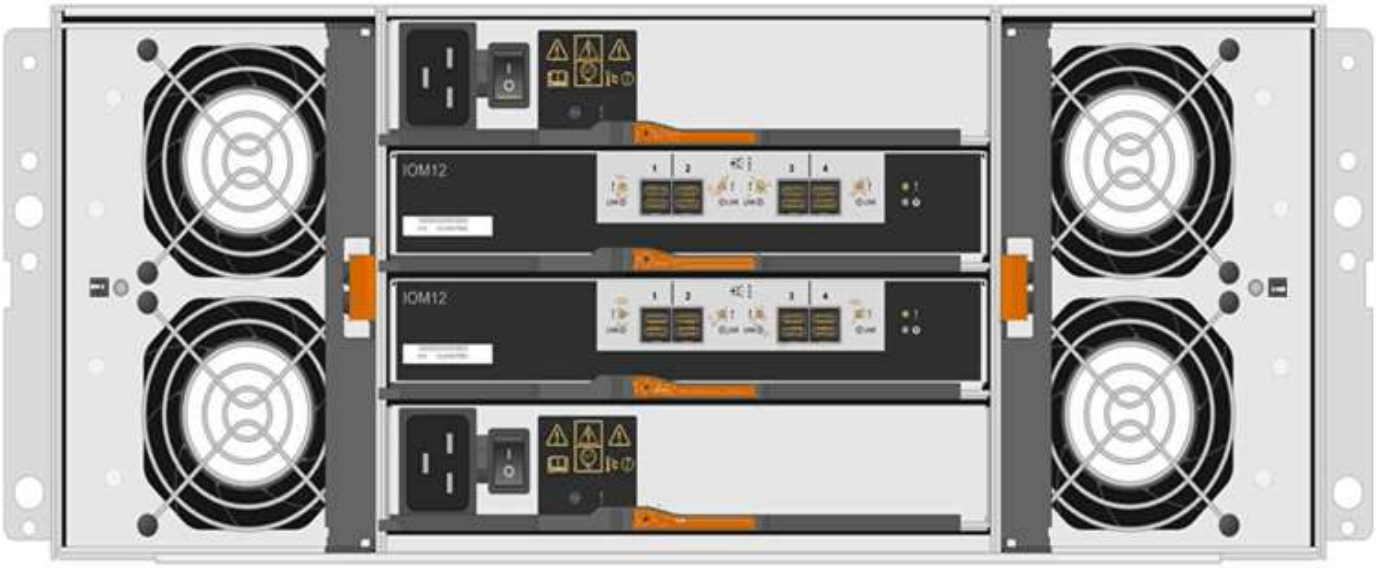
Tipi di shelf per un contenitore di alimentazione

È possibile sostituire un contenitore di alimentazione nei seguenti shelf:

- Shelf di controller E2860
- Shelf di dischi DE460C

La procedura per la sostituzione di un contenitore di alimentazione non descrive come sostituire un contenitore di alimentazione guasto in un vassoio del disco DE6600, che potrebbe essere collegato allo shelf del controller.

La figura seguente mostra il retro di uno shelf di dischi DE460C con i due contenitori di alimentazione:



La figura seguente mostra un contenitore di alimentazione:

Requisiti per la sostituzione di un contenitore di alimentazione

Se si prevede di sostituire un contenitore di alimentazione, tenere presenti i seguenti requisiti.

- Si dispone di un contenitore di alimentazione sostitutivo supportato per il modello di shelf di controller o di unità.
- Si dispone di un contenitore di alimentazione installato e funzionante.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- È possibile sostituire un contenitore di alimentazione mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:
  - L'altro contenitore di alimentazione nello shelf ha uno stato ottimale.

    Durante l'esecuzione della procedura, l'altro contenitore di alimentazione alimenta entrambe le ventole per garantire che l'apparecchiatura non si surriscaldi.

  - Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

    Se il secondo contenitore di alimentazione nel ripiano non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore di alimentazione, contattare il supporto tecnico.

Filtro della ventola

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori per ventole.

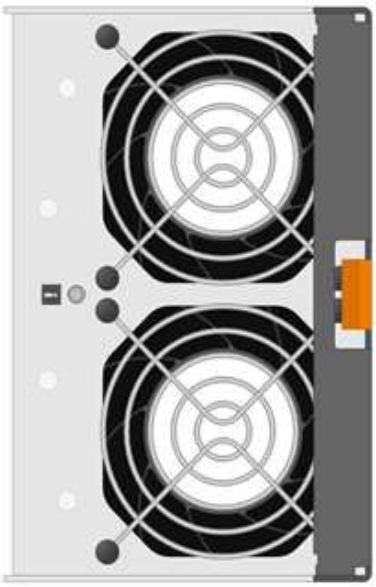
Tipi di shelf per un contenitore di ventole

È possibile sostituire un contenitore della ventola nei seguenti ripiani:

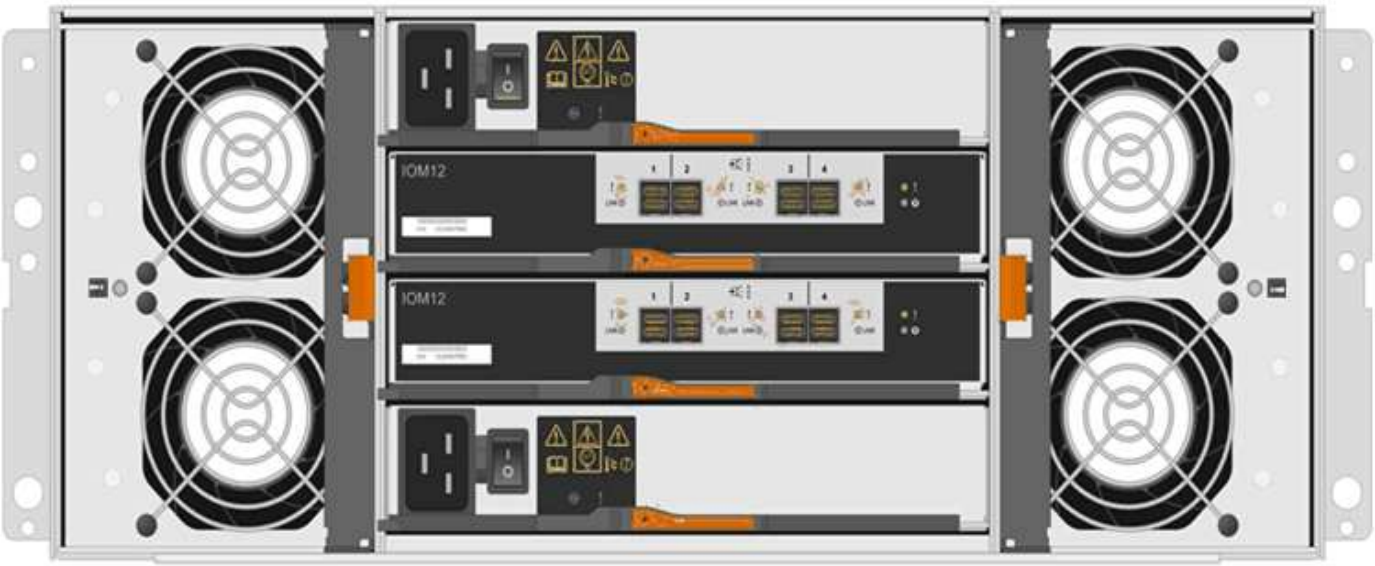
- Shelf di controller E2860
- Shelf di dischi DE460C

La procedura per la sostituzione di un contenitore della ventola non descrive come sostituire un contenitore della ventola guasto in un vassoio del disco DE6600, che potrebbe essere collegato allo shelf del controller.

La figura seguente mostra un filtro a carboni attivi della ventola:



La figura seguente mostra il retro di uno shelf DE460C con due contenitori per ventole:



Possibili danni all'apparecchiatura — se si sostituisce un contenitore della ventola con l'alimentazione accesa, è necessario completare la procedura di sostituzione entro 30 minuti per evitare il rischio di surriscaldamento dell'apparecchiatura.

Requisiti per la sostituzione di un filtro a carboni attivi della ventola

Se si prevede di sostituire un filtro a carboni attivi della ventola, tenere presenti i seguenti requisiti.

- Si dispone di una ventola sostitutiva (ventola) supportata per il proprio modello di shelf di controller o di unità.
- È presente un contenitore della ventola installato e in funzione.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Se si esegue questa procedura con l'alimentazione accesa, è necessario completarla entro 30 minuti per evitare il surriscaldamento dell'apparecchiatura.
- È possibile sostituire un contenitore di ventole mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:
  - Il secondo contenitore della ventola nello shelf ha uno stato ottimale.
  - Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Se il secondo contenitore della ventola nello shelf non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore della ventola, contattare il supporto tecnico.

Sostituire l'alimentatore E2800 (12 o 24 dischi)

È possibile sostituire un alimentatore in un array E2800 con uno shelf da 12 o 24 dischi, inclusi i seguenti tipi di shelf:

- Shelf di controller E2812
- Shelf di controller E2824
- Flash array EF280
- Shelf di dischi DE212C
- Shelf di dischi DE224C

A proposito di questa attività

Ogni shelf o shelf di controller da 12 o 24 dischi include due alimentatori con ventole integrate. In Gestione sistema di SANtricity, questi sono denominati *canister per ventole di alimentazione*. In caso di guasto di un contenitore della ventola di alimentazione, è necessario sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante e di un raffreddamento adeguato.

È possibile sostituire un alimentatore mentre lo storage array è acceso ed esegue operazioni di i/o host, Se il secondo alimentatore dello shelf ha uno stato ottimale e il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione di sistema di SANtricity visualizza **Sì**.

Prima di iniziare

- Esaminare i requisiti di alimentazione in "Requisiti per la sostituzione del contenitore".

- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con l'alimentatore. Selezionare **ricontrollare** dal Recovery Guru per assicurarsi che nessun altro elemento debba essere affrontato per primo.
- Verificare che il LED di attenzione ambra sull'alimentatore sia acceso, a indicare che l'alimentatore o la ventola integrata sono guasti. Contattare il supporto tecnico per assistenza se entrambi gli alimentatori dello shelf hanno i LED di attenzione ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un alimentatore sostitutivo supportato per il modello di shelf di controller o di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.

Fase 1: Preparazione alla sostituzione dell'alimentatore

Preparare la sostituzione di un alimentatore in uno shelf o uno shelf di controller da 12 o 24 dischi.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale alimentatore si è guastato.

   Queste informazioni sono disponibili nell'area Details (Dettagli) del Recovery Guru o nelle informazioni visualizzate per lo shelf.

   a. Selezionare **hardware**.
   b. Guarda la potenza e la ventola Icone a destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta l'alimentatore guasto.

      In caso di guasto di un componente, una o entrambe queste icone sono rosse.

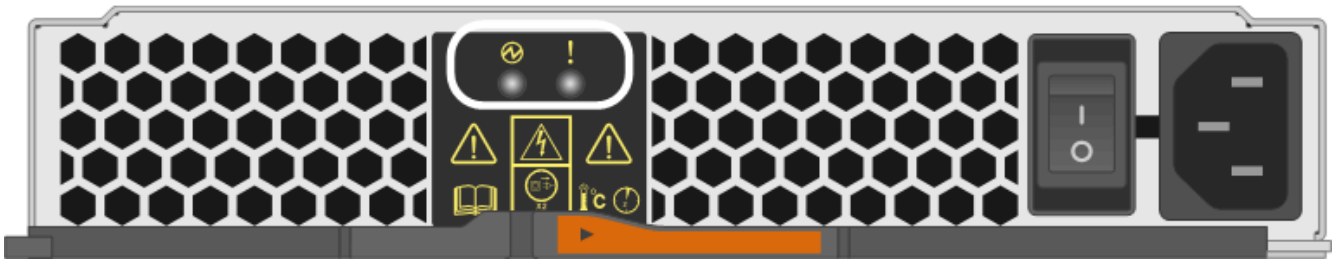
   c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.
   d. Selezionare uno degli alimentatori.
   e. Nelle schede **alimentatori** e **ventole**, controllare gli stati dei contenitori delle ventole di alimentazione, degli alimentatori e delle ventole per determinare quale alimentatore deve essere sostituito.

      Un componente con stato **Failed** deve essere sostituito.

      > Se il secondo contenitore dell'alimentatore nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo l'alimentatore guasto. Contattare invece il supporto tecnico per assistenza.

3. Dal retro dello storage array, osservare i LED di attenzione per individuare l'alimentatore da rimuovere.

   È necessario sostituire l'alimentatore con il LED attenzione acceso.



- LED di alimentazione: Se è **verde fisso**, l'alimentatore funziona correttamente. Se è **spento**, l'alimentatore è guasto, l'interruttore CA è spento, il cavo di alimentazione CA non è installato correttamente o la tensione di ingresso del cavo di alimentazione CA non rientra nei margini (si è verificato un problema all'estremità della fonte del cavo di alimentazione CA).
- LED attenzione: Se è **ambra fisso**, si è verificato un guasto nell'alimentatore o nella ventola integrata.

Fase 2: Rimuovere l'alimentatore guasto

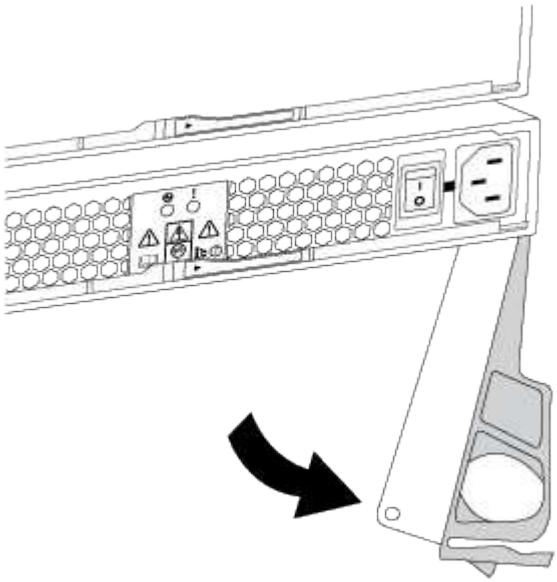
Rimuovere un alimentatore guasto per poterlo sostituire con uno nuovo.

Fasi

1. Disimballare il nuovo alimentatore e posizionare il nuovo alimentatore su una superficie piana vicino allo shelf del disco.

   Conservare tutti i materiali di imballaggio per l'utilizzo quando si restituisce l'alimentatore guasto.

2. Spegnere l'alimentatore e scollegare i cavi di alimentazione:
   a. Spegnere l'interruttore di alimentazione dell'alimentatore.
   b. Aprire il fermo del cavo di alimentazione, quindi scollegare il cavo di alimentazione dall'alimentatore.
   c. Scollegare il cavo di alimentazione dalla presa di corrente.
3. Premere il fermo sulla maniglia della camma dell'alimentatore, quindi aprire la maniglia della camma per rilasciare completamente l'alimentatore dal piano intermedio.



4. Utilizzare la maniglia della camma per estrarre l'alimentatore dal sistema.

> Quando si rimuove un alimentatore, utilizzare sempre due mani per sostenerne il peso.

Quando si rimuove l'alimentatore, un'aletta oscilla in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

Fase 3: Installare un nuovo alimentatore

Installare un nuovo alimentatore per sostituire quello guasto.

Fasi

1. Assicurarsi che l'interruttore di accensione/spegnimento del nuovo alimentatore sia in posizione **Off**.
2. Con entrambe le mani, sostenere e allineare i bordi dell'alimentatore con l'apertura nello chassis del sistema, quindi spingere delicatamente l'alimentatore nello chassis utilizzando la maniglia della camma.

   Gli alimentatori sono dotati di chiavi e possono essere installati in un solo modo.

   > Non esercitare una forza eccessiva quando si inserisce l'alimentatore nel sistema, poiché si potrebbe danneggiare il connettore.

3. Chiudere la maniglia della camma in modo che il fermo scatti in posizione di blocco e l'alimentatore sia inserito completamente.
4. Ricollegare il cablaggio dell'alimentatore:
   a. Ricollegare il cavo di alimentazione all'alimentatore e alla fonte di alimentazione.
   b. Fissare il cavo di alimentazione all'alimentatore utilizzando il relativo fermo.
5. Accendere il nuovo contenitore dell'alimentatore.

Fase 4: Sostituzione completa dell'alimentatore

Verificare che il nuovo alimentatore funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Sul nuovo alimentatore, verificare che il LED di alimentazione verde sia acceso e che il LED di attenzione ambra sia spento.
2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il problema persiste, ripetere la procedura descritta in Fase 2: Rimuovere l'alimentatore guastoe in Fase 3: Installare un nuovo alimentatore. Se il problema persiste, contattare il supporto tecnico.
4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione dell'alimentatore è completata. È possibile riprendere le normali operazioni.

Sostituire il contenitore di alimentazione E2800 (60 dischi)

È possibile sostituire un contenitore di alimentazione in un array E2800 con uno shelf da 60 dischi, che include i seguenti tipi di shelf:

- Shelf di controller E2860
- Shelf di dischi DE460C

A proposito di questa attività

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori di alimentazione per la ridondanza dell'alimentazione. In caso di guasto di un contenitore di alimentazione, sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante.

È possibile sostituire un contenitore di alimentazione mentre lo storage array è acceso ed esegue operazioni di i/o host, Finché il secondo contenitore di alimentazione nello shelf ha uno stato ottimale e il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione di sistema di SANtricity visualizza **Sì**.

Durante l'esecuzione di questa attività, l'altro contenitore di alimentazione alimenta entrambe le ventole per garantire che l'apparecchiatura non si surriscaldi.

Prima di iniziare

- Esaminare i requisiti del filtro a carboni attivi in "Requisiti per la sostituzione del contenitore".
- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con il contenitore di alimentazione e selezionare **ricontrollare** dal Recovery Guru per assicurarsi che non siano prima necessari altri elementi.
- Controllare che il LED di attenzione ambra sul filtro a carboni attivi sia acceso, a indicare che il filtro a carboni attivi è guasto. Contattare il supporto tecnico per assistenza se entrambi i contenitori di alimentazione presenti nello shelf hanno i LED di attenzione color ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un contenitore di alimentazione sostitutivo supportato per il modello di shelf di controller o di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.

Fase 1: Preparazione alla sostituzione del contenitore di alimentazione

Preparare la sostituzione di un contenitore di alimentazione in uno shelf di controller da 60 dischi o in uno shelf di dischi.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale contenitore di alimentazione si è guastato.

   a. Selezionare **hardware**.

   b. Guarda la potenza A destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta il contenitore di alimentazione guasto.

      In caso di guasto di un componente, questa icona è rossa.

   c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.

   d. Selezionare il filtro a carboni attivi o l'icona di alimentazione rossa.

   e. Nella scheda **alimentatori**, controllare gli stati dei contenitori di alimentazione per determinare quale contenitore di alimentazione deve essere sostituito.

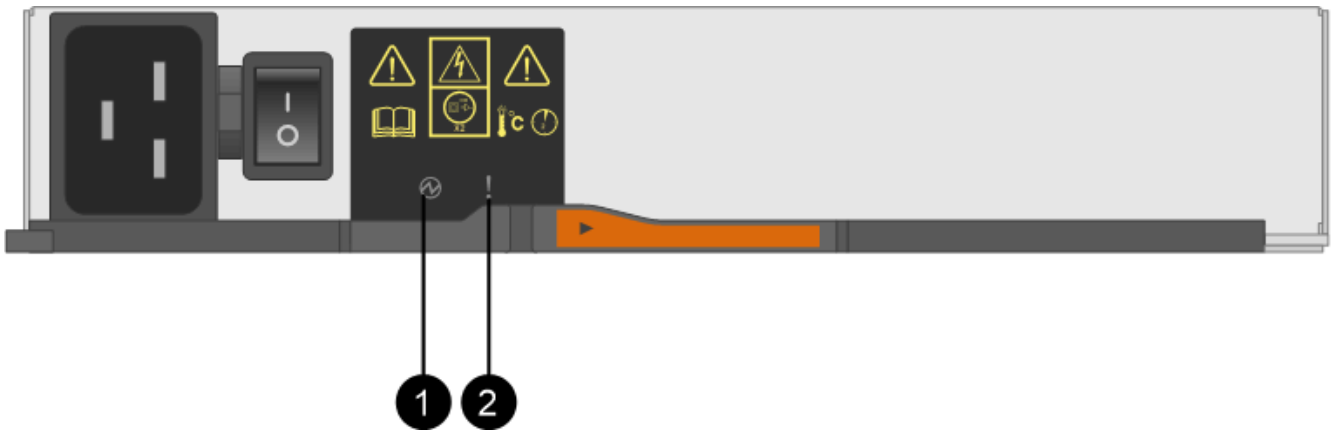
      Un componente con stato **Failed** deve essere sostituito.

> Se il secondo contenitore di alimentazione nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo il contenitore di alimentazione guasto. Contattare invece il supporto tecnico per assistenza.

> È inoltre possibile trovare informazioni sul contenitore di alimentazione guasto nell'area Details (Dettagli) del Recovery Guru, rivedere le informazioni visualizzate per lo shelf o consultare il registro eventi in Support (supporto) e Filter by Component Type (filtro per tipo di componente).

3. Dal retro dello storage array, osservare i LED di attenzione per individuare il contenitore di alimentazione da rimuovere.

   È necessario sostituire il filtro a carboni attivi con il LED attenzione acceso.



(1) *LED di alimentazione*. Se è **verde fisso**, il filtro a carboni attivi funziona correttamente. Se è **spento**, il contenitore di alimentazione è guasto, l'interruttore CA è spento, il cavo di alimentazione CA non è installato correttamente o la tensione di ingresso del cavo di alimentazione CA non rientra nei margini (si è verificato un problema all'estremità della fonte del cavo di alimentazione CA).

(2) *LED attenzione*. Se è di colore **ambra fisso**, il filtro a carboni attivi è guasto oppure non è presente alimentazione in ingresso al filtro a carboni attivi, ma l'altro è in funzione.

Fase 2: Rimuovere il contenitore di alimentazione guasto

Rimuovere un contenitore di alimentazione guasto in modo da poterlo sostituire con uno nuovo.

Fasi

1. Protezione antistatica.
2. Disimballare il nuovo contenitore di alimentazione e riutilizzarlo su una superficie piana vicino allo scaffale.

   Conservare tutti i materiali di imballaggio per l'utilizzo quando si restituisce il contenitore di alimentazione guasto.

3. Spegnere l'interruttore di alimentazione del contenitore di alimentazione da rimuovere.
4. Aprire il fermo del cavo di alimentazione del contenitore che si desidera rimuovere, quindi scollegare il cavo di alimentazione dal contenitore.
5. Premere il dispositivo di chiusura arancione sulla maniglia della camma del filtro a carboni attivi, quindi aprire la maniglia della camma per rilasciare completamente il filtro a carboni attivi dal piano intermedio.
6. Utilizzare la maniglia della camma per far scorrere il contenitore di alimentazione fuori dallo scaffale.

   Quando si rimuove un filtro a carboni attivi, utilizzare sempre due mani per sostenerne il peso.

Fase 3: Installare un nuovo filtro a carboni attivi

Installare un nuovo filtro a carboni attivi per sostituire quello guasto.

Fasi

1. Assicurarsi che l'interruttore on/off del nuovo contenitore di alimentazione sia in posizione off.
2. Con entrambe le mani, sostenere e allineare i bordi del contenitore di alimentazione con l'apertura nel telaio del sistema, quindi spingere delicatamente il contenitore di alimentazione nel telaio utilizzando la maniglia della camma fino a bloccarlo in posizione.

   Non esercitare una forza eccessiva quando si fa scorrere il contenitore di alimentazione nel sistema per evitare di danneggiare il connettore.

3. Chiudere la maniglia della camma in modo che il dispositivo di chiusura scatti nella posizione di blocco e che il contenitore dell'alimentazione sia completamente inserito.
4. Ricollegare il cavo di alimentazione al contenitore di alimentazione e fissarlo al contenitore utilizzando il fermo del cavo di alimentazione.
5. Accendere il nuovo contenitore di alimentazione.

Fase 4: Sostituzione completa del filtro a carboni attivi

Verificare che il nuovo power taniche funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Sul nuovo contenitore di alimentazione, verificare che il LED di alimentazione verde sia acceso e che il LED di attenzione ambra sia spento.
2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il

problema sia stato risolto.

3. Se viene ancora segnalato un guasto al contenitore di alimentazione, ripetere i passi descritti in Fase 2: Rimuovere il contenitore di alimentazione guasto e in Fase 3: Installare un nuovo filtro a carboni attivi. Se il problema persiste, contattare il supporto tecnico.
4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.
6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del filtro a carboni attivi è stata completata. È possibile riprendere le normali operazioni.

Sostituire il filtro della ventola E2800 (60 dischi)

È possibile sostituire un contenitore di ventole in un array E2800 con uno shelf da 60 dischi, che include i seguenti tipi di shelf:

- Shelf di controller E2860
- Shelf di dischi DE460C

A proposito di questa attività

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori per ventole. In caso di guasto di un contenitore della ventola, sostituirlo il prima possibile per garantire che il ripiano sia adeguatamente raffreddato.

> **Possibili danni all'apparecchiatura** — se si esegue questa procedura con l'alimentazione accesa, è necessario completarla entro 30 minuti per evitare il rischio di surriscaldamento dell'apparecchiatura.

Prima di iniziare

- Esaminare i requisiti del filtro a carboni attivi della ventola in "Requisiti per la sostituzione del contenitore".
- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con il filtro a carboni attivi della ventola e selezionare **ricontrollare** dal Recovery Guru per assicurarsi che non sia necessario risolvere prima altri elementi.
- Controllare che il LED di attenzione ambra sul filtro della ventola sia acceso, a indicare che la ventola è guasta. Contattare il supporto tecnico per assistenza se entrambi i contenitori delle ventole nello shelf hanno i LED di attenzione color ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un filtro della ventola di ricambio (ventola) supportato per il modello di shelf del controller o del disco.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.

Fase 1: Preparazione alla sostituzione del filtro a carboni attivi della ventola

Preparare la sostituzione di un contenitore di ventole in uno shelf di controller da 60 dischi o in uno shelf di dischi raccogliendo i dati di supporto relativi allo storage array e individuando il componente guasto.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale filtro a carboni attivi della ventola si è guastato.
   a. Selezionare **hardware**.
   b. Guardare la ventola A destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta il contenitore della ventola guasto.

      In caso di guasto di un componente, questa icona è rossa.

   c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.
   d. Selezionare il filtro a carboni attivi della ventola o l'icona rossa della ventola.
   e. Nella scheda **ventole**, controllare gli stati dei contenitori delle ventole per determinare quale filtro a carboni attivi deve essere sostituito.

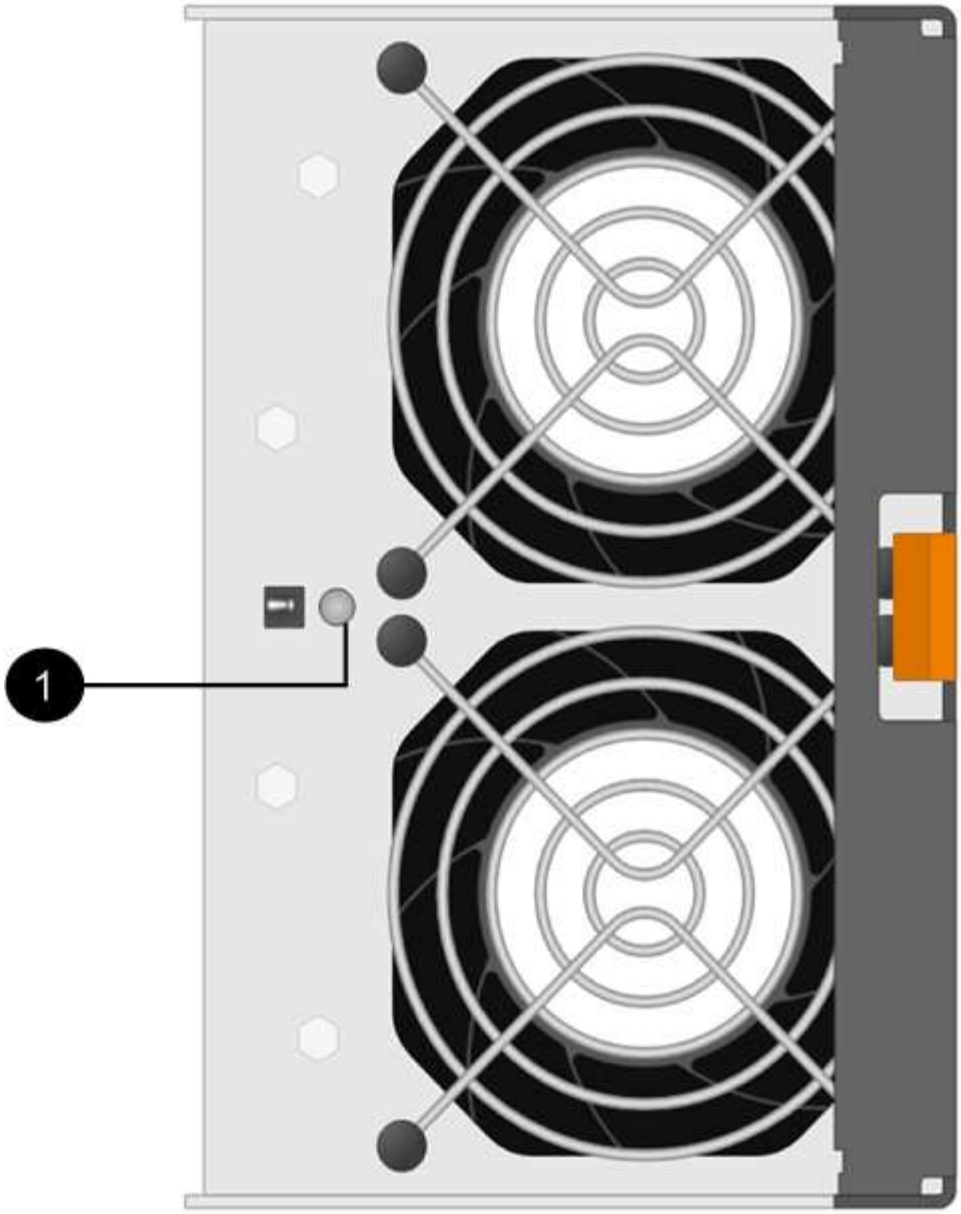
      Un componente con stato **Failed** deve essere sostituito.

      > Se il secondo contenitore della ventola nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo il contenitore della ventola guasto. Contattare invece il supporto tecnico per assistenza.

   È inoltre possibile trovare informazioni sul contenitore della ventola guasto nell'area Details (Dettagli) del Recovery Guru oppure consultare il registro eventi in Support (supporto) e Filter by Component Type (filtro per tipo di componente).

3. Dal retro dello storage array, osservare i LED di attenzione per individuare il contenitore della ventola da rimuovere.

   È necessario sostituire il filtro a carboni attivi della ventola con il LED attenzione acceso.



(1) *LED attenzione*. Se questo LED viene visualizzato come **giallo fisso**, significa che la ventola è guasta.

Fase 2: Rimuovere il filtro a carboni attivi della ventola guasto e installarne uno nuovo

Rimuovere un contenitore della ventola guasto in modo da poterlo sostituire con uno nuovo.

> Se non si spegne l'alimentazione dello storage array, assicurarsi di rimuovere e sostituire il contenitore della ventola entro 30 minuti per evitare il surriscaldamento del sistema.

Fasi

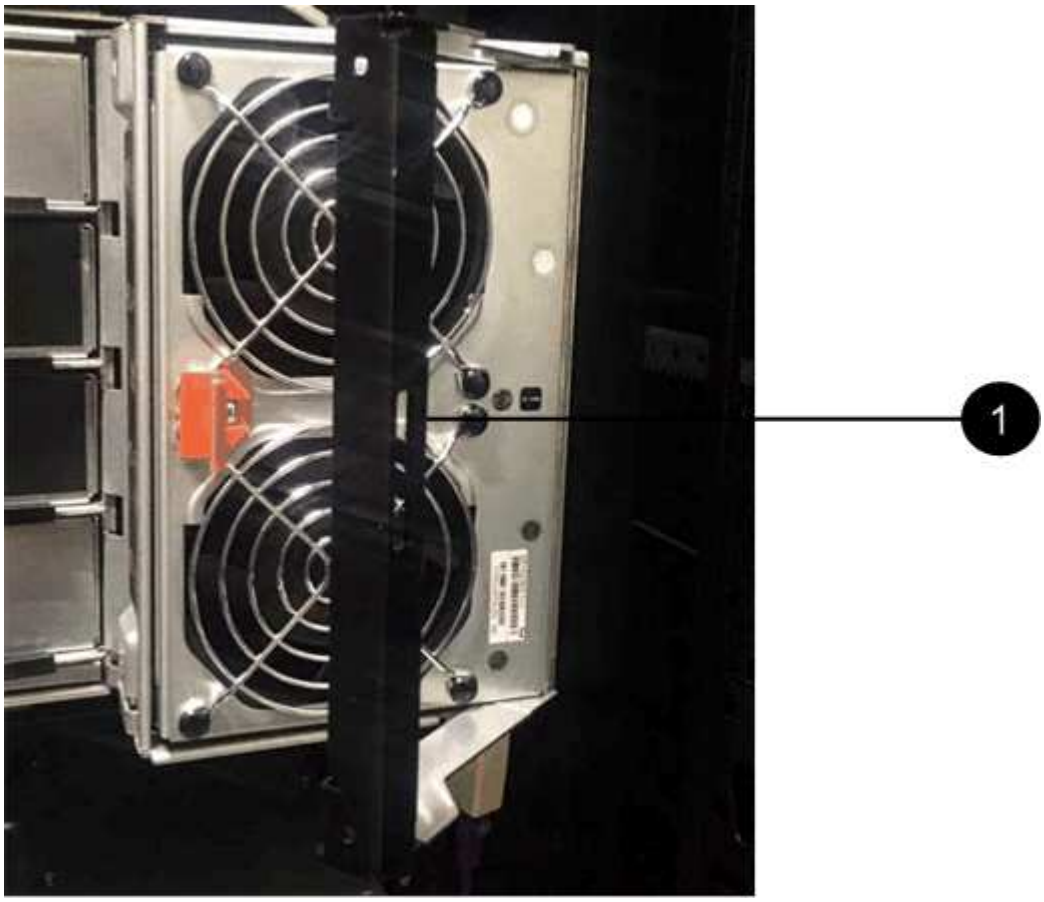
1. Disimballare il nuovo contenitore della ventola e posizionarlo su una superficie piana vicino allo scaffale.

   Conservare tutto il materiale di imballaggio da utilizzare quando si restituisce la ventola guasta.

2. Premere la linguetta arancione per rilasciare la maniglia del filtro a carboni attivi della ventola.

(1) *linguetta che si preme per rilasciare la maniglia del filtro della ventola*

3. Utilizzare la maniglia del filtro a carboni attivi per estrarre il filtro a carboni attivi dal ripiano.



(1) *maniglia per estrarre il contenitore della ventola*

4. Far scorrere completamente il contenitore della ventola di ricambio nello scaffale, quindi spostare la maniglia del contenitore della ventola fino a quando non si blocca con la linguetta arancione.

Fase 3: Sostituzione completa del filtro a carboni attivi della ventola

Verificare che il nuovo filtro a carboni attivi della ventola funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Controllare il LED di attenzione ambra sul nuovo filtro a carboni attivi della ventola.

> Dopo aver sostituito il filtro a carboni attivi della ventola, il LED attenzione rimane acceso (ambra fisso) mentre il firmware verifica che il filtro a carboni attivi della ventola sia stato installato correttamente. Il LED si spegne al termine del processo.

2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se viene ancora segnalato un guasto al filtro a carboni attivi della ventola, ripetere le operazioni descritte in Fase 2: Rimuovere il filtro a carboni attivi della ventola guasto e installarne uno nuovo. Se il problema persiste, contattare il supporto tecnico.

4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.
6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del filtro a carboni attivi della ventola è completata. È possibile riprendere le normali operazioni.

Dischi

Requisiti per la sostituzione del disco E2800

Prima di sostituire un'unità E2800, esaminare i requisiti e le considerazioni.

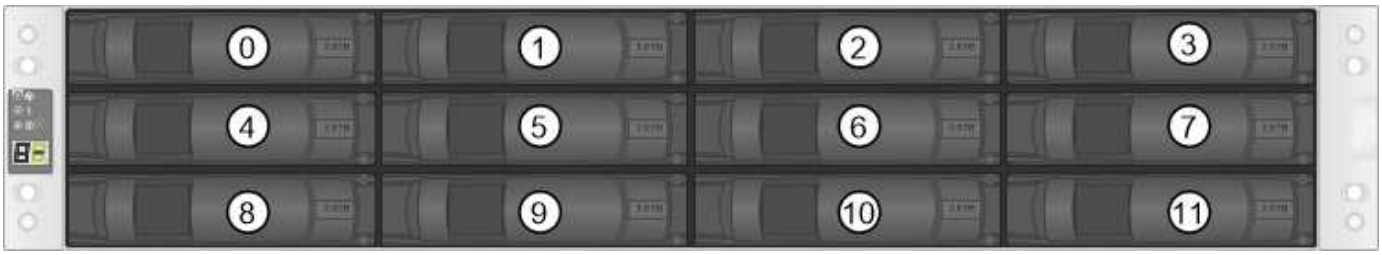
Tipi di shelf

È possibile sostituire un disco in uno shelf di controller da 12, 24 o 60 dischi o in uno shelf di dischi.

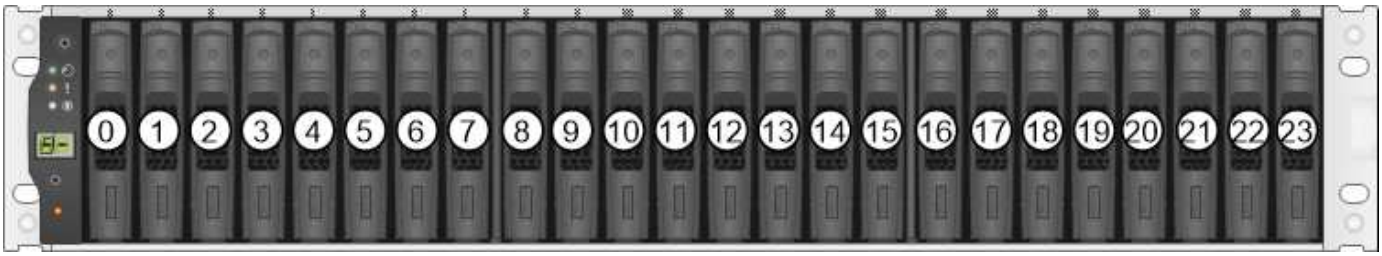
shelf da 12 o 24 dischi

Le figure mostrano come i dischi sono numerati in ogni tipo di shelf (il pannello anteriore o i cappucci terminali dello shelf sono stati rimossi).

Numerazione delle unità in uno shelf di controller E2812 o in uno shelf di dischi DE212C:



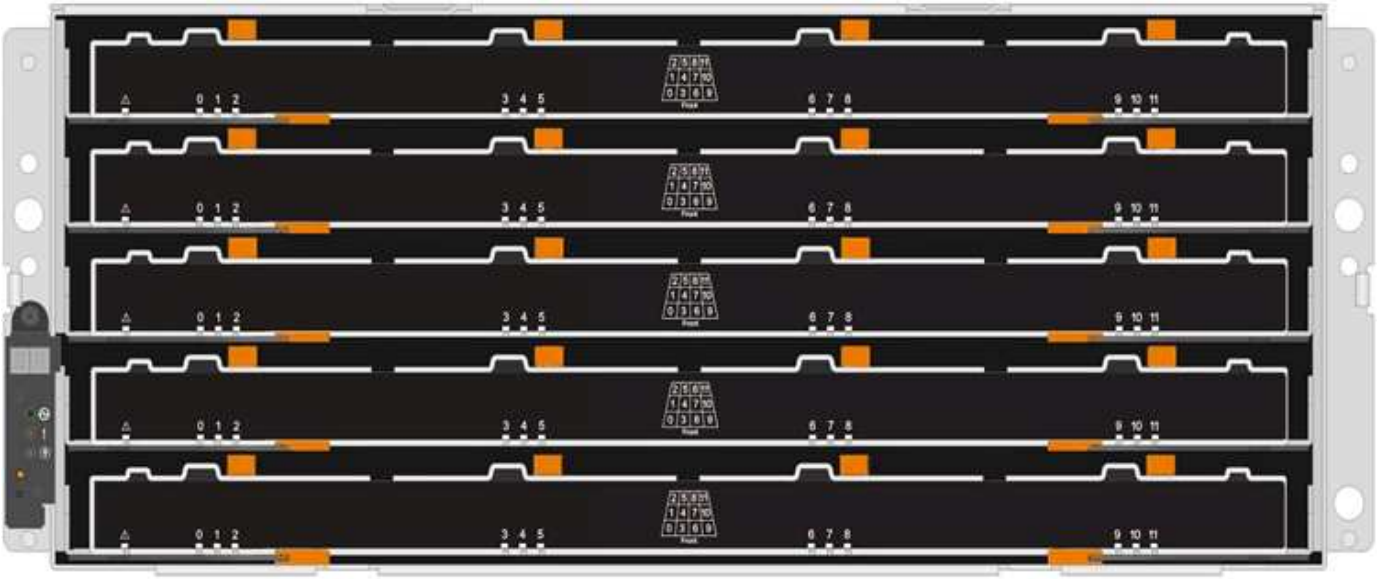
Numerazione delle unità in uno shelf di controller E2824, flash array EF280 o shelf di dischi DE224C:



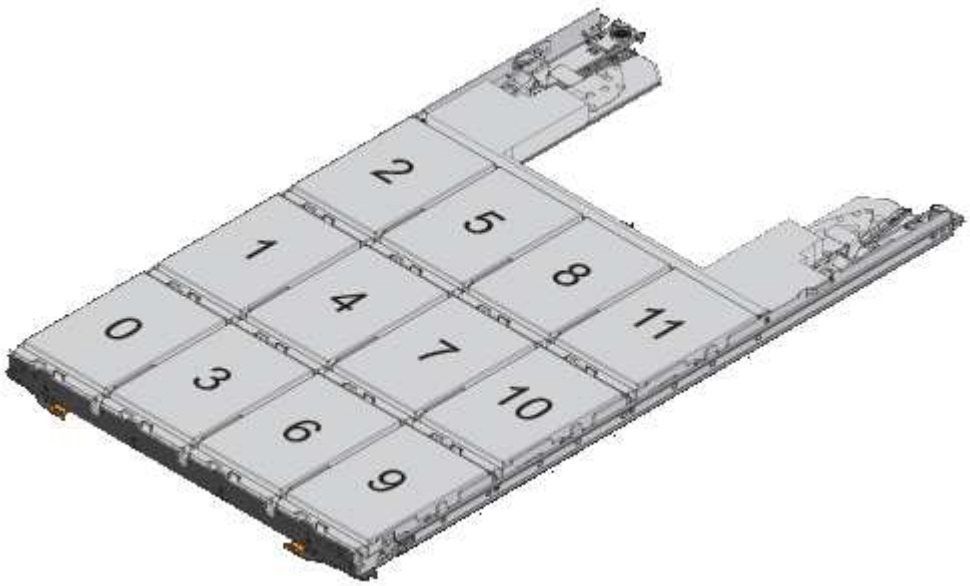
Lo storage array E2812, E2824, EF280 potrebbe includere uno o più tray di dischi di espansione SAS-2 legacy, tra cui il tray di 12 dischi DE1600, il tray di 24 dischi DE5600 o il tray di 60 dischi DE6600 Per istruzioni sulla sostituzione di un'unità in uno di questi vassoi, vedere "Sostituzione di un'unità nei vassoi E2660, E2760, E5460, E5560 o E5660" e. "Sostituzione di un'unità nei vassoi da 12 o 24 dischi E2600, E2700, E5400, E5500 e E5600".

shelf da 60 dischi

Sia lo shelf del controller E2860 che lo shelf del disco DE460C sono costituiti da cinque cassetti per unità contenenti ciascuno 12 slot per unità. Il cassetto dell'unità 1 si trova nella parte superiore e il cassetto dell'unità 5 nella parte inferiore.



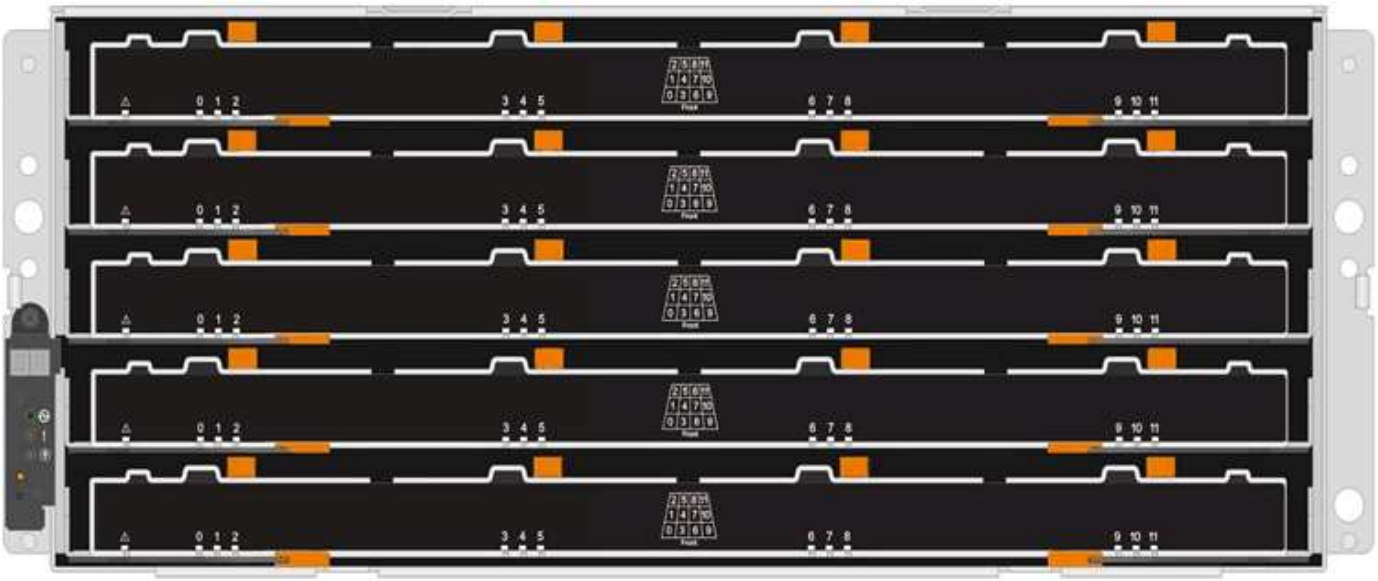
Per un cassetto per shelf controller E2860 e un cassetto per shelf dischi DE460C, i dischi sono numerati da 0 a 11 in ogni cassetto per unità all'interno dello shelf.



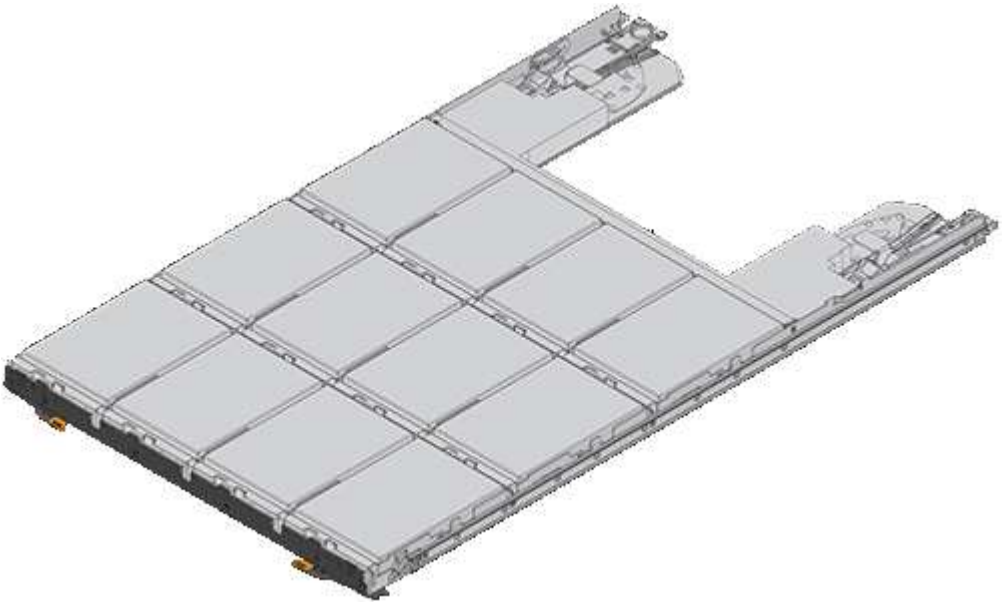
Lo storage array E2860 potrebbe includere uno o più tray di dischi di espansione SAS-2 preesistenti, tra cui il tray di 12 dischi DE1600, il tray di 24 dischi DE5600 o il tray di 60 dischi DE6600 Per istruzioni sulla sostituzione di un'unità in uno di questi vassoi, vedere "Sostituzione di un'unità nei vassoi E2660, E2760, E5460, E5560 o E5660" e. "Sostituzione di un'unità nei vassoi da 12 o 24 dischi E2600, E2700, E5400, E5500 e E5600".

Cassetto dell'unità

È possibile sostituire un cassetto dischi in uno shelf di controller E2860 e uno shelf di dischi DE460C. Ciascuno di questi shelf da 60 dischi dispone di cinque cassetti per dischi.



Ciascuno dei cinque cassetti può contenere fino a 12 dischi.



Gestione dei dischi

I dischi dello storage array sono fragili. Una gestione errata del disco è la causa principale del guasto del disco.

Attenersi alle seguenti regole per evitare di danneggiare le unità dello storage array:

- Prevenzione delle scariche elettrostatiche (ESD):
  - Tenere l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
  - Non inserire utensili metallici o coltelli nel sacchetto ESD.

    Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.
  - Conservare il sacchetto ESD e il materiale di imballaggio nel caso in cui sia necessario restituire un'unità in un secondo momento.
  - Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis dell'enclosure di storage.

    Se non è disponibile un braccialetto, toccare una superficie non verniciata sullo chassis del cabinet di storage prima di maneggiare il disco.
- Gestire i dischi con attenzione:
  - Utilizzare sempre due mani per rimuovere, installare o trasportare un disco.
  - Non forzare mai un'unità in uno shelf e esercitare una pressione leggera e decisa per inserire completamente il dispositivo di chiusura dell'unità.
  - Posizionare i dischi su superfici imbottite e non impilare mai i dischi uno sopra l'altro.
  - Non urtare i dischi contro altre superfici.
  - Prima di rimuovere un'unità da uno shelf, sganciare la maniglia e attendere 30 secondi affinché l'unità si spenda.
  - Utilizzare sempre imballaggi approvati per la spedizione delle unità.
- Evitare i campi magnetici:
  - Tenere le unità lontano da dispositivi magnetici.

    I campi magnetici possono distruggere tutti i dati presenti sul disco e causare danni irreparabili ai circuiti del disco.

Sostituire il disco in E2800 (shelf da 12 o 24 dischi)

È possibile sostituire un disco in un E2800 con uno shelf da 12 o 24 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array riceve i/O.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco E2800".
- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.

- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco

Preparare la sostituzione di un disco controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema di SANtricity per individuare l'unità all'interno dello storage array. Dal menu di scelta rapida del disco nella pagina hardware, selezionare **attiva indicatore di posizione**.

   Il LED di attenzione del disco (ambra) lampeggia per identificare il disco da sostituire.

   > Se si sostituisce un'unità in uno shelf dotato di pannello, rimuovere il pannello per visualizzare i LED dell'unità.

Fase 2: Rimuovere il disco guasto

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

   Conservare tutti i materiali di imballaggio.
2. Premere il pulsante di rilascio sul disco guasto.

- Per i dischi negli shelf di controller E2812 o negli shelf di dischi DE212C, il pulsante di rilascio si trova a sinistra del disco.
- Per i dischi negli shelf di controller E2824, nell'array flash EF280, per gli shelf di dischi DE224C, il pulsante di rilascio si trova nella parte superiore dell'unità. La maniglia della camma sulle molle del disco si apre parzialmente e il disco si disinnesta dalla scheda intermedia.

3. Aprire la maniglia della camma ed estrarre leggermente l'unità.
4. Attendere 30 secondi.
5. Rimuovere l'unità dallo shelf con entrambe le mani.
6. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
7. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

Fase 3: Installare un nuovo disco

Installare un nuovo disco per sostituire quello guasto.

> Installare l'unità sostitutiva il prima possibile dopo aver rimosso l'unità guasta. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

Fasi

1. Aprire la maniglia della camma.
2. Con due mani, inserire l'unità sostitutiva nell'alloggiamento aperto, spingendo con decisione fino a quando non si arresta.
3. Chiudere lentamente la maniglia della camma fino a quando l'unità non è completamente inserita nel piano intermedio e la maniglia non scatta in posizione.

   Il LED verde sull'unità si accende quando l'unità è inserita correttamente.

> A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco

Completare la sostituzione del disco per verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita. (Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.
   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.
4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire l'unità in E2800 (shelf da 60 dischi)

È possibile sostituire un disco in un E2800 con uno shelf da 60 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array sta ricevendo le operazioni di i/O.

Questa procedura si applica agli shelf di dischi DCM e DCM2.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco E2800".
- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.

- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco

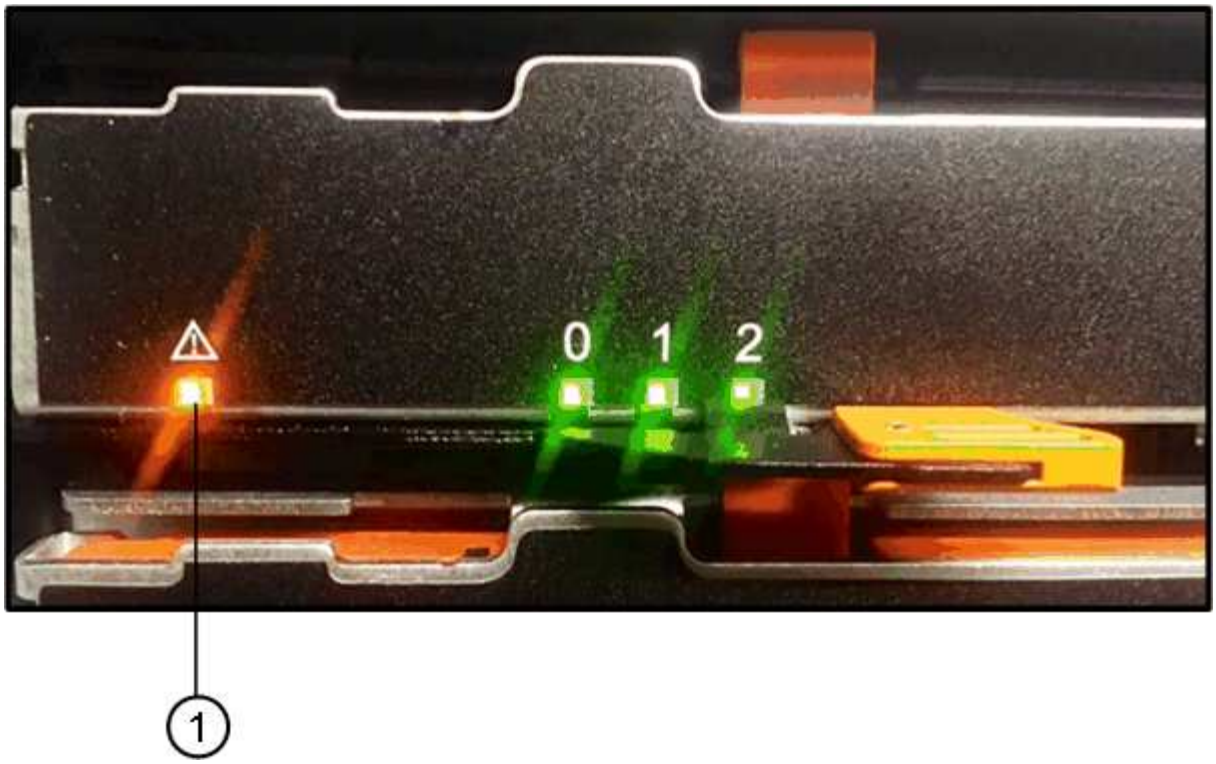
Preparare la sostituzione di un disco controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema di SANtricity per individuare il disco all'interno dello storage array.
   a. Se lo shelf è dotato di una cornice, rimuovetela per vedere i LED.
   b. Dal menu di scelta rapida del disco, selezionare **attiva indicatore di posizione**.

      Il LED di attenzione del cassetto dell'unità (ambra) lampeggia per consentire l'apertura del cassetto dell'unità corretto e identificare l'unità da sostituire.



(1) *LED attenzione*

a. Sganciare il cassetto dell'unità tirando entrambe le leve.
b. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta.
c. Controllare la parte superiore del cassetto dell'unità per individuare il LED di attenzione davanti a ciascun disco.

(1) *LED attenzione acceso per l'unità in alto a destra*

I LED attenzione cassetto unità si trovano sul lato sinistro davanti a ciascun disco, con un'icona di attenzione sulla maniglia del disco appena dietro il LED.

(1) *icona attenzione*

(2) *LED attenzione*

Fase 2: Rimuovere il disco guasto

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

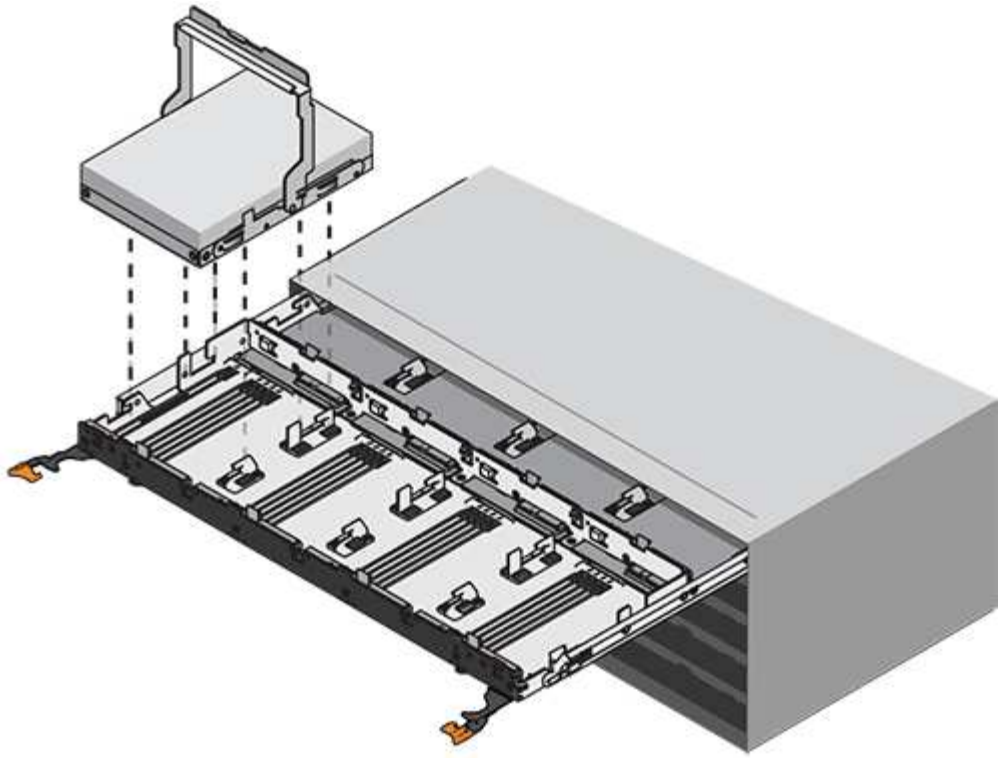
   Conservare tutti i materiali di imballaggio per la prossima volta che sarà necessario restituire un disco.

2. Rilasciare le leve del cassetto dell'unità dal centro del cassetto dell'unità appropriato, tirandole verso i lati del cassetto.
3. Tirare con cautela le leve del cassetto dell'unità esteso per estrarre il cassetto dell'unità fino alla sua estensione completa senza rimuoverlo dal contenitore.
4. Tirare delicatamente indietro il dispositivo di chiusura arancione che si trova davanti all'unità che si desidera rimuovere.

   La maniglia della camma sulle molle di azionamento si apre parzialmente e l'unità viene rilasciata dal cassetto.

(1) *dispositivo di chiusura arancione*

5. Aprire la maniglia della camma ed estrarre leggermente l’unità.
6. Attendere 30 secondi.
7. Utilizzare la maniglia della camma per sollevare l’unità dallo scaffale.



8. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
9. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

Fase 3: Installare un nuovo disco

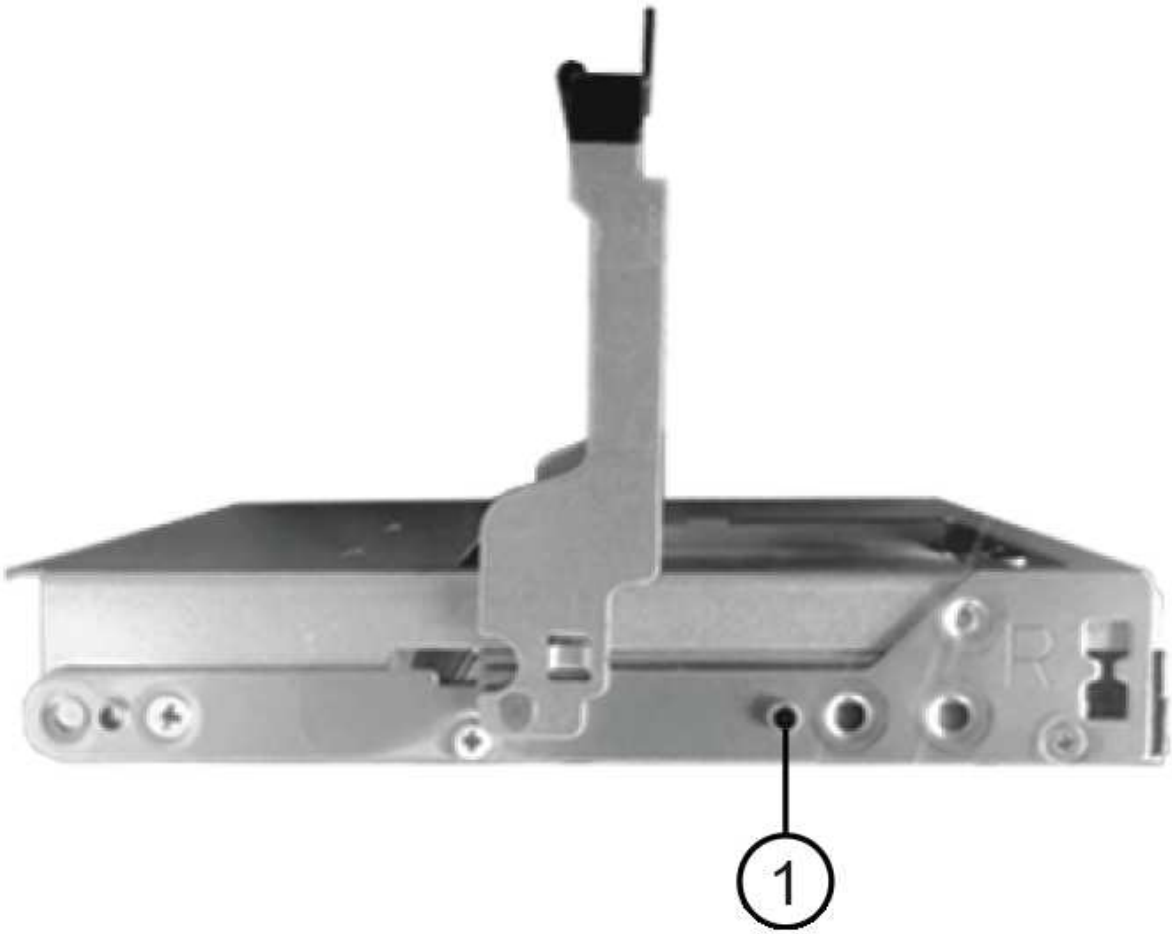
Installare un nuovo disco per sostituire quello guasto.

> Installare l'unità sostitutiva il prima possibile dopo aver rimosso l'unità guasta. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

> **Possibile perdita di accesso ai dati** — quando si reinserisce il cassetto del disco nel contenitore, non chiudere mai il cassetto. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.

Fasi

1. Sollevare la maniglia della camma sul nuovo disco in verticale.
2. Allineare i due pulsanti rialzati su ciascun lato del supporto dell'unità con lo spazio corrispondente nel canale dell'unità sul cassetto dell'unità.



(1) *pulsante sollevato sul lato destro del supporto del disco*

3. Abbassare l'unità, quindi ruotare la maniglia della camma verso il basso fino a quando non scatta in posizione sotto il dispositivo di chiusura arancione.
4. Spingere con cautela il cassetto dell'unità all'interno del contenitore. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.
5. Chiudere il cassetto dell'unità spingendo entrambe le leve verso il centro.

   Il LED di attività verde per l'unità sostituita nella parte anteriore del cassetto si accende quando l'unità è inserita correttamente.

   A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco

Verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita. (Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.
   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.
4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire il cassetto del disco in E2800 (shelf da 60 dischi)

È possibile sostituire un cassetto dischi in uno shelf di controller E2860 o in uno shelf di dischi DE460C.

A proposito di questa attività

La procedura per sostituire un cassetto del disco guasto in uno shelf di controller E2860 o in uno shelf di dischi DE460C dipende dalla protezione dei volumi nel cassetto dalla protezione contro la perdita di cassetto. Se tutti i volumi nel cassetto si trovano in pool di dischi o gruppi di volumi con protezione perdita cassetto, è possibile eseguire questa procedura online. In caso contrario, è necessario interrompere tutte le attività di i/o dell'host e spegnere lo shelf prima di sostituire il cassetto dell'unità.

Prima di iniziare

- Esaminare i requisiti del cassetto del disco in "Requisiti per la sostituzione del disco E2800".
- Assicurarsi che lo shelf di dischi soddisfi tutte le seguenti condizioni:
  - Lo shelf di dischi non può essere troppo freddo.
  - Entrambe le ventole devono essere installate e avere uno stato ottimale.
  - Tutti i componenti dello shelf dei dischi devono essere in posizione.

- I volumi nel cassetto del disco non possono essere degradati.

> **Possibile perdita di accesso ai dati** — se un volume si trova già in uno stato degradato e si rimuovono le unità dal cassetto, il volume potrebbe non funzionare.

- Assicurarsi di disporre di quanto segue:
  - Un cassetto dell'unità sostitutivo.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Una torcia.
  - Un indicatore permanente per annotare la posizione esatta di ciascuna unità durante la rimozione dell'unità dal cassetto.
  - Accesso all'interfaccia a riga di comando (CLI) dello storage array. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:
    - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
    - **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Fase 1: Preparazione alla sostituzione del cassetto dell'unità

Determinare se è possibile eseguire la procedura di sostituzione mentre lo shelf del disco è online o se è necessario interrompere l'attività di i/o dell'host e spegnere uno degli shelf accesi.

Se si sostituisce un cassetto in uno shelf con protezione perdita cassetto, non è necessario interrompere l'attività di i/o dell'host e spegnere uno degli shelf.

Fasi

1. Determinare se lo shelf di dischi è acceso.
   - Se l'alimentazione è spenta, non è necessario eseguire il comando CLI. Passare a. Fase 2: Rimuovere le catene di cavi.
   - Se l'alimentazione è accesa, passare alla fase successiva.
2. Accedere alla CLI, quindi immettere il seguente comando:

```
SMcli <ctlr_IP1\> -p "array_password" -c "set tray [trayID] drawer
[drawerID]
serviceAllowedIndicator=on;"
```

   dove:

   - `<ctlr_IP1>` è l'identificatore del controller.
   - `array_password` è la password per lo storage array. È necessario racchiudere il valore per `array_password` tra virgolette doppie ("").

- `[trayID]` è l'identificativo dello shelf di dischi che contiene il cassetto che si desidera sostituire. I valori dell'ID dello shelf del disco vanno da 0 a 99. È necessario racchiudere il valore per `trayID` tra parentesi quadre.
- `[drawerID]` è l'identificativo del cassetto dell'unità che si desidera sostituire. I valori dell'ID cassetto sono da 1 (cassetto superiore) a 5 (cassetto inferiore). È necessario racchiudere il valore per `drawerID` tra parentesi quadre.

  Questo comando consente di rimuovere il cassetto più in alto nello shelf 10:

```
SMcli <ctlr_IP1\> -p "safety-1" -c "set tray [10] drawer [1]
serviceAllowedIndicator=forceOnWarning;"
```

3. Determinare se è necessario interrompere l'attività di i/o dell'host, come segue:
   - Se il comando ha esito positivo, non è necessario interrompere l'attività di i/o dell'host. Tutti i dischi nel cassetto sono in pool o gruppi di volumi con protezione perdita cassetto. Passare a. Fase 2: Rimuovere le catene di cavi.

     Possibili danni ai dischi — attendere 30 secondi dopo il completamento del comando prima di aprire il cassetto del disco. L'attesa di 30 secondi consente lo spin down dei dischi, evitando possibili danni all'hardware.

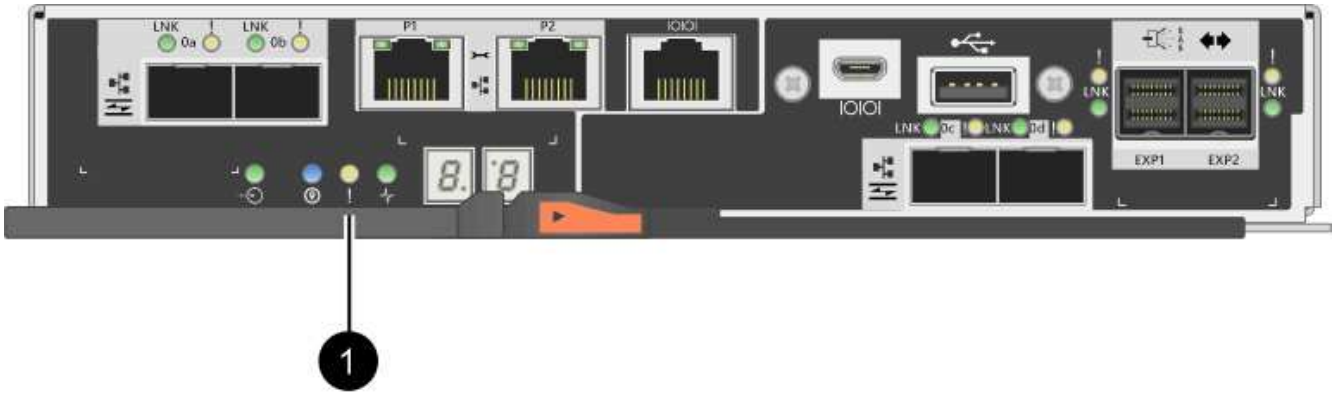
   - Se viene visualizzato un avviso che indica che non è stato possibile completare questo comando, è necessario interrompere l'attività di i/o dell'host prima di rimuovere il cassetto. L'avviso viene visualizzato perché uno o più dischi nel cassetto interessato sono in pool o gruppi di volumi senza protezione perdita cassetto. Per evitare la perdita di dati, è necessario completare i passaggi successivi per interrompere l'attività di i/o dell'host e spegnere lo shelf di dischi e lo shelf di controller.
4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

     I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.
5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.

   Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere i dati perché lo storage array non sarà accessibile.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati

nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



(1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
8. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
9. Spegnere gli shelf seguendo una delle seguenti procedure:
   - *Se si sostituisce un cassetto in uno shelf **con** protezione perdita cassetto*: NON è necessario spegnere nessuno degli shelf. È possibile eseguire la procedura di sostituzione mentre il cassetto dell'unità è in linea, poiché il comando Set Drawer Service Action Allowed Indicator CLI è stato completato correttamente.
   - *Se stai sostituendo un cassetto in uno shelf **controller senza** protezione perdita cassetto*:
     i. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere che tutti i LED sullo shelf del controller si oscuri.
   - *Se si sostituisce un cassetto in uno shelf di dischi **espansione senza** protezione perdita cassetto*:
     i. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere che tutti i LED sullo shelf del controller si oscuri.
     iii. Spegnere entrambi gli interruttori di alimentazione sullo shelf di dischi.
     iv. Attendere due minuti per interrompere l'attività del disco.

Fase 2: Rimuovere le catene di cavi

Rimuovere entrambe le catene per cavi in modo da poter rimuovere e sostituire un cassetto del disco guasto.

A proposito di questa attività

Ciascun cassetto dispone di catene di cavi destra e sinistra. Le catene per cavi sinistra e destra consentono ai cassetti di scorrere verso l'interno e verso l'esterno.

Le estremità metalliche delle catene per cavi scorrono nelle corrispondenti guide verticali e orizzontali all'interno del contenitore, come indicato di seguito:

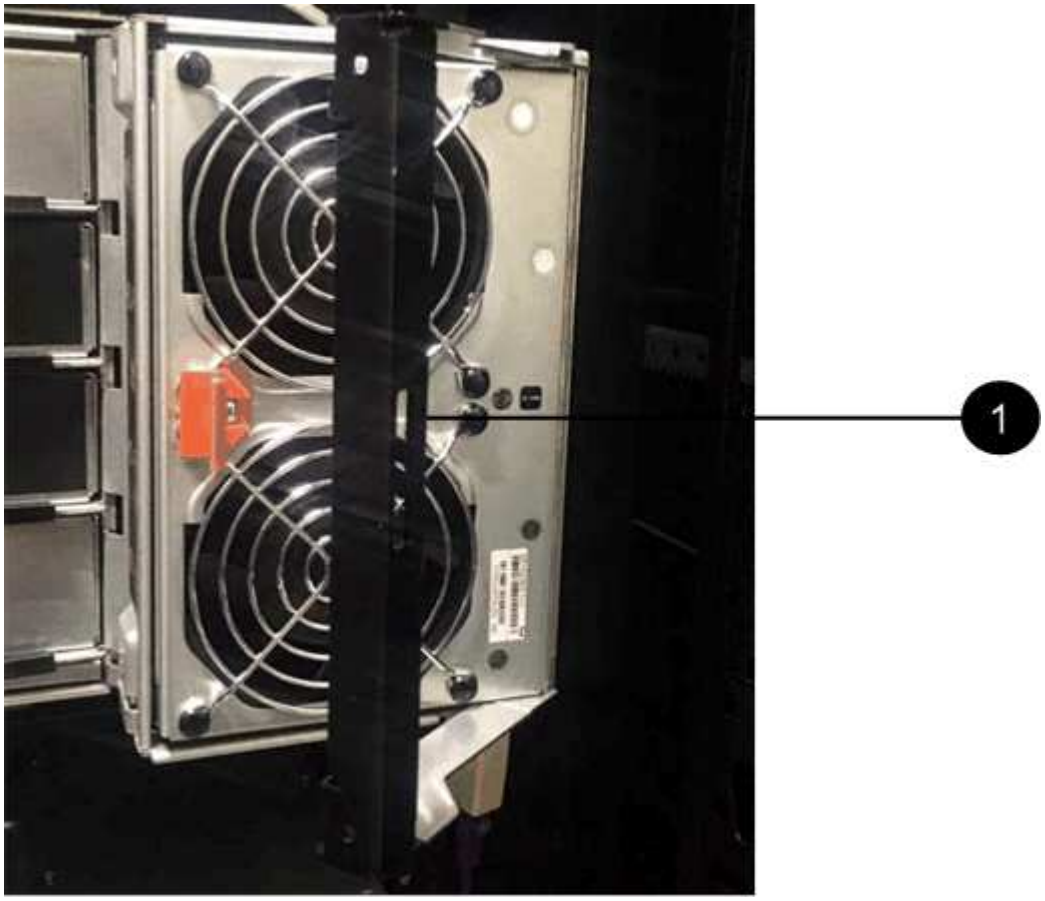
- Le guide verticali di destra e di sinistra collegano la catena di cavi alla scheda centrale del contenitore.
- Le guide orizzontali sinistra e destra collegano la catena di cavi al singolo cassetto.

Possibili danni all'hardware — se il vassoio dell'unità è acceso, la catena di cavi viene eccitata fino a quando entrambe le estremità non vengono scollegate. Per evitare di mettere in corto circuito l'apparecchiatura, evitare che il connettore della catena di cavi scollegato tocchi il telaio metallico se l'altra estremità della catena di cavi è ancora collegata.

Fasi

1. Assicurarsi che lo shelf di dischi e lo shelf del controller non abbiano più attività i/o e siano spenti oppure che sia stato emesso il `Set Drawer Attention Indicator` Comando CLI.
2. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola di destra:
   a. Premere la linguetta arancione per rilasciare la maniglia del filtro a carboni attivi della ventola.

      La figura mostra la maniglia del filtro a carboni attivi della ventola estesa e rilasciata dalla linguetta arancione a sinistra.



(1) *maniglia del filtro della ventola*

   a. Utilizzando la maniglia, estrarre il contenitore della ventola dal vassoio dell'unità e metterlo da parte.
   b. Se il vassoio è acceso, assicurarsi che la ventola sinistra sia alla massima velocità.

Possibili danni all'apparecchiatura dovuti al surriscaldamento — se il vassoio è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

3. Determinare la catena di cavi da scollegare:

- Se l’alimentazione è accesa, il LED di attenzione di colore ambra sulla parte anteriore del cassetto indica la catena di cavi da scollegare.
- Se l’alimentazione è spenta, è necessario determinare manualmente quale delle cinque catene di cavi scollegare. La figura mostra il lato destro dello shelf del disco con il contenitore della ventola rimosso. Una volta rimosso il contenitore della ventola, è possibile vedere le cinque catene di cavi e i connettori verticali e orizzontali per ciascun cassetto.

  La catena di cavi superiore è collegata al cassetto dell’unità 1. La catena dei cavi inferiore è collegata al cassetto dell’unità 5. Vengono fornite le didascalie per il cassetto unità 1.


2
1
3

(1) *catena di cavi*

(2) *connettore verticale (collegato alla scheda intermedia)*

(3) *connettore orizzontale (collegato al cassetto)*

4. Per un facile accesso, spostare la catena di cavi sul lato destro verso sinistra con un dito.
5. Scollegare una delle catene di cavi di destra dalla relativa guida verticale.

   a. Utilizzando una torcia, individuare l’anello arancione all’estremità della catena di cavi collegata alla guida verticale del contenitore.

(1) *anello arancione su guida verticale*

(2) *catena di cavi, parzialmente rimossa*

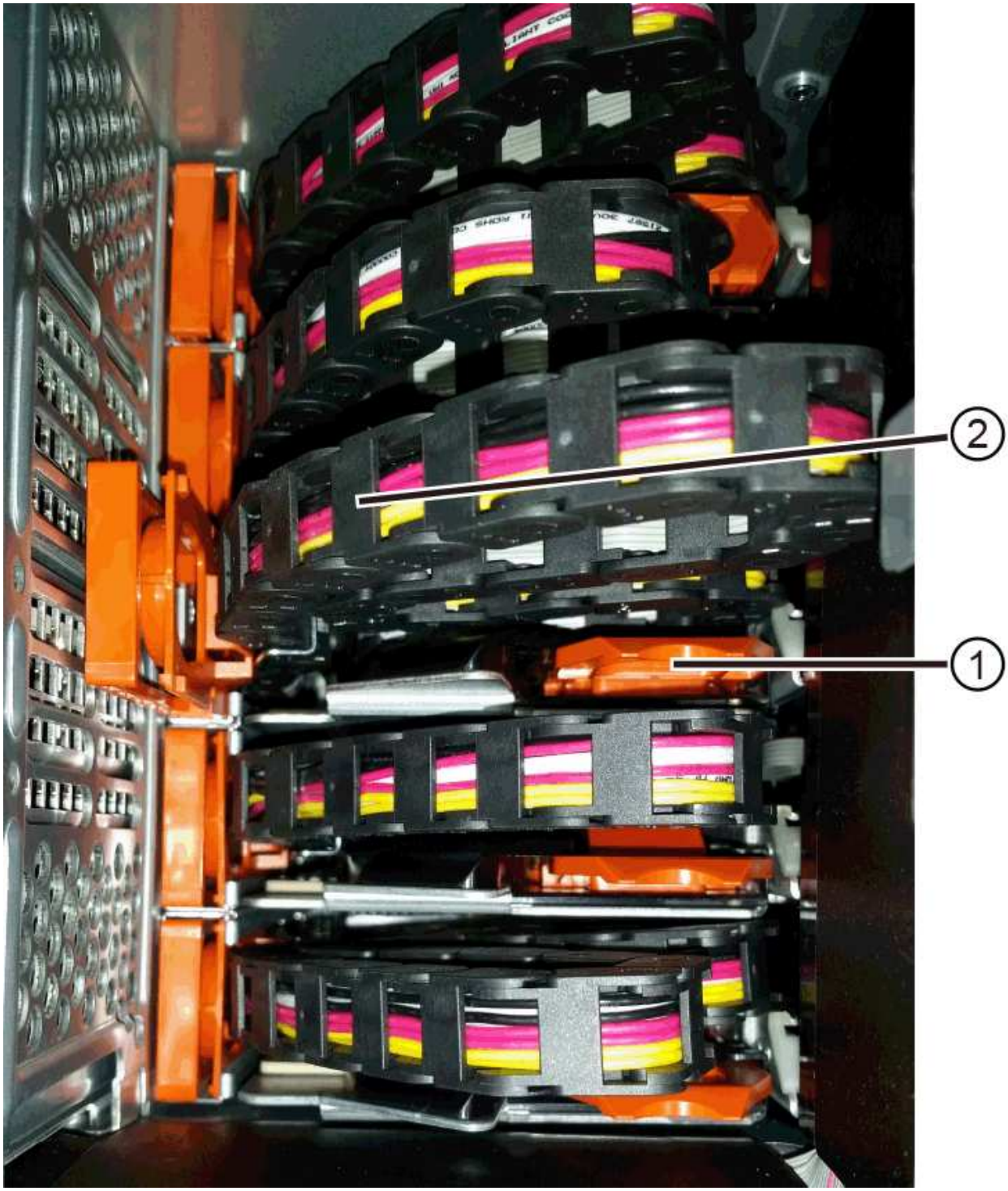
a. Per sganciare la catena di cavi, inserire il dito nell’anello arancione e premere verso il centro del sistema.

b. Per scollegare la catena di cavi, tirare con cautela il dito verso di sé circa 2.5 cm (1 pollice). Lasciare il connettore della catena di cavi all'interno della guida verticale. (Se il vassoio dell'unità è acceso, evitare che il connettore della catena di cavi tocchi il telaio metallico).

6. Scollegare l'altra estremità della catena portacavi:

   a. Utilizzando una torcia, individuare l'anello arancione all'estremità della catena di cavi collegata alla guida orizzontale del contenitore.

      La figura mostra il connettore orizzontale a destra e la catena dei cavi scollegata e parzialmente estratta sul lato sinistro.



(1) *anello arancione sulla guida orizzontale*

(2) *catena di cavi, parzialmente rimossa*

a. Per sganciare la catena di cavi, inserire delicatamente il dito nell'anello arancione e premere verso il basso.

   La figura mostra l'anello arancione sulla guida orizzontale (vedere l'elemento 1 nella figura precedente), in quanto viene spinto verso il basso in modo da poter estrarre il resto della catena di cavi dal contenitore.

b. Tirare il dito verso di sé per scollegare la catena di cavi.

7. Estrarre con cautela l'intera catena di cavi dallo shelf del disco.
8. Sostituire il filtro a carboni attivi della ventola destra:

   a. Far scorrere il contenitore della ventola fino in fondo nello scaffale.
   b. Spostare la maniglia del filtro a carboni attivi della ventola fino a quando non si blocca con la linguetta arancione.
   c. Se lo shelf del disco è alimentato, verificare che il LED di attenzione ambra sul retro della ventola non sia acceso e che l'aria stia uscendo dal retro della ventola.

      Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

   Se l'alimentazione è spenta, le ventole non funzionano e il LED non è acceso.

9. Dal retro dello shelf del disco, rimuovere il contenitore della ventola sinistro.
10. Se lo shelf di dischi riceve alimentazione, assicurarsi che la ventola giusta passi alla velocità massima.

> **Possibili danni all'apparecchiatura dovuti al surriscaldamento** — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

11. Scollegare la catena portacavi sinistra dalla relativa guida verticale:

    a. Utilizzando una torcia, individuare l'anello arancione all'estremità della catena di cavi collegata alla guida verticale.
    b. Per sganciare la catena di cavi, inserire il dito nell'anello arancione.
    c. Per scollegare la catena di cavi, tirare verso di sé circa 2.5 cm (1 poll.). Lasciare il connettore della catena di cavi all'interno della guida verticale.

> **Possibili danni all'hardware** — se il vassoio dell'unità è acceso, la catena di cavi viene eccitata fino a quando entrambe le estremità non vengono scollegate. Per evitare di mettere in corto circuito l'apparecchiatura, evitare che il connettore della catena di cavi scollegato tocchi il telaio metallico se l'altra estremità della catena di cavi è ancora collegata.

12. Scollegare la catena di cavi sinistra dalla guida orizzontale ed estrarre l'intera catena di cavi dallo shelf del disco.

    Se si esegue questa procedura con l'alimentazione accesa, tutti i LED si spengono quando si scollega l'ultimo connettore della catena di cavi, compreso il LED di attenzione di colore ambra.

13. Sostituire il filtro a carboni attivi della ventola sinistra. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola non sia acceso e che l'aria fuoriuscito dal retro della ventola.

    Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

Fase 3: Rimuovere il cassetto del disco guasto

Rimuovere un cassetto del disco guasto per sostituirlo con uno nuovo.

> **Possibile perdita di accesso ai dati** — i campi magnetici possono distruggere tutti i dati sul disco e causare danni irreparabili ai circuiti del disco. Per evitare la perdita di accesso ai dati e danni ai dischi, tenere i dischi sempre lontani da dispositivi magnetici.

Fasi

1. Assicurarsi che:
    - Le catene dei cavi destra e sinistra sono scollegate.
    - I contenitori delle ventole lato destro e sinistro vengono sostituiti.
2. Rimuovere il pannello frontale dallo shelf del disco.
3. Sganciare il cassetto dell'unità estraendo entrambe le leve.
4. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta. Non rimuovere completamente il cassetto dal ripiano del disco.
5. Se i volumi sono già stati creati e assegnati, utilizzare un indicatore permanente per annotare la posizione esatta di ciascun disco. Ad esempio, utilizzando il seguente disegno come riferimento, scrivere il numero di slot appropriato sulla parte superiore di ciascun disco.

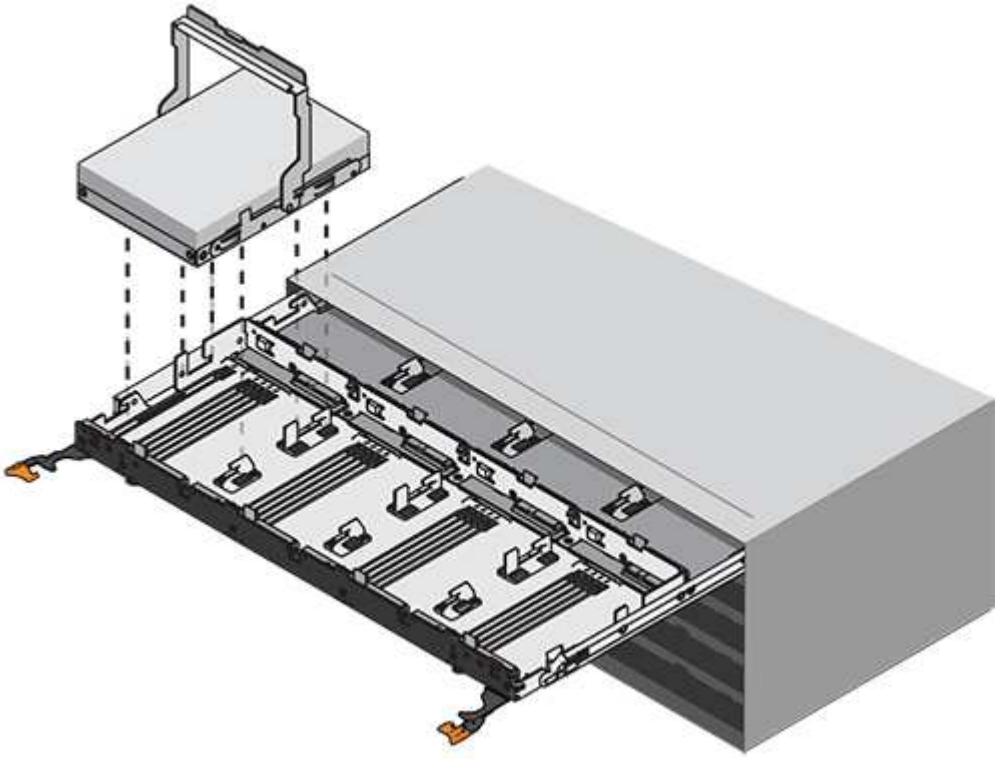
> **Possibile perdita di accesso ai dati** — assicurarsi di registrare la posizione esatta di ciascun disco prima di rimuoverlo.

6. Rimuovere le unità dal cassetto:
    a. Tirare delicatamente indietro il dispositivo di chiusura arancione visibile al centro della parte anteriore

di ciascun disco.

b. Sollevare la maniglia dell'unità in verticale.

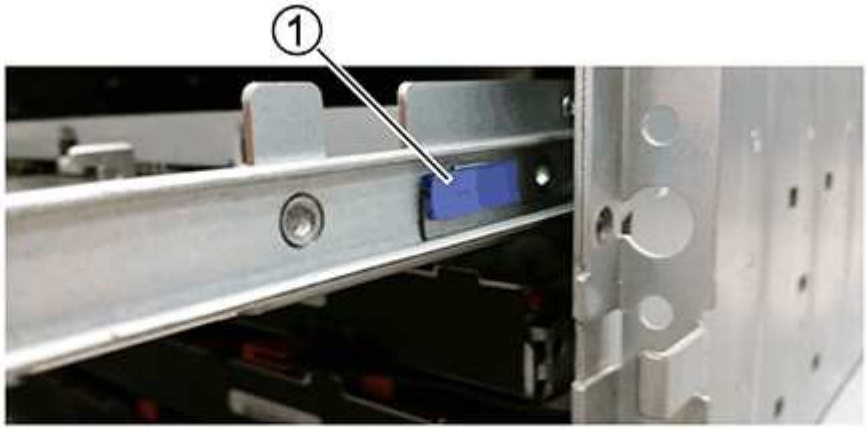
c. Utilizzare la maniglia per sollevare l'unità dal cassetto dell'unità.



d. Posizionare l'unità su una superficie piana, priva di scariche elettrostatiche e lontano da dispositivi magnetici.

7. Rimuovere il cassetto dell'unità:

a. Individuare la leva di rilascio in plastica su ciascun lato del cassetto dell'unità.



(1) *leva di rilascio cassetto unità*

a. Sganciare entrambe le leve di rilascio tirando i fermi verso di sé.

b. Tenendo entrambe le leve di rilascio, tirare il cassetto dell'unità verso di sé.

c. Rimuovere il cassetto del disco dallo shelf del disco.

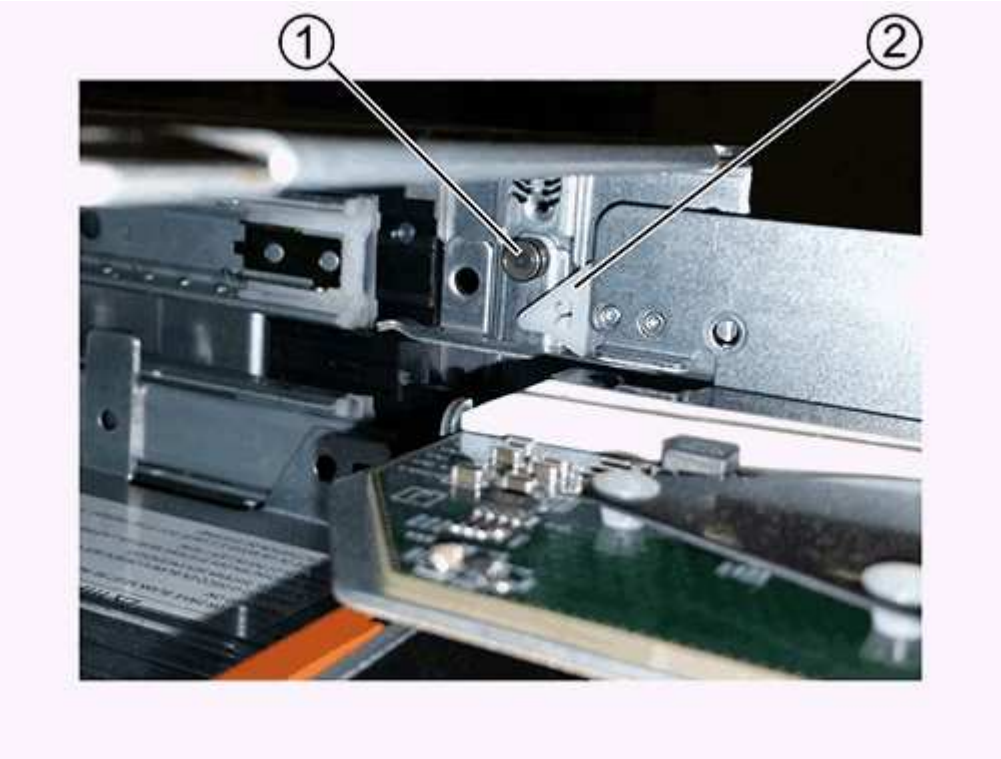
Fase 4: Installare un nuovo cassetto unità

Installare un nuovo cassetto per sostituire quello guasto.

Fasi

1. Dalla parte anteriore dello shelf del disco, far passare una torcia nello slot vuoto del cassetto e individuare il cilindretto di blocco dello slot.

   Il gruppo di blocco è una funzione di sicurezza che impedisce l'apertura di più cassetti per disco alla volta.



   (1) *Tumbler Lock-out*

   (2) *Guida cassetto*

2. Posizionare il cassetto dell'unità sostitutivo davanti allo slot vuoto e leggermente a destra rispetto al centro.

   Posizionando leggermente il cassetto a destra del centro, si garantisce che il nottolino di blocco e la guida del cassetto siano inseriti correttamente.

3. Far scorrere il cassetto dell'unità nello slot e assicurarsi che la guida del cassetto scorra sotto il nottolino di blocco.

   Rischio di danni all'apparecchiatura — si verifica un danno se la guida del cassetto non scorre sotto l'interruttore a levetta di blocco.

4. Spingere con cautela il cassetto dell'unità fino a quando il fermo non si aggancia completamente.

   Quando si chiude il cassetto per la prima volta, si verifica un livello di resistenza più elevato.

Rischio di danni all'apparecchiatura — interrompere la pressione del cassetto dell'unità se si ritiene che sia bloccato. Utilizzare le leve di rilascio nella parte anteriore del cassetto per far scorrere il cassetto all'indietro. Quindi, reinserire il cassetto nello slot, assicurarsi che il cilindretto si trovi sopra la guida e che le guide siano allineate correttamente.

Fase 5: Collegare le catene di cavi

Collegare le catene per cavi in modo da poter reinstallare in sicurezza le unità nel cassetto.

A proposito di questa attività

Quando si collega una catena di cavi, invertire l'ordine utilizzato per scollegare la catena di cavi. Inserire il connettore orizzontale della catena nella guida orizzontale del contenitore prima di inserire il connettore verticale della catena nella guida verticale del contenitore.

Fasi

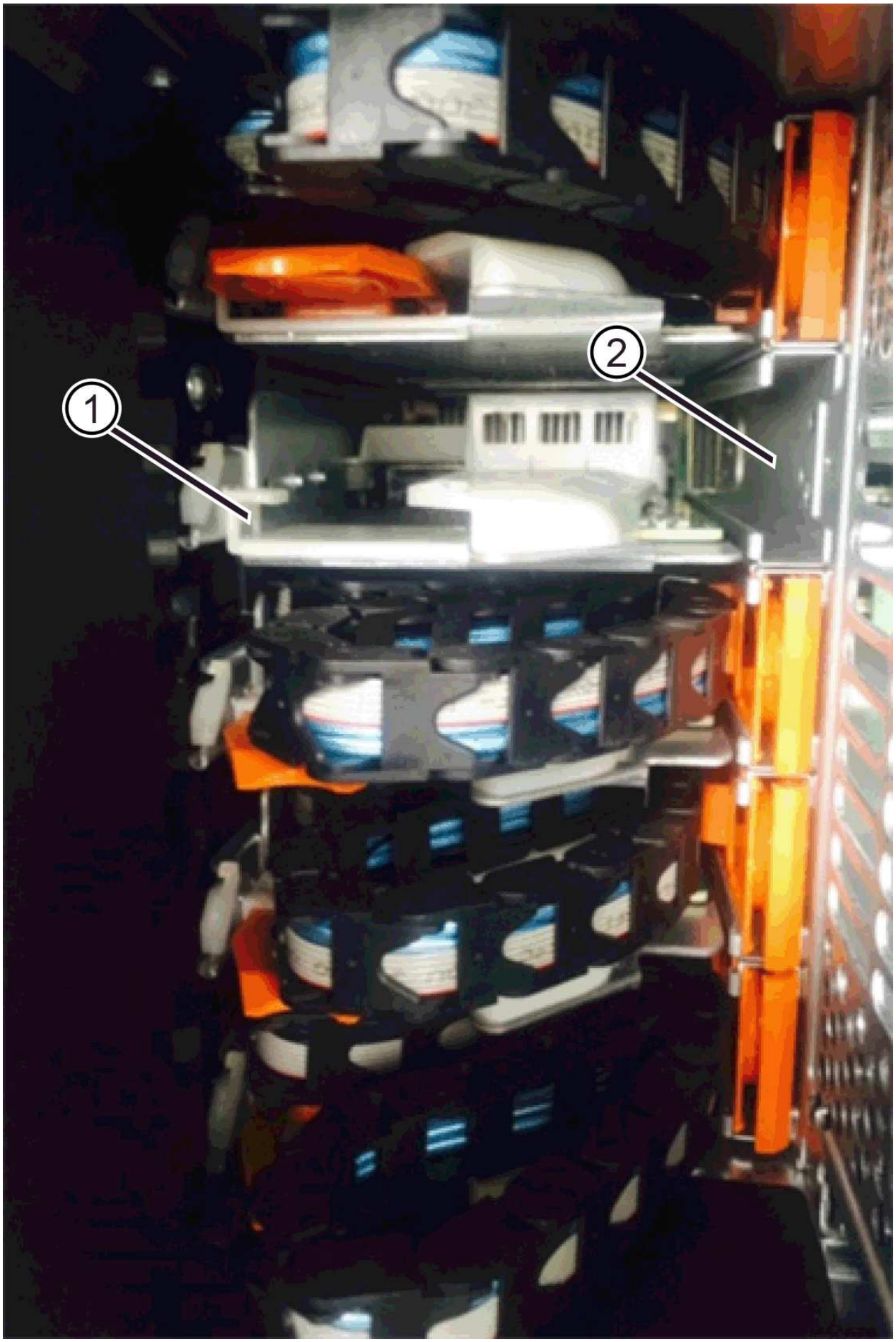
1. Assicurarsi che:
   - È stato installato un nuovo cassetto unità.
   - Sono presenti due catene di cavi sostitutive, contrassegnate come SINISTRA e DESTRA (sul connettore orizzontale accanto al cassetto dell'unità).
2. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola sul lato destro e metterlo da parte.
3. Se lo shelf è acceso, assicurarsi che la ventola sinistra sia alla massima velocità.

   Possibili danni all'apparecchiatura dovuti al surriscaldamento — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

4. Collegare la catena di cavi corretta:
   a. Individuare i connettori orizzontali e verticali sulla catena destra e la guida orizzontale e verticale corrispondenti all'interno del contenitore.
   b. Allineare entrambi i connettori delle catene di cavi con le guide corrispondenti.
   c. Far scorrere il connettore orizzontale della catena di cavi sulla guida orizzontale e spingerlo fino in fondo.

      Rischio di malfunzionamento dell'apparecchiatura — assicurarsi di far scorrere il connettore nella guida. Se il connettore si trova sulla parte superiore della guida, potrebbero verificarsi problemi quando il sistema è in funzione.

      La figura mostra le guide orizzontali e verticali per il secondo cassetto del disco nel contenitore.


1
2

(1) *guida orizzontale*

(2) *guida verticale*

a. Far scorrere il connettore verticale sulla catena portacavi destra nella guida verticale.

b. Dopo aver ricollegato entrambe le estremità della catena, tirare con cautela la catena per verificare che entrambi i connettori siano bloccati.

> **Rischio di malfunzionamento dell'apparecchiatura** — se i connettori non sono bloccati, la catena dei cavi potrebbe allentarsi durante il funzionamento del cassetto.

5. Rimontare il filtro a carboni attivi della ventola lato destro. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola sia spento e che l'aria stia uscendo dal retro.

   Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola mentre la ventola si trova alla velocità corretta.

6. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola sul lato sinistro dello shelf.
7. Se lo shelf è acceso, assicurarsi che la ventola giusta passi alla velocità massima.

> **Possibili danni all'apparecchiatura dovuti al surriscaldamento** — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

8. Ricollegare la catena del cavo sinistro:

   a. Individuare i connettori orizzontali e verticali sulla catena dei cavi e le relative guide orizzontali e verticali all'interno del contenitore.

   b. Allineare entrambi i connettori delle catene di cavi con le guide corrispondenti.

   c. Far scorrere il connettore orizzontale della catena nella guida orizzontale e spingerlo fino in fondo.

   > **Rischio di malfunzionamento dell'apparecchiatura** — assicurarsi di far scorrere il connettore all'interno della guida. Se il connettore si trova sulla parte superiore della guida, potrebbero verificarsi problemi quando il sistema è in funzione.

   d. Far scorrere il connettore verticale sulla catena sinistra nella guida verticale.

   e. Dopo aver ricollegato entrambe le estremità della catena, tirare con cautela la catena per verificare che entrambi i connettori siano bloccati.

   > **Rischio di malfunzionamento dell'apparecchiatura** — se i connettori non sono bloccati, la catena dei cavi potrebbe allentarsi durante il funzionamento del cassetto.

9. Rimontare il filtro a carboni attivi della ventola lato sinistro. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola sia spento e che l'aria stia uscendo dal retro.

   Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

Fase 6: Sostituzione completa del cassetto dell'unità

Reinserire le unità e riposizionare il pannello anteriore nell'ordine corretto.

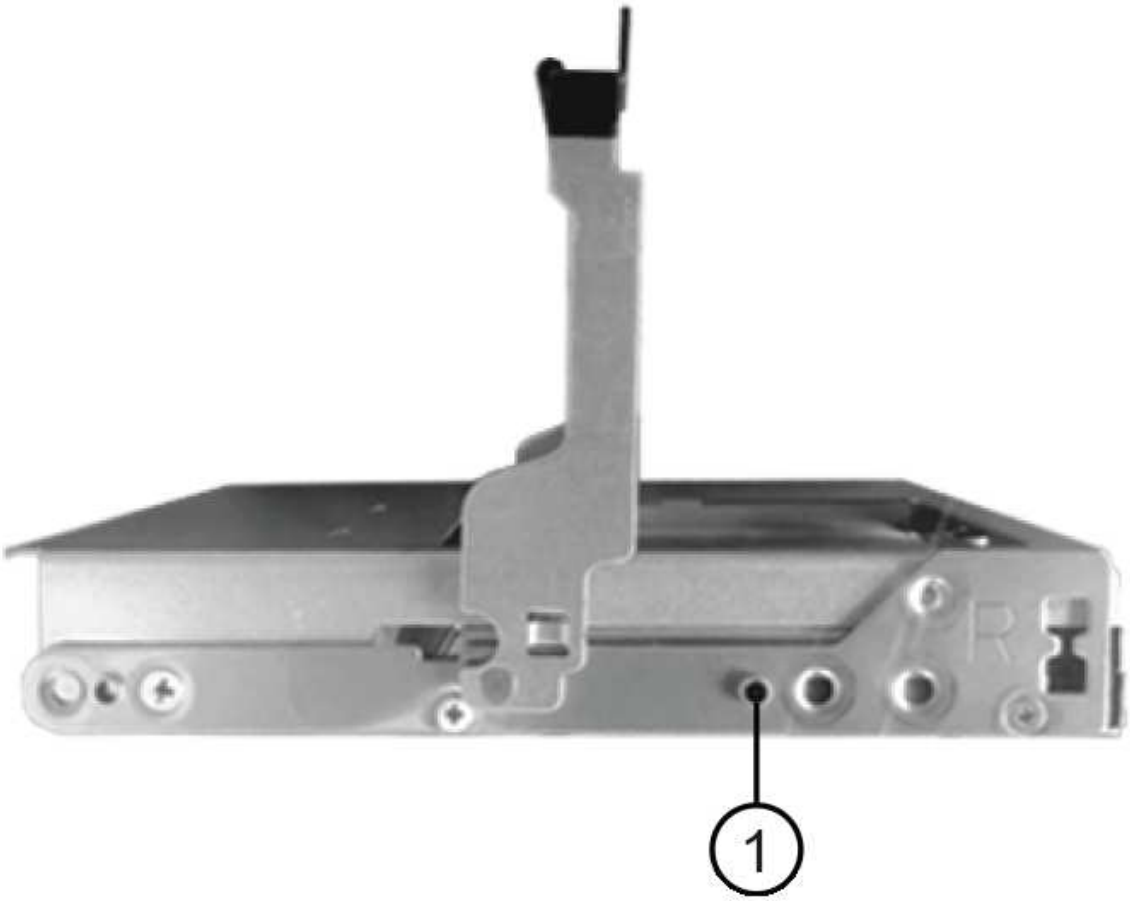
> **Possibile perdita di accesso ai dati** — è necessario installare ciascun disco nella posizione originale nel cassetto.

Fasi

1. Assicurarsi che:
   - Sai dove installare ogni disco.
   - Il cassetto dell'unità è stato sostituito.
   - I nuovi cavi del cassetto sono stati installati.
2. Reinstallare le unità nel cassetto:
   a. Sbloccare il cassetto dell'unità estraendo entrambe le leve nella parte anteriore del cassetto.
   b. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta. Non rimuovere completamente il cassetto dal ripiano del disco.
   c. Determinare il disco da installare in ogni slot utilizzando le note create durante la rimozione dei dischi.

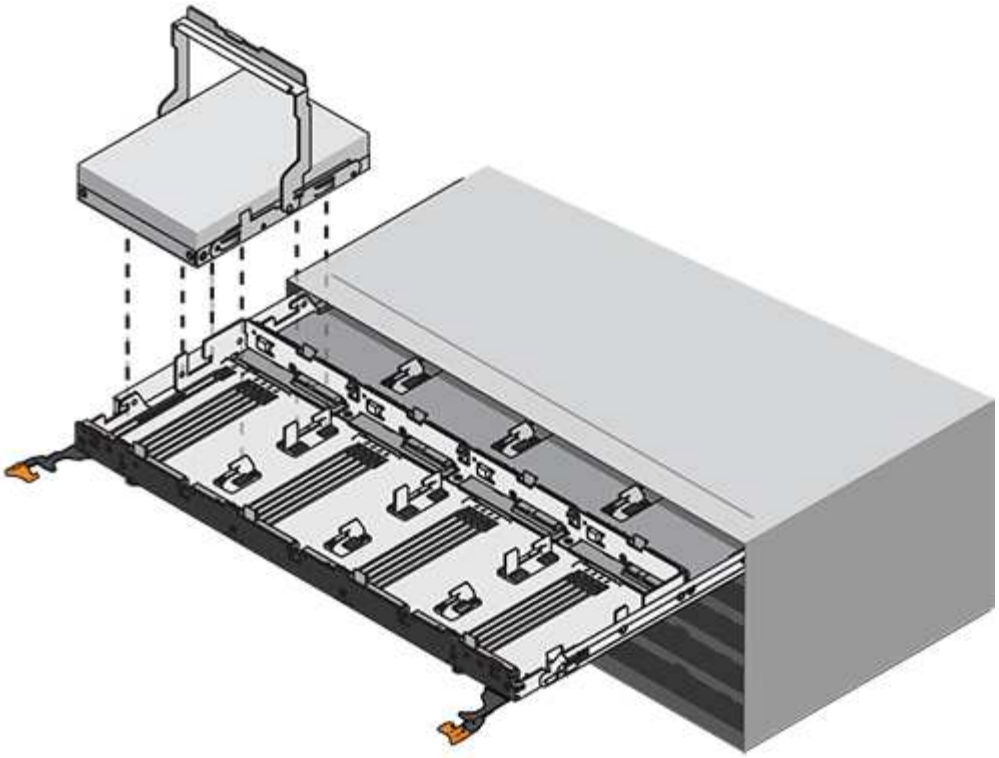
   d. Sollevare la maniglia dell'unità in verticale.
   e. Allineare i due pulsanti rialzati su ciascun lato dell'unità con le tacche del cassetto.

      La figura mostra la vista laterale destra di un'unità, che mostra la posizione dei pulsanti sollevati.



(1) *pulsante sollevato sul lato destro del disco*

a. Abbassare l'unità, accertandosi che sia premuta fino in fondo nell'alloggiamento, quindi ruotare la maniglia dell'unità verso il basso fino a farla scattare in posizione.



b. Ripetere questa procedura per installare tutti i dischi.

3. Far scorrere nuovamente il cassetto nello shelf dell'unità spingendolo dal centro e chiudendo entrambe le leve.

> **Rischio di malfunzionamento dell'apparecchiatura** — assicurarsi di chiudere completamente il cassetto dell'unità premendo entrambe le leve. Chiudere completamente il cassetto dell'unità per consentire un flusso d'aria adeguato ed evitare il surriscaldamento.

4. Fissare il pannello frontale alla parte anteriore dello shelf del disco.
5. Se uno o più shelf sono stati spenti, riapplicare l'alimentazione utilizzando una delle seguenti procedure:
   - *Se è stato sostituito un cassetto dischi in uno shelf* ***controller*** *senza protezione perdita cassetto*:
     i. Accendere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere 10 minuti per il completamento del processo di accensione. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.
   - *Se è stato sostituito un cassetto dischi in uno shelf di dischi* ***espansione*** *senza protezione perdita cassetto*:
     i. Accendere entrambi gli interruttori di alimentazione sullo shelf di dischi.
     ii. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.
     iii. Attendere due minuti prima di alimentare lo shelf del controller.
     iv. Accendere entrambi gli interruttori di alimentazione sullo shelf del controller.
     v. Attendere 10 minuti per il completamento del processo di accensione. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.

Quali sono le prossime novità?

La sostituzione del cassetto dell'unità è stata completata. È possibile riprendere le normali operazioni.

Aggiunta a caldo di uno shelf di dischi

È possibile aggiungere un nuovo shelf di dischi mentre gli altri componenti del sistema di storage sono ancora in funzione. È possibile configurare, riconfigurare, aggiungere o spostare la capacità del sistema storage senza interrompere l'accesso degli utenti ai dati.

Prima di iniziare

A causa della complessità di questa procedura, si consiglia quanto segue:

- Leggere tutti i passaggi prima di iniziare la procedura.
- Assicurarsi che l'aggiunta a caldo di uno shelf di dischi sia la procedura necessaria.

A proposito di questa attività

Questa procedura si applica all'aggiunta a caldo di uno shelf di dischi DE212C, DE224C o DE460C a E2800, E2800, EF280, E5700, E5700B, Shelf di controller EF570, EF300 o EF600.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

> Per mantenere l'integrità del sistema, seguire la procedura esattamente nell'ordine suggerito.

Fase 1: Preparazione all'aggiunta dello shelf di dischi

Per prepararsi all'aggiunta a caldo di uno shelf di dischi, è necessario verificare la presenza di eventi critici e lo stato degli IOM.

Prima di iniziare

- La fonte di alimentazione del sistema storage deve essere in grado di soddisfare i requisiti di alimentazione del nuovo shelf di dischi. Per le specifiche di alimentazione dello shelf di dischi, consultare "Hardware Universe".
- Lo schema di cablaggio per il sistema storage esistente deve corrispondere a uno degli schemi applicabili illustrati in questa procedura.

Fasi

1. In Gestore di sistema di SANtricity, selezionare **supporto** > **Centro di supporto** > **Diagnostica**.
2. Selezionare **Collect Support Data**.

   Viene visualizzata la finestra di dialogo Collect Support Data (raccolta dati di supporto).

3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome support-data.7z. I dati non vengono inviati automaticamente al supporto tecnico.

4. Selezionare **supporto** > **Registro eventi**.

   La pagina Registro eventi visualizza i dati dell'evento.

5. Selezionare l'intestazione della colonna **priorità** per ordinare gli eventi critici all'inizio dell'elenco.
6. Esaminare gli eventi critici di sistema per gli eventi che si sono verificati nelle ultime due o tre settimane e verificare che gli eventi critici recenti siano stati risolti o altrimenti risolti.

   > Se si sono verificati eventi critici non risolti nelle due o tre settimane precedenti, interrompere la procedura e contattare il supporto tecnico. Continuare la procedura solo dopo aver risolto il problema.

7. Selezionare **hardware**.
8. Selezionare l'icona **IOM (ESM)**.

   Viene visualizzata la finestra di dialogo Shelf Component Settings (Impostazioni componenti shelf) con la scheda **IOM (ESM)** selezionata.

9. Assicurarsi che lo stato visualizzato per ogni IOM/ESM sia *ottimale*.
10. Fare clic su **Mostra altre impostazioni**.
11. Verificare che sussistano le seguenti condizioni:
    - Il numero di ESM/IOM rilevati corrisponde al numero di ESM/IOM installati nel sistema e a quello di ogni shelf di dischi.
    - Entrambi gli ESM/IOM mostrano che la comunicazione è corretta.
    - La velocità di trasferimento dati è di 12 GB/s per gli shelf di dischi DE212C, DE224C e DE460C o di 6 GB/s per gli altri tray di dischi.

Fase 2: Installare lo shelf di dischi e alimentare

Si installa un nuovo shelf di dischi o uno shelf di dischi precedentemente installato, si accende l'alimentazione e si verifica la presenza di eventuali LED che richiedono attenzione.

Fasi

1. Se si sta installando uno shelf di dischi precedentemente installato in un sistema storage, rimuovere i dischi. I dischi devono essere installati uno alla volta più avanti in questa procedura.

   Se la cronologia di installazione dello shelf di dischi che si sta installando non è nota, si deve presumere che sia stato precedentemente installato in un sistema storage.

2. Installare lo shelf di dischi nel rack che contiene i componenti del sistema di storage.

> Consultare le istruzioni di installazione del modello in uso per la procedura completa per l'installazione fisica e il cablaggio di alimentazione. Le istruzioni di installazione del modello in uso includono note e avvisi da tenere in considerazione per installare in sicurezza uno shelf di dischi.

3. Accendere il nuovo shelf di dischi e verificare che sullo shelf non siano accesi LED di attenzione color ambra. Se possibile, risolvere eventuali condizioni di guasto prima di continuare con questa procedura.

Fase 3: Collegare il sistema via cavo

Selezionare una delle seguenti opzioni:

- Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700
- Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

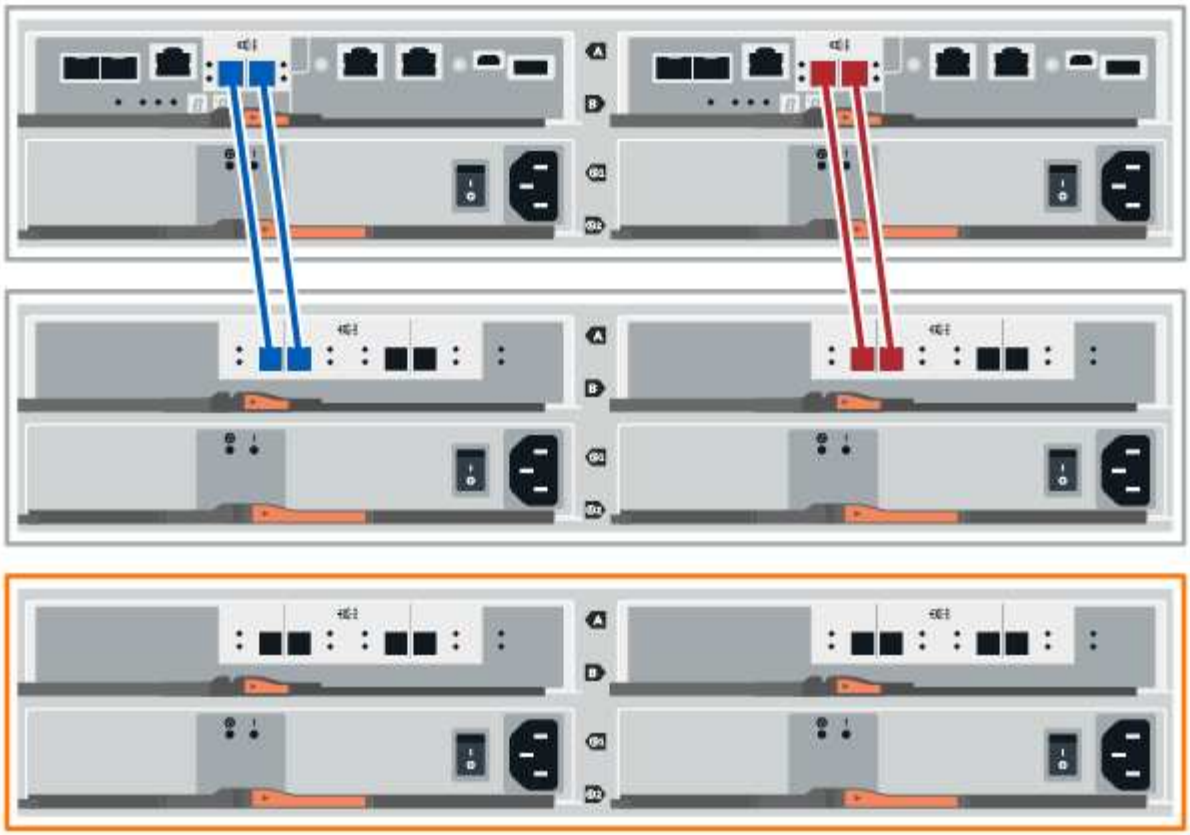
Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700

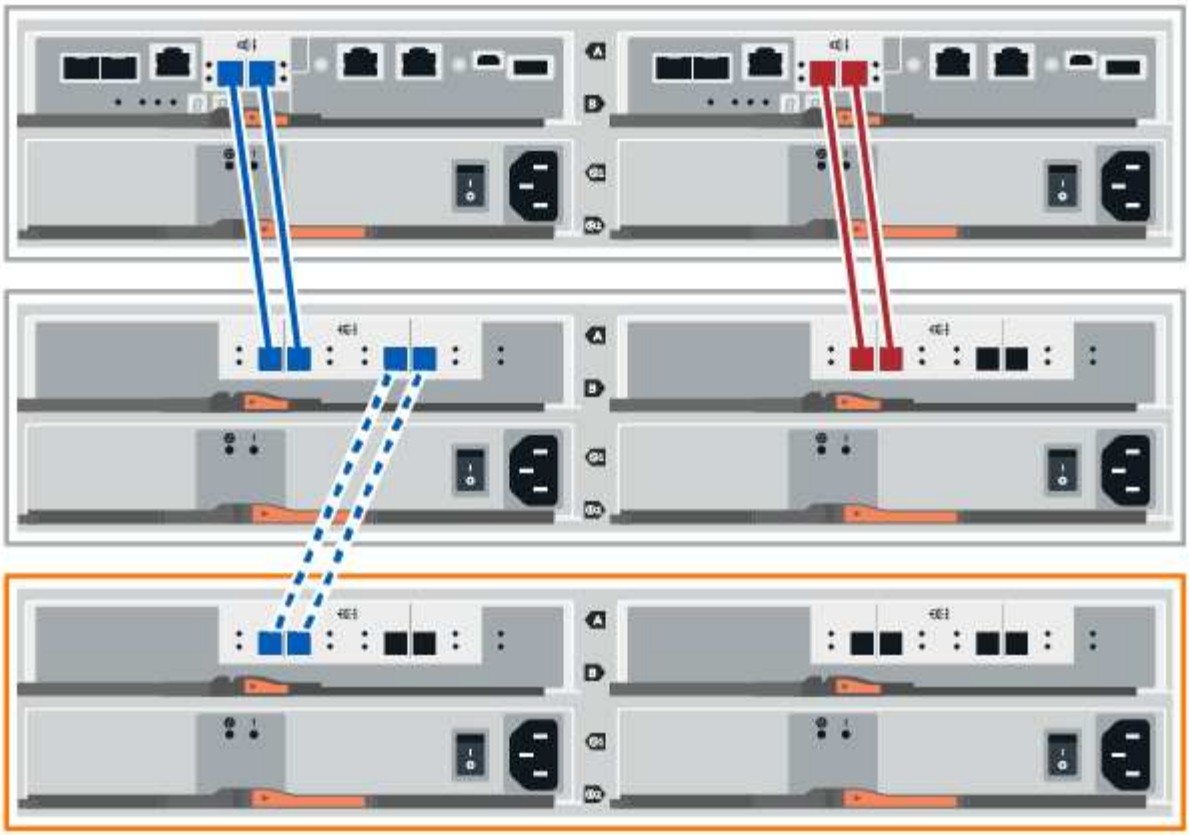
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Fasi

1. Collegare lo shelf di dischi al controller A.

   La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller A. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".





2. In Gestione sistema di SANtricity, fare clic su **hardware**.

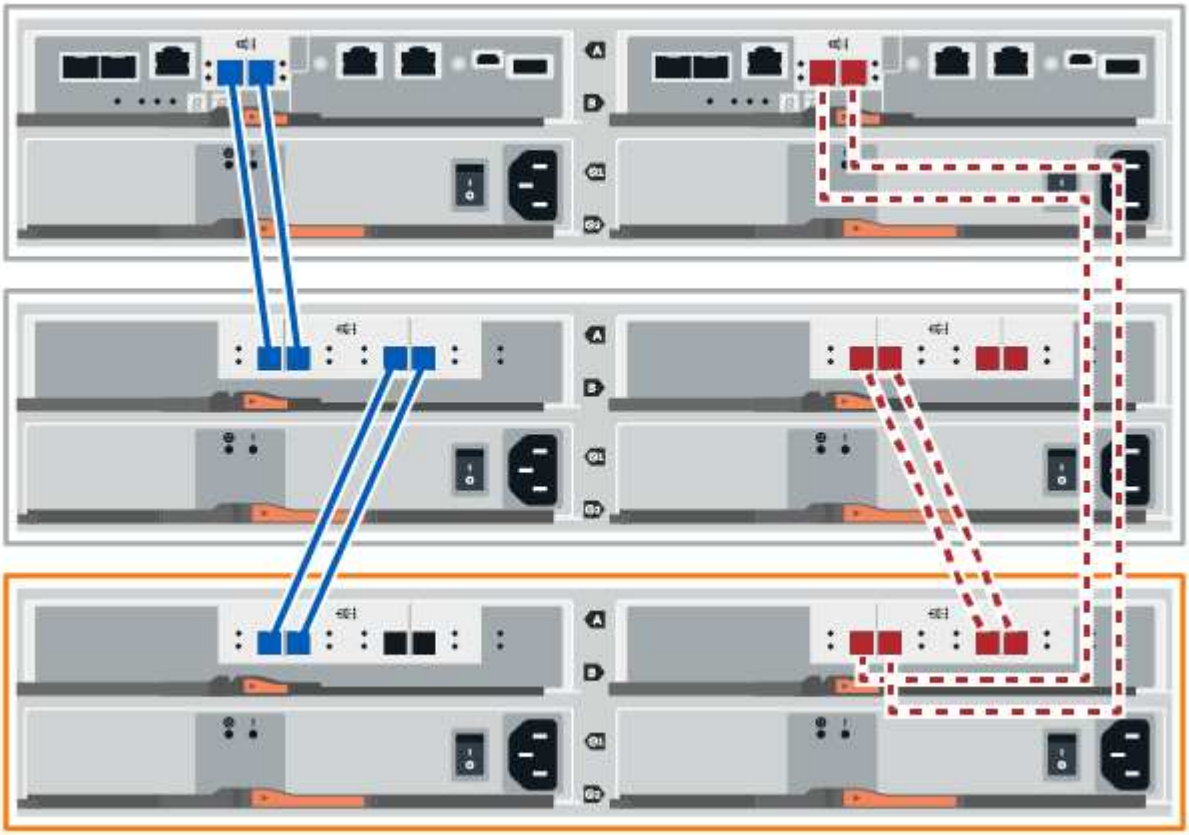
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

3. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
4. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

   Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

5. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
6. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
7. Scollegare tutti i cavi di espansione dal controller B.
8. Collegare lo shelf di dischi al controller B.

La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller B. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



9. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

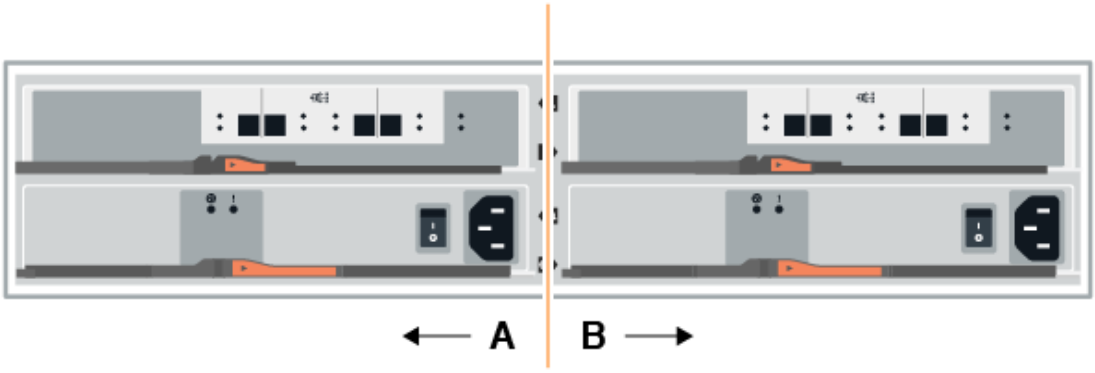
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Prima di iniziare

- Il firmware è stato aggiornato alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".

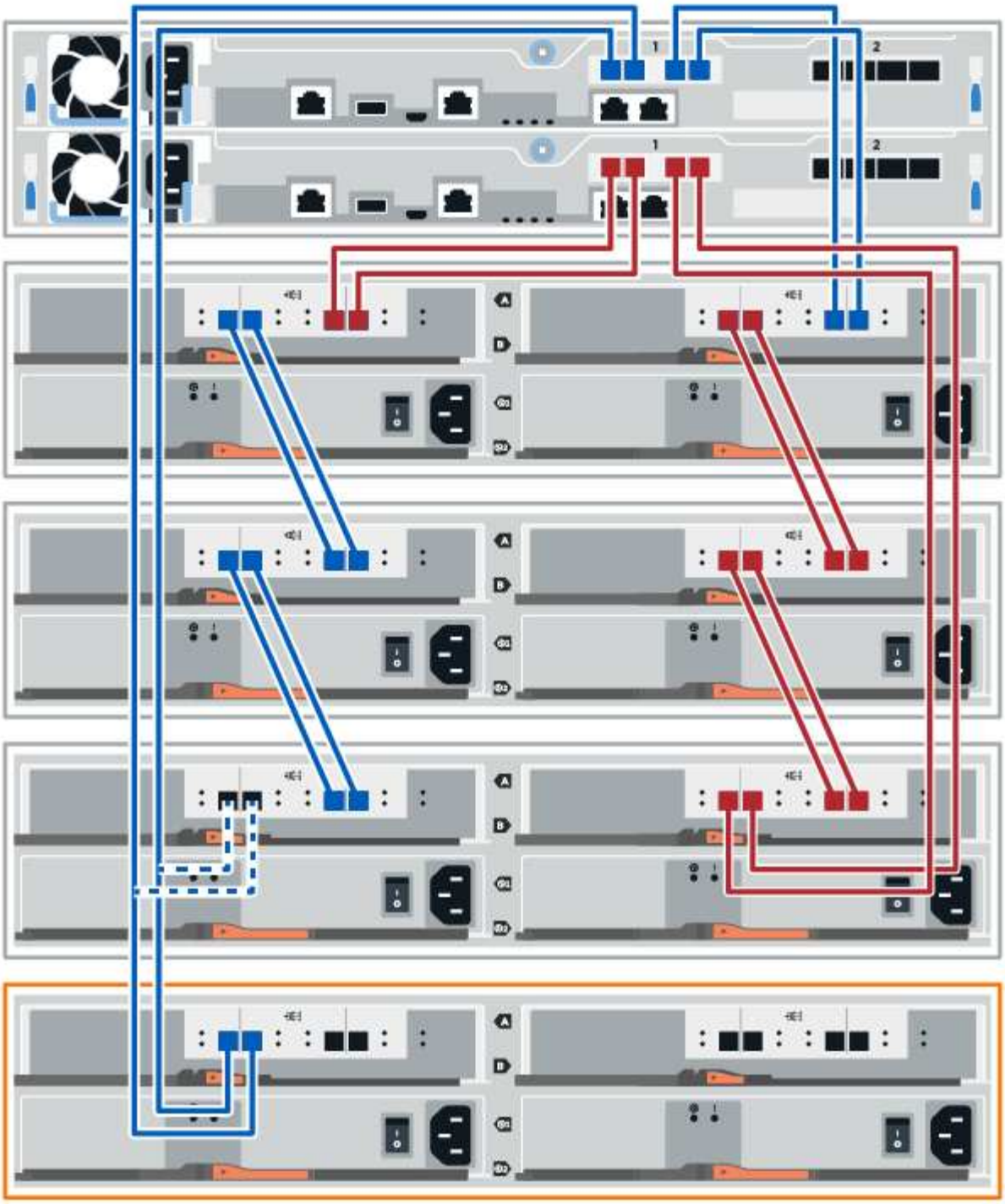
Fasi

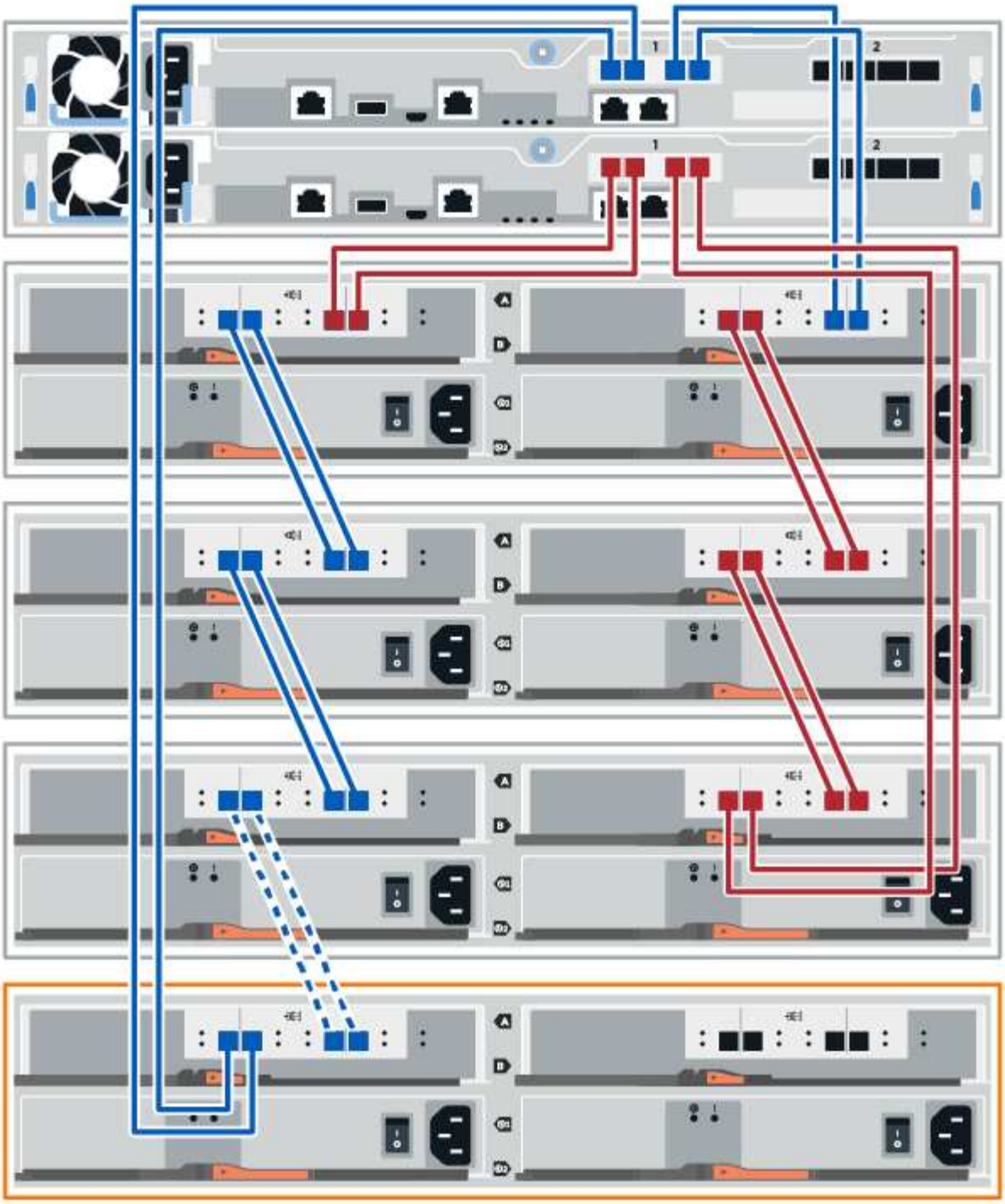
1. Scollegare entrambi i cavi del controller Lato A dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.



2. Collegare i cavi alle porte IOM12 lato A tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di connessione per un lato tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".


1
2
1
2
A
B



3. In Gestione sistema di SANtricity, fare clic su **hardware**.

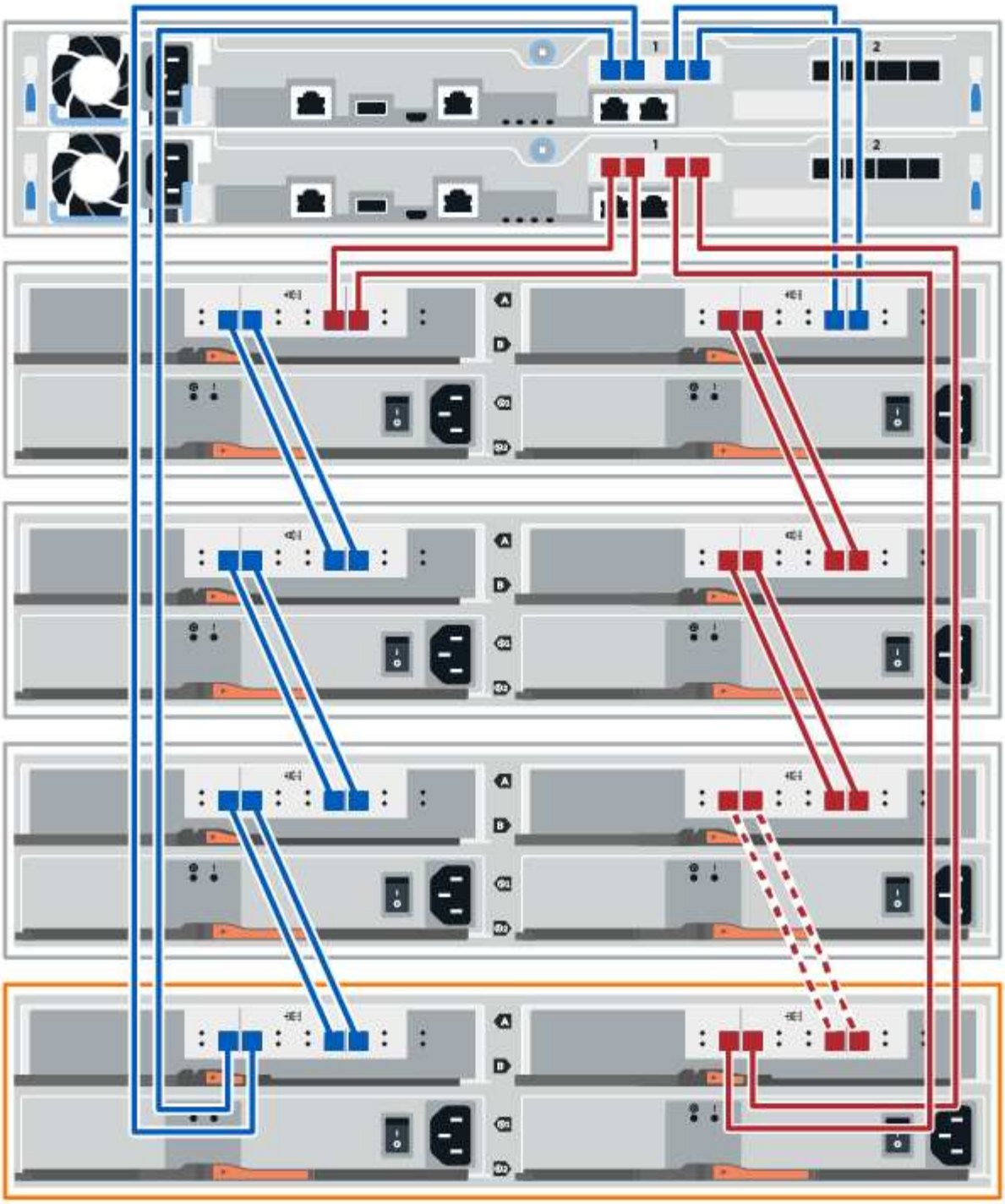
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

4. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
5. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

6. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
7. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
8. Scollegare entrambi i cavi del controller lato B dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.
9. Collegare i cavi alle porte IOM12 lato B tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di collegamento per il lato B tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



10. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Fase 4: Completare l'aggiunta a caldo

Per completare l'aggiunta a caldo, verificare la presenza di eventuali errori e confermare che lo shelf di dischi appena aggiunto utilizzi il firmware più recente.

Fasi

1. In Gestore di sistema di SANtricity, fare clic su **Home**.
2. Se il collegamento **Recover from Problems** (Ripristina da problemi) viene visualizzato al centro della pagina, fare clic sul collegamento e risolvere eventuali problemi indicati nel Recovery Guru.
3. In Gestione sistema di SANtricity, fare clic su **hardware** e scorrere verso il basso, se necessario, per visualizzare lo shelf di dischi appena aggiunto.
4. Per i dischi precedentemente installati in un sistema storage diverso, aggiungere un disco alla volta allo shelf di dischi appena installato. Attendere che ogni disco venga riconosciuto prima di inserire il disco successivo.

   Quando un disco viene riconosciuto dal sistema di storage, la rappresentazione dello slot nella pagina **hardware** viene visualizzata come un rettangolo blu.

5. Selezionare la scheda **Support** > **Support Center** > **Support Resources**.
6. Fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware) e verificare quali versioni del firmware IOM/ESM e del firmware del disco sono installate sul nuovo shelf di dischi.

   > Potrebbe essere necessario scorrere la pagina verso il basso per individuare questo collegamento.

7. Se necessario, aggiornare il firmware del disco.

   Il firmware IOM/ESM viene aggiornato automaticamente alla versione più recente, a meno che non sia stata disattivata la funzione di aggiornamento.

La procedura di aggiunta a caldo è stata completata. È possibile riprendere le normali operazioni.

Schede di interfaccia host

Requisiti per la sostituzione HIC E2800

Prima di aggiungere, aggiornare o sostituire una scheda di interfaccia host (HIC) in un E2800, esaminare i requisiti e le considerazioni.

Panoramica della procedura

La procedura per sostituire un HIC dipende dal fatto che si disponga di uno o due controller, come segue:

Se lo storage array dispone di…	Devi…
Un controller (E2812 o E2824 simplex)	1. Interrompere le operazioni di i/o dell'host 2. Spegnere lo shelf del controller 3. Rimuovere il contenitore del controller 4. Sostituire la batteria 5. Sostituire il contenitore del controller 6. Alimentare lo shelf del controller
Due controller (duplex E2860, E2812 o E2824)	1. Portare il controller offline 2. Rimuovere il contenitore del controller 3. Sostituire la batteria 4. Sostituire il contenitore del controller 5. Portare il controller online

Requisiti per l'aggiunta, l'aggiornamento o la sostituzione di un HIC

Se si intende aggiungere, aggiornare o sostituire una scheda di interfaccia host (HIC), tenere presenti i seguenti requisiti.

- È stata pianificata una finestra di manutenzione dei downtime per questa procedura. Quando si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).
- Si dispone di uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve essere compatibile con i controller.

  Se si dispone di una configurazione duplex (due controller), l'HICS installato nei due contenitori del controller deve essere identico. La presenza di HICS non corrispondenti causa il blocco del controller con l'HIC sostitutivo quando lo si porta online.

- Sono disponibili tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host Bus Adapter) necessari per collegare le nuove porte host.

  Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Hai un cacciavite Phillips n. 1.
- Sono presenti etichette per identificare ciascun cavo collegato al contenitore del controller.
- Si dispone di una stazione di gestione con un browser in grado di accedere a Gestore di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Aggiunta della scheda di interfaccia host E2800 (HIC)

È possibile aggiungere una scheda di interfaccia host (HIC) ai canister dei controller

E2800 con porte host della scheda base. Questa aggiunta aumenta il numero di porte host nell'array di storage E2800 e fornisce protocolli host aggiuntivi.

A proposito di questa attività

Durante questa procedura, è necessario spegnere lo storage array, installare l'HIC e riapplicare l'alimentazione.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E2800".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).
- Assicurarsi di disporre di quanto segue:
  - Uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve essere compatibile con i controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un cacciavite Phillips n. 1.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Qualsiasi hardware host richiesto installato per le nuove porte host, come switch o HBA (host bus adapter).
  - Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte host.

    Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" e a. "NetApp Hardware Universe".

  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione all'aggiunta di HIC

Preparare l'aggiunta dell'HIC eseguendo il backup del database di configurazione dello storage array, raccogliendo i dati di supporto e interrompendo le operazioni di i/o dell'host. Quindi, è possibile spegnere lo shelf del controller.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

- Da System Manager:
  i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
  ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
  iii. Fare clic su **Collect**.

  Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

- In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

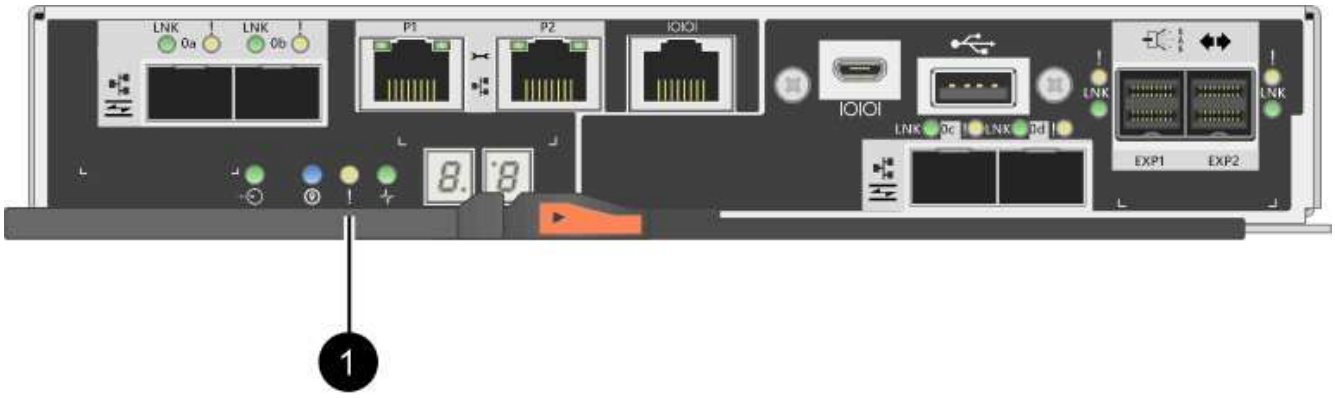
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



(1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
8. Spegnere lo shelf del controller.
   a. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
   b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter aggiungere la nuova scheda di interfaccia host.

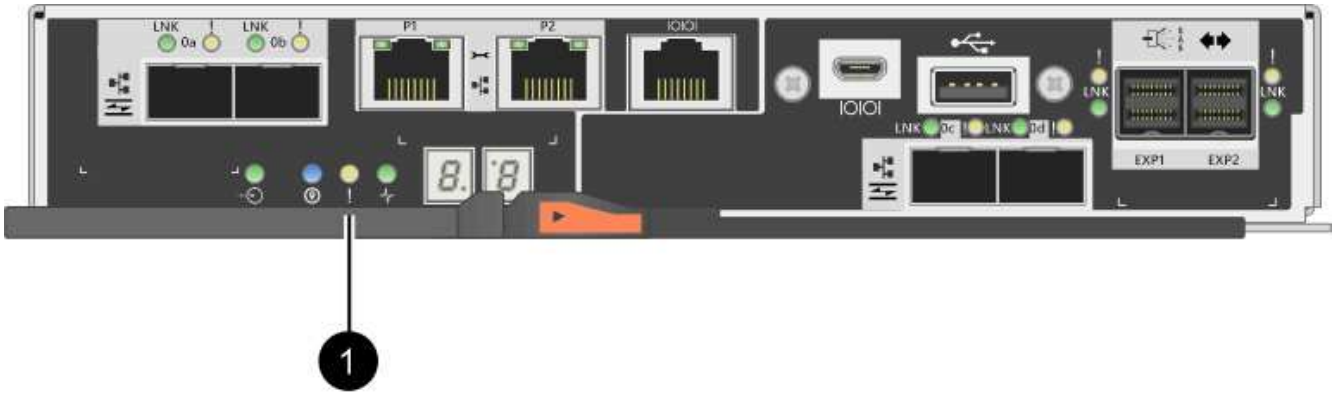
Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

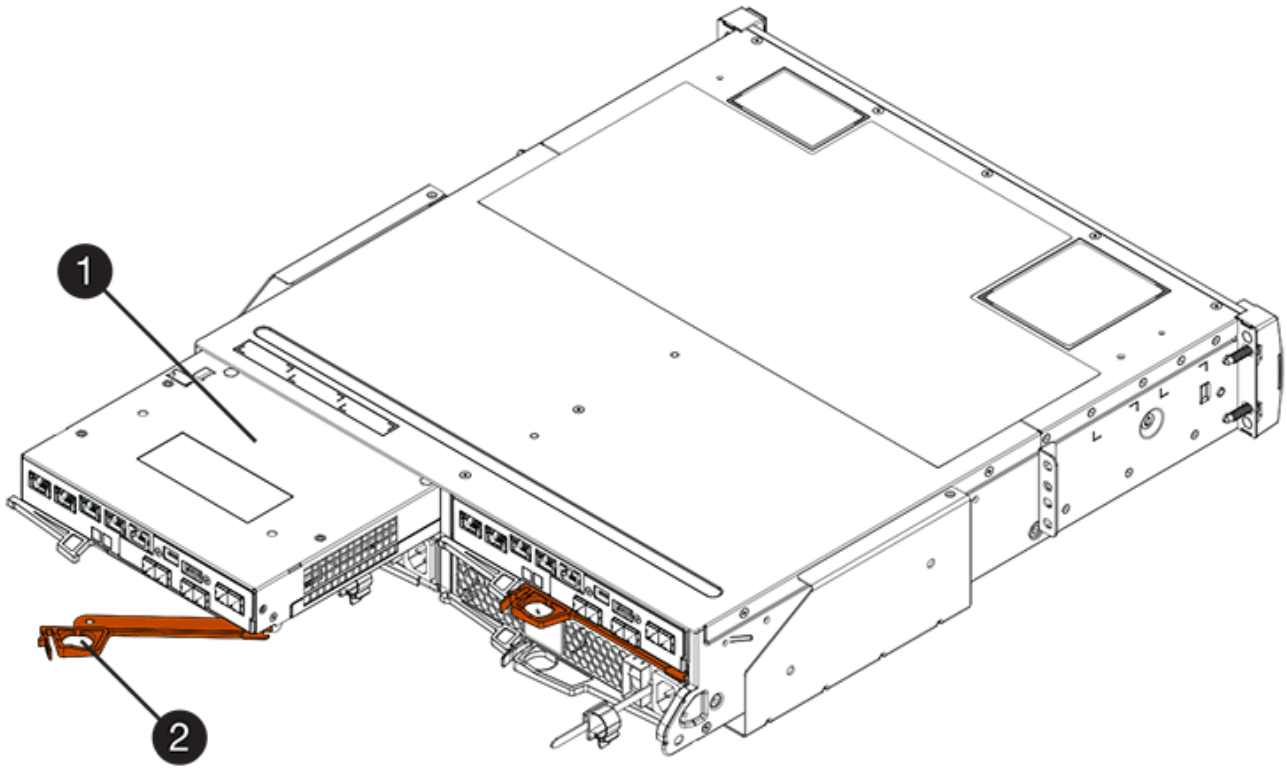
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



(1) *LED cache attiva*

4. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

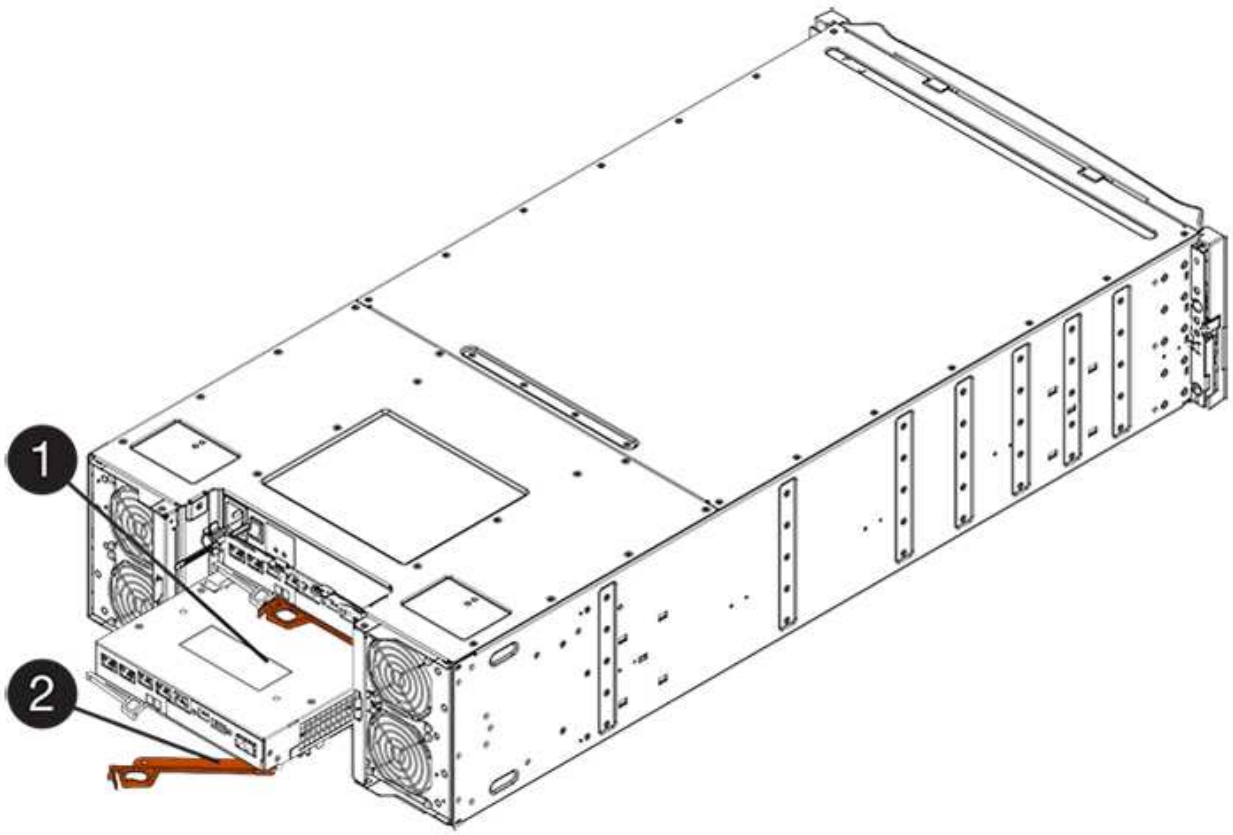
La figura seguente è un esempio di shelf di controller E2812, shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

5. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

6. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Installare l'HIC

Installare l'HIC per aumentare il numero di porte host nell'array di storage.

Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore del controller E2800 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.

2. Premere il pulsante sul coperchio del contenitore del controller ed estrarre il coperchio.
3. Verificare che il LED verde all'interno del controller (accanto ai DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

   (1) *cache interna attiva*

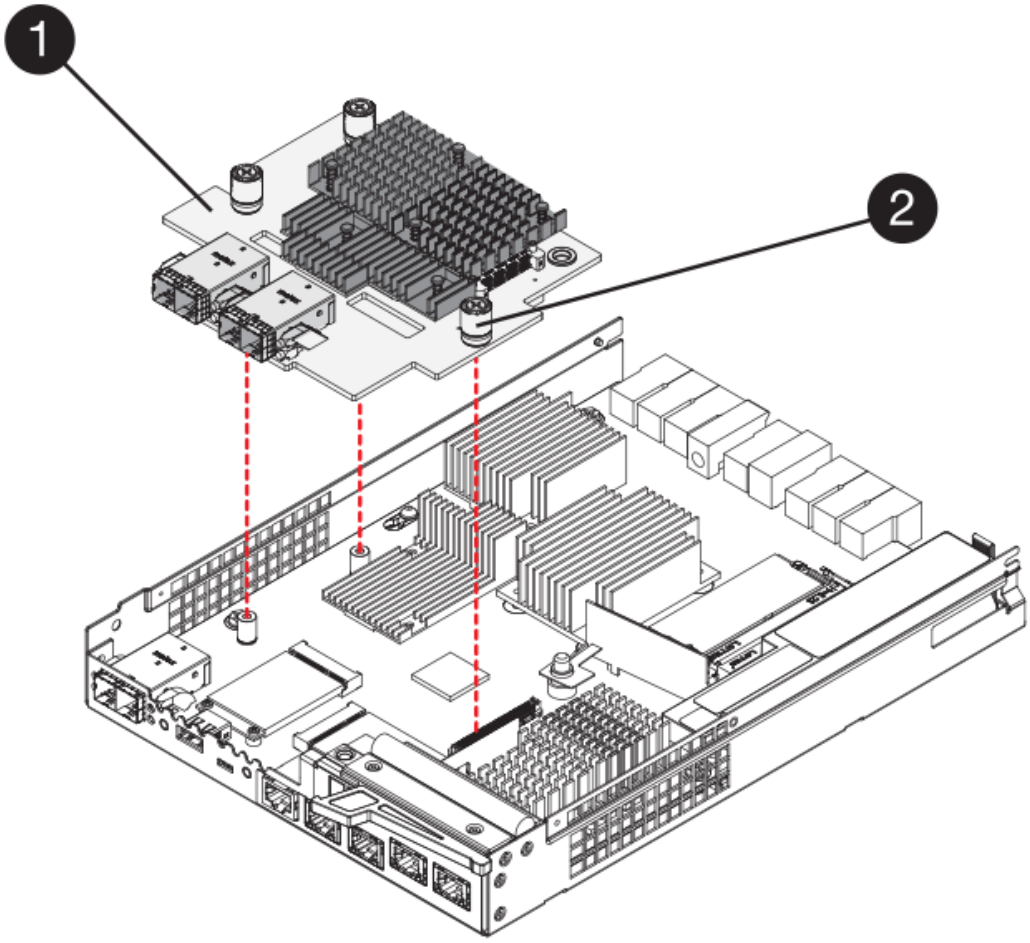
   (2) *batteria*

4. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller, quindi rimuovere la piastra frontale.
5. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

6. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



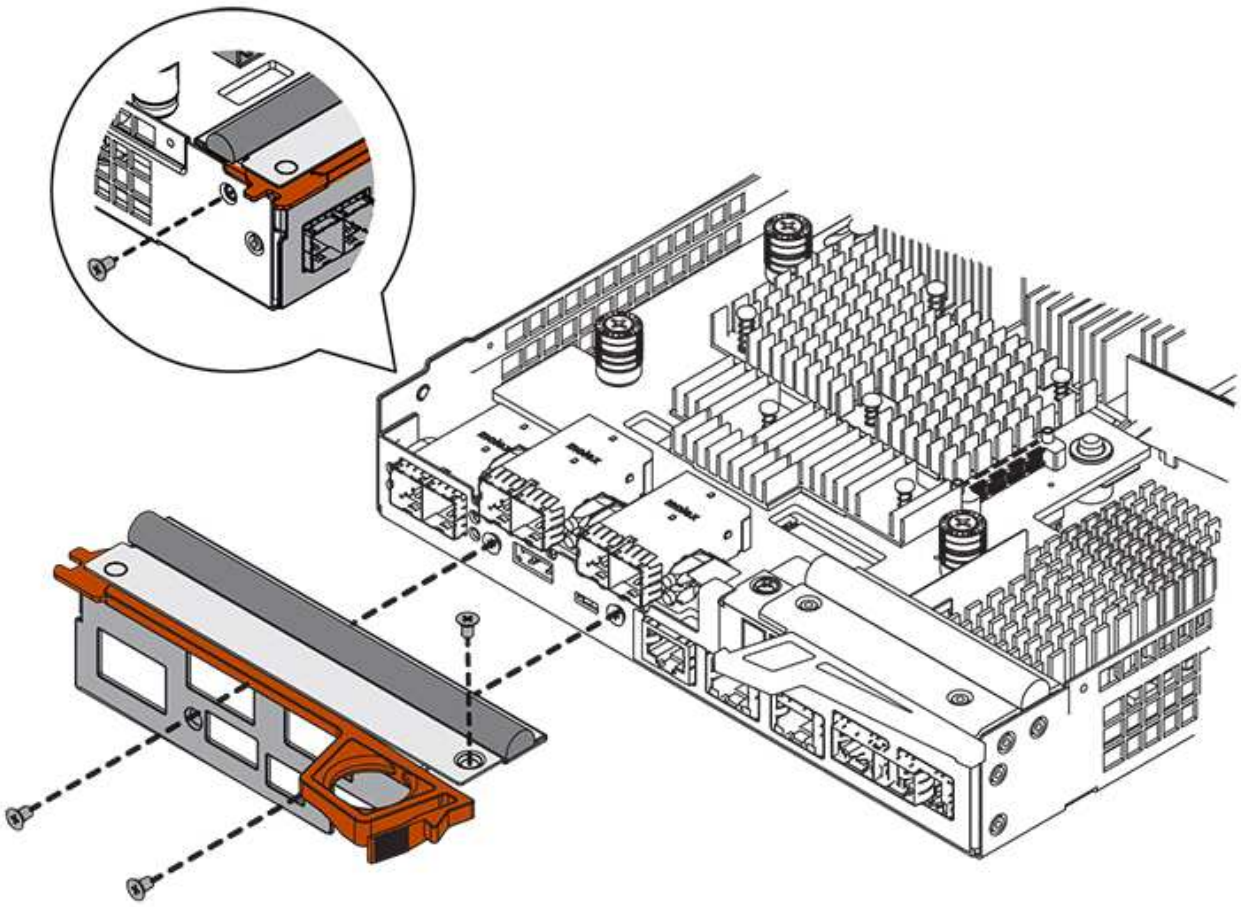
(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

7. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

8. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.



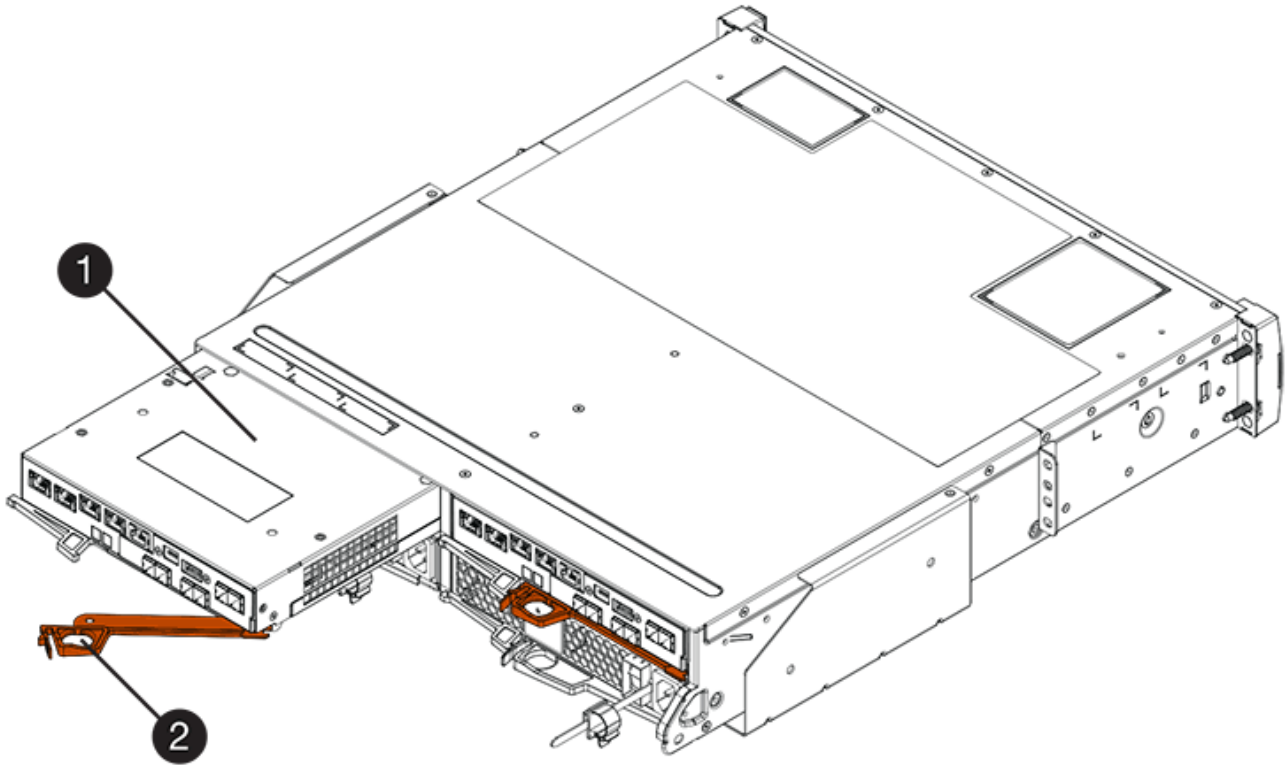
Fase 4: Reinstallare il contenitore del controller

Reinstallare il contenitore del controller nello shelf del controller dopo aver installato il nuovo HIC.

Fasi

1. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
2. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

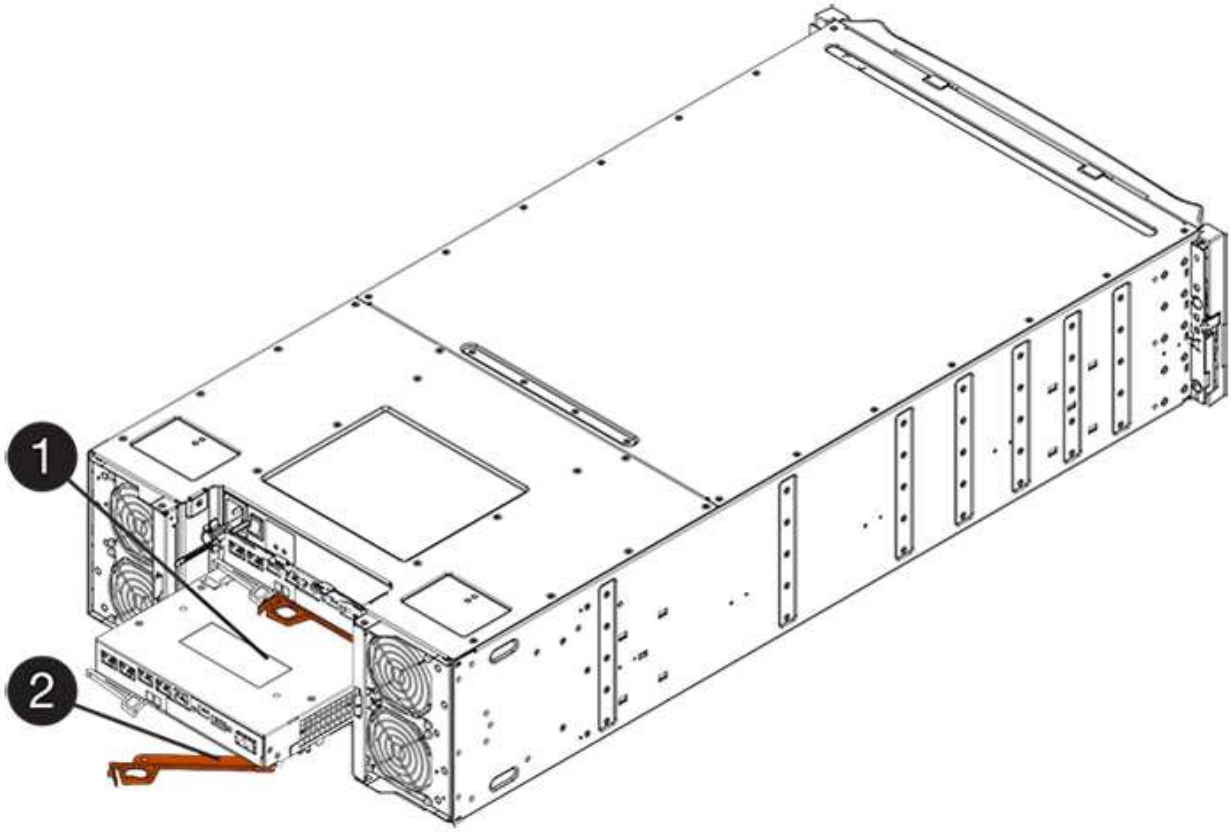
   La figura seguente è un esempio di shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

3. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
4. Ricollegare tutti i cavi rimossi.

> Non collegare i cavi dati alle nuove porte HIC in questo momento.

5. (Facoltativo) se si aggiunge HICS a una configurazione duplex, ripetere tutti i passaggi per rimuovere il secondo elemento filtrante del controller, installare il secondo HIC e reinstallare il secondo elemento filtrante del controller.

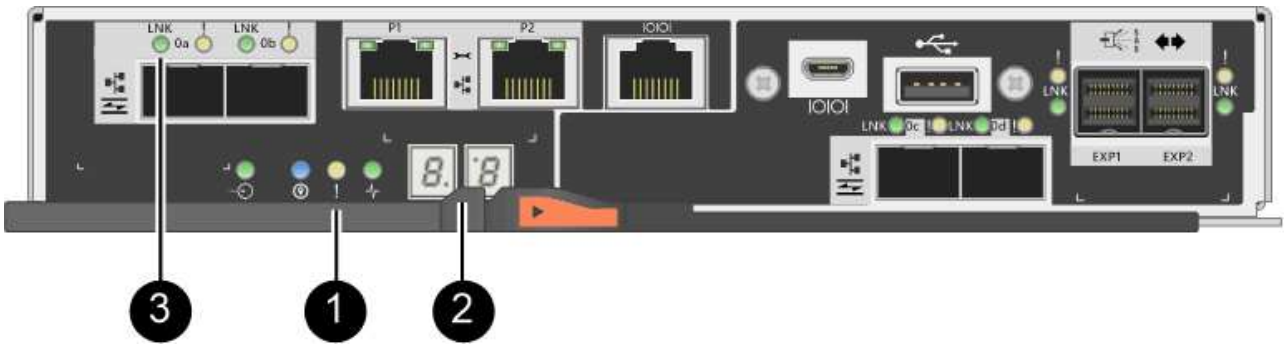
Fase 5: Completare l'aggiunta di HIC

Controllare i LED del controller e il display a sette segmenti, quindi verificare che lo stato del controller sia ottimale.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a sette segmenti dovrebbe visualizzare l'ID del vassoio.
   - Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
   - I LED verdi del collegamento host rimangono spenti fino a quando non si collegano i cavi host.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

3. Da Gestore di sistema di SANtricity, verificare che lo stato del controller sia ottimale.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se le nuove porte HIC richiedono ricetrasmettitori SFP+, installarli.
5. Se è stato installato un HIC con porte SFP+ (ottiche), verificare che le nuove porte dispongano del protocollo host previsto.
   a. Da Gestione sistema di SANtricity, selezionare **hardware**.
   b. Se la figura mostra i dischi, fare clic su **Mostra retro dello shelf**.
   c. Selezionare l'immagine per Controller A o Controller B.
   d. Selezionare **Visualizza impostazioni** dal menu di scelta rapida.
   e. Selezionare la scheda **interfacce host**.
   f. Fare clic su **Mostra altre impostazioni**.
   g. Esaminare i dettagli mostrati per le porte HIC (le porte etichettate **e0*x*** o **0*x*** in posizione HIC **slot 1**) per determinare se si è pronti per collegare le porte host agli host dati:
      - *Se le nuove porte HIC dispongono del protocollo previsto:* si è pronti per collegare le nuove porte HIC agli host dati; passare alla fase successiva.
      - *Se le nuove porte HIC **non** hanno il protocollo previsto:* è necessario applicare un pacchetto di funzionalità software prima di poter collegare le nuove porte HIC agli host dati. Vedere "Modificare il protocollo host per E2800". Quindi, collegare le porte host agli host dati e riprendere le operazioni.
6. Collegare i cavi dalle porte host del controller agli host dati.

   Per istruzioni sulla configurazione e l'utilizzo di un nuovo protocollo host, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Quali sono le prossime novità?

Il processo di aggiunta di una scheda di interfaccia host all'array di storage è completo. È possibile riprendere le normali operazioni.

Upgrade della scheda di interfaccia host (HIC) E2800

È possibile aggiornare una scheda di interfaccia host (HIC) in un array E2800 per aumentare il numero di porte host o modificare i protocolli host.

A proposito di questa attività

Quando si aggiorna l'HICS, è necessario spegnere lo storage array, rimuovere l'HIC esistente da ciascun controller, installare un nuovo HIC e riapplicare l'alimentazione.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E2800".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa

HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).

- Assicurarsi di disporre di quanto segue:
  - Uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve essere compatibile con i controller.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un cacciavite Phillips n. 1.
  - Qualsiasi nuovo hardware host installato per le nuove porte host, come switch o HBA (host bus adapter).
  - Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte host.

    Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione per l'aggiornamento delle schede di interfaccia host

Preparare l'aggiornamento delle schede di interfaccia host (HICS) eseguendo il backup del database di configurazione dello storage array, raccogliendo i dati di supporto e interrompendo le operazioni di i/o host. Quindi, è possibile spegnere lo shelf del controller.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

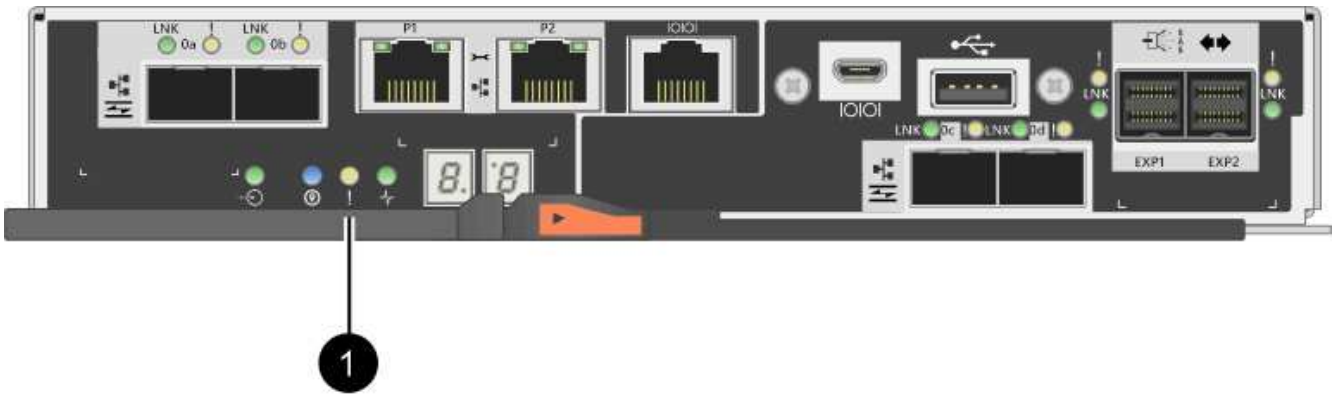
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



(1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
8. Spegnere lo shelf del controller.
   a. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
   b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter aggiornare la nuova scheda di interfaccia host (HIC). Quando si rimuove un contenitore del controller, scollegare tutti i cavi. Quindi, far scorrere il contenitore del controller fuori dallo shelf del controller.

Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

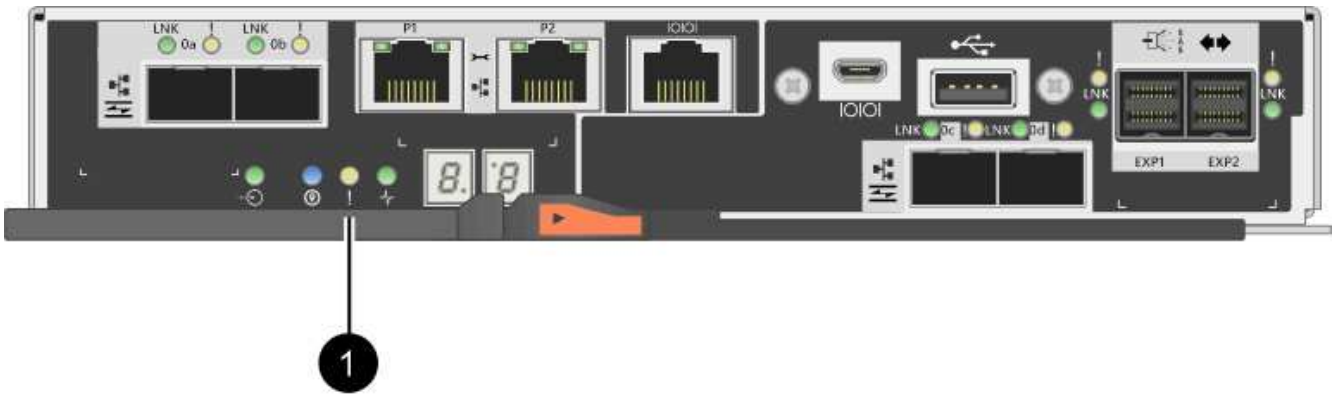
   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Se le porte HIC utilizzano ricetrasmettitori SFP+, rimuoverli.

   A seconda del tipo di HIC a cui si esegue l'aggiornamento, potrebbe essere possibile riutilizzare questi SFP.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

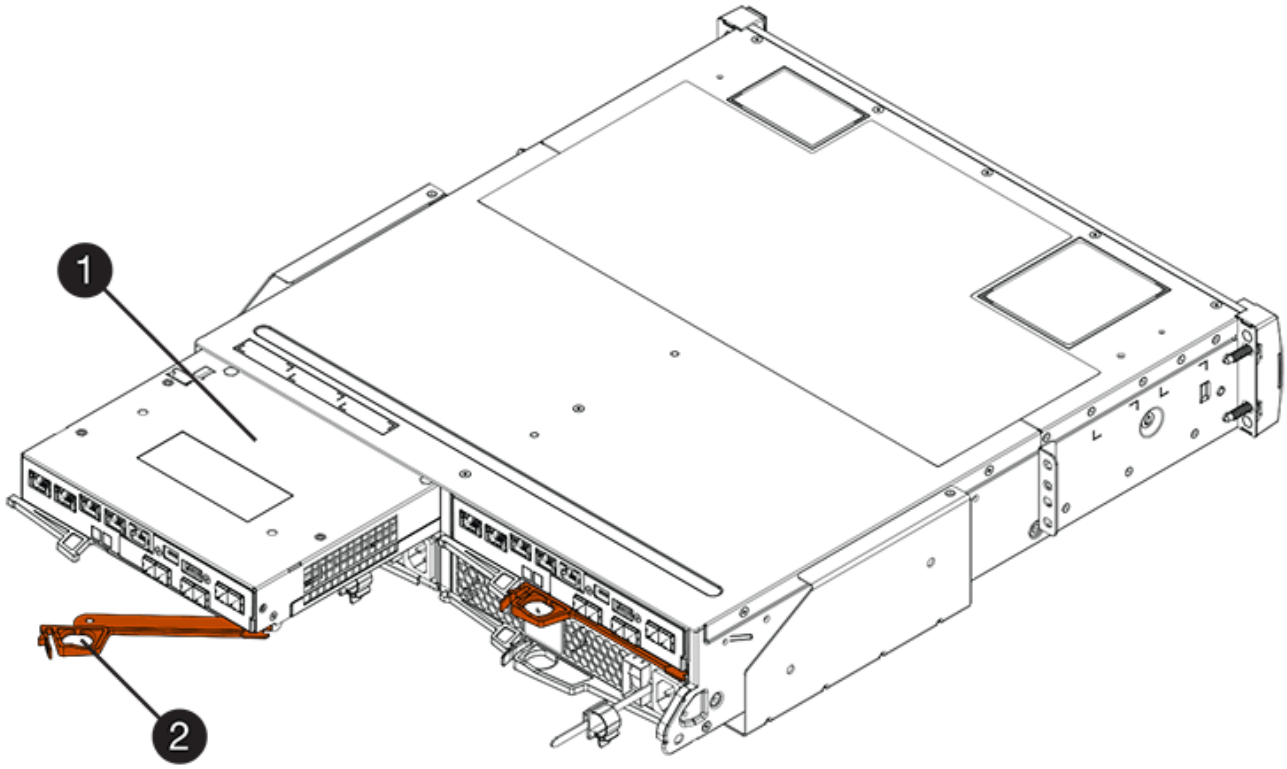
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



(1) *LED cache attiva*

5. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

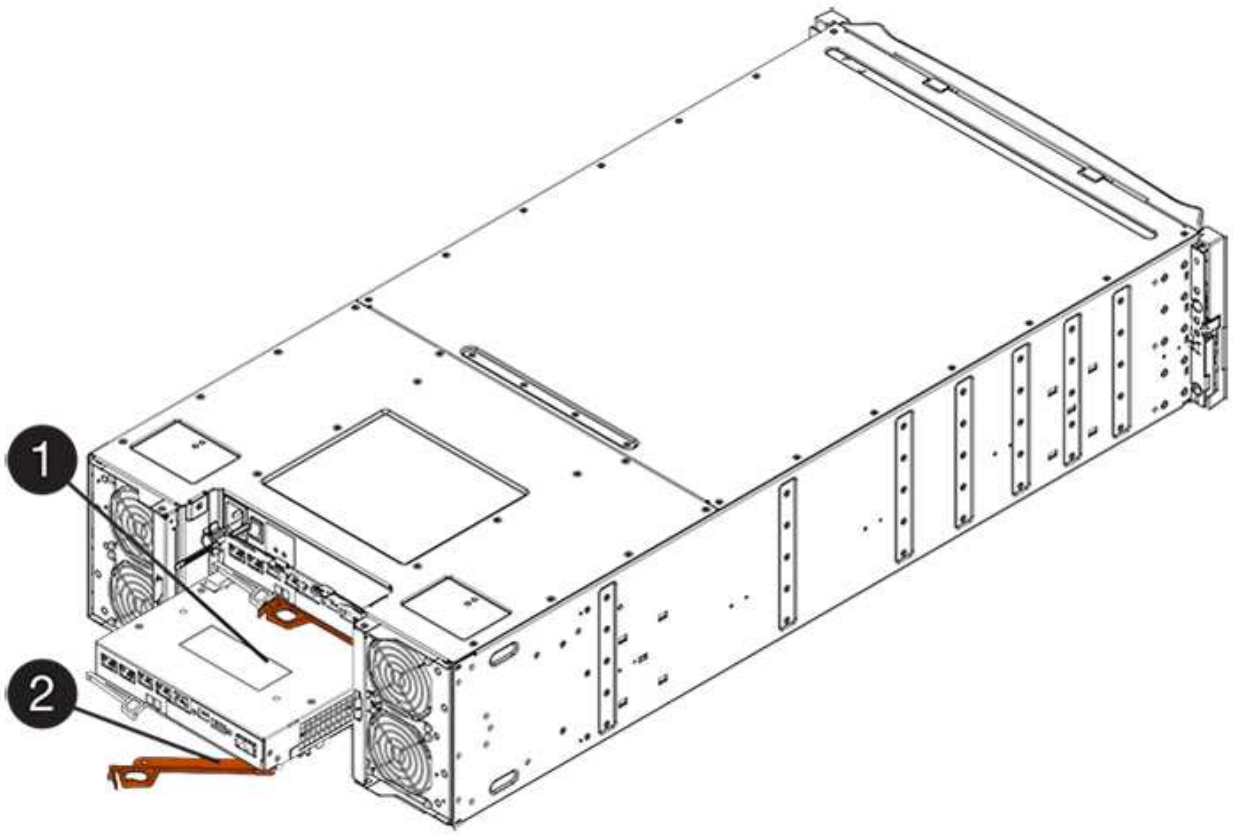
   La figura seguente è un esempio di shelf di controller E2812, shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

6. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

7. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
8. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere una scheda di interfaccia host

Rimuovere la scheda di interfaccia host (HIC) originale in modo da poterla sostituire con una aggiornata.

Fasi

1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

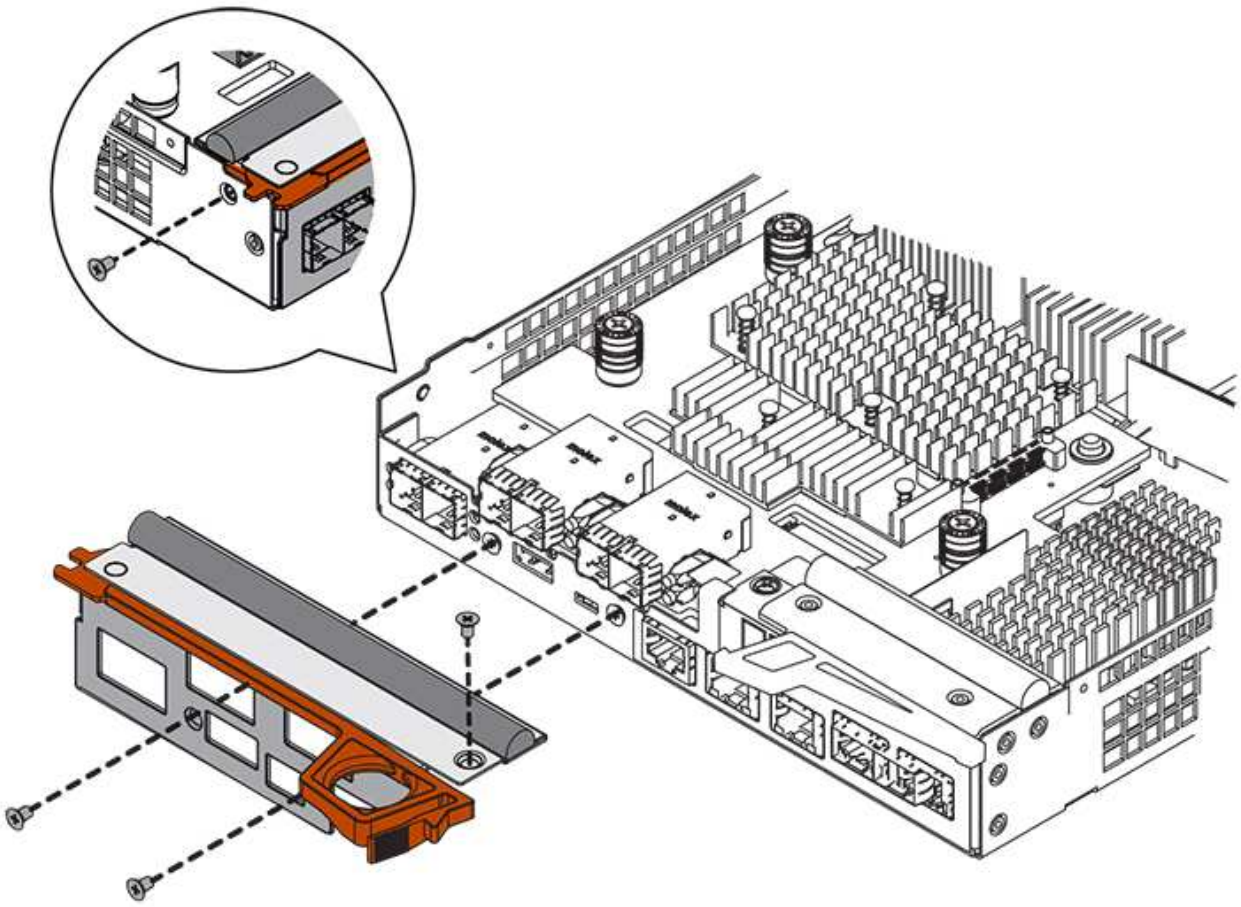
   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *cache interna attiva*

(2) *batteria*

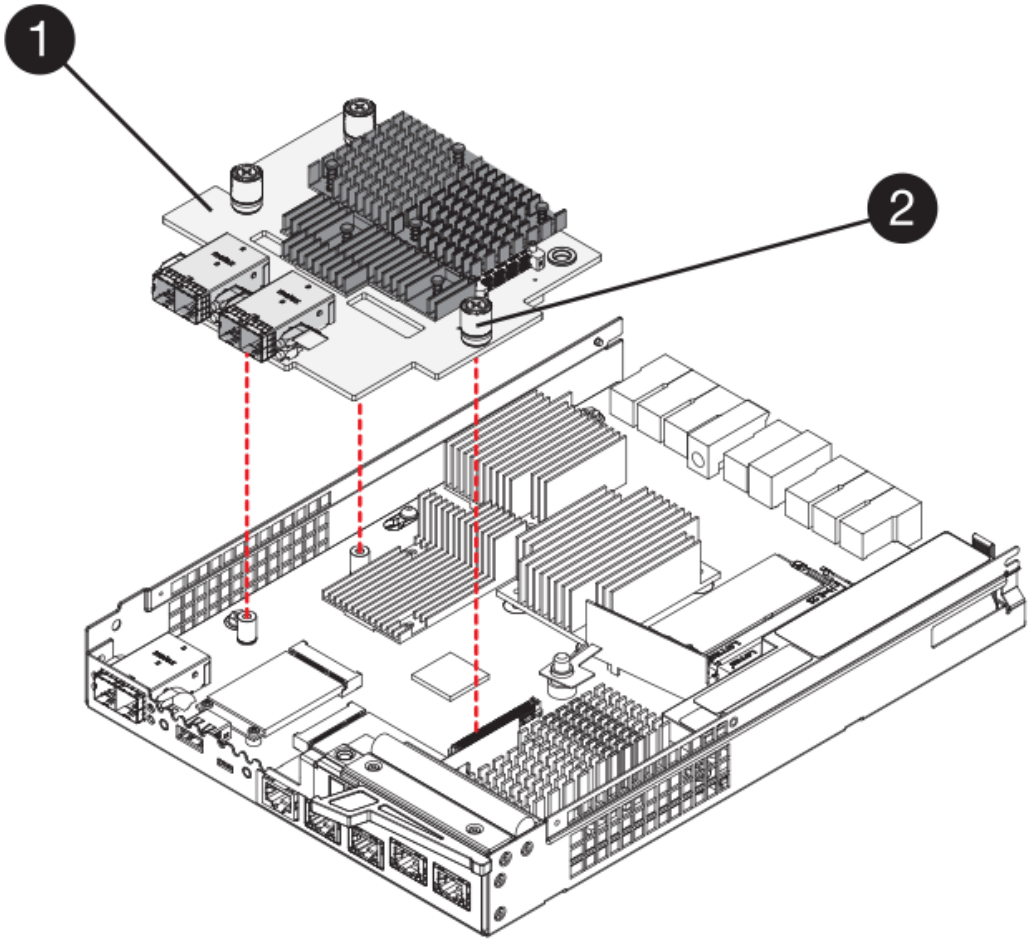
3. Utilizzando un cacciavite Phillips n. 1, rimuovere le viti che fissano la mascherina HIC al contenitore del controller.

   Sono presenti quattro viti: Una sulla parte superiore, una laterale e due sulla parte anteriore.



4. Rimuovere la piastra anteriore dell'HIC.
5. Utilizzando le dita o un cacciavite Phillips, allentare le tre viti a testa zigrinata che fissano l'HIC alla scheda del controller.
6. Scollegare con cautela l'HIC dalla scheda del controller sollevandola e facendola scorrere all'indietro.

> Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

7. Posizionare l'HIC su una superficie priva di elettricità statica.

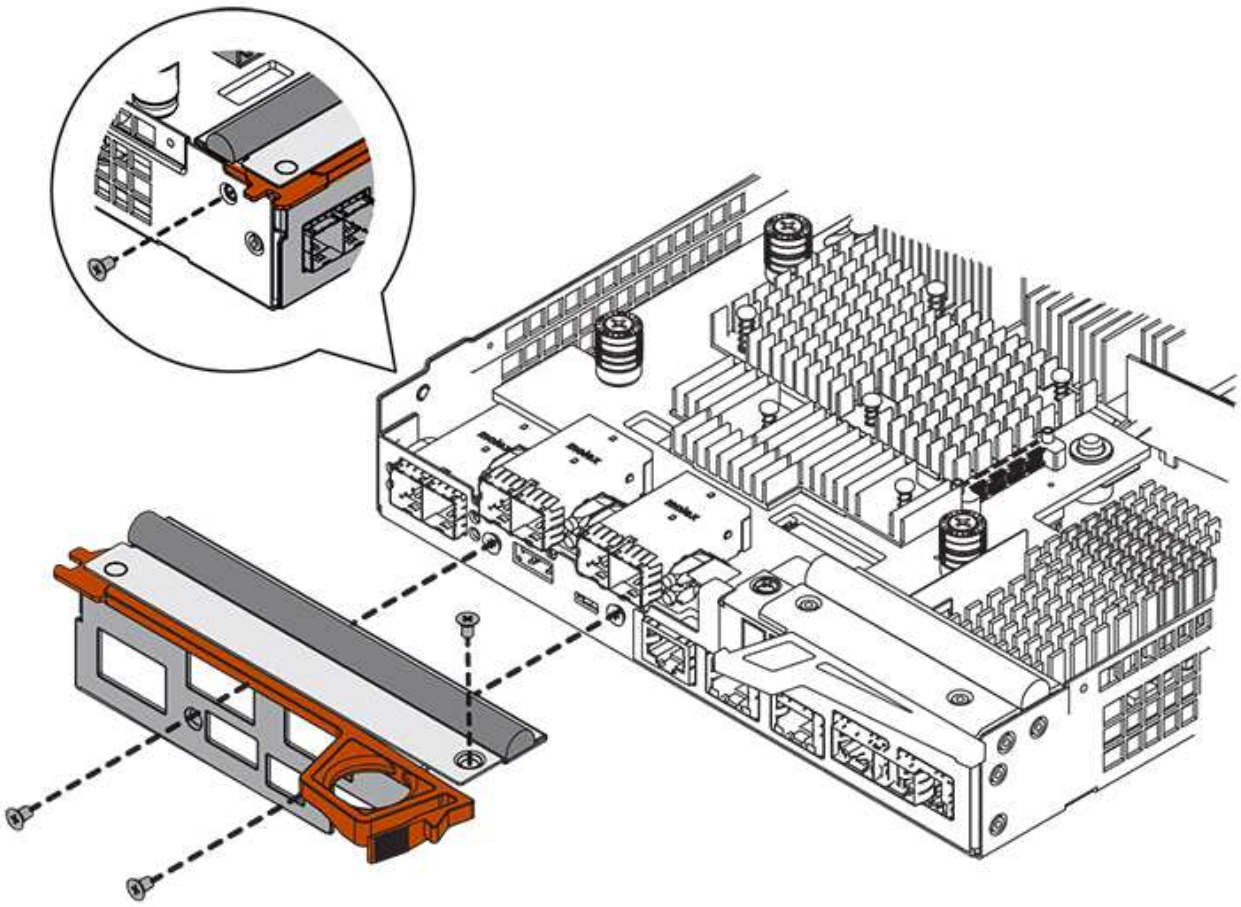
Fase 4: Installare la scheda di interfaccia host

Installare la nuova scheda di interfaccia host (HIC) per aumentare il numero di porte host nell'array di storage.

> **Possibile perdita di accesso ai dati** — non installare mai un HIC in un contenitore del controller E2800 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la piastra anteriore HIC al contenitore del controller, quindi rimuovere la piastra frontale.

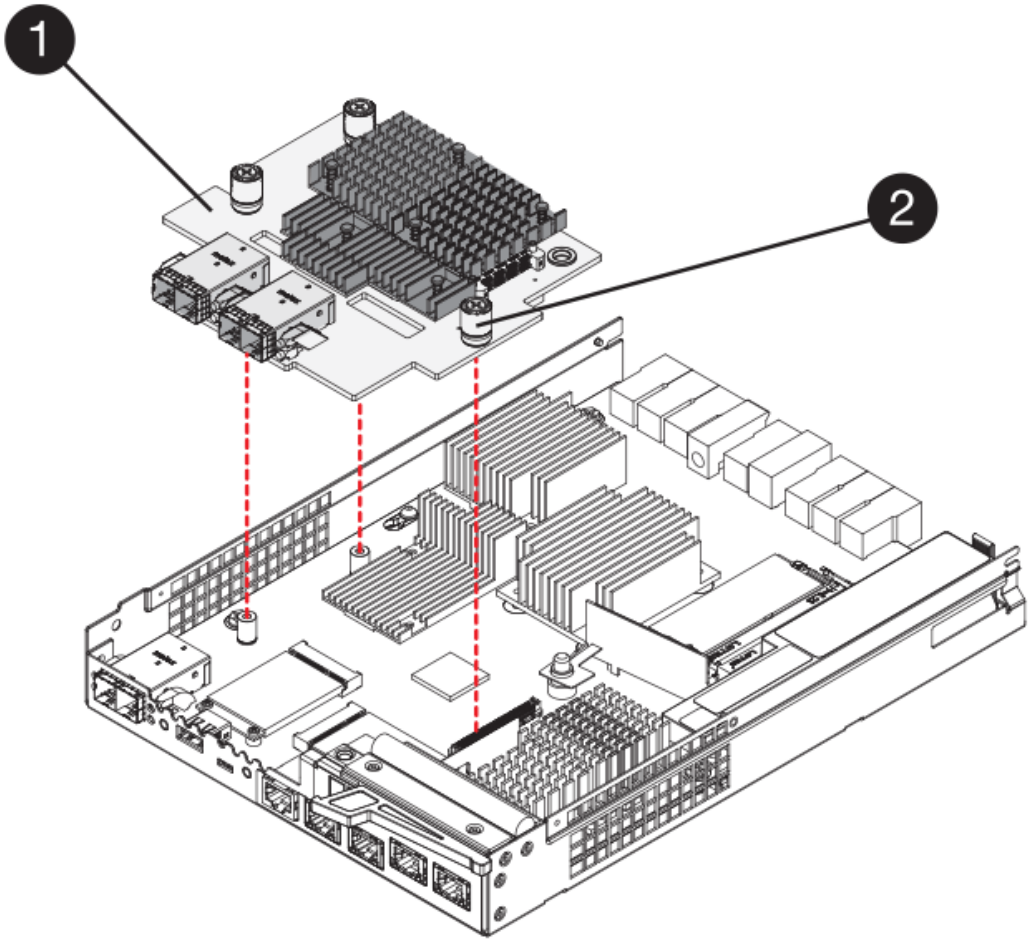


3. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

4. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

> **Possibili danni alle apparecchiature** — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



(1) *scheda di interfaccia host*

(2) *viti a testa zigrinata*

5. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

6. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.

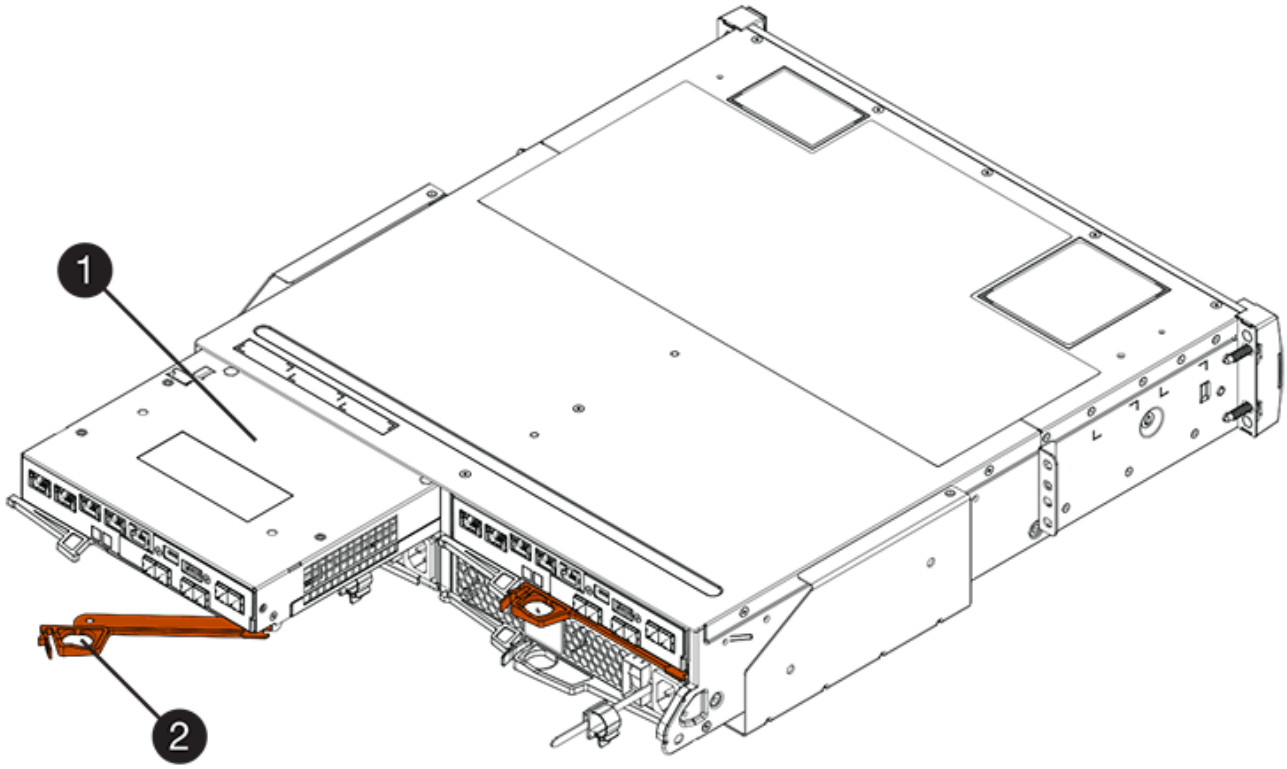
Fase 5: Reinstallare il contenitore del controller

Reinstallare il contenitore del controller nello shelf del controller dopo aver installato la nuova scheda di interfaccia host (HIC).

Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

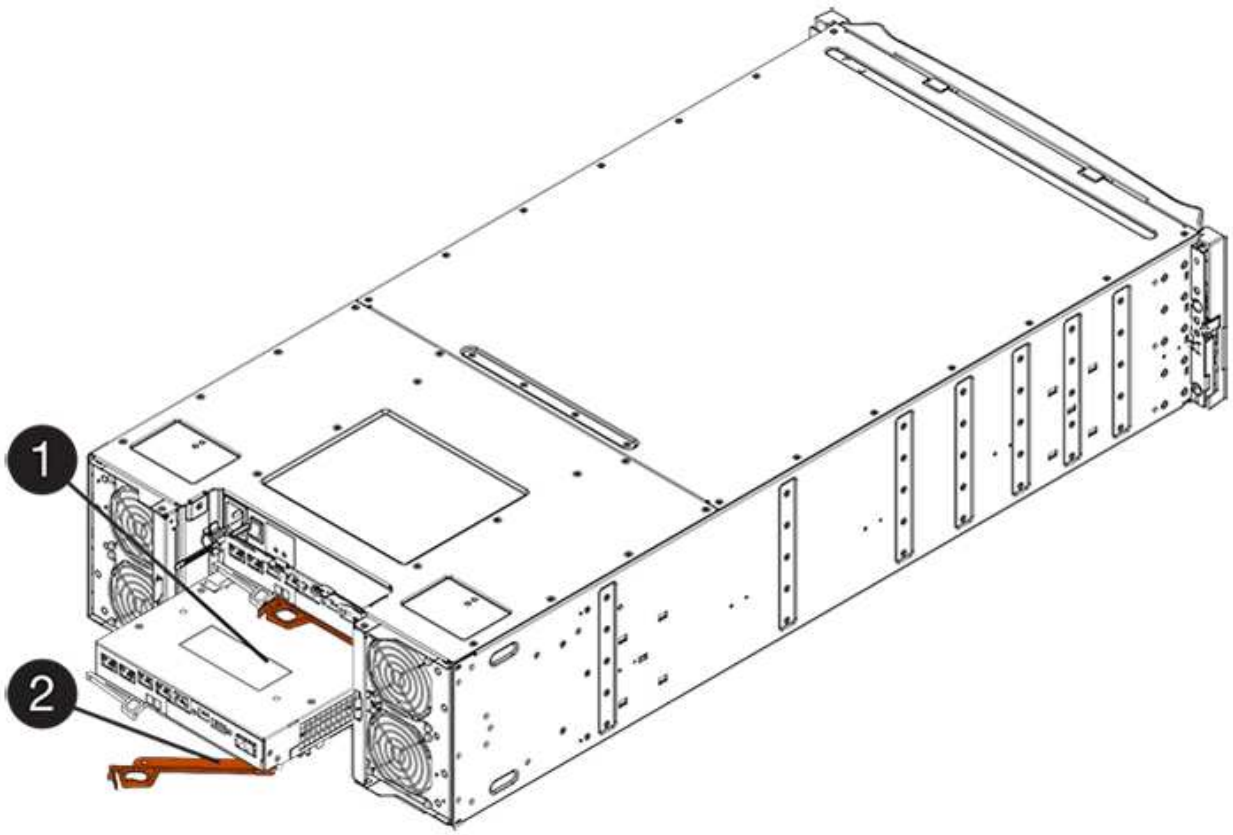
   La figura seguente è un esempio di shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Ricollegare tutti i cavi rimossi.

> Non collegare i cavi dati alle nuove porte HIC in questo momento.

6. (Facoltativo) se si sta aggiornando HICS in una configurazione duplex, ripetere tutti i passaggi per rimuovere l'altro elemento filtrante del controller, rimuovere l'HIC, installare il nuovo HIC e sostituire il secondo elemento filtrante del controller.

Fase 6: Completare l'aggiornamento della scheda di interfaccia host

Completare il processo di aggiornamento di una scheda di interfaccia host controllando i LED del controller e il display a sette segmenti e confermando che lo stato del controller è ottimale.

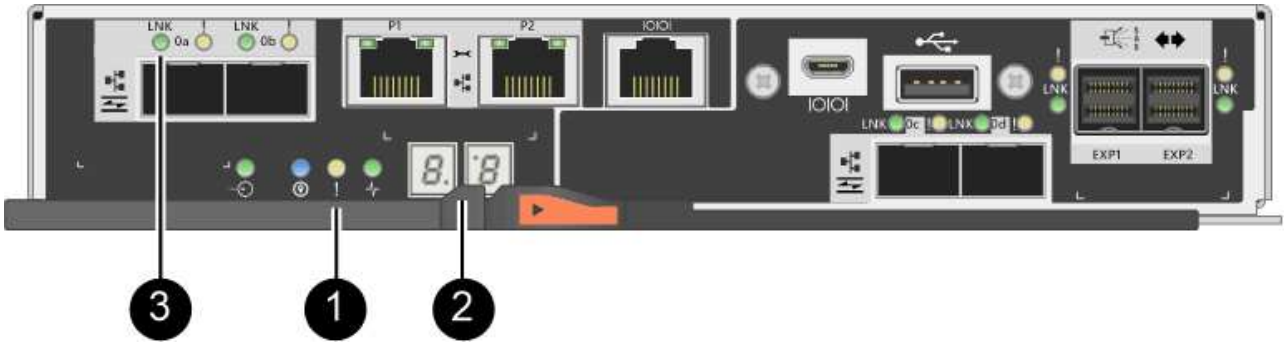
Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a

sette segmenti dovrebbe visualizzare l'ID del vassoio.

- Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
- I LED verdi del collegamento host rimangono spenti fino a quando non si collegano i cavi host.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

3. Da Gestore di sistema di SANtricity, verificare che lo stato del controller sia ottimale.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se le nuove porte HIC richiedono ricetrasmettitori SFP+, installarli.
5. Collegare i cavi dalle porte host del controller agli host dati.

Quali sono le prossime novità?

Il processo di aggiornamento di una scheda di interfaccia host nell'array di storage è completo. È possibile riprendere le normali operazioni.

Sostituire la scheda di interfaccia host (HIC) E2800

È possibile sostituire una scheda di interfaccia host (HIC) guasta.

A proposito di questa attività

Quando si sostituisce un HIC, il controller viene posizionato offline, si rimuove il contenitore del controller, si installa il nuovo HIC, si sostituisce il contenitore del controller, quindi si porta il controller online.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E2800".
- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando

si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).

- Assicurarsi che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Assicurarsi di disporre di quanto segue:
  - Uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve essere compatibile con i controller. Se sono presenti due controller, ciascun controller deve avere un HICS identico.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un cacciavite Phillips n. 1.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare il controller offline

La procedura per mettere un controller offline dipende dal fatto che si disponga di un controller (simplex) o di due controller (duplex). Consultare le istruzioni appropriate per:

- Duplex: Posiziona il controller offline
- Simplex: Spegnere lo shelf del controller

Duplex: Posiziona il controller offline

Se si dispone di una configurazione duplex, seguire questa procedura per posizionare il controller offline in modo da poter rimuovere in modo sicuro l'HIC guasto.

> Eseguire questa operazione solo se lo storage array dispone di due controller (configurazione duplex).

Fasi

1. Dall'area Details (Dettagli) del Recovery Guru, determinare quale dei controller canister presenta l'HIC guasto.
2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

- In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

```
save storageArray dbmDatabase sourceLocation=onboard contentType=all
file="filename";
```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
     iii. Selezionare il controller che si desidera mettere offline.
     iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

     > Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

   - In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=offline`

   Per il controller B: `set controller [b] availability=offline`

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

Simplex: Spegnere lo shelf del controller

Se si dispone di una configurazione simplex, spegnere lo shelf del controller in modo da poter rimuovere in sicurezza l'HIC guasto.

Eseguire questa attività solo se lo storage array dispone di un controller (configurazione simplex).

Fasi

1. Da Gestore di sistema di SANtricity, rivedere i dettagli nel guru del ripristino per confermare che si è verificato un errore HIC e per assicurarsi che non siano necessari altri elementi prima di poter rimuovere e sostituire l'HIC.
2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.
   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, si potrebbero perdere i dati.

5. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.

6. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
7. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
8. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
9. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter aggiungere la nuova scheda di interfaccia host (HIC).

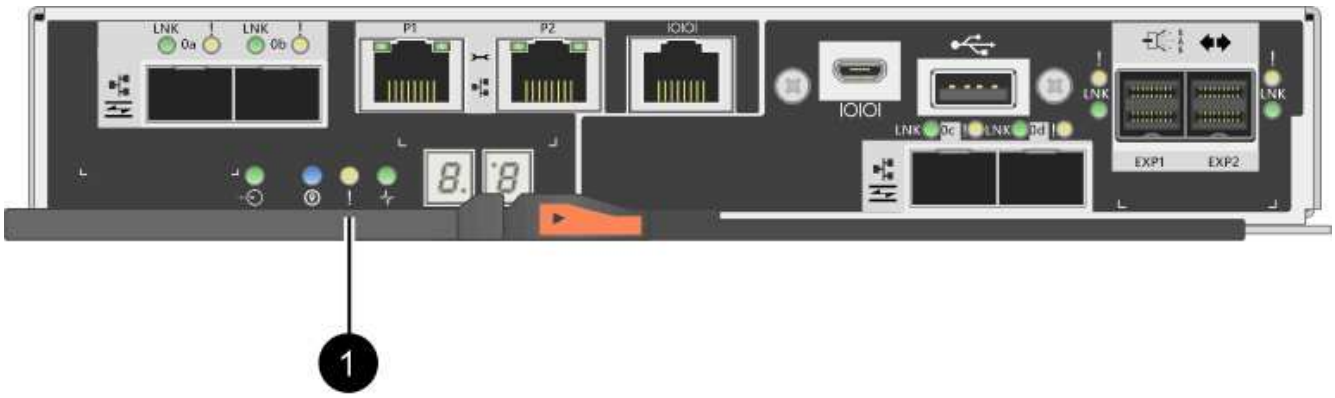
Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

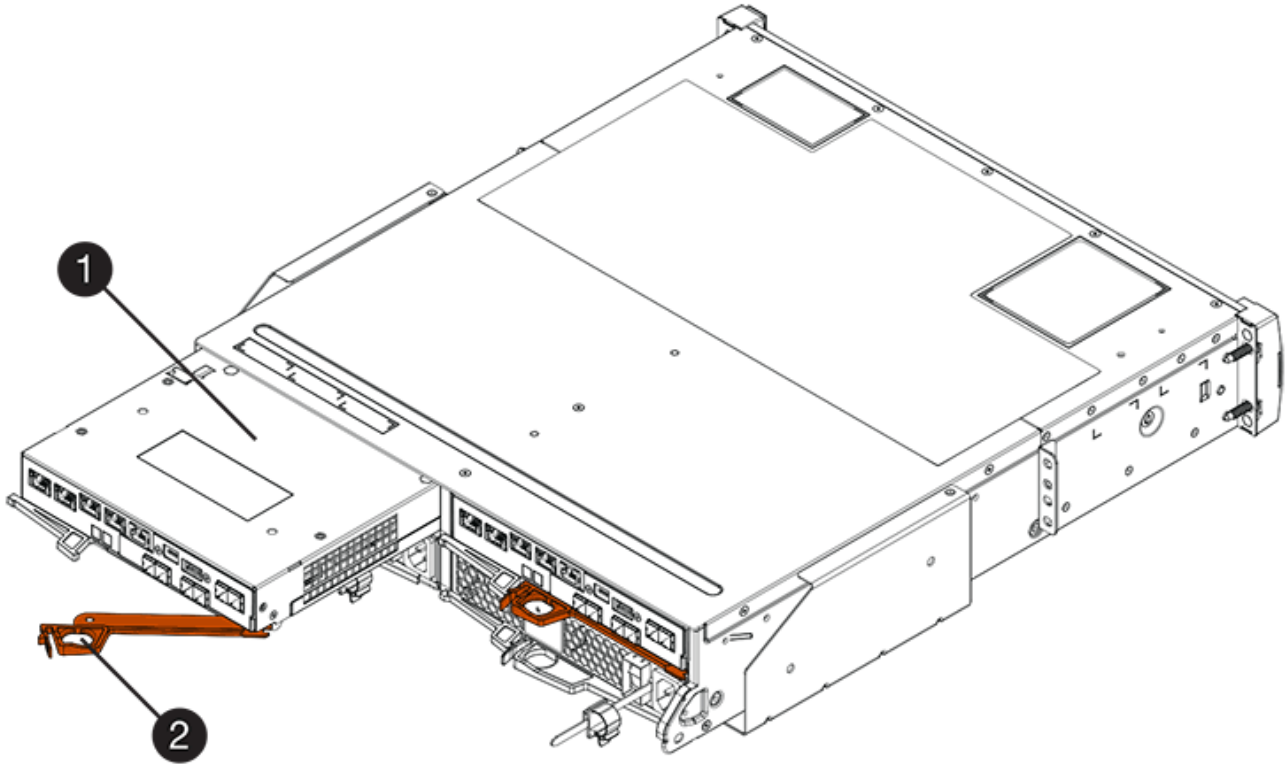
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



(1) *LED cache attiva*

4. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

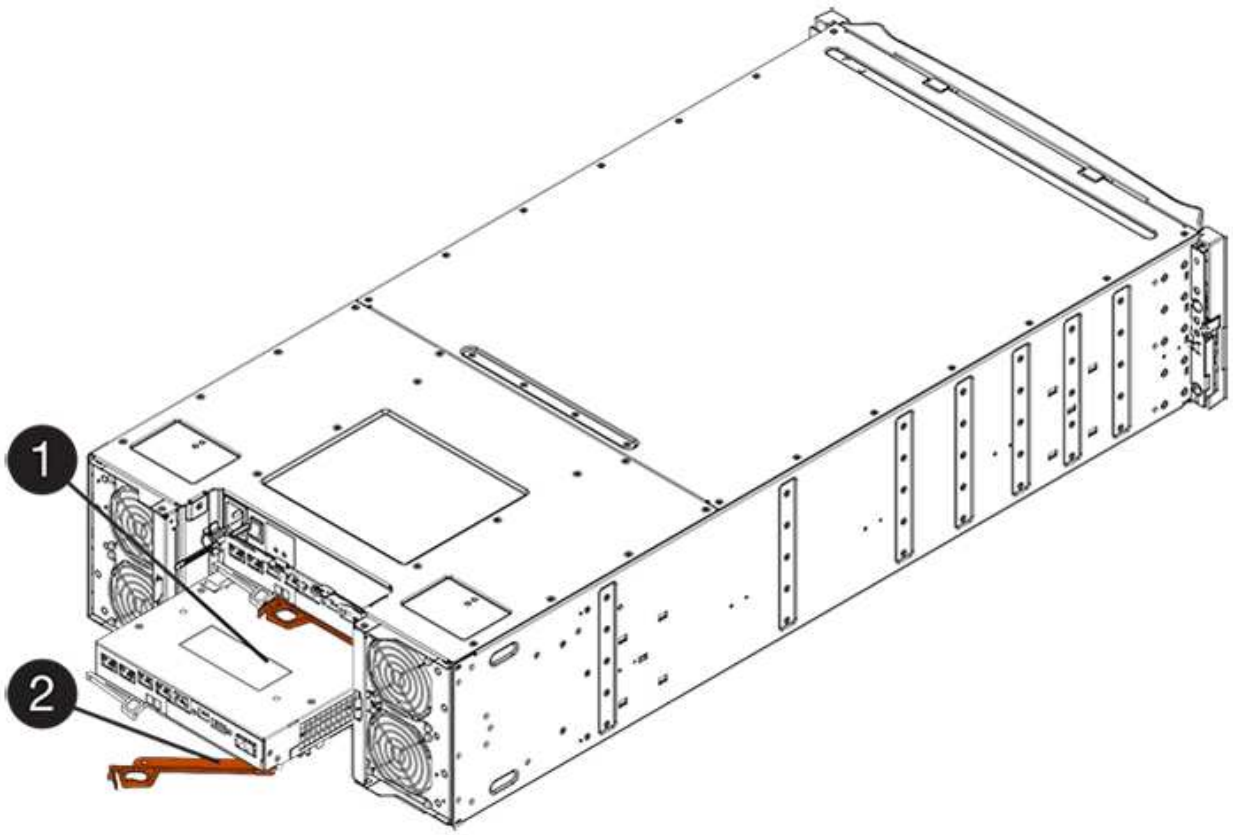
La figura seguente è un esempio di shelf di controller E2812, shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

5. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf di controller E2812, uno shelf di controller E2824 o un array flash EF280, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

6. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Installare un HIC

Installare un HIC per sostituire quello guasto con un nuovo HIC.

Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore del controller E2800 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.

2. Premere il pulsante sul coperchio del contenitore del controller ed estrarre il coperchio.
3. Verificare che il LED verde all'interno del controller (accanto ai DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

   (1) *LED cache interna attiva*

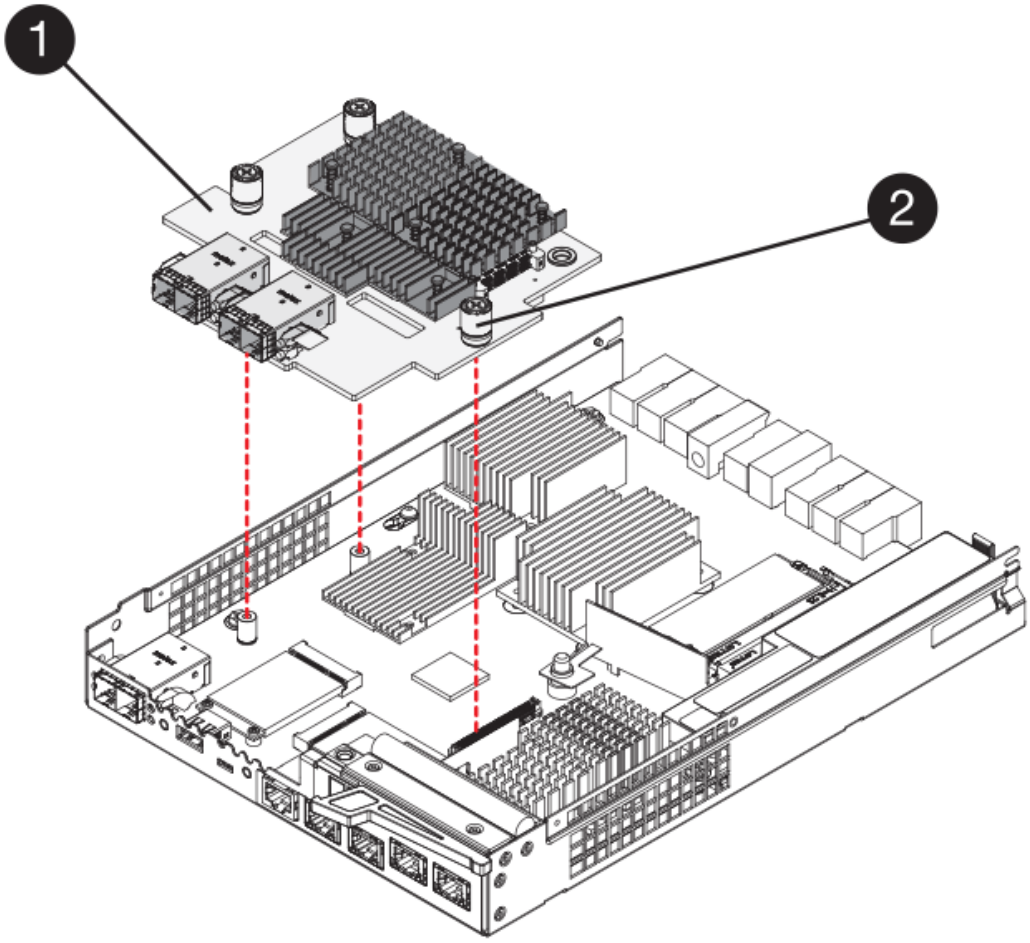
   (2) *batteria*

4. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller, quindi rimuovere la piastra frontale.
5. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

6. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



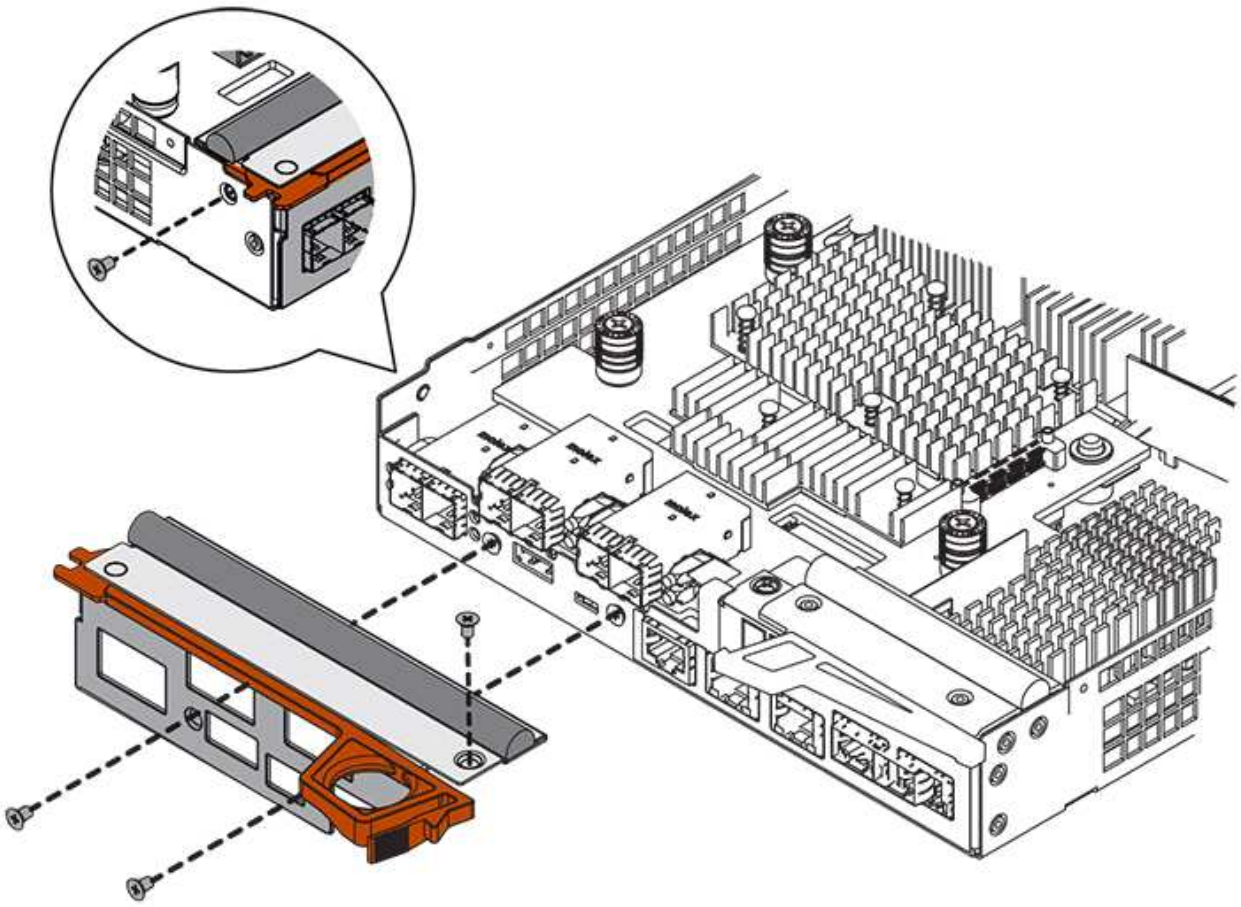
(1) *scheda di interfaccia host*

(2) *viti a testa zigrinata*

7. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

8. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.



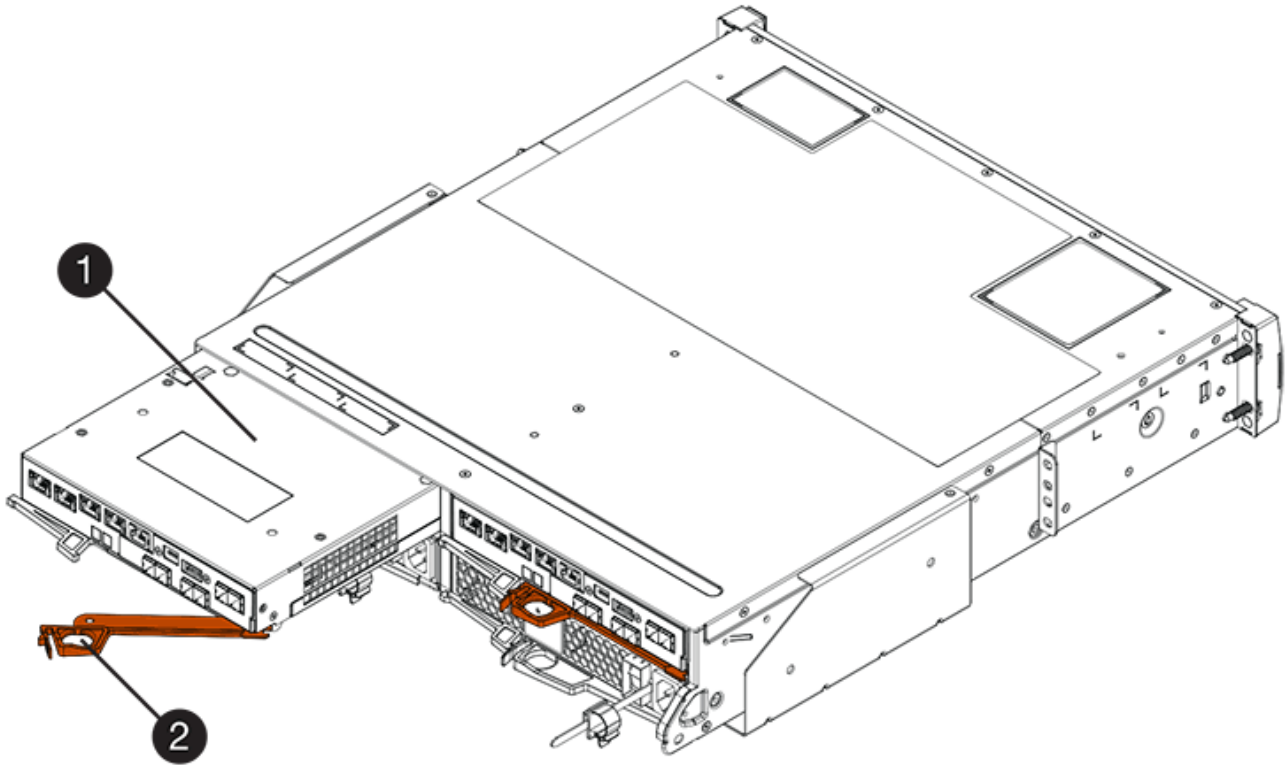
Fase 4: Reinstallare il contenitore del controller

Dopo aver installato l'HIC, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
2. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

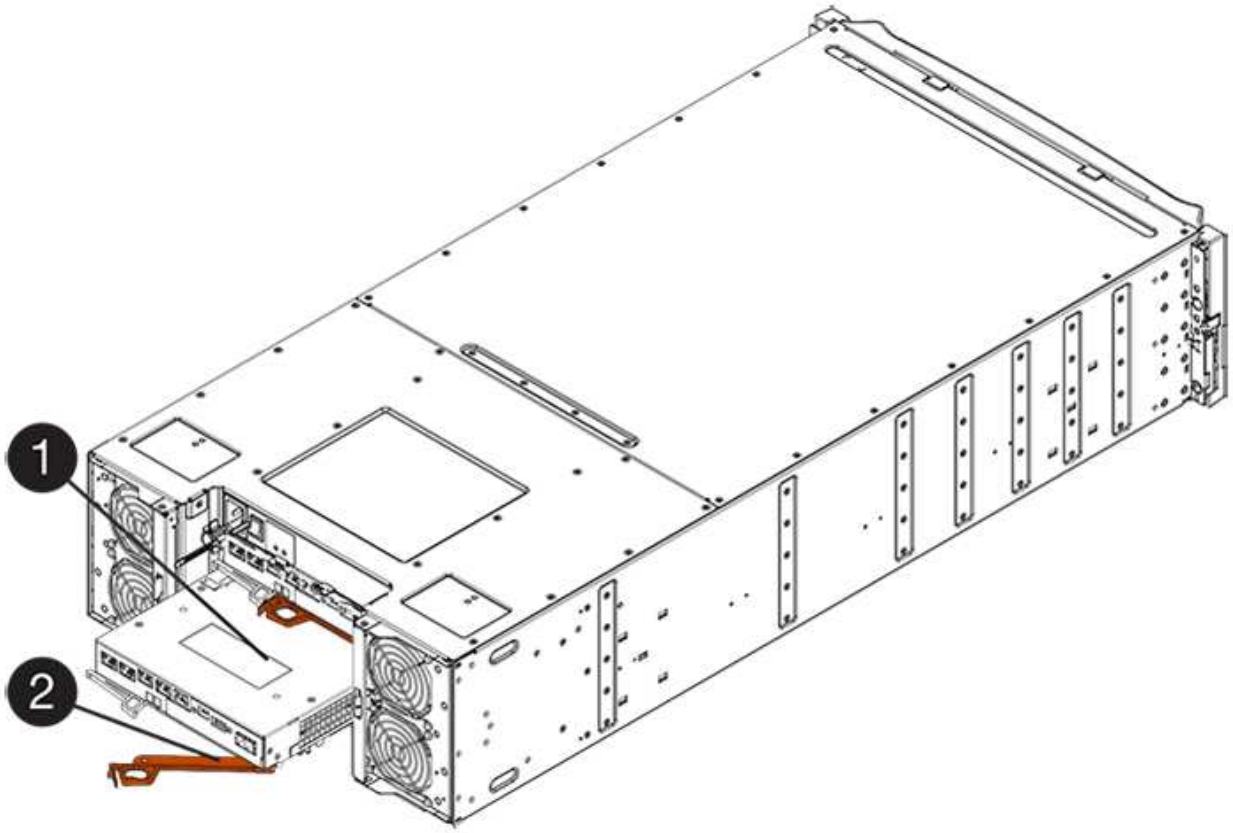
   La figura seguente è un esempio di shelf di controller E2824 o array flash EF280:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E2860:



(1) *contenitore controller*

(2) *maniglia della camma*

3. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
4. Ricollegare tutti i cavi rimossi.

> Non collegare i cavi dati alle nuove porte HIC in questo momento.

5. (Facoltativo) se si aggiunge HICS a una configurazione duplex, ripetere tutti i passaggi per rimuovere il secondo elemento filtrante del controller, installare il secondo HIC e reinstallare il secondo elemento filtrante del controller.

Fase 5: Posizionare il controller online

La procedura per posizionare un controller online dipende dal fatto che si disponga di un controller (simplex) o di due controller (duplex).

Duplex: Consente di posizionare il controller in linea

Per una configurazione duplex, portare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

> Eseguire questa operazione solo se lo storage array dispone di due controller.

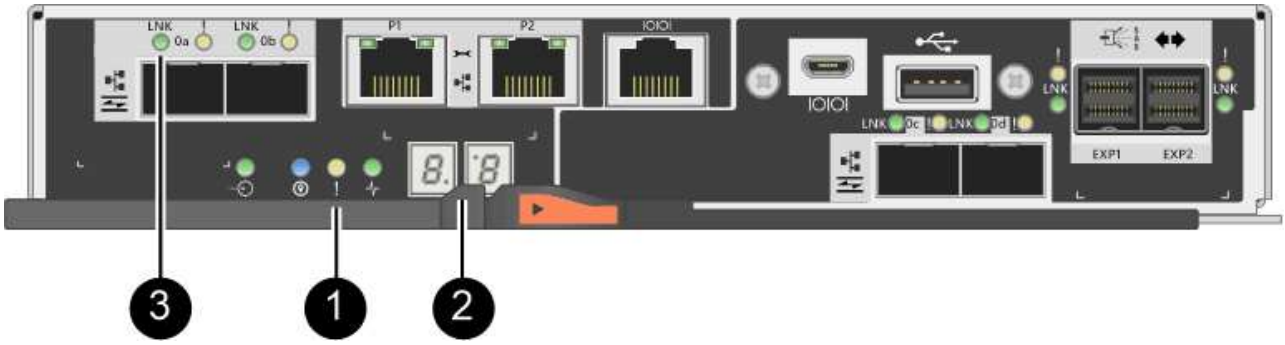
Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

Quando la comunicazione con l'altro controller viene ristabilita:

- Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
- Il LED di attenzione di colore ambra rimane acceso.
- I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

2. Portare il controller online utilizzando Gestione di sistema di SANtricity.
   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf**.
     iii. Selezionare il controller che si desidera mettere in linea.
     iv. Selezionare **Place Online** (Esegui online) dal menu di scelta rapida e confermare che si desidera eseguire l'operazione.

     Il sistema mette il controller in linea.
   - In alternativa, è possibile utilizzare i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=online;`

   Per il controller B: `set controller [b] availability=online;`

3. Controllare i codici sul display a sette segmenti del controller quando torna online. Se sul display viene visualizzata una delle seguenti sequenze di ripetizione, rimuovere immediatamente il controller.
   - **OE**, **L0**, ***blank*** (controller non corrispondenti)
   - **OE**, **L6**, ***blank*** (HIC non supportato)

Possibile perdita di accesso ai dati — se il controller appena installato mostra uno di questi codici e l'altro controller viene resettato per qualsiasi motivo, anche il secondo controller potrebbe bloccarsi.

4. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

   Contattare il supporto tecnico all'indirizzo "Supporto NetApp", 888-463-8277 (Nord America), 00-800-44-638277 (Europa) o +800-800-80-800 (Asia/Pacifico) se è necessario il numero RMA.

Simplex: Accendere lo shelf del controller

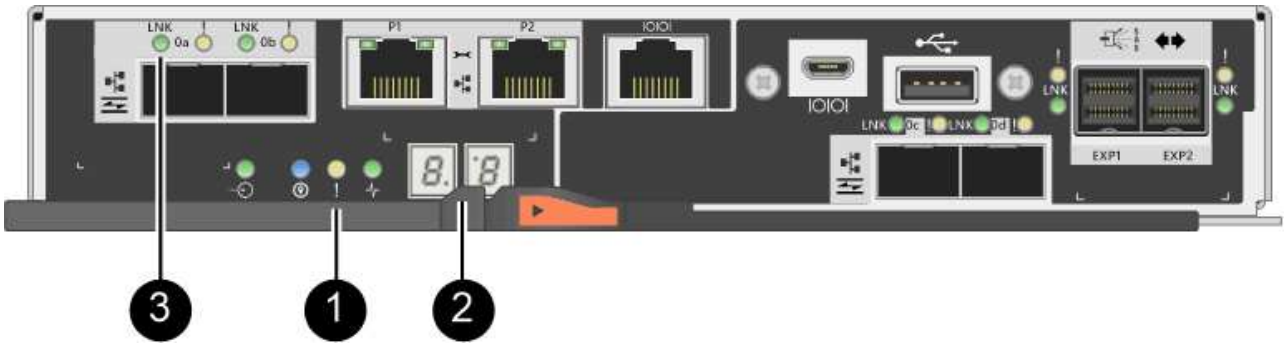
Per una configurazione simplex, alimentare lo shelf del controller, raccogliere i dati di supporto e riprendere le operazioni.

Eseguire questa attività solo se lo storage array dispone di un controller.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a sette segmenti dovrebbe visualizzare l'ID del vassoio.
   - Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
   - I LED verdi del collegamento host si accendono.

   La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.



(1) *LED di attenzione (ambra)*

(2) *Display a sette segmenti*

(3) *LED collegamento host*

3. Verificare che lo stato del controller sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

   Contattare il supporto tecnico all'indirizzo "Supporto NetApp", 888-463-8277 (Nord America), 00-800-44-638277 (Europa) o +800-800-80-800 (Asia/Pacifico) se è necessario il numero RMA.

Quali sono le prossime novità?

La sostituzione dell'HIC è completata. È possibile riprendere le normali operazioni.

Conversione del protocollo della porta host

Requisiti per la modifica del protocollo della porta host E2800

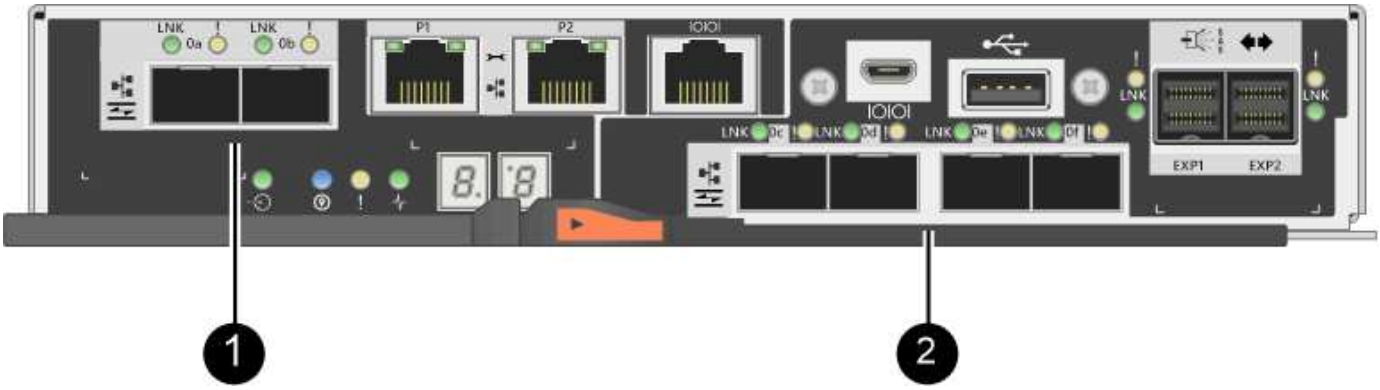
Prima di convertire il protocollo host per un array E2800, esaminare i requisiti.

Porte host modificabili

> Solo le porte HICS FC da 16 GB/iSCSI da 10 GB e le porte di base ottiche su un controller E2800 possono essere convertite.

La figura seguente mostra il retro di un controller E2800 dotato di due porte host SFP+ (ottiche) per scheda

base **(1)** e quattro porte HIC SFP+ (ottiche) **(2)**.



È disponibile anche un HIC a due porte.

Il controller E2800 o i controller nell'array di storage potrebbero avere diversi tipi di porte host per scheda base e diversi tipi di porte HIC. La tabella mostra quali porte host possono essere modificate con un Feature Pack.

Se si dispone di queste porte host baseboard…	E hai queste porte HIC…	È possibile modificare…
Due porte SFP+ (ottiche)	Nessuno	Solo le porte host della scheda base
Due porte SFP+ (ottiche)	Quattro porte SFP+ (ottiche)	Tutte le porte
Due porte SFP+ (ottiche)	Due porte SFP+ (ottiche)	Tutte le porte
Due porte SFP+ (ottiche)	Due o quattro porte SAS	Solo le porte host della scheda base
Due porte SFP+ (ottiche)	Due porte RJ-45 (base-T)	Solo le porte host della scheda base
Due porte RJ-45 (base-T)	Nessuno	Nessuna porta
Due porte RJ-45 (base-T)	Due porte RJ-45 (base-T)	Nessuna porta

Le porte host della scheda base e le porte HIC possono utilizzare lo stesso protocollo host o protocolli host diversi.

Requisiti per la modifica del protocollo host

- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura.
- Quando si esegue la conversione, è necessario interrompere le operazioni di i/o dell'host e non sarà possibile accedere ai dati sull'array di storage fino a quando la conversione non sarà stata completata correttamente.
- È necessario utilizzare la gestione out-of-band. Non è possibile utilizzare la gestione in-band per completare questa procedura.

- Hai ottenuto l'hardware necessario per la conversione. Il tuo rappresentante commerciale NetApp può aiutarti a determinare l'hardware di cui hai bisogno e a ordinare le parti corrette.
- Se si tenta di modificare le porte host della scheda base dell'array di storage e attualmente si utilizzano ricetrasmettitori SFP a doppio protocollo (denominati anche *unificati*) acquistati da NetApp, non è necessario cambiare i ricetrasmettitori SFP.
- Assicurarsi che i ricetrasmettitori SFP a doppio protocollo supportino sia FC (a 4 Gbps, 16 Gbps) che iSCSI (a 10 Gbps), ma non supportano iSCSI a 1 Gbps. Vedere "Fase 1: Determinare se si dispone di SFP a doppio protocollo" Per determinare il tipo di ricetrasmettitori SFP installati.

Considerazioni per la modifica del protocollo host

Le considerazioni per la modifica del protocollo host dipendono dai protocolli iniziali e finali delle porte host della scheda base e delle porte HIC.

Se si utilizza una funzione di mirroring o la funzione Data Assurance (da), è necessario comprendere cosa accade a queste funzioni quando si modifica il protocollo della porta host come descritto di seguito.

> Le seguenti considerazioni si applicano solo se si sta convertendo un array di storage già in uso. Queste considerazioni non si applicano se si sta convertendo un nuovo array di storage che non ha ancora host e volumi definiti.

Conversione da FC a iSCSI

- Se la configurazione contiene host DI avvio SAN collegati alle porte della scheda base FC, controllare "Matrice di interoperabilità NetApp" Per garantire che la configurazione sia supportata su iSCSI. In caso contrario, non è possibile convertire il protocollo host in iSCSI.
- La funzione da non è supportata per iSCSI.
  - Se si utilizza da e si desidera convertire le porte host FC in iSCSI, è necessario disattivare da su tutti i volumi.
  - Se non si disattiva da prima della conversione in iSCSI, l'array di storage non sarà conforme dopo la conversione.
- La funzione di mirroring sincrono non è supportata per iSCSI.
  - Se si utilizzano attualmente relazioni di mirroring sincrono e si desidera convertire le porte host FC in iSCSI, è necessario disattivare il mirroring sincrono.
  - Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per rimuovere tutte le coppie di mirroring sincrono, che rimuove le relazioni di mirroring sull'array di storage locale e sull'array di storage remoto. Inoltre, seguire le istruzioni della guida in linea per disattivare Synchronous Mirroring.

    > Se non si disattivano le relazioni di mirroring sincrono prima della conversione in iSCSI, il sistema perde l'accesso ai dati e potrebbe verificarsi una perdita di dati.

- Il mirroring asincrono richiede che sia lo storage array locale che quello remoto utilizzino lo stesso protocollo.
  - Se si utilizza attualmente il mirroring asincrono e si desidera convertire tutte le porte host da FC a iSCSI, è necessario disattivare il mirroring asincrono prima di applicare il Feature Pack.
  - Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per eliminare tutti i gruppi di coerenza dei mirror e rimuovere tutte le coppie mirrorate dagli array di storage locali e remoti. Inoltre, seguire le istruzioni della guida in linea per disattivare il mirroring asincrono.

Conversione da iSCSI a FC

- Il mirroring asincrono richiede che sia lo storage array locale che quello remoto utilizzino lo stesso protocollo. Se si utilizza attualmente il mirroring asincrono con le porte della scheda base, è necessario disattivare il mirroring asincrono prima di modificare il protocollo.
- Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per eliminare tutti i gruppi di coerenza dei mirror e rimuovere tutte le coppie mirrorate dagli array di storage locali e remoti. Inoltre, seguire le istruzioni della guida in linea per disattivare il mirroring asincrono.

Conversione da FC a FC/iSCSI

Considerazioni sul mirroring:

- Il mirroring sincrono non è supportato per iSCSI.
- Se un array di storage utilizzato per il mirroring dispone attualmente solo di porte FC e si desidera convertirne alcune in iSCSI, è necessario determinare quali porte utilizzare per il mirroring.
- Non è necessario convertire le porte dell'array di storage locale e dell'array di storage remoto nello stesso protocollo, purché entrambi gli array di storage dispongano di almeno una porta FC attiva dopo la conversione.
- Se si prevede di convertire le porte utilizzate per le relazioni mirrorate, è necessario disattivare qualsiasi relazione mirror sincrona o asincrona prima di applicare il Feature Pack.
- Se si prevede di convertire le porte utilizzate per il mirroring, le operazioni di mirroring asincrono non verranno influenzate.
- Prima di applicare il Feature Pack, verificare che tutti i gruppi di coerenza mirror siano sincronizzati. Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto.

Considerazioni su Data Assurance:

- La funzione Data Assurance (da) non è supportata per iSCSI.

  Per garantire che l'accesso ai dati rimanga ininterrotto, potrebbe essere necessario rimappare o rimuovere i volumi da dai cluster host prima di applicare il Feature Pack.

  > La funzione Data Assurance per iSCSI è supportata su SANtricity versione 11.40 e successive.

Se hai…	Devi…
Volumi DA nel cluster predefinito	Rimappare tutti i volumi da nel cluster predefinito. • Se non si desidera condividere volumi da tra host, attenersi alla seguente procedura: i. Creare una partizione host per ciascun set di porte host FC (a meno che non sia già stato fatto). ii. Rimappare i volumi da alle porte host appropriate. • Se si desidera condividere volumi da tra host, attenersi alla seguente procedura: i. Creare una partizione host per ciascun set di porte host FC (a meno che non sia già stato fatto). ii. Creare un cluster host che includa le porte host appropriate. iii. Rimappare i volumi da nel nuovo cluster host. Questo approccio elimina l'accesso ai volumi che rimangono nel cluster predefinito.
Volumi DA in un cluster host che contiene host solo FC e si desidera aggiungere host solo iSCSI	Rimuovere tutti i volumi da appartenenti al cluster, utilizzando una di queste opzioni. I volumi DA non possono essere condivisi in questo scenario. • Se non si desidera condividere volumi da tra host, rimappare tutti i volumi da a singoli host FC all'interno del cluster. • Separare gli host solo iSCSI nel proprio cluster host e mantenere il cluster host FC così com'è (con volumi da condivisi). • Aggiungere un HBA FC agli host solo iSCSI per consentire la condivisione di volumi da e non da.
Volumi DA in un cluster host che contiene host solo FC o volumi da mappati a una singola partizione host FC	Prima di applicare il Feature Pack, non è necessaria alcuna azione. I volumi DA rimarranno mappati al rispettivo host FC.

Se hai…	Devi…
Nessuna partizione definita	Non è necessaria alcuna azione prima di applicare il Feature Pack, in quanto non sono attualmente mappati volumi. Dopo aver convertito il protocollo host, seguire la procedura appropriata per creare partizioni host e, se si desidera, cluster host.

Conversione da iSCSI a FC/iSCSI

- Se si intende convertire una porta utilizzata per il mirroring, è necessario spostare le relazioni di mirroring in una porta che rimarrà iSCSI dopo la conversione.

  In caso contrario, il collegamento di comunicazione potrebbe essere inattivo dopo la conversione a causa di una mancata corrispondenza del protocollo tra la nuova porta FC sull'array locale e la porta iSCSI esistente sull'array remoto.

- Se si prevede di convertire le porte non utilizzate per il mirroring, le operazioni di mirroring asincrono non verranno influenzate.

  Prima di applicare il Feature Pack, verificare che tutti i gruppi di coerenza mirror siano sincronizzati. Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto.

Conversione da FC/iSCSI a FC

- Quando si convertono tutte le porte host in FC, tenere presente che il mirroring asincrono su FC deve avvenire sulla porta FC con il numero più alto.
- Se si prevede di convertire le porte utilizzate per le relazioni mirrorate, è necessario disattivare queste relazioni prima di applicare il Feature Pack.

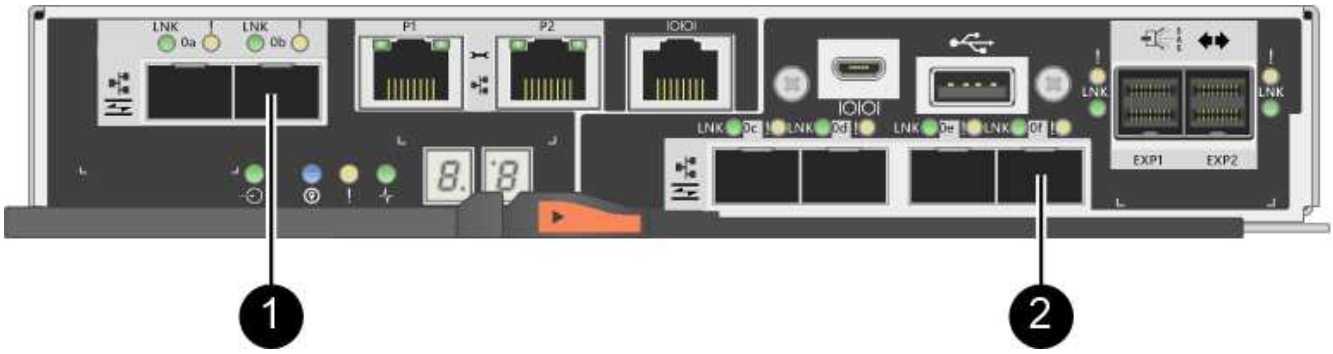
  Possibile perdita di dati — se non si eliminano le relazioni di mirroring asincrono che si sono verificate su iSCSI prima di convertire le porte in FC, i controller potrebbero bloccarsi e si potrebbero perdere i dati.

- Se lo storage array dispone attualmente di porte per scheda base iSCSI e porte FC HIC, le operazioni di mirroring asincrono non verranno influenzate.

  Prima e dopo la conversione, il mirroring viene eseguito sulla porta FC con il numero più alto, che rimane la porta HIC contrassegnata con **2** nella figura. Prima di applicare il Feature Pack, verificare che tutti i gruppi di coerenza mirror siano sincronizzati. Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto.

- Se lo storage array dispone attualmente di porte FC per scheda base e porte iSCSI HIC, è necessario eliminare le relazioni di mirroring che si verificano su FC prima di applicare il Feature Pack.

  Quando si applica il Feature Pack, il supporto del mirroring passa dalla porta host della scheda base con il numero più alto (contrassegnata con **1** nella figura) alla porta HIC con il numero più alto (contrassegnata con **2** nella figura).



Prima della conversione			Dopo la conversione			Passaggi richiesti
Porte baseboard	Porte HIC	Porta utilizzata per il mirroring	Porte baseboard	Porte HIC	Porta utilizzata per il mirroring	
ISCSI	FC	**(2)**	FC	FC	**(2)**	Sincronizzare i gruppi di coerenza mirror prima e testare le comunicazioni dopo
FC	ISCSI	**(1)**	FC	FC	**(2)**	Eliminare le relazioni di mirroring prima e ristabilire il mirroring dopo

Conversione da FC/iSCSI a iSCSI

- Il mirroring sincrono non è supportato per iSCSI.
- Se si intende convertire le porte utilizzate per le relazioni mirrorate, è necessario disattivare le relazioni di mirroring prima di applicare il Feature Pack.

> **Possibile perdita di dati** — se non si eliminano le relazioni di mirroring che si sono verificate su FC prima di convertire le porte in iSCSI, i controller potrebbero bloccarsi e si potrebbero perdere i dati.

- Se non si prevede di convertire le porte utilizzate per il mirroring, le operazioni di mirroring non verranno influenzate.
- Prima di applicare il Feature Pack, verificare che tutti i gruppi di coerenza mirror siano sincronizzati.
- Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto.

Stesso protocollo host e operazioni di mirroring

Le operazioni di mirroring non vengono influenzate se le porte host utilizzate per il mirroring mantengono lo stesso protocollo dopo l'applicazione del Feature Pack. Tuttavia, prima di applicare il Feature Pack, è necessario verificare che tutti i gruppi di coerenza mirror siano sincronizzati.

Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto. In caso di domande su come eseguire questa operazione, consultare la guida in linea di Gestore di sistema di SANtricity.

Modificare il protocollo host per E2800

Se si dispone di uno storage array E2800 con porte host SFP+ (ottiche), è possibile modificare il protocollo della porta host da Fibre Channel (FC) a iSCSI o da iSCSI a FC.

È possibile modificare il protocollo utilizzato dalle porte host integrate nel controller (*baseboard host ports*), il protocollo utilizzato dalle porte host sulla scheda di interfaccia host (*HIC ports*) o il protocollo di tutte le porte host.

Fase 1: Determinare se si dispone di SFP a doppio protocollo

Utilizzare Gestore di sistema SANtricity per determinare il tipo di ricetrasmettitori SFP in uso. Poiché questi SFP possono essere utilizzati con protocolli FC e iSCSI, vengono definiti come *dual-Protocol* o *Unified* SFP.

Fasi

1. Da Gestore di sistema di SANtricity, selezionare **supporto**.
2. Selezionare il riquadro **Support Center**.
3. Nella scheda Support Resources (risorse di supporto), individuare e selezionare il collegamento **Storage Array Profile** (Profilo array di storage).
4. Digitare **SFP** nella casella di testo e fare clic su **Find** (trova).
5. Per ogni SFP elencato nel profilo dell'array di storage, individuare la voce **velocità dati supportata**.

```
SFP status:                Optimal
Attached to:               Host-side of controller B
Location:                  Unknown
Supported data rate(s):    16 Gbps, 10 Gbps, 8 Gbps, 4 Gbps
Link length:               Short
Connector:                 LC
Transmitter type:          Shortwave Laser w/o OFC
Transmission media:        TM Multi-mode 62.5m(M6)
IEEE company ID:           00 17 6a
Revision:                  Not Available
Part number:               AFBR-57F5UMZ
Serial number:             AA1317J14X7
Vendor:                    AVAGO
Date of manufacture:       4/28/13
```

6. Fare riferimento alla tabella per determinare se è possibile riutilizzare gli SFP, come indicato di seguito:

Velocità di trasferimento dati supportata	Tipo di SFP	Protocollo supportato
16 Gbps, 10 Gbps, 4 Gbps	Protocollo doppio	• **FC:** 16 Gbps, 4 Gbps • **ISCSI:**10 Gbps
25 Gbps, 10 Gbps	25 Gbps. 10 Gbps,	Solo iSCSI
32 Gbps, 16 Gbps, 8 Gbps, 4 Gbps	32 Gbps, 16 Gbps	Solo FC

- Se si dispone di SFP a doppio protocollo, è possibile continuare a utilizzarli dopo aver convertito il protocollo.

> Gli SFP a doppio protocollo non supportano iSCSI da 1 GB. Se si stanno convertendo le porte host in iSCSI, tenere presente che gli SFP a doppio protocollo supportano solo un collegamento da 10 GB alla porta connessa.

- Se si utilizzano SFP a 16 Gbps e si stanno convertendo le porte host in iSCSI, è necessario rimuovere gli SFP e sostituirli con SFP a doppio protocollo o a 10 Gbps dopo la conversione del protocollo. In base alle esigenze, è anche possibile utilizzare il rame iSCSI a 10 Gbps utilizzando uno speciale cavo Twin-Ax con SFP.

> Gli SFP FC a 8 Gbps NON sono supportati nei controller E28xx o E57xx. Sono supportati SOLO SFP FC a 16 Gbps e 32 Gbps.

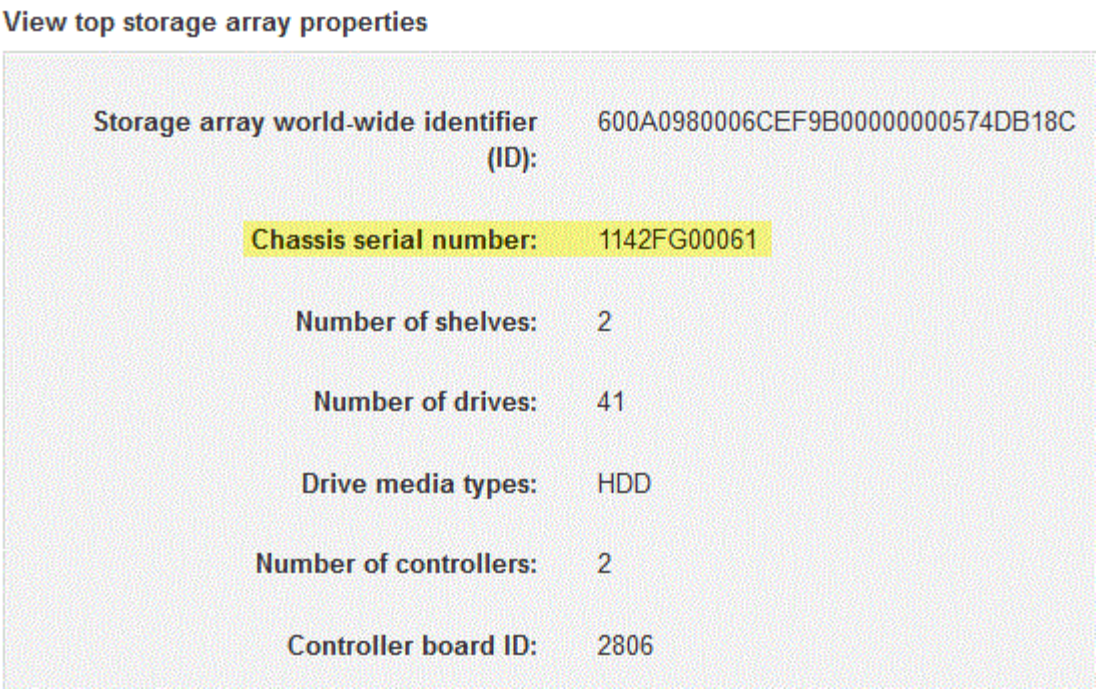
- Se si utilizzano SFP a 10 Gbps e si stanno convertendo le porte host in FC, è necessario rimuovere gli SFP da queste porte e sostituirli con SFP a doppio protocollo o a 16 Gbps dopo aver convertito il protocollo.

Fase 2: Ottenere il Feature Pack

Per ottenere il Feature Pack, è necessario il numero di serie dallo shelf del controller, un codice di attivazione delle funzioni e l'identificatore di abilitazione delle funzioni per lo storage array.

Fasi

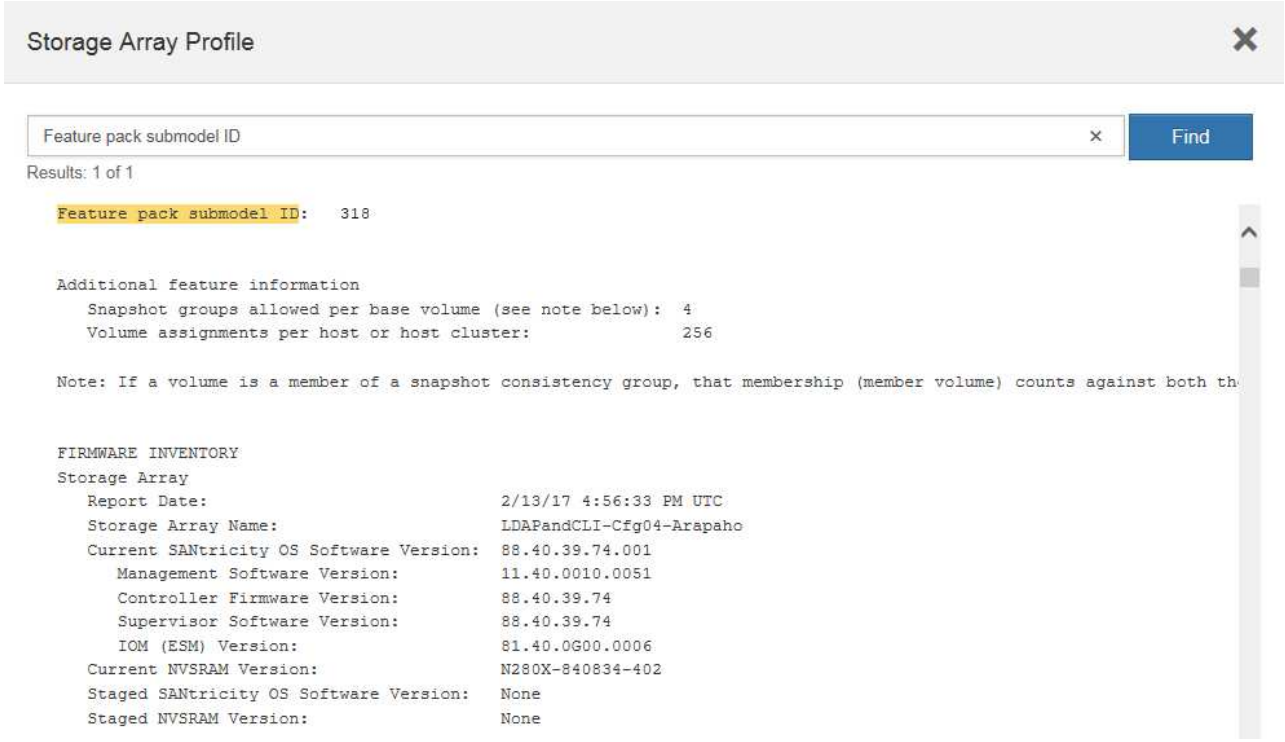
1. Individuare il numero di serie.
   a. Da Gestore di sistema di SANtricity, selezionare **supporto › Centro di supporto**.
   b. Con la scheda **Support Resources** (risorse di supporto) selezionata, scorrere fino alla sezione **View top storage array properties** (Visualizza proprietà principali storage array).
   c. Individuare **chassis Serial Number** (numero di serie chassis) e copiare questo valore in un file di testo.



2. Individuare l'ID del sottomodello **Feature Pack**.
   a. Nella scheda Support Resources (risorse di supporto), individuare e selezionare il collegamento **Storage Array Profile** (Profilo array di storage).
   b. Digitare **Feature Pack submodel ID** nella casella di testo e fare clic su **Find** (trova).

   > Il "modello secondario" può anche essere scritto come "modello secondario".

   c. Individuare l'ID del sottomodello del Feature Pack per la configurazione iniziale.



3. Utilizzando l'ID del sottomodello del Feature Pack, individuare l'ID del sottomodello del controller corrispondente per la configurazione iniziale e individuare il codice di attivazione della funzione per la configurazione finale desiderata all'interno della tabella riportata di seguito. Quindi, copiare il codice di attivazione della funzione in un file di testo.

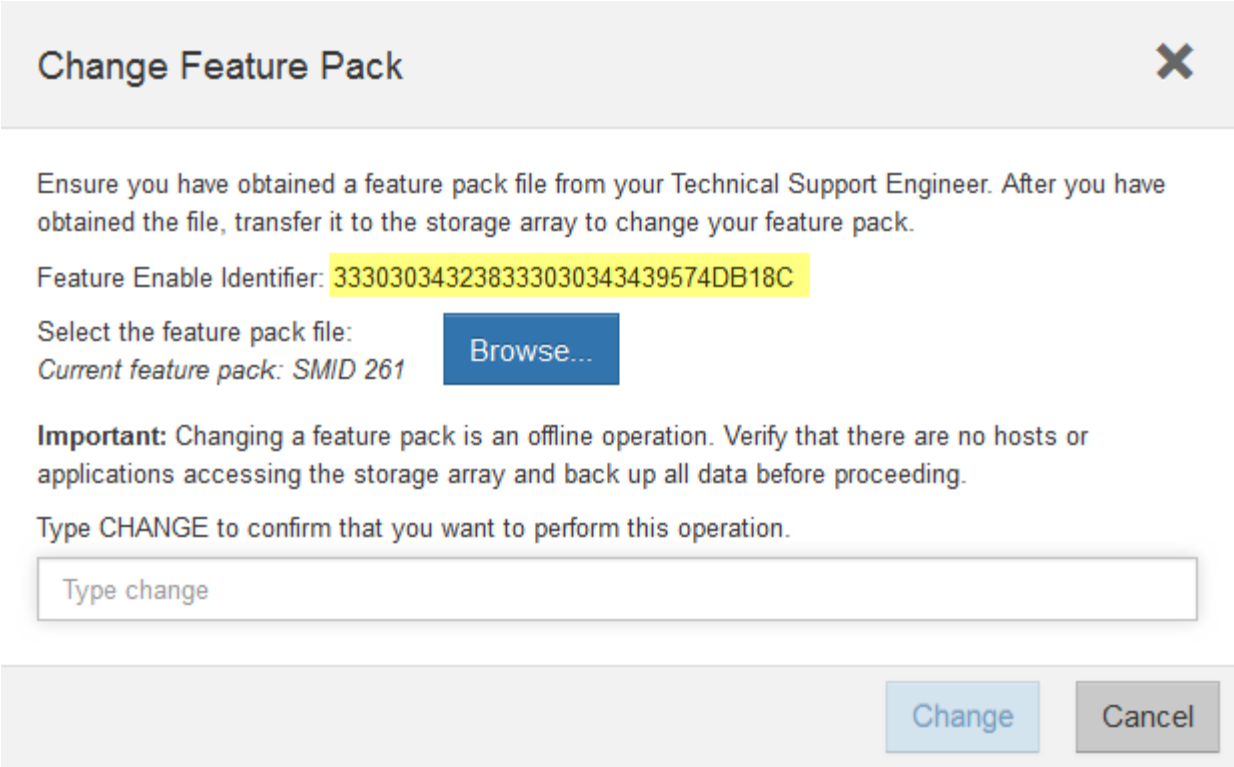
Avvio della configurazione			**Fine della configurazione**			**Codice di attivazione della funzione**
ID del sottomodello del controller	Porte baseboard	Porte HIC	ID del sottomodello del controller	Porte baseboard	Porte HIC	
318	FC	FC	319	FC	ISCSI	ZGW-4L2-Z36IJ
320	ISCSI	FC	4GZ-NL2-Z4NRP	321	ISCSI	ISCSI
TG2-7L2-Z5485	*Nessun HIC o non un HIC ottico*	321	ISCSI	TG2-7L2-Z5485	319	FC
ISCSI	318	FC	FC	1G5-QL2-Z7LFC	320	ISCSI
FC	FG7-AL2-Z82RW	321	ISCSI	ISCSI	5G7-0K2-Z0G8X	320
ISCSI	FC	318	FC	FC	4GP-HL2-ZYRKP	319
FC	ISCSI	PGU-KL2-Z1P7I	321	ISCSI	ISCSI	BGA-8K2-ZQWM5
321	ISCSI	ISCSI	318	FC	FC	SGH-UK2-ZUCJG
319	FC	ISCSI	1GK-EK2-ZVSW1	320	ISCSI	FC

Avvio della configurazione			**Fine della configurazione**			**Codice di attivazione della funzione**
ID del sottomodello del controller	Porte baseboard	Porte HIC	ID del sottomodello del controller	Porte baseboard	Porte HIC	

Avvio della configurazione			Fine della configurazione			Codice di attivazione della funzione
338	FC	FC	339	FC	ISCSI	PGC-RK2-ZREUT
340	ISCSI	FC	MGF-BK2-ZSU3Z	341	ISCSI	ISCSI
NGR-1L2-ZZ8QC	*Nessun HIC o non un HIC ottico*	341	ISCSI	NGR-1L2-ZZ8QC	339	FC
ISCSI	338	FC	FC	DGT-7M2-ZKBMD	340	ISCSI
FC	GGA-TL2-Z9J50	341	ISCSI	ISCSI	WGC-DL2-ZBZIB	340
ISCSI	FC	338	FC	FC	4GM-KM2-ZGWS1	339
FC	ISCSI	PG0-4M2-ZHDZ6	341	ISCSI	ISCSI	XGR-NM2-ZJUGR
341	ISCSI	ISCSI	338	FC	FC	3GE-WL2-ZCHNY
339	FC	ISCSI	FGH-HL2-ZDY3R	340	ISCSI	FC

Se l'ID del modello secondario del controller non è presente nell'elenco, contattare "Supporto NetApp".

4. In System Manager, individuare Feature Enable Identifier.
   a. Accedere al **Impostazioni › sistema**.
   b. Scorrere verso il basso fino a **componenti aggiuntivi**.
   c. In **Change Feature Pack**, individuare **Feature Enable Identifier**.
   d. Copiare e incollare questo numero di 32 cifre in un file di testo.



5. Passare a. "Attivazione della licenza NetApp: Attivazione della funzionalità Premium dello storage Array"e immettere le informazioni necessarie per ottenere il feature pack.
   - Numero di serie dello chassis
   - Codice di attivazione della funzione
   - Identificatore di abilitazione della funzione

> Il sito Web di attivazione delle funzionalità Premium include un collegamento a “istruzioni di attivazione delle funzioni Premium”. Non tentare di seguire queste istruzioni per questa procedura.

6. Scegliere se ricevere il file delle chiavi per il Feature Pack in un’e-mail o scaricarlo direttamente dal sito.

Fase 3: Arrestare l’i/o host

È necessario interrompere tutte le operazioni di i/o dall’host prima di convertire il protocollo delle porte host. Non è possibile accedere ai dati sull’array di storage fino a quando la conversione non viene completata correttamente.

Fasi

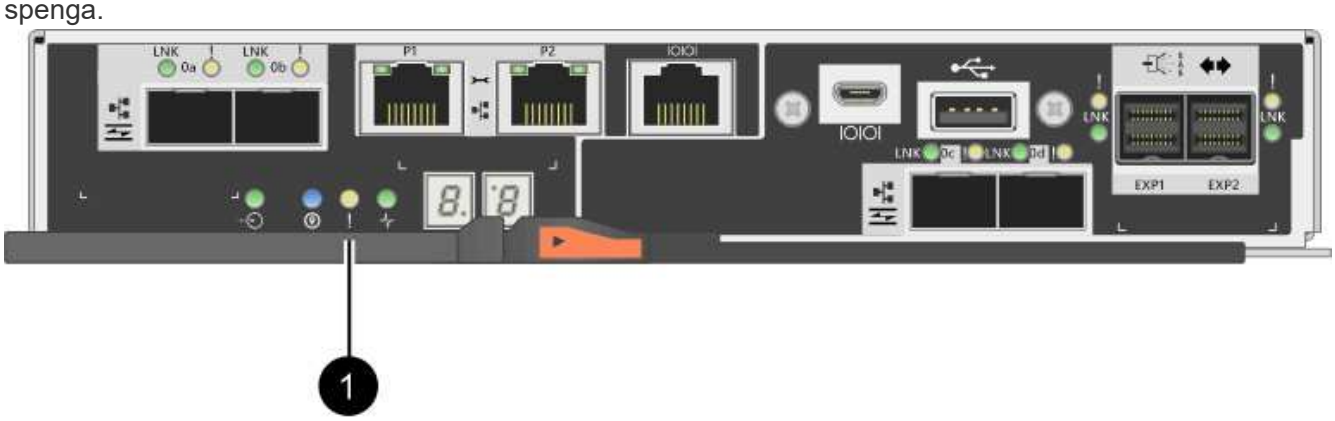
1. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull’array.

I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

2. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
3. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



Didascalia	Tipo di porte host
(1)	LED cache Active (cache attiva)

4. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
5. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.

Fase 4: Modificare il Feature Pack

Modificare il Feature Pack per convertire il protocollo host delle porte host della scheda base, delle porte IB HIC o di entrambi i tipi di porte.

Fasi

1. Da Gestore di sistema di SANtricity, selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **Cambia Feature Pack**.

3. Fare clic su **Sfoglia**, quindi selezionare il Feature Pack che si desidera applicare.
4. Tipo `CHANGE` sul campo.
5. Fare clic su **Cambia**.

   Viene avviata la migrazione dei Feature Pack. Entrambi i controller si riavviano automaticamente due volte per rendere effettivo il nuovo Feature Pack. Una volta completato il riavvio, lo storage array torna allo stato di risposta.

6. Verificare che le porte host dispongano del protocollo previsto.
   a. Da Gestione sistema di SANtricity, selezionare **hardware**.
   b. Fare clic su **Mostra retro dello shelf**.
   c. Selezionare l'immagine per Controller A o Controller B.
   d. Selezionare **Visualizza impostazioni** dal menu di scelta rapida.
   e. Selezionare la scheda **interfacce host**.
   f. Fare clic su **Mostra altre impostazioni**.
   g. Esaminare i dettagli mostrati per le porte della scheda base e le porte HIC (etichettate "slotto 1") e verificare che ciascun tipo di porta disponga del protocollo previsto.

Quali sono le prossime novità?

Passare a. "Completa la conversione del protocollo host".

Conversione completa del protocollo host per E2800

Dopo aver convertito il protocollo delle porte host, è necessario eseguire ulteriori operazioni prima di poter utilizzare il nuovo protocollo.

I passaggi dipendono dai protocolli di inizio e fine delle porte host della scheda base e delle porte HIC.

Conversione completa da FC a iSCSI

Se tutte le porte host sono state convertite da FC a iSCSI, è necessario configurare la rete iSCSI.

Fasi

1. Configurare gli switch.

   È necessario configurare gli switch utilizzati per il trasporto del traffico iSCSI in base alle raccomandazioni

del vendor per iSCSI. Questi consigli possono includere sia direttive di configurazione che aggiornamenti del codice.

2. Da Gestore di sistema di SANtricity, selezionare **hardware › Configura porte iSCSI**.
3. Selezionare le impostazioni della porta.

   È possibile configurare la rete iSCSI in diversi modi. Rivolgersi all'amministratore di rete per suggerimenti sulla scelta della configurazione migliore per l'ambiente in uso.

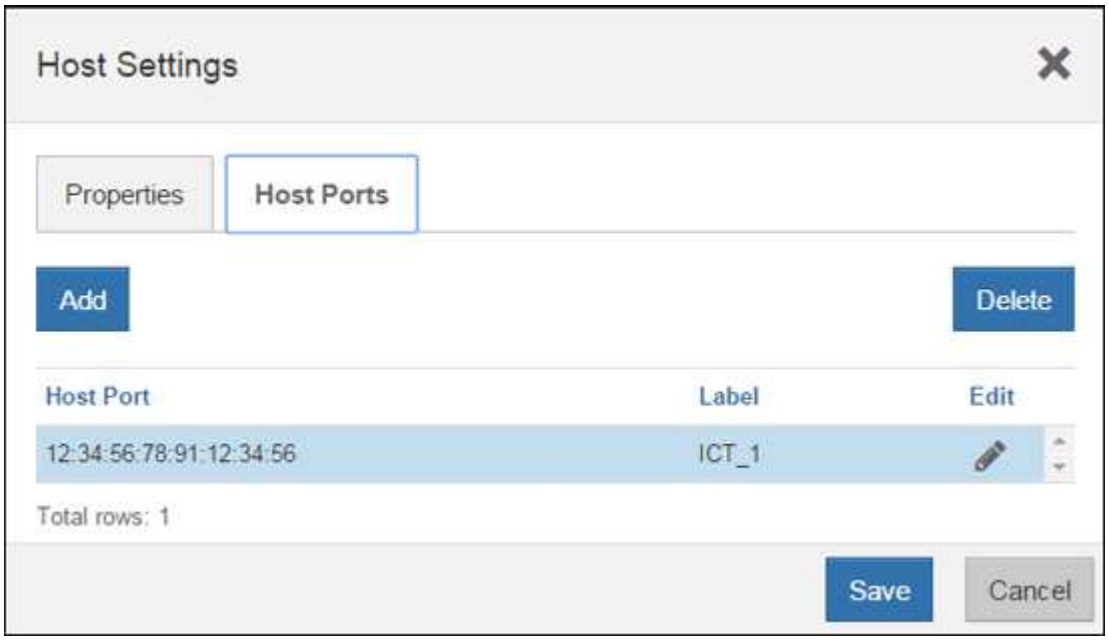
4. Aggiornare le definizioni degli host in Gestore di sistema di SANtricity.

   Per istruzioni su come aggiungere host o cluster di host, consultare la guida in linea di Gestione di sistema di SANtricity.

   a. Selezionare **Storage › Hosts** (Storage[host]).
   b. Selezionare l'host a cui associare la porta e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

      Viene visualizzata la finestra di dialogo host Settings (Impostazioni host).

   c. Fare clic sulla scheda **host Ports** (Porte host).



   d. Fare clic su **Add** (Aggiungi) e utilizzare la finestra di dialogo **Add host Port** (Aggiungi porta host) 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 FC 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.

   e. Fare clic su **Delete** (Elimina) e utilizzare la finestra di dialogo **Delete host Port** (Elimina porta host) per rimuovere (annullare l'associazione) un identificatore di porta host.

      L'opzione **Delete** 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.

f. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni dell'identificatore della porta host.

g. Ripetere questa procedura per aggiungere e rimuovere eventuali identificatori di porta host aggiuntivi.

5. Riavviare l'host o eseguire una nuova scansione in modo che l'host scopra correttamente le LUN.
6. Eseguire il remount dei volumi o iniziare a utilizzare il volume a blocchi.

Conversione completa da iSCSI a FC

Se tutte le porte host sono state convertite da iSCSI a FC, è necessario configurare la rete FC.

Fasi

1. Installare l'utility HBA e determinare le WWPN dell'iniziatore.
2. Fare una zona tra gli switch.

   Lo zoning degli switch consente agli host di connettersi allo storage e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

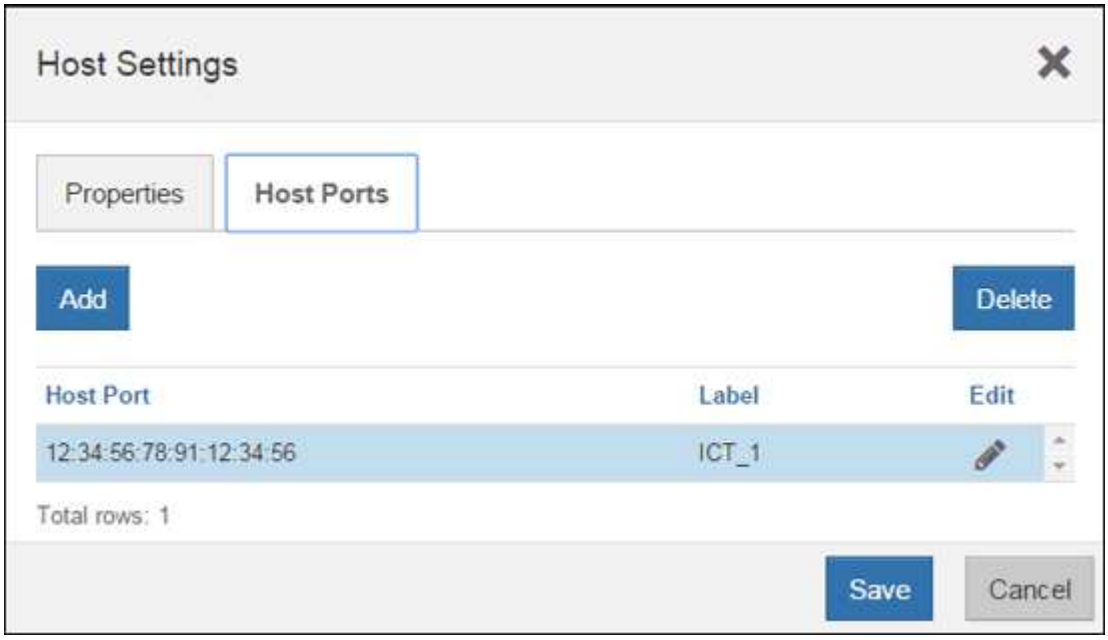
3. Aggiornare le definizioni degli host in Gestore di sistema di SANtricity.

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

   b. Selezionare l'host a cui associare la porta e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

      Viene visualizzata la finestra di dialogo host Settings (Impostazioni host).

   c. Fare clic sulla scheda **host Ports** (Porte host).



   d. Fare clic su **Add** (Aggiungi) e utilizzare la finestra di dialogo **Add host Port** (Aggiungi porta host) 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 FC 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.

e. Fare clic su **Delete** (Elimina) e utilizzare la finestra di dialogo **Delete host Port** (Elimina porta host) per rimuovere (annullare l'associazione) un identificatore di porta host.

   L'opzione **Delete** 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.

f. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni dell'identificatore della porta host.

g. Ripetere questa procedura per aggiungere e rimuovere eventuali identificatori di porta host aggiuntivi.

4. Riavviare l'host o eseguire una nuova scansione in modo che l'host scopra correttamente lo storage mappato.
5. Eseguire il remount dei volumi o iniziare a utilizzare il volume a blocchi.

Conversione completa da FC a FC/iSCSI

Se in precedenza disponevano di tutte le porte host FC e ne sono state convertite alcune in iSCSI, potrebbe essere necessario modificare la configurazione esistente per supportare iSCSI.

È possibile utilizzare una delle seguenti opzioni per utilizzare le nuove porte iSCSI. Le fasi esatte dipendono dalle topologie di rete attuali e pianificate. L'opzione 1 presuppone che si desideri collegare nuovi host iSCSI all'array. L'opzione 2 presuppone che si desideri convertire gli host collegati alle porte convertite da FC a iSCSI.

Opzione 1: Spostare gli host FC e aggiungere nuovi host iSCSI

1. Spostare gli host FC dalle nuove porte iSCSI alle porte che rimangono FC.
2. Se non si utilizzano già SFP a doppio protocollo, rimuovere eventuali SFP FC.
3. Collegare nuovi host iSCSI a queste porte, direttamente o utilizzando uno switch.
4. Configurare la rete iSCSI per i nuovi host e porte. Per istruzioni, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Opzione 2: Conversione degli host FC in iSCSI

1. Spegnere gli host FC collegati alle porte convertite.
2. Fornire una topologia iSCSI per le porte convertite. Ad esempio, convertire qualsiasi switch da FC a iSCSI.
3. Se non si utilizzano già SFP a doppio protocollo, rimuovere gli SFP FC dalle porte convertite e sostituirli con SFP iSCSI o SFP a doppio protocollo.
4. Collegare i cavi agli SFP nelle porte convertite e verificare che siano collegati allo switch o all'host iSCSI corretto.
5. Accendere gli host.
6. Utilizzare "Matrice di interoperabilità NetApp" Tool per configurare gli host iSCSI.
7. Modificare la partizione host per aggiungere gli ID delle porte host iSCSI e rimuovere gli ID delle porte host FC.
8. Dopo il riavvio degli host iSCSI, utilizzare le procedure applicabili sugli host per registrare i volumi e renderli disponibili per il sistema operativo.

- A seconda del sistema operativo in uso, il software per la gestione dello storage (hot_add e SMdevices) include due utility. Queste utility consentono di registrare i volumi con gli host e di visualizzare i nomi dei dispositivi applicabili ai volumi.
- Potrebbe essere necessario utilizzare strumenti e opzioni specifici forniti con il sistema operativo per rendere disponibili i volumi (ovvero, assegnare lettere di unità, creare punti di montaggio e così via). Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Conversione completa da iSCSI a FC/iSCSI

Se in precedenza disponevano di tutte le porte host iSCSI e ne sono state convertite alcune in FC, potrebbe essere necessario modificare la configurazione esistente per supportare FC.

È possibile utilizzare una delle seguenti opzioni per utilizzare le nuove porte FC. Le fasi esatte dipendono dalle topologie di rete attuali e pianificate. L'opzione 1 presuppone che si desideri collegare nuovi host FC all'array. L'opzione 2 presuppone che si desideri convertire gli host collegati alle porte convertite da iSCSI a FC.

Opzione 1: Spostare gli host iSCSI e aggiungere nuovi host FC

1. Spostare gli host iSCSI dalle nuove porte FC alle porte che rimangono iSCSI.
2. Se non si utilizzano già SFP a doppio protocollo, rimuovere eventuali SFP FC.
3. Collegare i nuovi host FC a queste porte, direttamente o utilizzando uno switch.
4. Configurare la rete FC per i nuovi host e porte. Per istruzioni, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Opzione 2: Conversione degli host iSCSI in FC

1. Spegnere gli host iSCSI collegati alle porte convertite.
2. Fornire una topologia FC per le porte convertite. Ad esempio, convertire qualsiasi switch da iSCSI a FC.
3. Se non si utilizzano già SFP a doppio protocollo, rimuovere gli SFP iSCSI dalle porte convertite e sostituirli con SFP FC o SFP a doppio protocollo.
4. Collegare i cavi agli SFP nelle porte convertite e verificare che siano collegati allo switch o all'host FC corretto.
5. Accendere gli host.
6. Utilizzare "Matrice di interoperabilità NetApp" Tool per configurare gli host FC.
7. Modificare la partizione host per aggiungere gli ID delle porte host FC e rimuovere gli ID delle porte host iSCSI.
8. Dopo il riavvio dei nuovi host FC, utilizzare le procedure applicabili sugli host per registrare i volumi e renderli disponibili per il sistema operativo.
   - A seconda del sistema operativo in uso, il software per la gestione dello storage (hot_add e SMdevices) include due utility. Queste utility consentono di registrare i volumi con gli host e di visualizzare i nomi dei dispositivi applicabili ai volumi.
   - Potrebbe essere necessario utilizzare strumenti e opzioni specifici forniti con il sistema operativo per rendere disponibili i volumi (ovvero, assegnare lettere di unità, creare punti di montaggio e così via). Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Conversione completa da FC/iSCSI a FC

Se in precedenza si utilizzava una combinazione di porte host FC e porte host iSCSI e si convertivano tutte le porte in FC, potrebbe essere necessario modificare la configurazione esistente per utilizzare le nuove porte

FC.

È possibile utilizzare una delle seguenti opzioni per utilizzare le nuove porte FC. Le fasi esatte dipendono dalle topologie di rete attuali e pianificate. L'opzione 1 presuppone che si desideri collegare nuovi host FC all'array. L'opzione 2 presuppone che si desideri convertire gli host collegati alle porte 1 e 2 da iSCSI a FC.

Opzione 1: Rimuovere gli host iSCSI e aggiungere gli host FC

1. Se non si utilizzano già SFP a doppio protocollo, rimuovere eventuali SFP iSCSI e sostituirli con SFP FC o SFP a doppio protocollo.
2. Se non si utilizzano già SFP a doppio protocollo, rimuovere eventuali SFP FC.
3. Collegare i nuovi host FC a queste porte, direttamente o utilizzando uno switch
4. Configurare la rete FC per i nuovi host e porte. Per istruzioni, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Opzione 2: Conversione degli host iSCSI in FC

1. Spegnere gli host iSCSI collegati alle porte convertite.
2. Fornire una topologia FC per queste porte. Ad esempio, convertire qualsiasi switch connesso a tali host da iSCSI a FC.
3. Se non si utilizzano già SFP a doppio protocollo, rimuovere gli SFP iSCSI dalle porte e sostituirli con SFP FC o SFP a doppio protocollo.
4. Collegare i cavi agli SFP e verificare che siano collegati allo switch o all'host FC corretto.
5. Accendere gli host.
6. Utilizzare "Matrice di interoperabilità NetApp" Tool per configurare gli host FC.
7. Modificare la partizione host per aggiungere gli ID delle porte host FC e rimuovere gli ID delle porte host iSCSI.
8. Dopo il riavvio dei nuovi host FC, utilizzare le procedure applicabili sugli host per registrare i volumi e renderli disponibili per il sistema operativo.
    - A seconda del sistema operativo in uso, il software per la gestione dello storage (hot_add e SMdevices) include due utility. Queste utility consentono di registrare i volumi con gli host e di visualizzare i nomi dei dispositivi applicabili ai volumi.
    - Potrebbe essere necessario utilizzare strumenti e opzioni specifici forniti con il sistema operativo per rendere disponibili i volumi (ovvero, assegnare lettere di unità, creare punti di montaggio e così via). Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Conversione completa da FC/iSCSI a iSCSI

Se in precedenza si utilizzava una combinazione di porte host FC e porte host iSCSI e si convertivano tutte le porte in iSCSI, potrebbe essere necessario modificare la configurazione esistente per utilizzare le nuove porte iSCSI.

È possibile utilizzare una delle seguenti opzioni per utilizzare le nuove porte iSCSI. Le fasi esatte dipendono dalle topologie di rete attuali e pianificate. L'opzione 1 presuppone che si desideri collegare nuovi host iSCSI all'array. L'opzione 2 presuppone che si desideri convertire gli host da FC a iSCSI.

Opzione 1: Rimuovere gli host FC e aggiungere gli host iSCSI

1. Se non si utilizzano già SFP a doppio protocollo, rimuovere eventuali SFP FC e sostituirli con SFP iSCSI o

SFP a doppio protocollo.

2. Collegare nuovi host iSCSI a queste porte, direttamente o utilizzando uno switch.
3. Configurare la rete iSCSI per i nuovi host e porte. Per istruzioni, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Opzione 2: Conversione degli host FC in iSCSI

1. Spegnere gli host FC collegati alle porte convertite.
2. Fornire una topologia iSCSI per queste porte. Ad esempio, convertire qualsiasi switch connesso a tali host da FC a iSCSI.
3. Se non si utilizzano già SFP a doppio protocollo, rimuovere gli SFP FC dalle porte e sostituirli con SFP iSCSI o SFP a doppio protocollo.
4. Collegare i cavi agli SFP e verificare che siano collegati all'host o allo switch iSCSI corretto.
5. Accendere gli host.
6. Utilizzare "Matrice di interoperabilità NetApp" Tool per configurare gli host ISCSI.
7. Modificare la partizione host per aggiungere gli ID delle porte host iSCSI e rimuovere gli ID delle porte host FC.
8. Dopo il riavvio dei nuovi host iSCSI, utilizzare le procedure applicabili sugli host per registrare i volumi e renderli disponibili per il sistema operativo.
   - A seconda del sistema operativo in uso, il software per la gestione dello storage (hot_add e SMdevices) include due utility. Queste utility consentono di registrare i volumi con gli host e di visualizzare i nomi dei dispositivi applicabili ai volumi.
   - Potrebbe essere necessario utilizzare strumenti e opzioni specifici forniti con il sistema operativo per rendere disponibili i volumi (ovvero, assegnare lettere di unità, creare punti di montaggio e così via). Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

E5700

Manutenzione dell'hardware E5700

Per il sistema storage E5700, è possibile eseguire procedure di manutenzione sui seguenti componenti.

Batterie

Una batteria è inclusa in un contenitore del controller e conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA.

Controller

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

Canister

I contenitori sono costituiti da tre tipi diversi: Contenitori per ventole di alimentazione (alimentatori) che forniscono una fonte di alimentazione ridondante e un raffreddamento adeguato in uno shelf o uno shelf di controller da 12 o 24 dischi; contenitori di alimentazione utilizzati per la ridondanza dell'alimentazione in uno

shelf di controller da 60 dischi o in uno shelf di dischi; e i contenitori per ventole utilizzati per il raffreddamento dello shelf di controller da 60 dischi o dello shelf di dischi.

Dischi

Un'unità è un dispositivo elettromeccanico che fornisce i supporti di storage fisici per i dati.

HICS (host Interface Card)

È possibile installare una scheda di interfaccia host (HIC) all'interno di un contenitore di controller. Il controller E5700 include porte host integrate sulla scheda controller stessa, nonché porte host sull'HIC opzionale. Le porte host integrate nel controller sono chiamate porte host baseboard. Le porte host integrate nell'HIC sono chiamate porte HIC.

Protocollo della porta host

È possibile convertire il protocollo di un host in un protocollo diverso in modo da stabilire compatibilità e comunicazione.

Batterie

Requisiti per la sostituzione della batteria E5700

Prima di sostituire una batteria E5700, esaminare i requisiti e le considerazioni.

Ogni contenitore del controller include una batteria che conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA.

Recovery Guru

Se il guru del ripristino in Gestione sistema di SANtricity riporta uno dei seguenti stati, è necessario sostituire la batteria interessata:

- Guasto alla batteria
- Sostituzione della batteria necessaria

Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.

Panoramica della procedura

Per proteggere i dati, è necessario sostituire una batteria guasta il prima possibile.

Di seguito è riportata una panoramica dei passaggi per la sostituzione di una batteria nei controller E5700 (E5724, EF570 o E5760):

1. Portare il controller offline (solo duplex).
2. Rimuovere il contenitore del controller.
3. Sostituire la batteria.
4. Sostituire il contenitore del controller.
5. Portare il controller online (solo duplex).

Requisiti

Se si intende sostituire una batteria guasta, è necessario disporre di:

- Una batteria sostitutiva.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

  In alternativa, è possibile utilizzare l'interfaccia della riga di comando (CLI) per eseguire alcune procedure. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:

  - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
  - **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Sostituire la batteria E5700

È possibile sostituire una batteria guasta in un sistema storage E5700.

A proposito di questa attività

Ogni contenitore del controller E5700 include una batteria che conserva i dati memorizzati nella cache in caso di interruzione dell'alimentazione CA. Se il guru del ripristino in Gestione sistema di SANtricity segnala lo stato di batteria guasta o lo stato Sostituzione batteria richiesta, è necessario sostituire la batteria interessata.

Prima di iniziare

- Verificare che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Revisione "Requisiti per la sostituzione della batteria E5700".
- Assicurarsi di disporre di quanto segue:
  - Una batteria sostitutiva.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare il controller offline (duplex)

Se si dispone di una configurazione duplex, posizionare il controller interessato offline in modo da poter rimuovere in sicurezza la batteria guasta. Il controller che non si sta mettendo offline deve essere in linea (nello stato ottimale).

Eseguire questa operazione solo se lo storage array dispone di due controller (configurazione duplex).

Fasi

1. Da Gestore di sistema di SANtricity, esaminare i dettagli nel guru del ripristino per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi da risolvere.
2. Dall'area Details (Dettagli) del Recovery Guru, determinare quale batteria sostituire.
3. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

4. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

5. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
     iii. Selezionare il controller che si desidera mettere offline.
     iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

> Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

- In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

  Per il controller A: `set controller [a] availability=offline`

  Per il controller B: `set controller [b] availability=offline`

6. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

Fase 2: Rimuovere il contenitore del controller

Prima di poter rimuovere la batteria guasta, è necessario rimuovere il contenitore del controller.

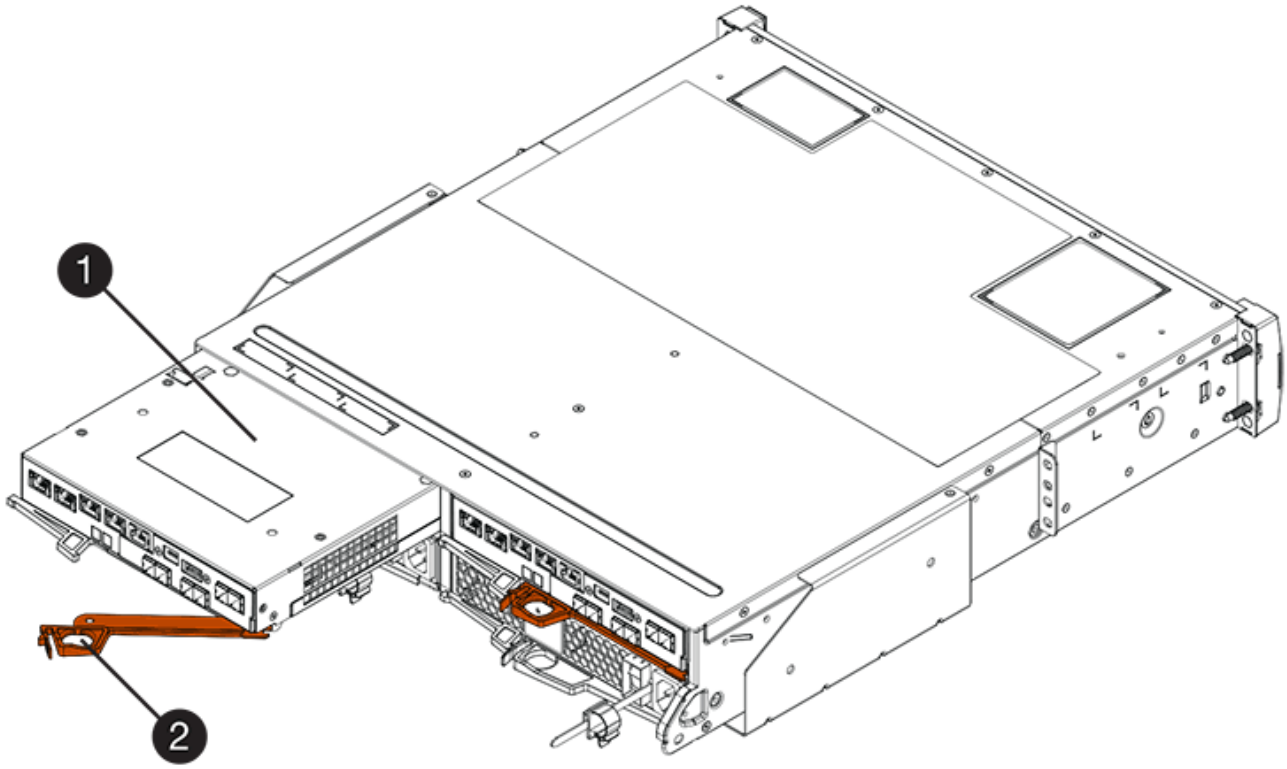
Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

   > Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se le porte host sul contenitore del controller utilizzano ricetrasmettitori SFP+, lasciarli installati.
5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
6. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

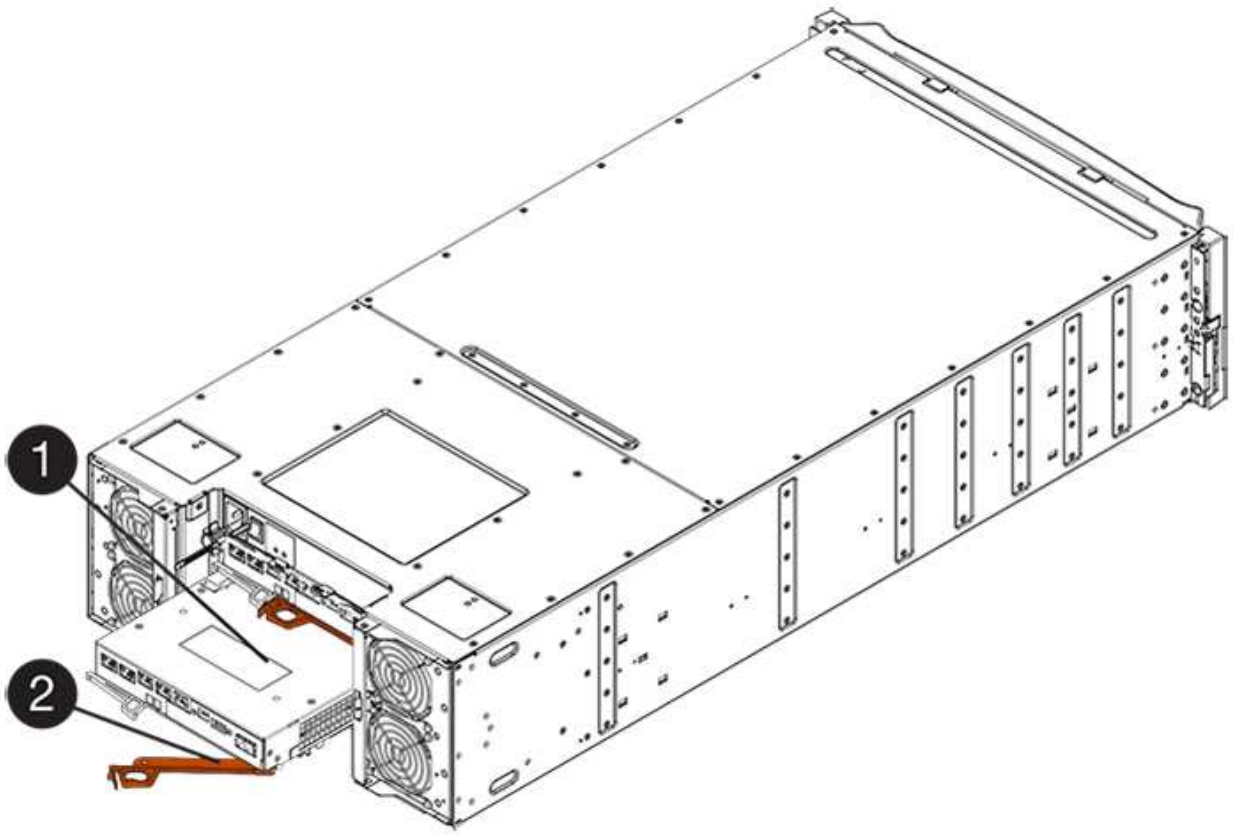
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

7. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf del controller E5724, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

8. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
9. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere la batteria guasta

Dopo aver rimosso il contenitore del controller dallo shelf del controller, rimuovere la batteria.

Fasi

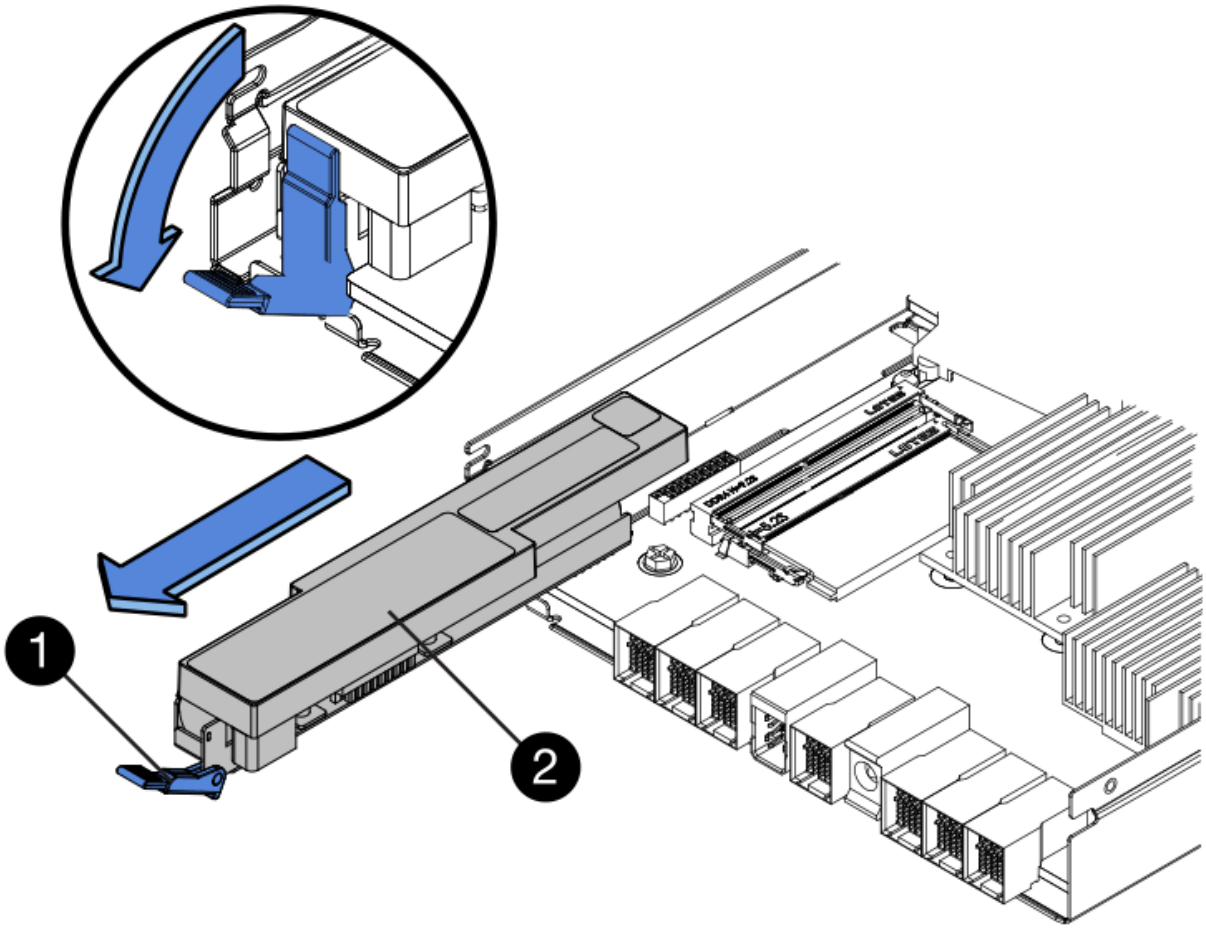
1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *LED cache interna attiva*

(2) *batteria*

3. Individuare il dispositivo di chiusura blu della batteria.
4. Sbloccare la batteria spingendo il dispositivo di chiusura verso il basso e lontano dal contenitore del controller.



(1) *dispositivo di chiusura a scatto della batteria*

(2) *batteria*

5. Sollevare la batteria ed estrarla dal contenitore del controller.
6. Seguire le procedure appropriate per il riciclaggio o lo smaltimento della batteria guasta.

> Per rispettare le normative IATA (International Air Transport Association), non spedire mai una batteria al litio via etere se non è installata nello shelf del controller.

Fase 4: Installare una nuova batteria

Dopo aver rimosso la batteria guasta, installarne una nuova.

Fasi

1. Disimballare la nuova batteria e riutilizzarla su una superficie piana e priva di scariche elettrostatiche.

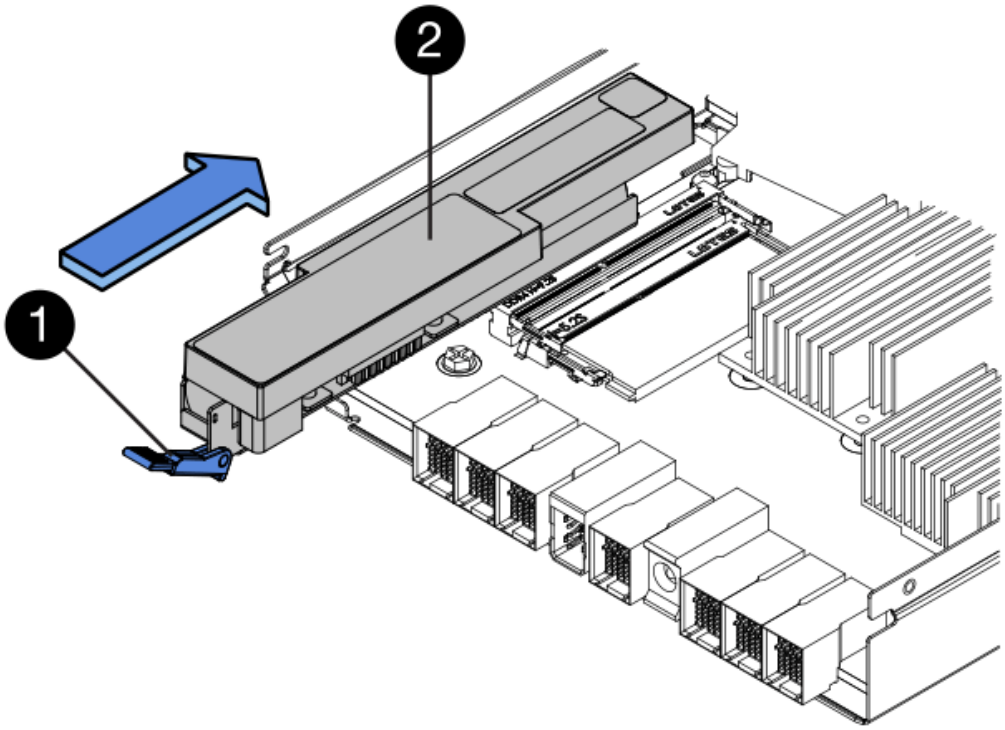
> Per rispettare le normative IATA in materia di sicurezza, le batterie sostitutive vengono spedite con uno stato di carica (SoC) pari o inferiore al 30%. Quando si riattiva l'alimentazione, tenere presente che il caching in scrittura non viene ripristinato fino a quando la batteria sostitutiva non viene completamente caricata e non viene completato il ciclo di apprendimento iniziale.

2. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
3. Inserire la batteria nel contenitore del controller inclinandola leggermente verso il basso.

   Inserire la flangia metallica nella parte anteriore della batteria nello slot sul fondo del contenitore del controller e far scorrere la parte superiore della batteria sotto il piccolo perno di allineamento sul lato sinistro del contenitore.

4. Spostare il dispositivo di chiusura della batteria verso l'alto per fissare la batteria.

   Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.



   (1) *dispositivo di chiusura a scatto della batteria*

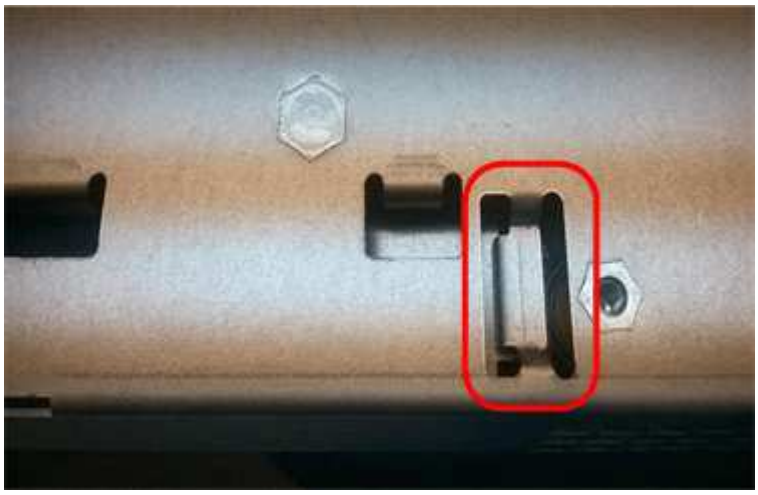
   (2) *batteria*

5. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

   Possibili danni all'hardware — la flangia metallica sulla parte anteriore della batteria deve essere inserita completamente nello slot sul contenitore del controller (come mostrato nella prima figura). Se la batteria non è installata correttamente (come mostrato nella seconda figura), la flangia metallica potrebbe entrare in contatto con la scheda del controller, danneggiando il controller quando si applica l'alimentazione.

   - **Corretto** — la flangia metallica della batteria è completamente inserita nello slot del controller:

- **Errato** — la flangia metallica della batteria non è inserita nello slot del controller:

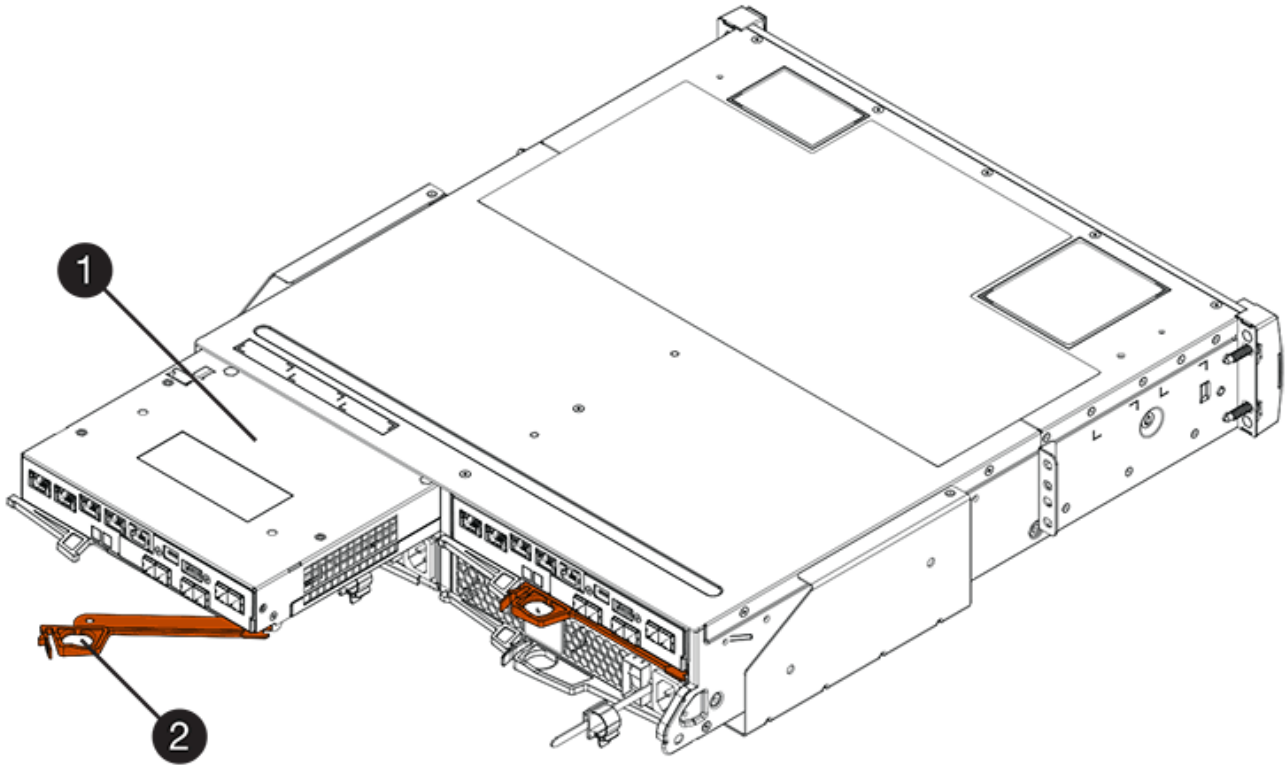


Fase 5: Reinstallare il contenitore del controller

Dopo aver installato la nuova batteria, reinstallare il contenitore del controller nello shelf del controller.

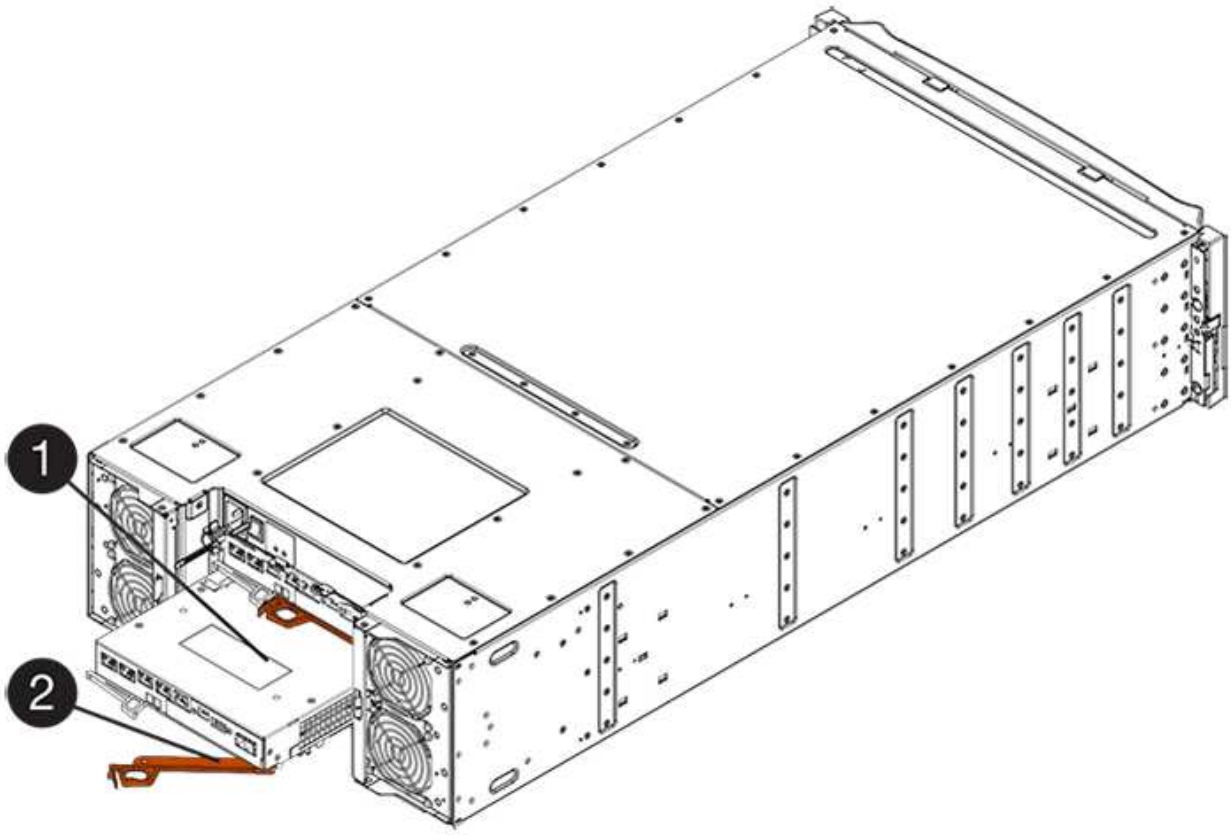
Fasi

1. Per reinstallare il coperchio sul contenitore del controller, far scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Ricollegare tutti i cavi.

Fase 6: Posizionamento del controller online (duplex)

Per una configurazione duplex, posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

> Eseguire questa operazione solo se lo storage array dispone di due controller.

Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   > La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
     host.

(1) *LED collegamento host*

(2) *LED di attenzione (ambra)*

(3) *Display a sette segmenti*

2. Portare il controller online utilizzando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf**.

iii. Selezionare il controller che si desidera mettere in linea.

iv. Selezionare **Place Online** (Esegui online) dal menu di scelta rapida e confermare che si desidera eseguire l'operazione.

Il sistema mette il controller in linea.

- In alternativa, è possibile portare i controller online utilizzando i seguenti comandi CLI:

Per il controller A: `set controller [a] availability=online;`

Per il controller B: `set controller [b] availability=online;`

3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che la batteria e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e la batteria.

   Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se necessario, raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support** > **Support Center** > **Diagnostics**.
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione della batteria è completata. È possibile riprendere le normali operazioni.

Controller

Requisiti per la sostituzione del controller E5700

Prima di sostituire un controller E5700, esaminare i requisiti e le considerazioni.

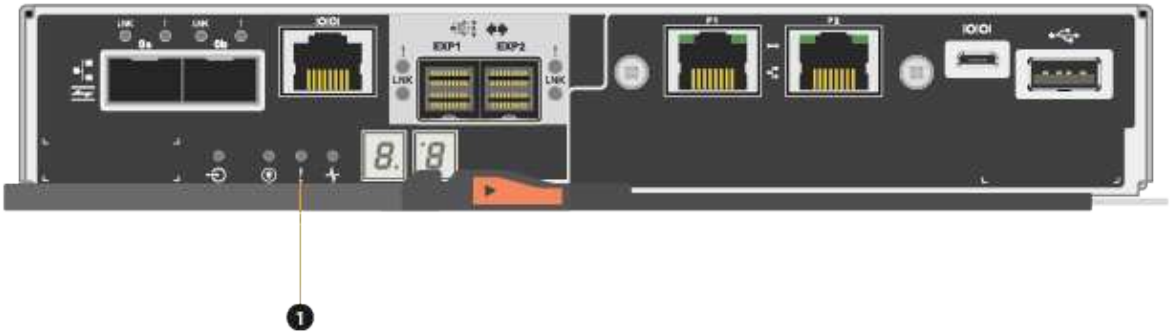
Ogni contenitore di controller contiene una scheda controller, una batteria e una scheda di interfaccia host (HIC) opzionale.

Panoramica della procedura

Quando si sostituisce un contenitore del controller guasto, rimuovere la batteria e l'HIC, se installato, dal contenitore del controller originale e installarli nel contenitore del controller sostitutivo.

È possibile determinare se si dispone di un contenitore del controller guasto in due modi:

- Il guru del ripristino in Gestione di sistema di SANtricity richiede la sostituzione del contenitore del controller.
- Il LED di attenzione ambra sul contenitore del controller è acceso, a indicare che il controller è guasto.



(1) *LED attenzione*

> La figura mostra un esempio di contenitore del controller; le porte host sul contenitore del controller potrebbero essere diverse.

- Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Requisiti per la sostituzione di un controller guasto

Prima di sostituire un controller, è necessario disporre di:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo.

> I controller sostitutivi vengono forniti con 16 GB di memoria preinstallati. Se il controller richiede la configurazione da 64 GB, utilizzare il kit di aggiornamento fornito prima di installare il controller sostitutivo.

- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Un cacciavite Phillips n. 1.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del

controller.

In alternativa, è possibile utilizzare l'interfaccia della riga di comando (CLI) per eseguire alcune procedure. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:

- **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
- **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Requisiti di configurazione duplex

Per uno shelf di controller con due controller (configurazione duplex), è possibile sostituire un contenitore di controller mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:

- Il secondo contenitore del controller nello shelf ha uno stato ottimale.
- Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Sostituire il controller in configurazione duplex

È possibile sostituire un contenitore di controller in una configurazione duplex (a due controller) per i seguenti shelf di controller:

- Shelf di controller E5724
- Shelf di controller E5760

A proposito di questa attività

Ogni contenitore di controller contiene una scheda controller, una batteria e una scheda di interfaccia host (HIC) opzionale. Quando si sostituisce un contenitore del controller, è necessario rimuovere la batteria e l'HIC, se installato, dal contenitore del controller originale, quindi installarli nel contenitore del controller sostitutivo.

> Questa attività è valida solo per gli array di storage con due controller (configurazione duplex).

Prima di iniziare

Assicurarsi di disporre di quanto segue:

- Un contenitore del controller sostitutivo con lo stesso numero di parte del contenitore del controller che si sta sostituendo. (Vedere il passaggio 1 per verificare il codice del ricambio).
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Cacciavite Phillips n. 1.
- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del controller (duplex)

Preparare la sostituzione di un contenitore del controller verificando che il contenitore del controller di ricambio disponga del numero di parte FRU corretto, eseguendo il backup della configurazione e raccogliendo i dati di supporto. Se il controller è ancora online, è necessario portarlo offline.

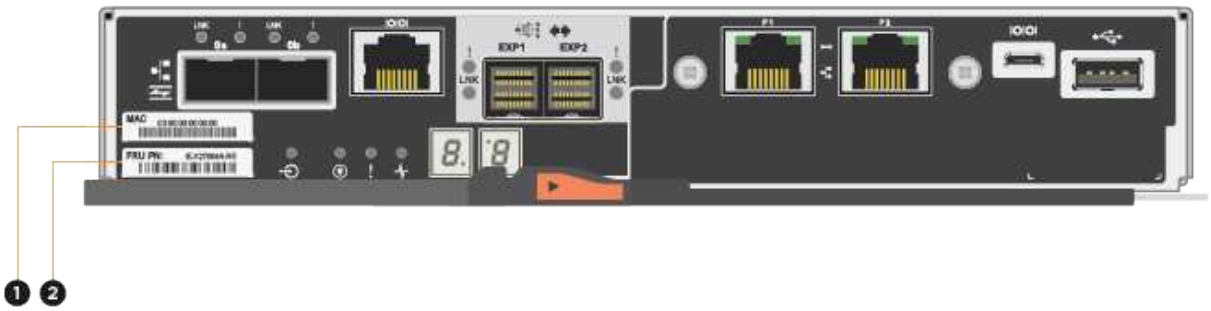
Fasi

1. Disimballare il nuovo contenitore del controller e riutilizzarlo su una superficie piana e priva di elettricità statica.

   Conservare il materiale di imballaggio da utilizzare per la spedizione del contenitore del controller guasto.

   > I controller sostitutivi vengono forniti con 16 GB di memoria preinstallati. Se il controller richiede la configurazione da 64 GB, utilizzare il kit di aggiornamento fornito prima di installare il controller sostitutivo.

2. Individuare le etichette dell'indirizzo MAC e del numero di parte della FRU sul retro del contenitore del controller.



   (1) *MAC address:* Indirizzo MAC per la porta di gestione 1 ("P1"). Se si è utilizzato DHCP per ottenere l'indirizzo IP del controller originale, è necessario questo indirizzo per connettersi al nuovo controller.

   (2) *numero di parte FRU:* questo numero deve corrispondere al numero di parte di ricambio per il controller attualmente installato.

3. Da Gestore di sistema di SANtricity, individuare il numero di parte di ricambio del contenitore del controller che si sta sostituendo.

   Quando un controller presenta un guasto e deve essere sostituito, il codice del ricambio viene visualizzato nell'area Details (Dettagli) del Recovery Guru. Se è necessario trovare questo numero manualmente, attenersi alla seguente procedura:

   a. Selezionare **hardware**.
   b. Individuare lo shelf del controller, contrassegnato dall'icona del controller .

c. Fare clic sull'icona del controller.

d. Selezionare il controller e fare clic su **Avanti**.

e. Nella scheda **base**, annotare il **numero di parte di ricambio** del controller.

4. Verificare che il numero di parte sostitutivo del controller guasto sia lo stesso del numero di parte FRU del controller sostitutivo.

> **Possibile perdita di accesso ai dati** — se i due numeri di parte non sono gli stessi, non tentare questa procedura. Inoltre, se il contenitore del controller guasto include una scheda di interfaccia host (HIC), è necessario installare tale HIC nel nuovo contenitore del controller. La presenza di controller non corrispondenti o HICS causa il blocco del nuovo controller quando lo si porta online.

5. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:

     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).

     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).

     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

6. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante la rimozione di un controller, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).

   b. Selezionare **Collect Support Data**.

   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

7. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:

     i. Selezionare **hardware**.

ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.

iii. Selezionare il controller che si desidera mettere offline.

iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

> Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

- In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

  Per il controller A: `set controller [a] availability=offline`

  Per il controller B: `set controller [b] availability=offline`

8. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

9. Selezionare **ricontrollare** dal Recovery Guru e confermare che nel campo **OK per rimuovere** nell'area Dettagli sia visualizzato **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

Fase 2: Rimozione del contenitore del controller (duplex)

Rimuovere un contenitore del controller per sostituire il contenitore guasto con uno nuovo.

Fasi

1. Indossare un braccialetto ESD o adottare altre precauzioni antistatiche.
2. Etichettare ciascun cavo collegato al contenitore del controller.
3. Scollegare tutti i cavi dal contenitore del controller.

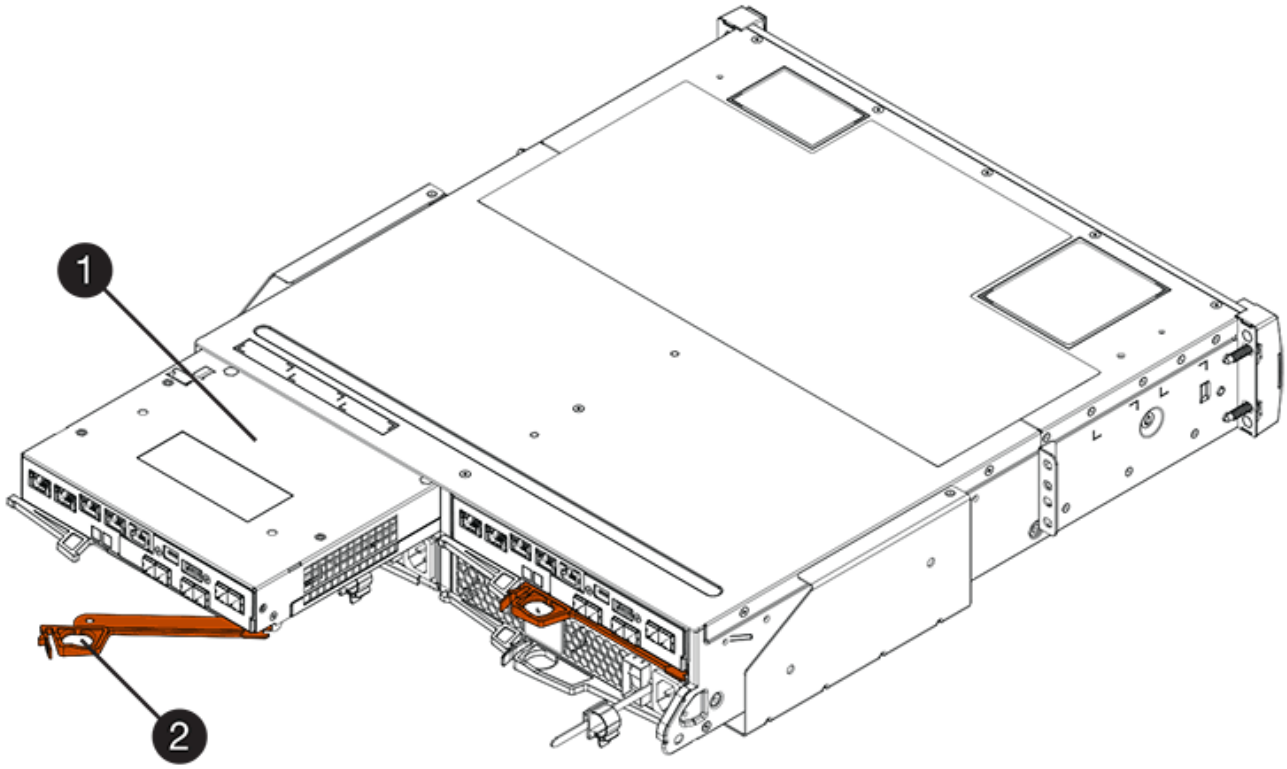
   > Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

4. Se il contenitore del controller dispone di un HIC che utilizza ricetrasmettitori SFP+, rimuovere gli SFP.

   Poiché è necessario rimuovere l'HIC dal contenitore del controller guasto, è necessario rimuovere eventuali SFP dalle porte HIC. Tuttavia, è possibile lasciare qualsiasi SFP installato nelle porte host della scheda base. Quando si ricollegano i cavi, è possibile spostare questi SFP nel nuovo contenitore del controller.

5. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.
6. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

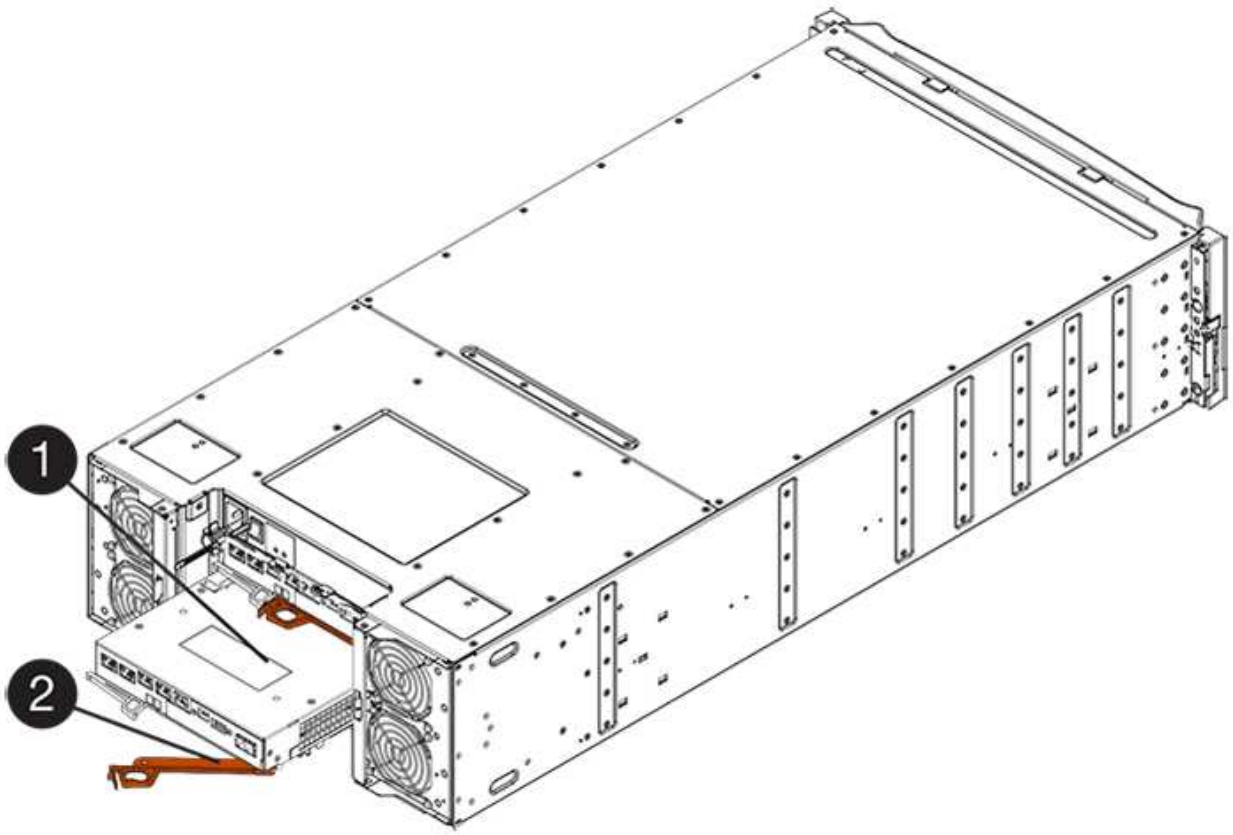
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

7. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf del controller E5724, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

8. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
9. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimozione della batteria (duplex)

Rimuovere la batteria per installare il nuovo controller.

Fasi

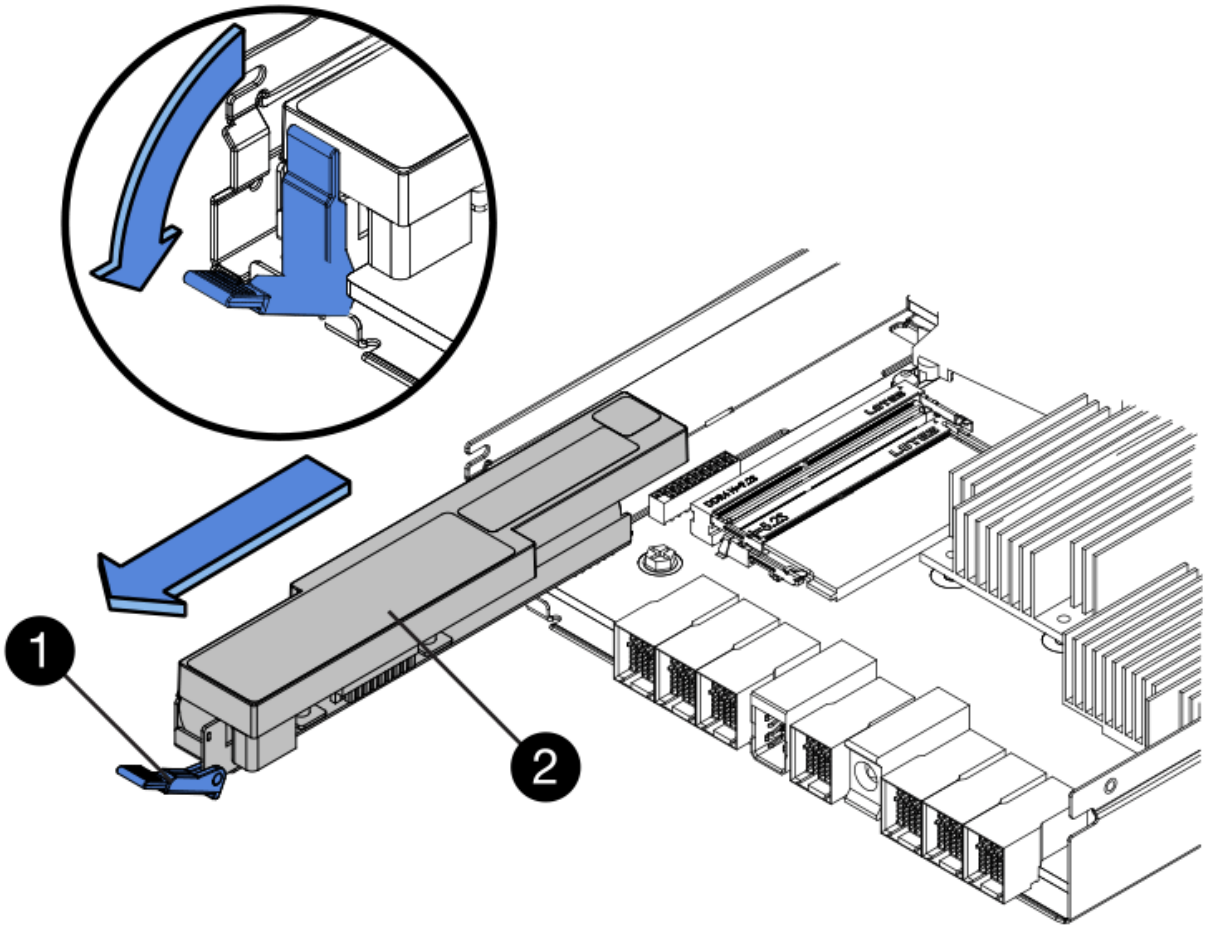
1. Per rimuovere il coperchio del contenitore del controller, premere il pulsante e rimuovere il coperchio facendolo scorrere.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *LED cache interna attiva*

(2) *batteria*

3. Individuare il dispositivo di chiusura blu della batteria.
4. Sbloccare la batteria spingendo il dispositivo di chiusura verso il basso e lontano dal contenitore del controller.



(1) *dispositivo di chiusura a scatto della batteria*

(2) *batteria*

5. Sollevare la batteria ed estrarla dal contenitore del controller.

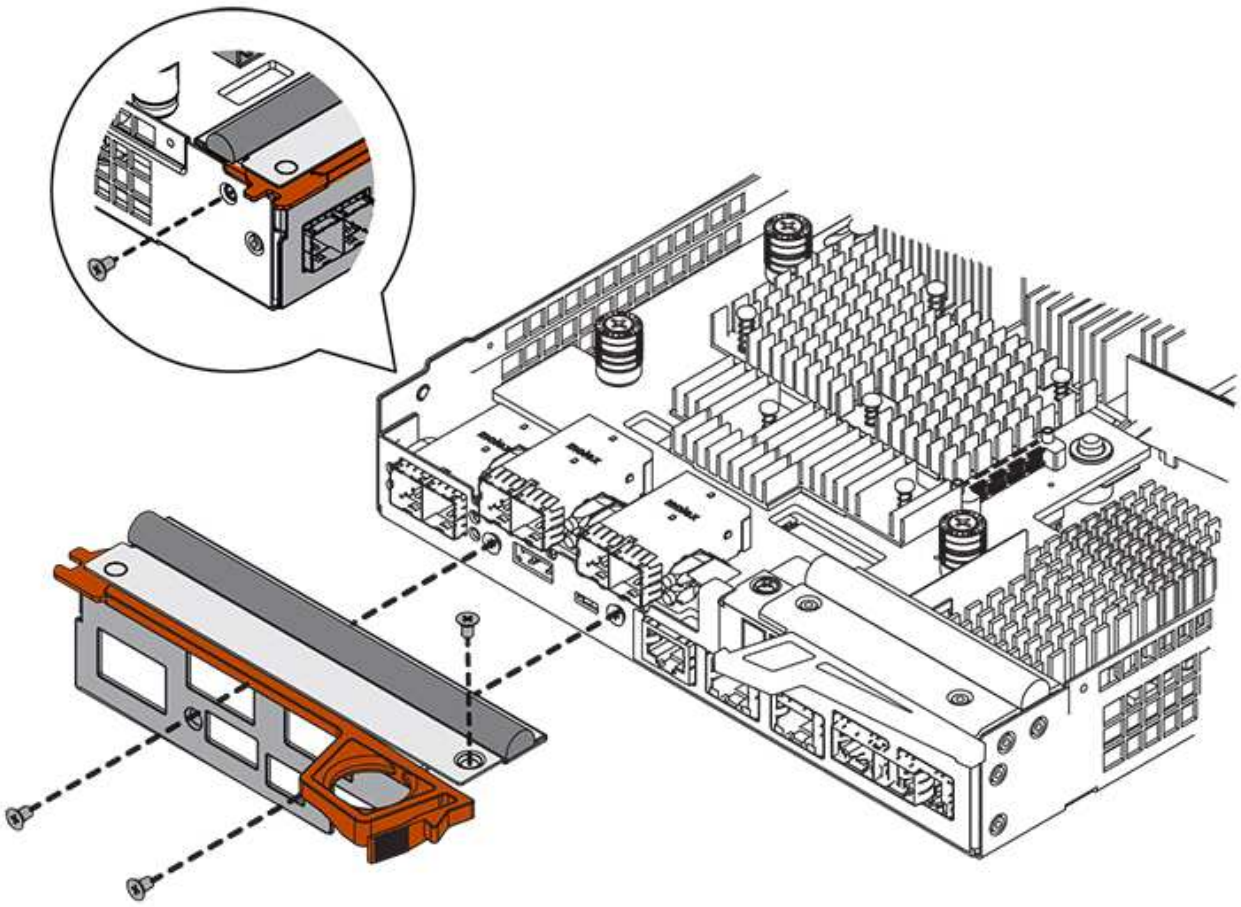
Fase 4: Rimozione della scheda di interfaccia host (duplex)

Se il contenitore del controller include una scheda di interfaccia host (HIC), rimuovere l'HIC dal contenitore del controller originale in modo da poterlo riutilizzare nel nuovo contenitore del controller.

Fasi

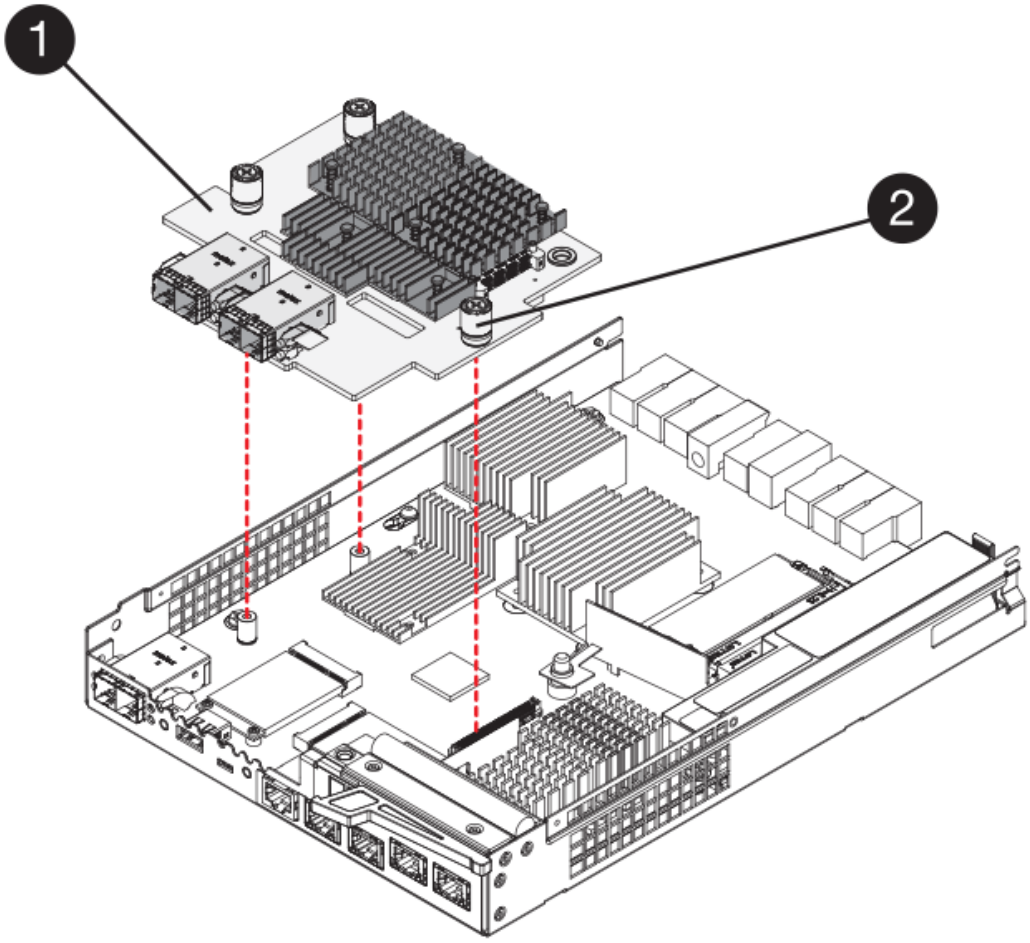
1. Utilizzando un cacciavite Phillips n. 1, rimuovere le viti che fissano la mascherina HIC al contenitore del controller.

   Sono presenti quattro viti: Una sulla parte superiore, una laterale e due sulla parte anteriore.



2. Rimuovere la piastra anteriore dell'HIC.
3. Utilizzando le dita o un cacciavite Phillips, allentare le tre viti a testa zigrinata che fissano l'HIC alla scheda del controller.
4. Scollegare con cautela l'HIC dalla scheda del controller sollevandola e facendola scorrere all'indietro.

> Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

5. Posizionare l'HIC su una superficie priva di elettricità statica.

Fase 5: Installazione della batteria (duplex)

Installare la batteria nel contenitore del controller di ricambio. È possibile installare la batteria rimossa dal contenitore del controller originale o installare una nuova batteria ordinata.

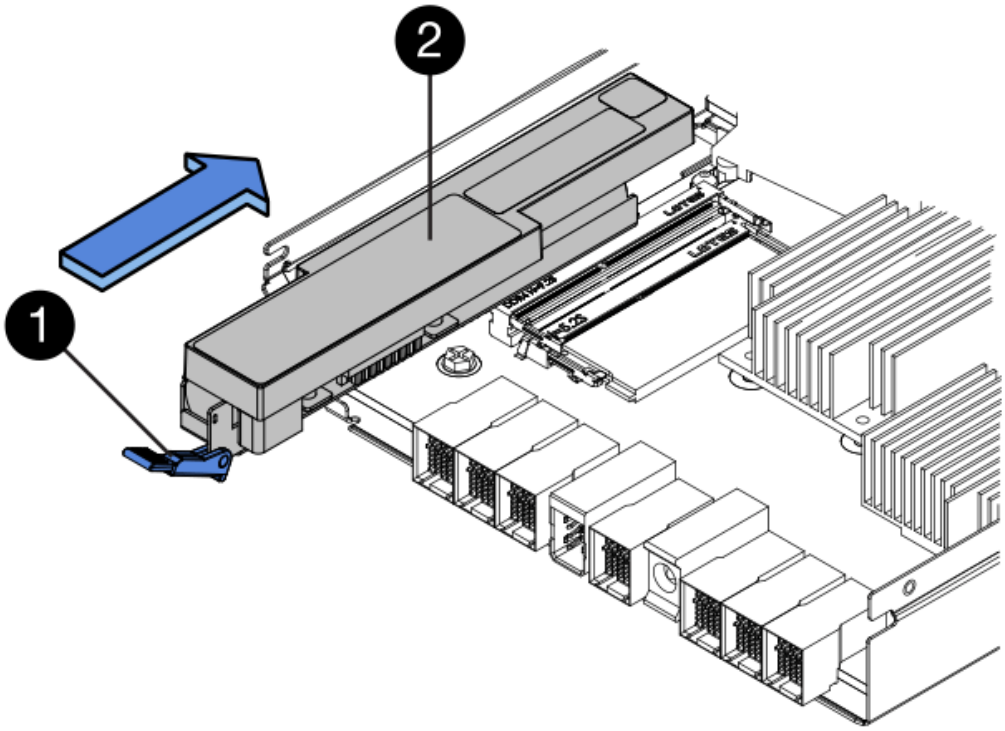
Fasi

1. Capovolgere il contenitore del controller sostitutivo, in modo che il coperchio rimovibile sia rivolto verso l'alto.
2. Premere il pulsante del coperchio verso il basso ed estrarre il coperchio.
3. Orientare il contenitore del controller in modo che lo slot della batteria sia rivolto verso di sé.
4. Inserire la batteria nel contenitore del controller inclinandola leggermente verso il basso.

   Inserire la flangia metallica nella parte anteriore della batteria nello slot sul fondo del contenitore del controller e far scorrere la parte superiore della batteria sotto il piccolo perno di allineamento sul lato sinistro del contenitore.

5. Spostare il dispositivo di chiusura della batteria verso l'alto per fissare la batteria.

Quando il dispositivo di chiusura scatta in posizione, la parte inferiore del dispositivo di chiusura si aggancia in uno slot metallico sul telaio.



(1) *dispositivo di chiusura a scatto della batteria*

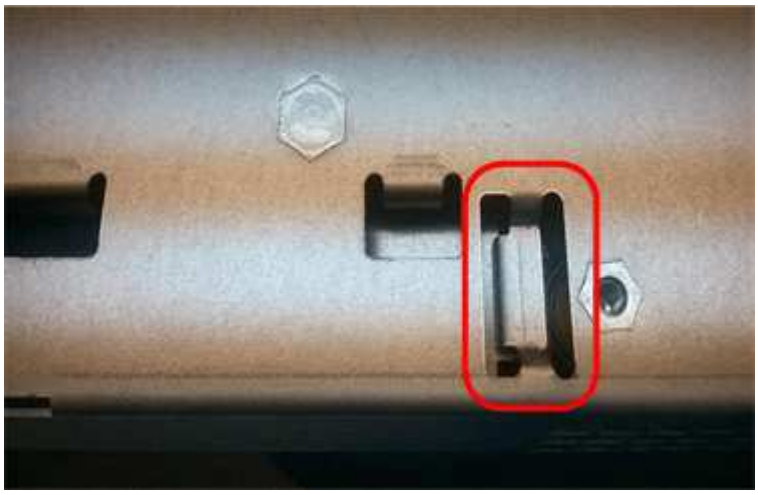
(2) *batteria*

6. Capovolgere il contenitore del controller per verificare che la batteria sia installata correttamente.

> **Possibili danni all'hardware** — la flangia metallica sulla parte anteriore della batteria deve essere inserita completamente nello slot sul contenitore del controller (come mostrato nella prima figura). Se la batteria non è installata correttamente (come mostrato nella seconda figura), la flangia metallica potrebbe entrare in contatto con la scheda del controller, danneggiando il controller quando si applica l'alimentazione.

   - **Corretto** — la flangia metallica della batteria è completamente inserita nello slot del controller:

- **Errato** — la flangia metallica della batteria non è inserita nello slot del controller:



Fase 6: Installazione della scheda di interfaccia host (duplex)

Se è stato rimosso un HIC dal contenitore del controller originale, è necessario installarlo nel nuovo contenitore del controller.

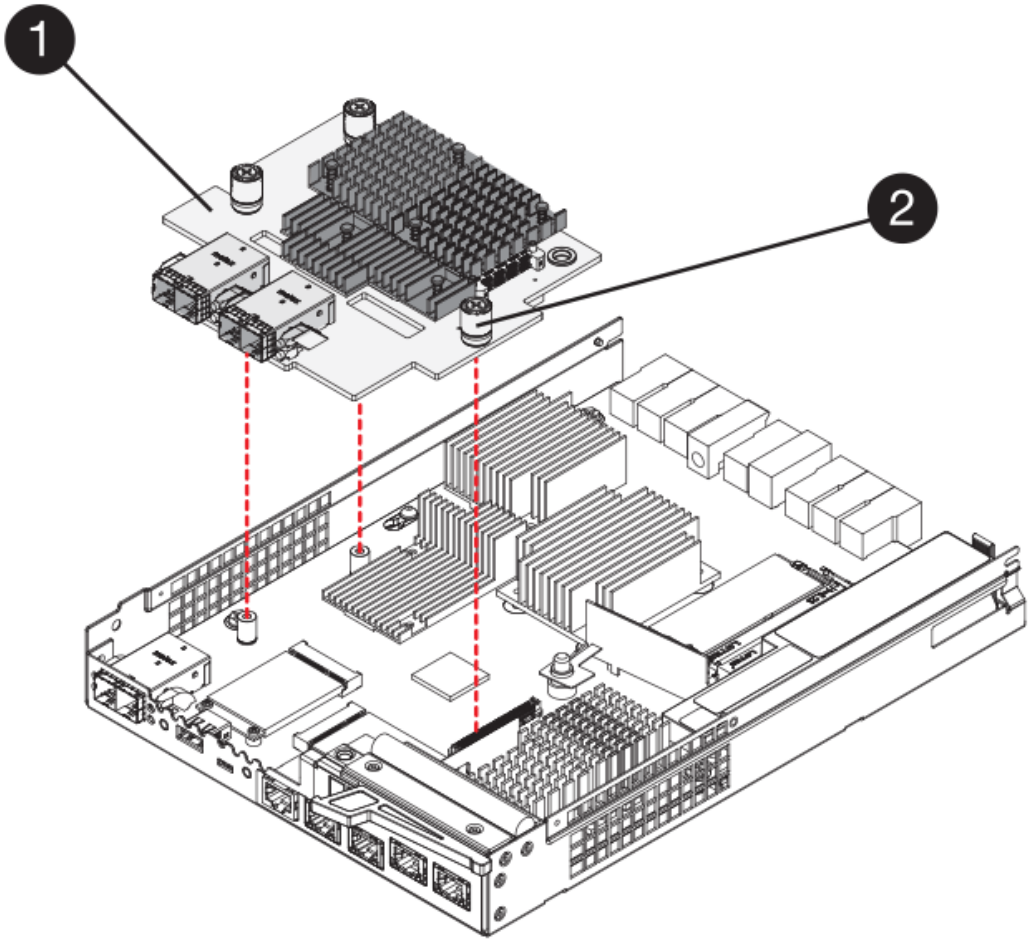
Fasi

1. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller sostitutivo, quindi rimuovere la piastra frontale.
2. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

3. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



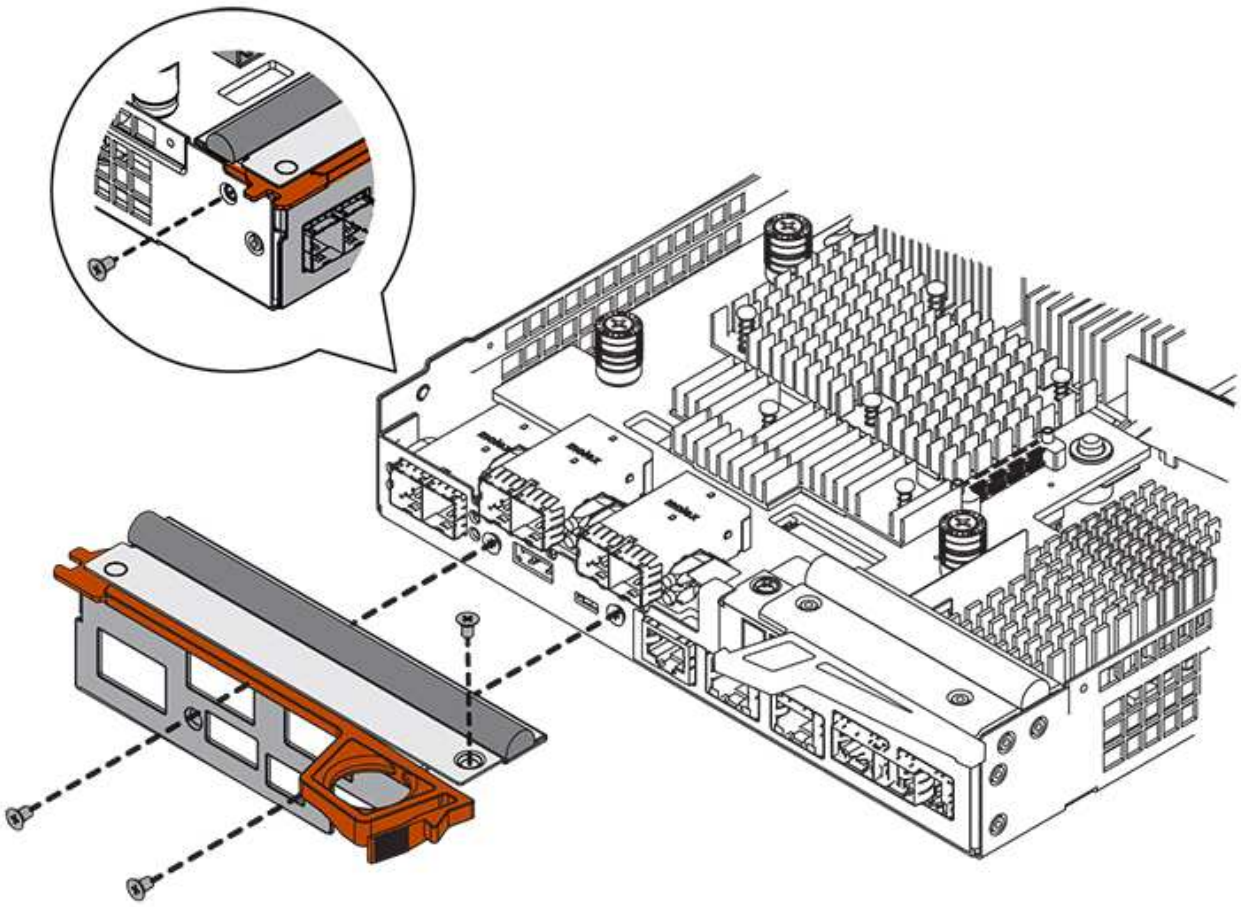
(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

4. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

5. Utilizzando un cacciavite Phillips n. 1, fissare la piastra anteriore HIC rimossa dal contenitore del controller originale al nuovo contenitore del controller con quattro viti.

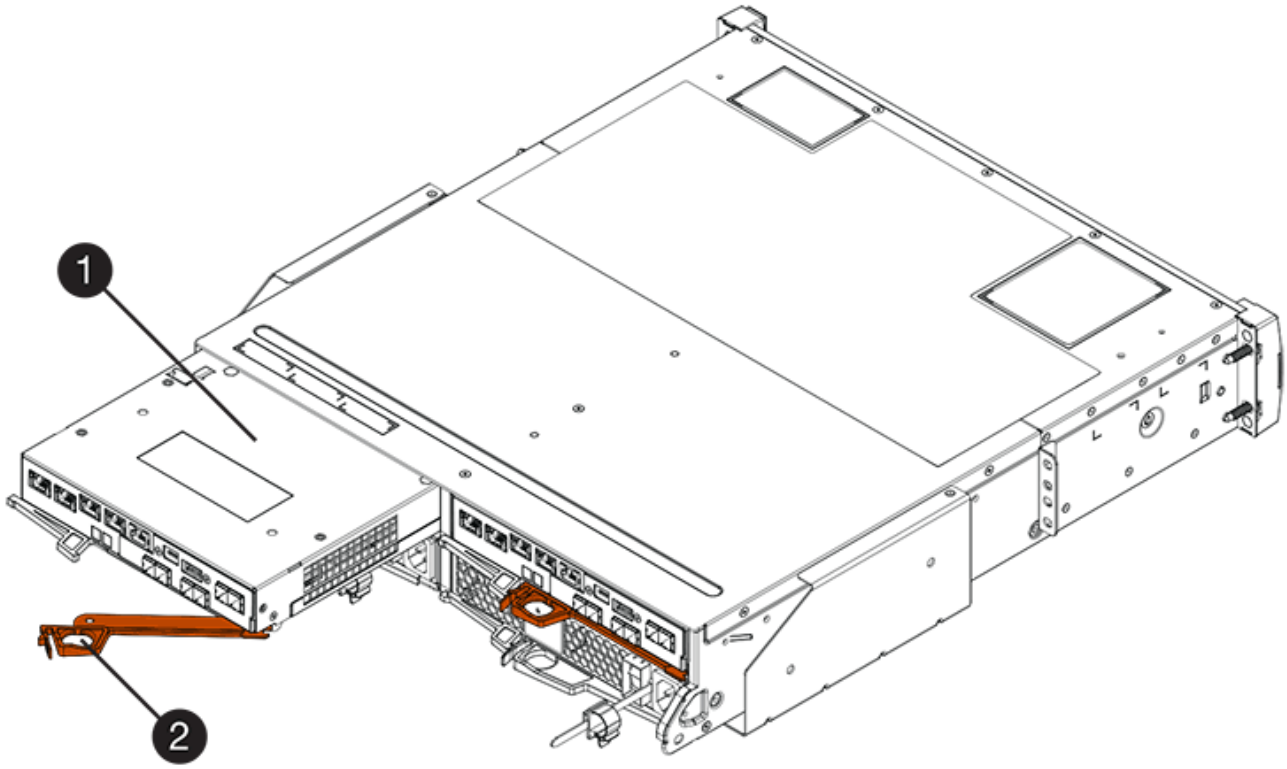


Fase 7: Installare il nuovo contenitore del controller (duplex)

Dopo aver installato la batteria e la scheda di interfaccia host (HIC), se inizialmente installata, è possibile installare il nuovo contenitore del controller nello shelf del controller.

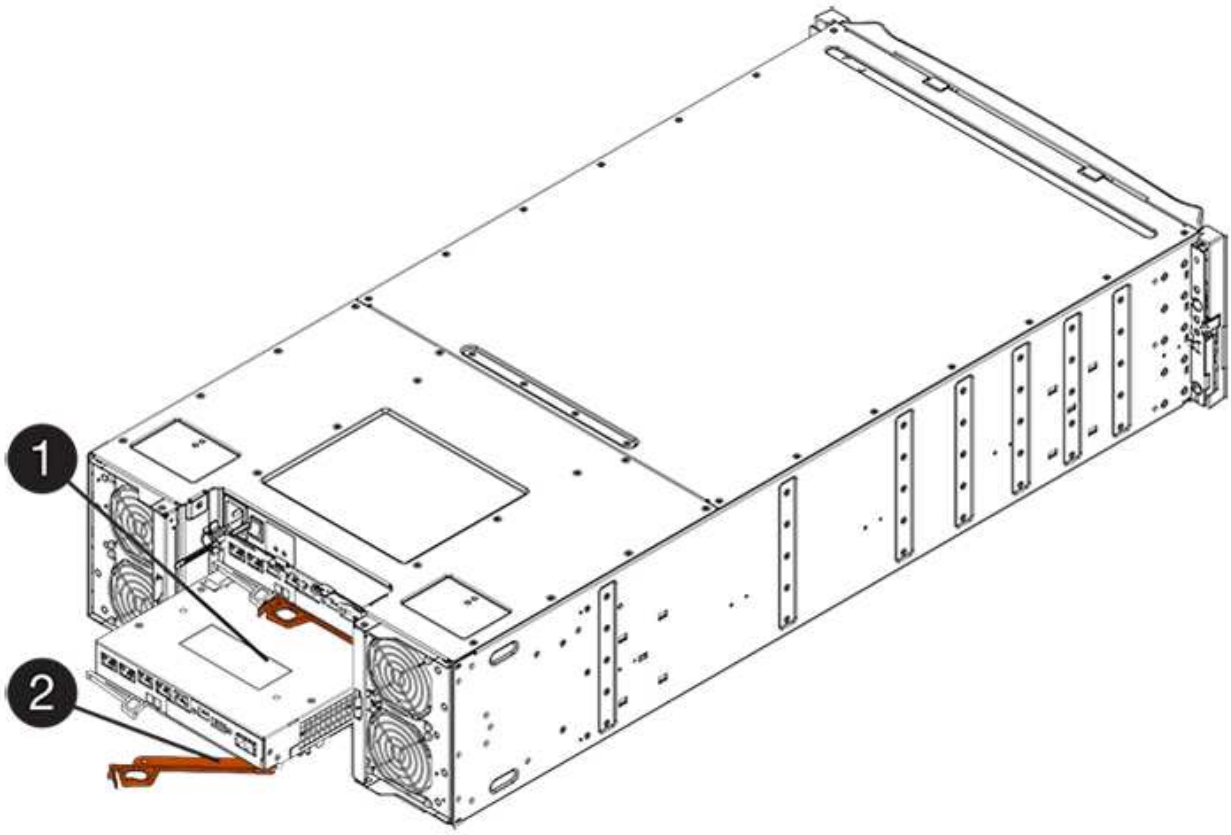
Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.



(1) *contenitore controller*

(2) *maniglia della camma*



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Installare gli SFP dal controller originale nelle porte host del nuovo controller e ricollegare tutti i cavi.

   Se si utilizzano più protocolli host, assicurarsi di installare gli SFP nelle porte host corrette.

6. Se il controller originale utilizzava DHCP per l'indirizzo IP, individuare l'indirizzo MAC sull'etichetta sul retro del controller sostitutivo. Chiedere all'amministratore di rete di associare il DNS/rete e l'indirizzo IP del controller rimosso con l'indirizzo MAC del controller sostitutivo.

   > Se il controller originale non ha utilizzato DHCP per l'indirizzo IP, il nuovo controller adotterà l'indirizzo IP del controller rimosso.

Fase 8: Sostituzione completa del controller (duplex)

Posizionare il controller online, raccogliere i dati di supporto e riprendere le operazioni.

Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

   Quando la comunicazione con l'altro controller viene ristabilita:

   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
   - Il LED di attenzione di colore ambra rimane acceso.
   - I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
     host.

(1) *LED collegamento host*

(2) *LED di attenzione (ambra)*

(3) *Display a sette segmenti*

2. Controllare i codici sul display a sette segmenti del controller quando torna online. Se sul display viene visualizzata una delle seguenti sequenze di ripetizione, rimuovere immediatamente il controller.

- **OE**, **L0**, ***blank*** (controller non corrispondenti)
- **OE**, **L6**, ***blank*** (HIC non supportato)

> **Possibile perdita di accesso ai dati** — se il controller appena installato mostra uno di questi codici e l'altro controller viene resettato per qualsiasi motivo, anche il secondo controller potrebbe bloccarsi.

3. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che il contenitore del controller sia installato correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se necessario, ridistribuire tutti i volumi al proprietario preferito.
   a. Selezionare **Storage › Volumes** (Storage[volumi]).
   b. Selezionare il **More › redistribuisci volumi**.
5. Fare clic su **hardware › supporto › Centro aggiornamenti** per verificare che sia installata la versione più recente del software SANtricity OS (firmware del controller).

   Se necessario, installare la versione più recente.

6. Se necessario, raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

Quali sono le prossime novità?

La sostituzione del controller è completata. È possibile riprendere le normali operazioni.

Canister

Requisiti per la sostituzione del filtro E5700

Prima di sostituire un contenitore E5700, esaminare i requisiti e le considerazioni.

I contenitori sono costituiti da tre tipi diversi: Contenitori per ventole di alimentazione (alimentatori) che forniscono una fonte di alimentazione ridondante e un raffreddamento adeguato in uno shelf o uno shelf di controller da 12 o 24 dischi; contenitori di alimentazione utilizzati per la ridondanza dell'alimentazione in uno shelf di controller da 60 dischi o in uno shelf di dischi; e i contenitori per ventole utilizzati per il raffreddamento dello shelf di controller da 60 dischi o dello shelf di dischi.

Alimentatore

> La procedura di sostituzione dell'alimentatore è applicabile per le sostituzioni IOM. Per sostituire il modulo IOM, eseguire la procedura di sostituzione dell'alimentatore.

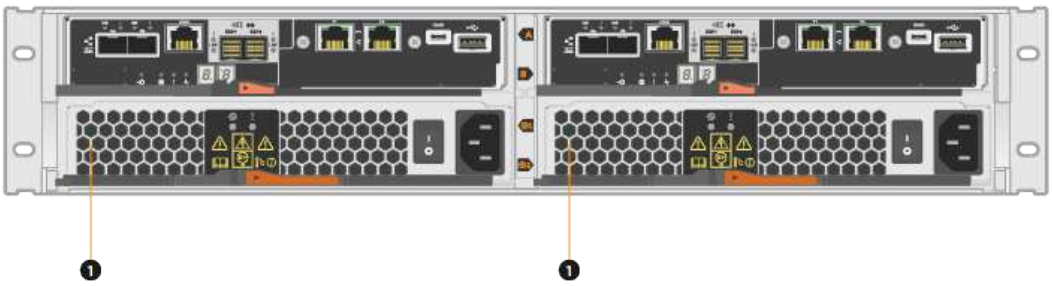
Ogni shelf di controller da 24 dischi o shelf di dischi include due alimentatori con ventole integrate. In Gestione sistema di SANtricity, questi sono denominati *canister per ventole di alimentazione*. In caso di guasto di un contenitore della ventola di alimentazione, è necessario sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante e di un raffreddamento adeguato.

Tipi di shelf per un alimentatore

È possibile sostituire un alimentatore nei seguenti shelf:

- Shelf di controller E5724
- Shelf di dischi DE224C

La figura seguente mostra un esempio di shelf di controller E5724 con due alimentatori (contenitori per ventole di alimentazione). Gli shelf di dischi DE224C sono identici, ma includono i moduli i/o (IOM) invece dei server di controllo.



(1) *Shelf del controller con due alimentatori (contenitori per ventole di alimentazione) sotto i contenitori del controller.*

Gli argomenti *sostituire l'alimentatore* non descrivono come sostituire un contenitore della ventola di alimentazione guasto in un vassoio dell'unità DE1600 o DE5600, che potrebbe essere collegato agli shelf dei controller E5700 o E2800. Per istruzioni su questi modelli di tray di dischi, fare riferimento a. "Ricollocamento di un contenitore della ventola di alimentazione nel vassoio dell'unità DE1600 o nel vassoio dell'unità DE5600".

Requisiti per la sostituzione di un alimentatore

Se si prevede di sostituire un alimentatore, tenere presenti i seguenti requisiti.

- È necessario disporre di un alimentatore sostitutivo (contenitore della ventola di alimentazione) supportato per il modello di shelf di controller o di unità.
- È necessario disporre di un braccialetto antistatico o adottare altre precauzioni antistatiche.
- È possibile sostituire un alimentatore (contenitore della ventola di alimentazione) mentre lo storage array è

acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:

- Il secondo alimentatore (contenitore della ventola di alimentazione) nello shelf ha uno stato ottimale.
- Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

> Se il secondo alimentatore (contenitore della ventola di alimentazione) nello shelf non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore della ventola di alimentazione, contattare il supporto tecnico.

Filtro a carboni attivi

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori di alimentazione per la ridondanza dell'alimentazione.

Tipi di shelf per un contenitore di alimentazione

È possibile sostituire un contenitore di alimentazione nei seguenti shelf:

- Shelf di controller E5760
- Shelf di dischi DE460C

Gli argomenti di *sostituire il contenitore di alimentazione* non descrivono come sostituire un contenitore di alimentazione guasto in un vassoio del disco DE6600, che potrebbe essere collegato allo shelf del controller.

La figura seguente mostra il retro di uno shelf di dischi DE460C con i due contenitori di alimentazione:

La figura seguente mostra un contenitore di alimentazione:

Requisiti per la sostituzione di un contenitore di alimentazione

Se si prevede di sostituire un contenitore di alimentazione, tenere presenti i seguenti requisiti.

- Si dispone di un contenitore di alimentazione sostitutivo supportato per il modello di shelf di controller o di unità.
- Si dispone di un contenitore di alimentazione installato e funzionante.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- È possibile sostituire un contenitore di alimentazione mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:
- L'altro contenitore di alimentazione nello shelf ha uno stato ottimale.

> Durante l'esecuzione della procedura, l'altro contenitore di alimentazione alimenta entrambe le ventole per garantire che l'apparecchiatura non si surriscaldi.

- Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

> Se il secondo contenitore di alimentazione nel ripiano non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore di alimentazione, contattare il supporto tecnico.

Filtro della ventola

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori per ventole.

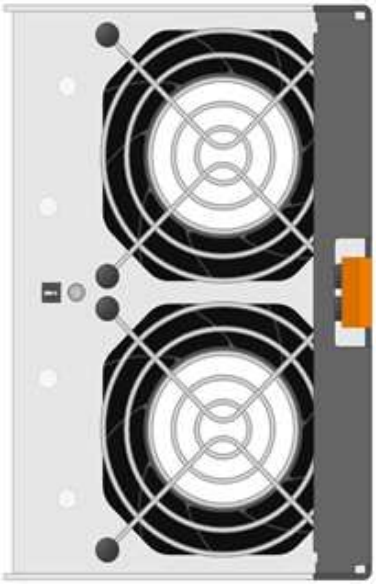
Tipi di shelf per un contenitore di ventole

È possibile sostituire un contenitore della ventola nei seguenti ripiani:

- Shelf di controller E5760
- Shelf di dischi DE460C

Gli argomenti di *sostituire il contenitore della ventola* non descrivono come sostituire un contenitore della ventola guasto in un vassoio del disco DE6600, che potrebbe essere collegato allo shelf del controller.

La figura seguente mostra un filtro a carboni attivi della ventola:



La figura seguente mostra il retro di uno shelf DE460C con due contenitori per ventole:

Possibili danni all'apparecchiatura — se si sostituisce un contenitore della ventola con l'alimentazione accesa, è necessario completare la procedura di sostituzione entro 30 minuti per evitare il rischio di surriscaldamento dell'apparecchiatura.

Requisiti per la sostituzione di un filtro a carboni attivi della ventola

Se si prevede di sostituire un filtro a carboni attivi della ventola, tenere presenti i seguenti requisiti.

- Si dispone di una ventola sostitutiva (ventola) supportata per il proprio modello di shelf di controller o di unità.
- È presente un contenitore della ventola installato e in funzione.
- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Se si esegue questa procedura con l'alimentazione accesa, è necessario completarla entro 30 minuti per evitare il surriscaldamento dell'apparecchiatura.

- È possibile sostituire un contenitore di ventole mentre lo storage array è acceso ed esegue operazioni di i/o host, a condizione che siano soddisfatte le seguenti condizioni:
  - Il secondo contenitore della ventola nello shelf ha uno stato ottimale.
  - Il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione sistema di SANtricity visualizza **Sì**, a indicare che è possibile rimuovere questo componente in tutta sicurezza.

> Se il secondo contenitore della ventola nello shelf non ha uno stato ottimale o se il Recovery Guru indica che non è possibile rimuovere il contenitore della ventola, contattare il supporto tecnico.

Sostituire l'alimentatore E5700 (24 dischi)

È possibile sostituire un alimentatore in un array E5700 con uno shelf da 24 dischi, che include i seguenti tipi di shelf:

- Shelf di controller E5724
- Shelf di dischi DE224C

A proposito di questa attività

Ogni shelf di controller da 24 dischi o shelf di dischi include due alimentatori con ventole integrate. In Gestione sistema di SANtricity, questi sono denominati *canister per ventole di alimentazione*. In caso di guasto di un contenitore della ventola di alimentazione, è necessario sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante e di un raffreddamento adeguato.

È possibile sostituire un alimentatore mentre lo storage array è acceso ed esegue operazioni di i/o host, Se il secondo alimentatore dello shelf ha uno stato ottimale e il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione di sistema di SANtricity visualizza **Sì**.

Prima di iniziare

- Revisione "Requisiti per la sostituzione del filtro E5700".
- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con l'alimentatore. Selezionare **ricontrollare** dal Recovery Guru per assicurarsi che nessun altro elemento debba essere affrontato per primo.
- Verificare che il LED di attenzione ambra sull'alimentatore sia acceso, a indicare che l'alimentatore o la ventola integrata sono guasti. Contattare il supporto tecnico per assistenza se entrambi gli alimentatori dello shelf hanno i LED di attenzione ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un alimentatore sostitutivo supportato per il modello di shelf di controller o di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione dell'alimentatore

Preparare la sostituzione di un alimentatore in uno shelf di controller da 24 dischi o in uno shelf di dischi.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale alimentatore si è guastato. Queste informazioni sono disponibili nell'area Details (Dettagli) del Recovery Guru o nelle informazioni visualizzate per lo shelf.

   a. Selezionare **hardware**.
   b. Guarda la potenza e la ventola Icone a destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta l'alimentatore guasto.

      In caso di guasto di un componente, una o entrambe le icone sono rosse.

   c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.
   d. Selezionare uno degli alimentatori.
   e. Nelle schede **alimentatori** e **ventole**, controllare gli stati dei contenitori delle ventole di alimentazione, degli alimentatori e delle ventole per determinare quale alimentatore deve essere sostituito.

      Un componente con stato **Failed** deve essere sostituito.

      > Se il secondo contenitore dell'alimentatore nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo l'alimentatore guasto. Contattare invece il supporto tecnico per assistenza.

3. Dal retro dello storage array, osservare i LED di attenzione per individuare l'alimentatore da rimuovere.

   È necessario sostituire l'alimentatore con il LED attenzione acceso.

   - Se il LED di alimentazione è **verde fisso**, l'alimentatore funziona correttamente. Se è **spento**, l'alimentatore è guasto, l'interruttore CA è spento, il cavo di alimentazione CA non è installato correttamente o la tensione di ingresso del cavo di alimentazione CA non rientra nei margini (si è verificato un problema all'estremità della fonte del cavo di alimentazione CA).

     Se il LED attenzione è di colore **ambra fisso**, l'alimentatore o la ventola integrata presentano un

guasto.

Fase 2: Rimuovere l'alimentatore guasto

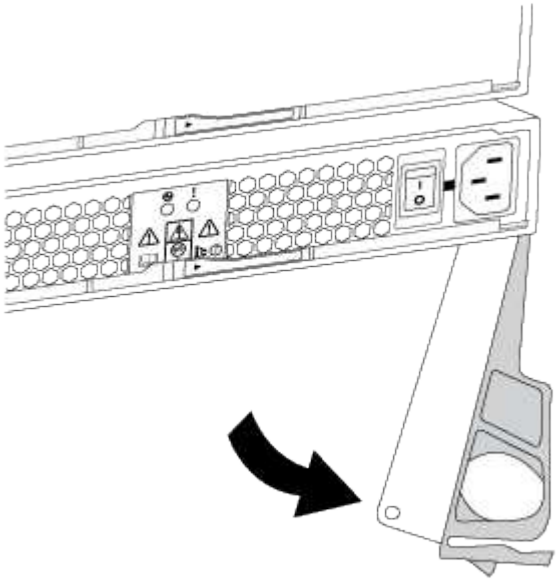
Rimuovere un alimentatore guasto per poterlo sostituire con uno nuovo.

Fasi

1. Disimballare il nuovo alimentatore e posizionare il nuovo alimentatore su una superficie piana vicino allo shelf del disco.

   Conservare tutti i materiali di imballaggio per l'utilizzo quando si restituisce l'alimentatore guasto.

2. Spegnere l'alimentatore e scollegare i cavi di alimentazione:
   a. Spegnere l'interruttore di alimentazione dell'alimentatore.
   b. Aprire il fermo del cavo di alimentazione, quindi scollegare il cavo di alimentazione dall'alimentatore.
   c. Scollegare il cavo di alimentazione dalla presa di corrente.
3. Premere il fermo sulla maniglia della camma dell'alimentatore, quindi aprire la maniglia della camma per rilasciare completamente l'alimentatore dal piano intermedio.



4. Utilizzare la maniglia della camma per estrarre l'alimentatore dal sistema.

   Quando si rimuove un alimentatore, utilizzare sempre due mani per sostenerne il peso.

   Quando si rimuove l'alimentatore, un'aletta oscilla in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

Fase 3: Installare un nuovo alimentatore

Installare un nuovo alimentatore per sostituire quello guasto.

Fasi

1. Assicurarsi che l'interruttore di accensione/spegnimento del nuovo alimentatore sia in posizione **Off**.
2. Con entrambe le mani, sostenere e allineare i bordi dell'alimentatore con l'apertura nello chassis del sistema, quindi spingere delicatamente l'alimentatore nello chassis utilizzando la maniglia della camma.

   Gli alimentatori sono dotati di chiavi e possono essere installati in un solo modo.

   > Non esercitare una forza eccessiva quando si inserisce l'alimentatore nel sistema, poiché si potrebbe danneggiare il connettore.

3. Chiudere la maniglia della camma in modo che il fermo scatti in posizione di blocco e l'alimentatore sia inserito completamente.
4. Ricollegare il cablaggio dell'alimentatore:
   a. Ricollegare il cavo di alimentazione all'alimentatore e alla fonte di alimentazione.
   b. Fissare il cavo di alimentazione all'alimentatore utilizzando il relativo fermo.
5. Accendere il nuovo contenitore della ventola di alimentazione.

Fase 4: Sostituzione completa dell'alimentatore

Verificare che il nuovo alimentatore funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Sul nuovo alimentatore, verificare che il LED di alimentazione verde sia acceso e che il LED di attenzione ambra sia spento.
2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il problema persiste, ripetere la procedura descritta in Fase 2: Rimuovere l'alimentatore guasto e in Fase 3: Installare un nuovo alimentatore. Se il problema persiste, contattare il supporto tecnico.
4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione dell'alimentatore è completata. È possibile riprendere le normali operazioni.

Sostituire il contenitore di alimentazione E5700 (60 dischi)

È possibile sostituire un alimentatore in un array E5700 con uno shelf da 60 dischi, che include i seguenti tipi di shelf:

- Shelf di controller E5760
- Shelf di dischi DE460C

A proposito di questa attività

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori di alimentazione per la ridondanza dell'alimentazione. In caso di guasto di un contenitore di alimentazione, sostituirlo il prima possibile per assicurarsi che lo shelf disponga di una fonte di alimentazione ridondante.

È possibile sostituire un contenitore di alimentazione mentre lo storage array è acceso ed esegue operazioni di i/o host, Finché il secondo contenitore di alimentazione nello shelf ha uno stato ottimale e il campo **OK per rimuovere** nell'area Dettagli del guru del ripristino in Gestione di sistema di SANtricity visualizza **Sì**.

Durante l'esecuzione di questa attività, l'altro contenitore di alimentazione alimenta entrambe le ventole per garantire che l'apparecchiatura non si surriscaldi.

Prima di iniziare

- Revisione "Requisiti per la sostituzione del filtro E5700".
- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi.
- Controllare che il LED di attenzione ambra sul filtro a carboni attivi sia acceso, a indicare che il filtro a carboni attivi è guasto. Contattare il supporto tecnico per assistenza se entrambi i contenitori di alimentazione presenti nello shelf hanno i LED di attenzione color ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un contenitore di alimentazione installato e funzionante.
  - Un contenitore di alimentazione sostitutivo supportato per il modello di shelf di controller o di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del contenitore di alimentazione

Preparare la sostituzione di un contenitore di alimentazione in uno shelf di controller da 60 dischi o in uno shelf di dischi.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale contenitore di alimentazione si è guastato.

a. Selezionare **hardware**.

b. Guarda la potenza A destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta il contenitore di alimentazione guasto.

   In caso di guasto di un componente, questa icona è rossa.

c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.

d. Selezionare il filtro a carboni attivi o l'icona di alimentazione rossa.

e. Nella scheda **alimentatori**, controllare gli stati dei contenitori di alimentazione per determinare quale contenitore di alimentazione deve essere sostituito.

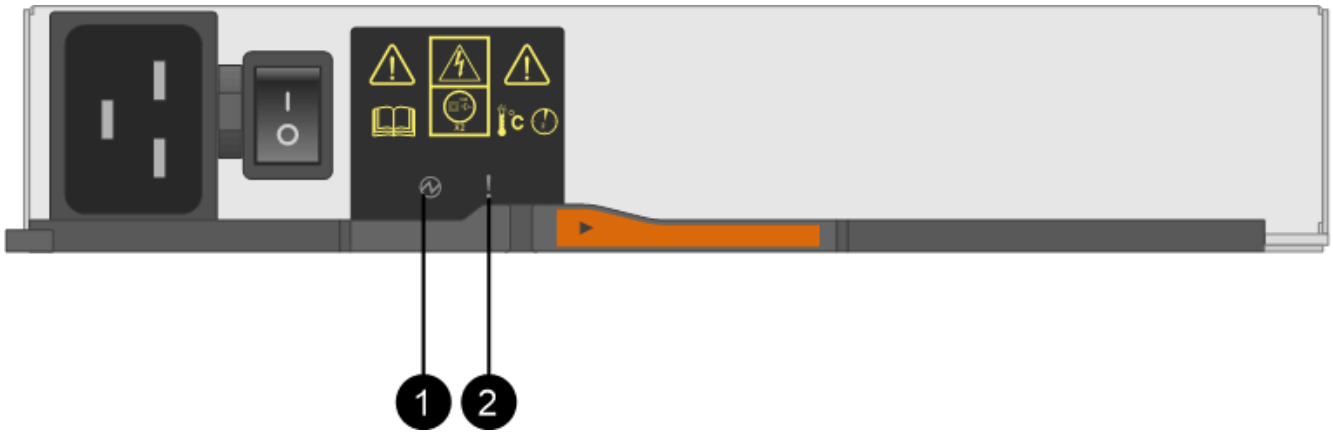
   Un componente con stato **Failed** deve essere sostituito.

> Se il secondo contenitore di alimentazione nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo il contenitore di alimentazione guasto. Contattare invece il supporto tecnico per assistenza.

> È inoltre possibile trovare informazioni sul contenitore di alimentazione guasto nell'area Details (Dettagli) del Recovery Guru, rivedere le informazioni visualizzate per lo shelf o consultare il registro eventi in Support (supporto) e Filter by Component Type (filtro per tipo di componente).

3. Dal retro dello storage array, osservare i LED di attenzione per individuare il contenitore di alimentazione da rimuovere.

   È necessario sostituire il filtro a carboni attivi con il LED attenzione acceso.



   (1) *LED di alimentazione*. Se è **verde fisso**, il filtro a carboni attivi funziona correttamente. Se è **spento**, il contenitore di alimentazione è guasto, l'interruttore CA è spento, il cavo di alimentazione CA non è installato correttamente o la tensione di ingresso del cavo di alimentazione CA non rientra nei margini (si è verificato un problema all'estremità della fonte del cavo di alimentazione CA).

   (2) *LED attenzione*. Se è di colore **ambra fisso**, il filtro a carboni attivi è guasto oppure non è presente alimentazione in ingresso al filtro a carboni attivi, ma l'altro è in funzione.

Fase 2: Rimuovere il contenitore di alimentazione guasto

Rimuovere un contenitore di alimentazione guasto in modo da poterlo sostituire con uno nuovo.

Fasi

1. Protezione antistatica.
2. Disimballare il nuovo contenitore di alimentazione e riutilizzarlo su una superficie piana vicino allo scaffale.

   Conservare tutti i materiali di imballaggio per l'utilizzo quando si restituisce il contenitore di alimentazione guasto.

3. Spegnere l'interruttore di alimentazione del contenitore di alimentazione da rimuovere.
4. Aprire il fermo del cavo di alimentazione del contenitore che si desidera rimuovere, quindi scollegare il cavo di alimentazione dal contenitore.
5. Premere il dispositivo di chiusura arancione sulla maniglia della camma del filtro a carboni attivi, quindi aprire la maniglia della camma per rilasciare completamente il filtro a carboni attivi dal piano intermedio.
6. Utilizzare la maniglia della camma per far scorrere il contenitore di alimentazione fuori dallo scaffale.

   Quando si rimuove un filtro a carboni attivi, utilizzare sempre due mani per sostenerne il peso.

Fase 3: Installare un nuovo filtro a carboni attivi

Installare un nuovo filtro a carboni attivi per sostituire quello guasto.

Fasi

1. Assicurarsi che l'interruttore on/off del nuovo contenitore di alimentazione sia in posizione off.
2. Con entrambe le mani, sostenere e allineare i bordi del contenitore di alimentazione con l'apertura nel telaio del sistema, quindi spingere delicatamente il contenitore di alimentazione nel telaio utilizzando la maniglia della camma fino a bloccarlo in posizione.

   Non esercitare una forza eccessiva quando si fa scorrere il contenitore di alimentazione nel sistema per evitare di danneggiare il connettore.

3. Chiudere la maniglia della camma in modo che il dispositivo di chiusura scatti nella posizione di blocco e che il contenitore dell'alimentazione sia completamente inserito.
4. Ricollegare il cavo di alimentazione al contenitore di alimentazione e fissarlo al contenitore utilizzando il fermo del cavo di alimentazione.
5. Accendere il nuovo contenitore di alimentazione.

Fase 4: Sostituzione completa del filtro a carboni attivi

Verificare che il nuovo power taniche funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Sul nuovo contenitore di alimentazione, verificare che il LED di alimentazione verde sia acceso e che il LED di attenzione ambra sia spento.
2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se viene ancora segnalato un guasto al contenitore di alimentazione, ripetere i passi descritti in Fase 2: Rimuovere il contenitore di alimentazione guasto e in Fase 3: Installare un nuovo filtro a carboni attivi. Se il problema persiste, contattare il supporto tecnico.

4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del filtro a carboni attivi è stata completata. È possibile riprendere le normali operazioni.

Sostituire il filtro della ventola E5700 (60 dischi)

È possibile sostituire un contenitore di ventole in un array E5700 con uno shelf da 60 dischi, che include i seguenti tipi di shelf:

- Shelf di controller E5760
- Shelf di dischi DE460C

A proposito di questa attività

Ogni shelf di controller da 60 dischi o shelf di dischi include due contenitori per ventole. In caso di guasto di un contenitore della ventola, sostituirlo il prima possibile per garantire che il ripiano sia adeguatamente raffreddato.

> **Possibili danni all'apparecchiatura** — se si esegue questa procedura con l'alimentazione accesa, è necessario completarla entro 30 minuti per evitare il rischio di surriscaldamento dell'apparecchiatura.

Prima di iniziare

- Revisione "Requisiti per la sostituzione del filtro E5700".
- Esaminare i dettagli nel Recovery Guru per confermare che si è verificato un problema con una batteria e per assicurarsi che non siano prima necessari altri elementi.
- Controllare che il LED di attenzione ambra sul filtro della ventola sia acceso, a indicare che la ventola è guasta. Contattare il supporto tecnico per assistenza se entrambi i contenitori delle ventole nello shelf hanno i LED di attenzione color ambra accesi.
- Assicurarsi di disporre di quanto segue:
  - Un filtro della ventola di ricambio (ventola) supportato per il modello di shelf del controller o del disco.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del filtro a carboni attivi della ventola

Preparare la sostituzione di un contenitore di ventole in uno shelf di controller da 60 dischi o in uno shelf di dischi.

Fasi

1. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

2. Da Gestore di sistema di SANtricity, determinare quale filtro a carboni attivi della ventola si è guastato.

   a. Selezionare **hardware**.
   b. Guardare la ventola A destra degli elenchi a discesa **Shelf** per determinare quale shelf presenta il contenitore della ventola guasto.

      In caso di guasto di un componente, questa icona è rossa.

   c. Quando trovi lo shelf con un'icona rossa, seleziona **Mostra retro dello shelf**.
   d. Selezionare il filtro a carboni attivi della ventola o l'icona rossa della ventola.
   e. Nella scheda **ventole**, controllare gli stati dei contenitori delle ventole per determinare quale filtro a carboni attivi deve essere sostituito.

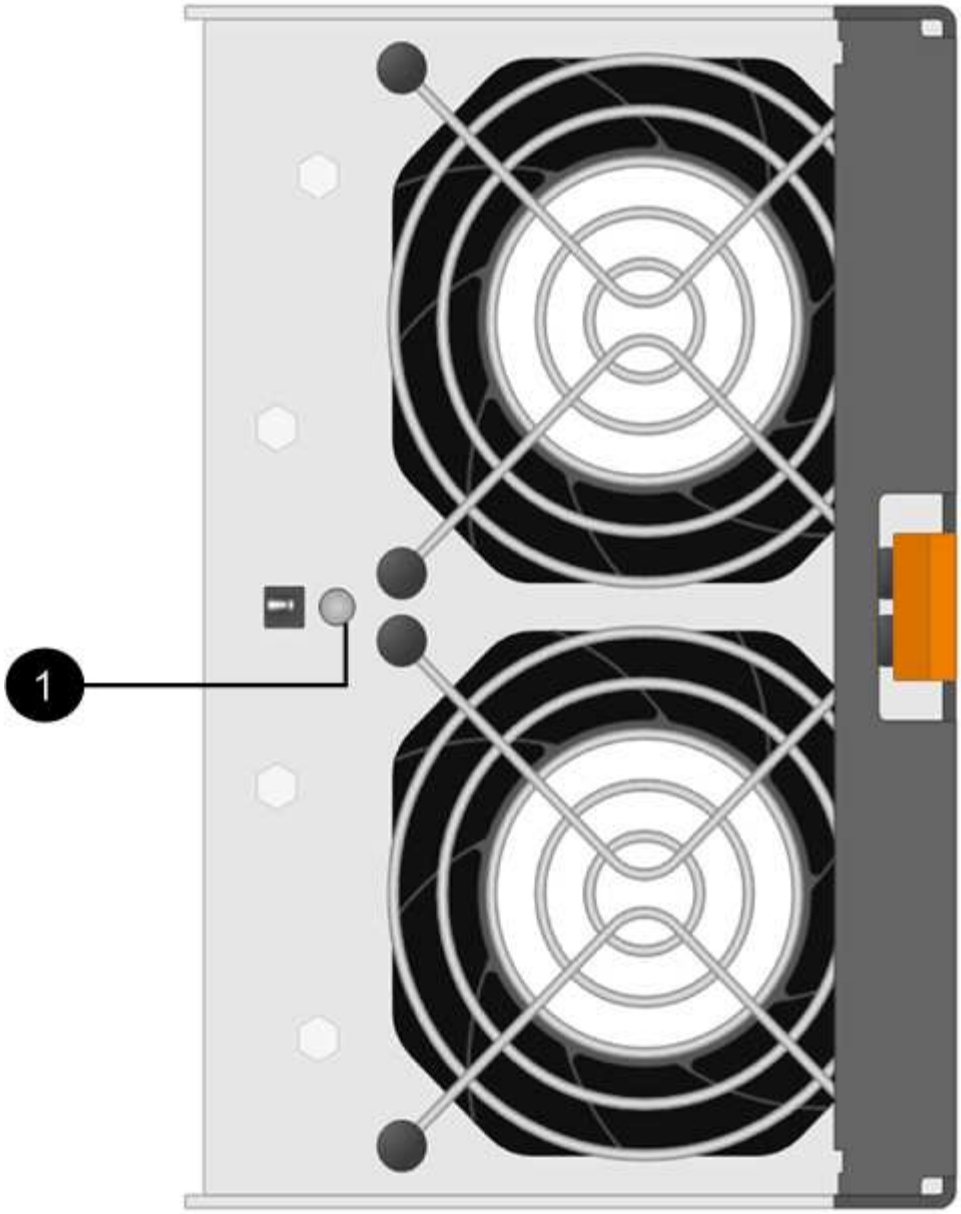
      Un componente con stato **Failed** deve essere sostituito.

      > Se il secondo contenitore della ventola nello shelf non ha lo stato **ottimale**, non tentare di sostituire a caldo il contenitore della ventola guasto. Contattare invece il supporto tecnico per assistenza.

   È inoltre possibile trovare informazioni sul contenitore della ventola guasto nell'area Details (Dettagli) del Recovery Guru oppure consultare il registro eventi in Support (supporto) e Filter by Component Type (filtro per tipo di componente).

3. Dal retro dello storage array, osservare i LED di attenzione per individuare il contenitore della ventola da rimuovere.

   È necessario sostituire il filtro a carboni attivi della ventola con il LED attenzione acceso.



(1) *LED attenzione*. Se questo LED viene visualizzato come **giallo fisso**, significa che la ventola è guasta.

Fase 2: Rimuovere il filtro a carboni attivi della ventola guasto e installarne uno nuovo

Rimuovere un contenitore della ventola guasto in modo da poterlo sostituire con uno nuovo.

> Se non si spegne l'alimentazione dello storage array, assicurarsi di rimuovere e sostituire il contenitore della ventola entro 30 minuti per evitare il surriscaldamento del sistema.

Fasi

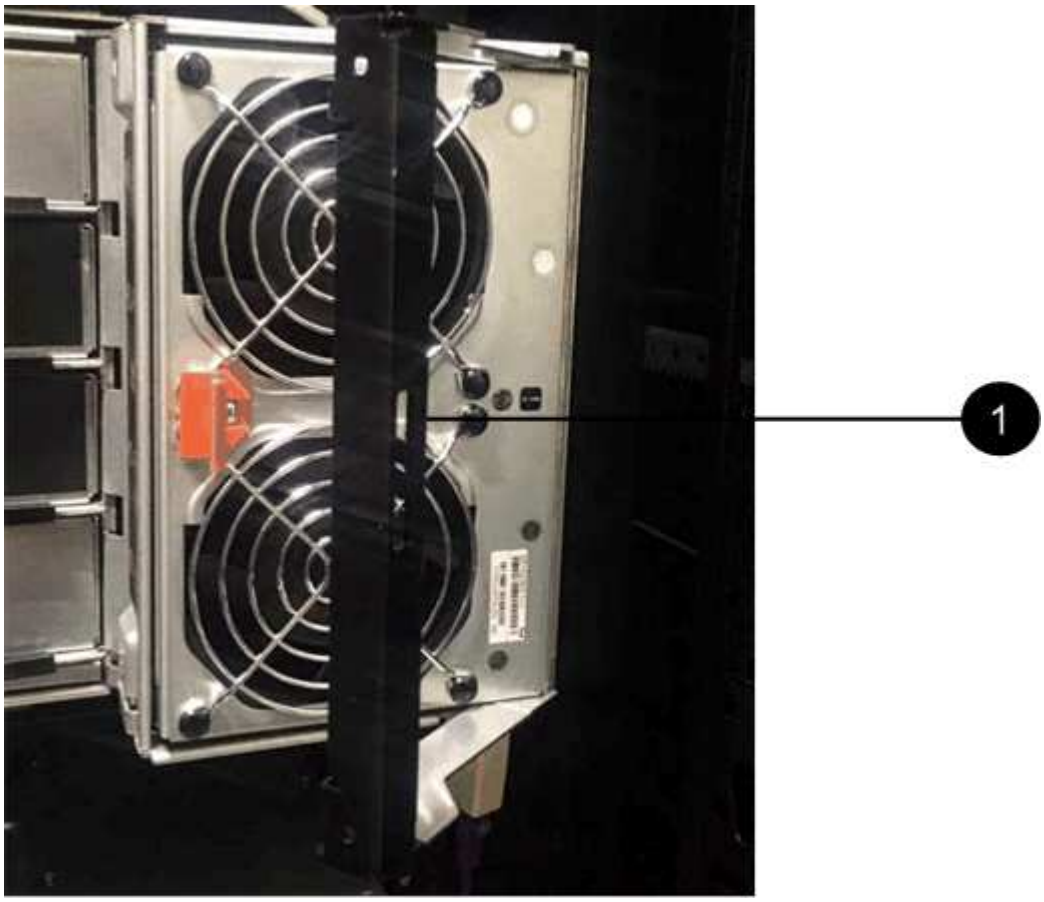
1. Disimballare il nuovo contenitore della ventola e posizionarlo su una superficie piana vicino allo scaffale.

   Conservare tutto il materiale di imballaggio da utilizzare quando si restituisce la ventola guasta.

2. Premere la linguetta arancione per rilasciare la maniglia del filtro a carboni attivi della ventola.

(1) *linguetta che si preme per rilasciare la maniglia del filtro a carboni attivi della ventola.*

3. Utilizzare la maniglia del filtro a carboni attivi per estrarre il filtro a carboni attivi dal ripiano.



(1) *maniglia per estrarre il contenitore della ventola.*

4. Far scorrere completamente il contenitore della ventola di ricambio nello scaffale, quindi spostare la maniglia del contenitore della ventola fino a quando non si blocca con la linguetta arancione.

Fase 3: Sostituzione completa del filtro a carboni attivi della ventola

Verificare che il nuovo filtro a carboni attivi della ventola funzioni correttamente, raccogliere i dati di supporto e riprendere le normali operazioni.

Fasi

1. Controllare il LED di attenzione ambra sul nuovo filtro a carboni attivi della ventola.

> Dopo aver sostituito il filtro a carboni attivi della ventola, il LED attenzione rimane acceso (ambra fisso) mentre il firmware verifica che il filtro a carboni attivi della ventola sia stato installato correttamente. Il LED si spegne al termine del processo.

2. Dal guru del ripristino in Gestione sistema di SANtricity, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se viene ancora segnalato un guasto al filtro a carboni attivi della ventola, ripetere le operazioni descritte in Fase 2: Rimuovere il filtro a carboni attivi della ventola guasto e installarne uno nuovo. Se il problema persiste, contattare il supporto tecnico.

4. Rimuovere la protezione antistatica.
5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del filtro a carboni attivi della ventola è completata. È possibile riprendere le normali operazioni.

Dischi

Requisiti per la sostituzione del disco E5700

Prima di sostituire un disco, esaminare i requisiti e le considerazioni.

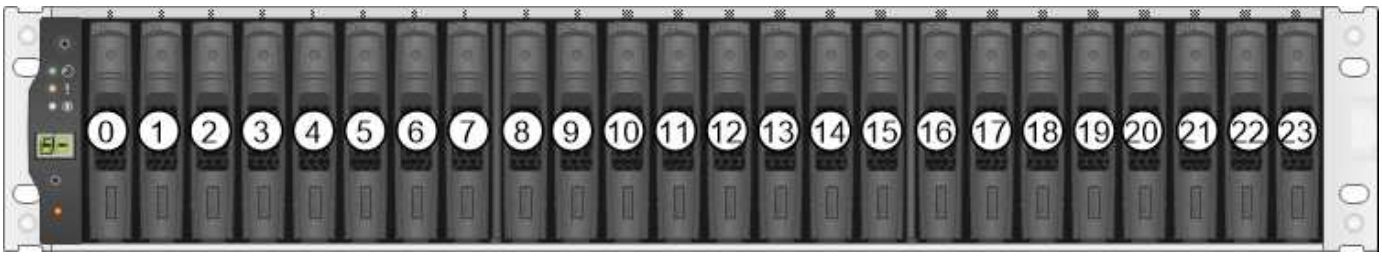
Tipi di shelf

È possibile sostituire un disco in uno shelf da 24 dischi, in uno shelf da 60 dischi o in un cassetto.

shelf da 24 dischi

Le figure mostrano come i dischi sono numerati in ogni tipo di shelf (il pannello anteriore o i cappucci terminali dello shelf sono stati rimossi).

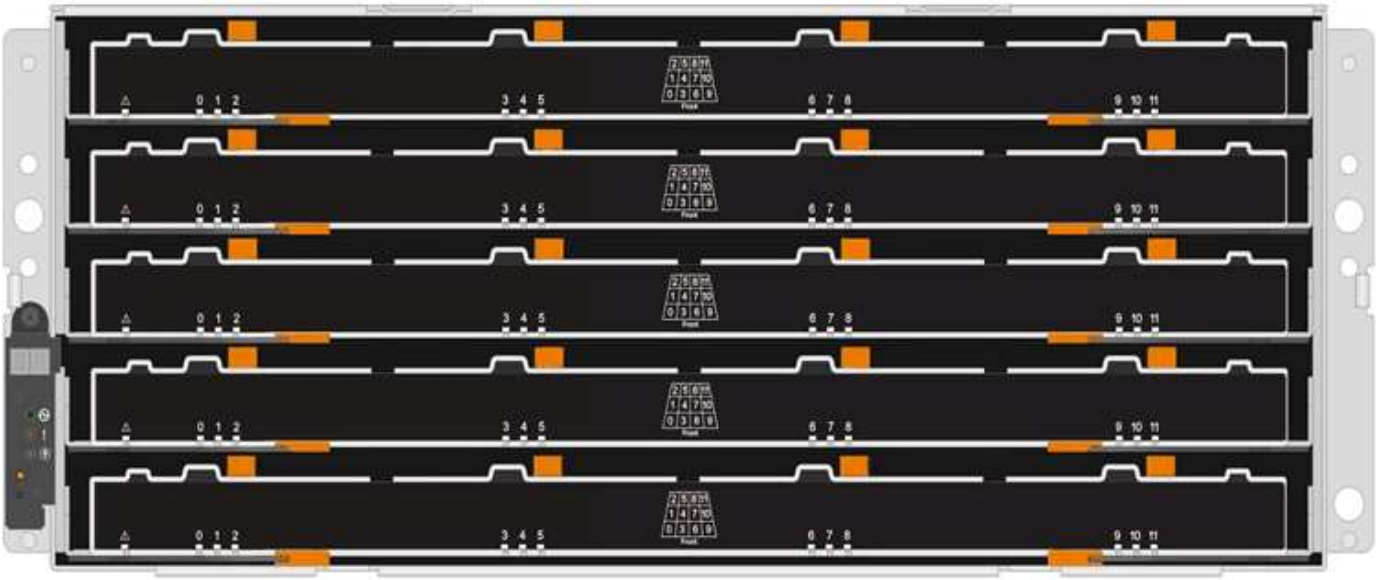
Numerazione delle unità in uno shelf di controller E5724 o in uno shelf di dischi DE224C



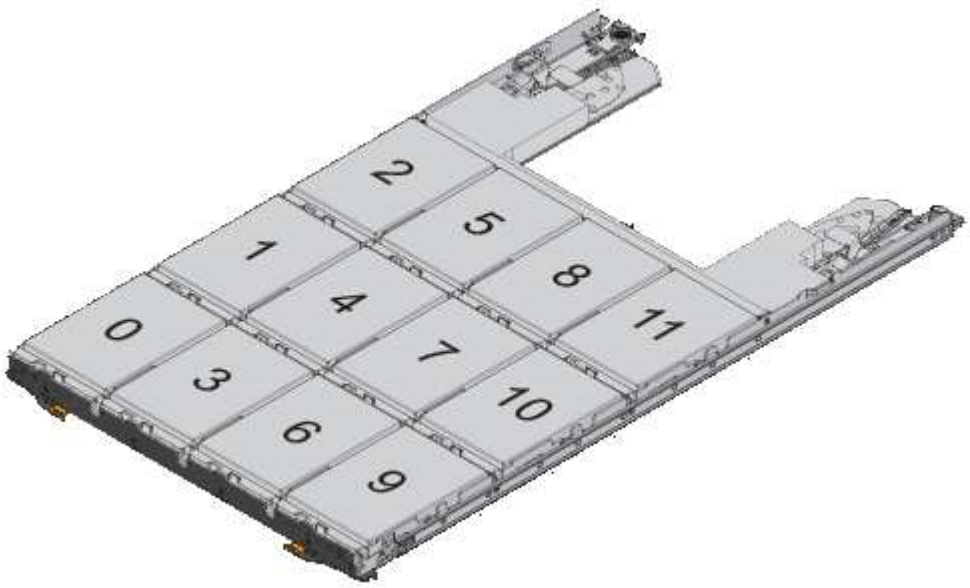
Lo storage array E5724 potrebbe includere uno o più tray di dischi di espansione SAS-2 preesistenti, incluso il tray di 24 dischi DE5600 o il tray di 60 dischi DE6600 Per istruzioni sulla sostituzione di un'unità in uno di questi vassoi, vedere "Sostituzione di un'unità nei tray di dischi E2660, E2760, E5460, E5560 o E5660" e. "Sostituzione di un'unità nei vassoi da 12 o 24 dischi E2600, E2700, E5400, E5500 e E5600".

shelf da 60 dischi

Sia lo shelf del controller E5760 che lo shelf del disco DE460C sono costituiti da cinque cassetti per unità contenenti ciascuno 12 slot per unità. Il cassetto dell'unità 1 si trova nella parte superiore e il cassetto dell'unità 5 nella parte inferiore.



Sia per un cassetto per shelf controller E5760 che per un cassetto per shelf dischi DE460C, i dischi sono numerati da 0 a 11 in ogni cassetto all'interno dello shelf.

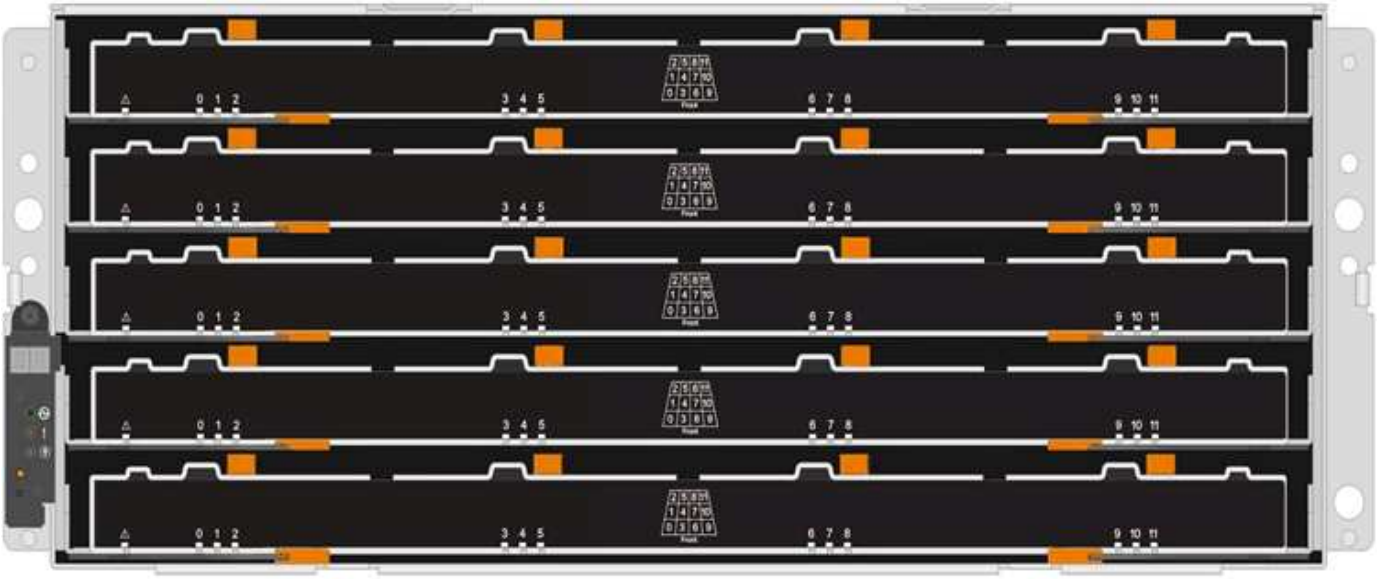


> Lo storage array E5760 potrebbe includere uno o più vassoi di espansione SAS-2 legacy, tra cui il vassoio DE1600 da 12 dischi, il vassoio DE5600 da 24 dischi o il vassoio DE6600 da 60 dischi Per istruzioni sulla sostituzione di un'unità in uno di questi vassoi, vedere "Sostituzione di un'unità nei tray di dischi E2660, E2760, E5460, E5560 o E5660" e. "Sostituzione di un'unità nei vassoi da 12 o 24 dischi E2600, E2700, E5400, E5500 e E5600".

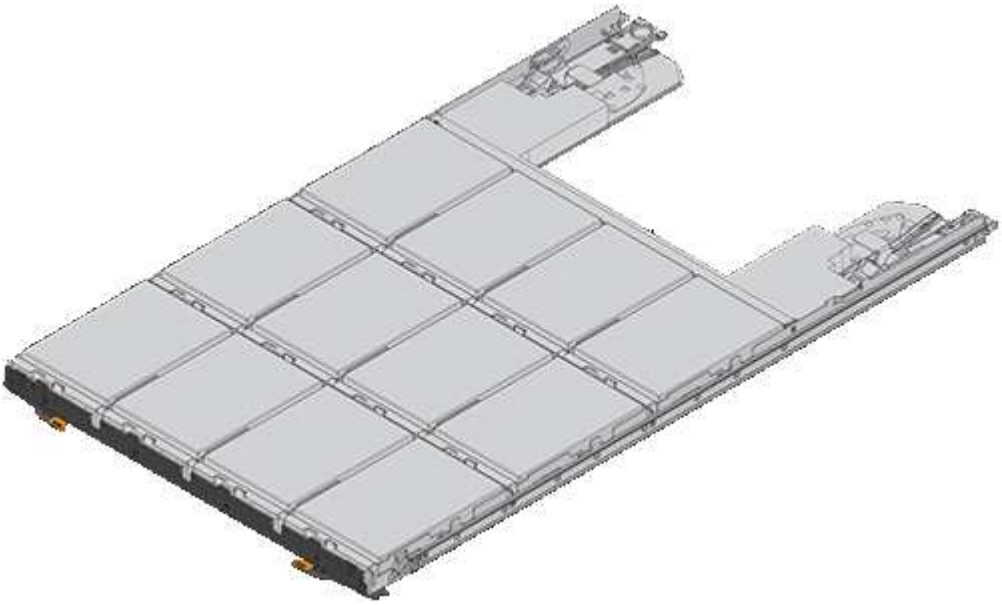
Cassetto dell'unità

È possibile sostituire un cassetto dischi in uno shelf di controller E5760 e uno shelf di dischi DE460C.

Ciascuno di questi shelf da 60 dischi dispone di cinque cassetti per dischi.



Ciascuno dei cinque cassetti può contenere fino a 12 dischi.



Requisiti per la gestione dei dischi

> I dischi dello storage array sono fragili. Una gestione errata del disco è la causa principale del guasto del disco.

Attenersi alle seguenti regole per evitare di danneggiare le unità dello storage array:

- Prevenzione delle scariche elettrostatiche (ESD):
  - Tenere l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
  - Non inserire utensili metallici o coltelli nel sacchetto ESD.

    Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.

    - Conservare il sacchetto ESD e il materiale di imballaggio nel caso in cui sia necessario restituire un'unità in un secondo momento.
    - Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis dell'enclosure di storage.

      Se non è disponibile un braccialetto, toccare una superficie non verniciata sullo chassis del cabinet di storage prima di maneggiare il disco.
- Gestire i dischi con attenzione:
    - Utilizzare sempre due mani per rimuovere, installare o trasportare un disco.
    - Non forzare mai un'unità in uno shelf e esercitare una pressione leggera e decisa per inserire completamente il dispositivo di chiusura dell'unità.
    - Posizionare i dischi su superfici imbottite e non impilare mai i dischi uno sopra l'altro.
    - Non urtare i dischi contro altre superfici.
    - Prima di rimuovere un'unità da uno shelf, sganciare la maniglia e attendere 30 secondi affinché l'unità si spenda.
    - Utilizzare sempre imballaggi approvati per la spedizione delle unità.
- Evitare i campi magnetici:
    - Tenere le unità lontano da dispositivi magnetici.

      I campi magnetici possono distruggere tutti i dati presenti sul disco e causare danni irreparabili ai circuiti del disco.

Sostituire l'unità in E5700 (shelf da 24 dischi)

È possibile sostituire un disco in uno shelf da 24 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array riceve i/O.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco E5700".
- Assicurarsi di disporre di quanto segue:
    - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
    - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
    - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco (24 dischi)

Preparare la sostituzione di un disco controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.
   a. Selezionare **hardware**.
   b. Selezionare il disco guasto sul grafico dello shelf.
   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.
   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta sostituendo e che disponga delle funzioni previste.

      Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.
3. Se necessario, utilizzare Gestore di sistema SANtricity per individuare l'unità all'interno dell'array di storage: Dal menu di scelta rapida dell'unità, selezionare **attiva indicatore localizzatore**.

   Il LED di attenzione del disco (ambra) lampeggia per identificare il disco da sostituire.

   > Se si sostituisce un'unità in uno shelf dotato di pannello, rimuovere il pannello per visualizzare i LED dell'unità.

Fase 2: Rimozione del disco guasto (24 dischi)

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

   Conservare tutti i materiali di imballaggio.
2. Premere il pulsante di rilascio sul disco guasto.

   - Per i dischi negli shelf di controller E5724 o negli shelf di dischi DE224C, il pulsante di rilascio si trova nella parte superiore dell'unità. La maniglia della camma sulle molle del disco si apre parzialmente e il disco si disinnesta dalla scheda intermedia.
3. Aprire la maniglia della camma ed estrarre leggermente l'unità.
4. Attendere 30 secondi.
5. Rimuovere l'unità dallo shelf con entrambe le mani.
6. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.

7. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

Fase 3: Installazione di un nuovo disco (24 dischi)

Viene installata una nuova unità per sostituire quella guasta. Installare l'unità sostitutiva il prima possibile dopo aver rimosso l'unità guasta. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

Fasi

1. Aprire la maniglia della camma.
2. Con due mani, inserire l'unità sostitutiva nell'alloggiamento aperto, spingendo con decisione fino a quando non si arresta.
3. Chiudere lentamente la maniglia della camma fino a quando l'unità non è completamente inserita nel piano intermedio e la maniglia non scatta in posizione.

   Il LED verde sull'unità si accende quando l'unità è inserita correttamente.

   > A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco (24 dischi)

Verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita.

   Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.

   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   > Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.

b. Fare clic sull'unità sostituita.

c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).

d. Confermare che si desidera eseguire questa operazione.

Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.

4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire l'unità in E5700 (shelf da 60 dischi)

È possibile sostituire un disco in uno shelf da 60 dischi.

A proposito di questa attività

Il guru del ripristino in Gestione di sistema di SANtricity monitora i dischi nell'array di storage e può notificare un guasto imminente del disco o un guasto effettivo del disco. In caso di guasto di un disco, il LED di attenzione di colore ambra si accende. È possibile sostituire a caldo un disco guasto mentre lo storage array sta ricevendo le operazioni di i/O.

Questa attività si applica agli shelf di dischi DCM e DCM2.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco E5700".
- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione alla sostituzione del disco (60 dischi)

Preparare la sostituzione di un disco in uno shelf da 60 dischi controllando il guru del ripristino in Gestore di sistema di SANtricity e completando i passaggi necessari. Quindi, individuare il componente guasto.

Fasi

1. Se il guru del ripristino in Gestione sistema di SANtricity ha notificato un *imminente guasto al disco*, ma il disco non è ancora guasto, seguire le istruzioni nel guru del ripristino per eseguire il guasto al disco.
2. Se necessario, utilizzare Gestione di sistema di SANtricity per verificare di disporre di un'unità sostitutiva adatta.

   a. Selezionare **hardware**.

   b. Selezionare il disco guasto sul grafico dello shelf.

   c. Fare clic sull'unità per visualizzarne il menu di scelta rapida, quindi selezionare **Visualizza impostazioni**.

   d. Verificare che l'unità sostitutiva abbia una capacità uguale o superiore a quella dell'unità che si sta

sostituendo e che disponga delle funzioni previste.

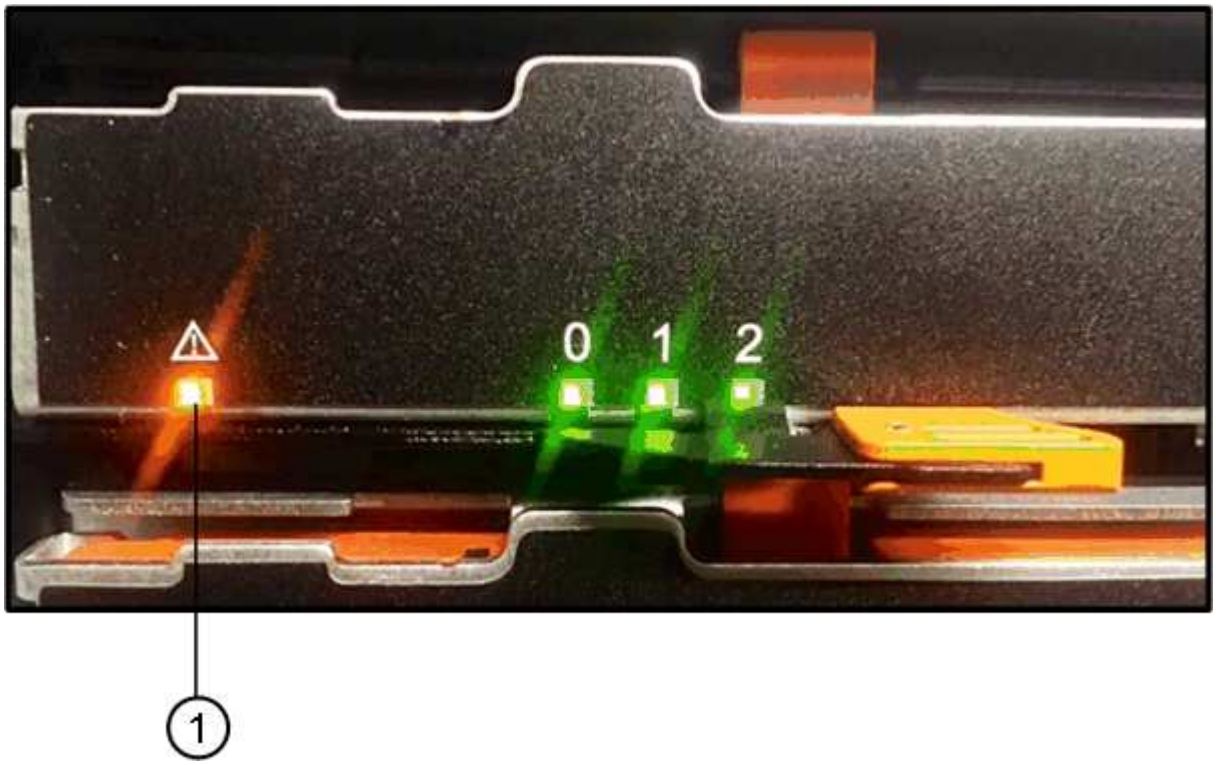
Ad esempio, non tentare di sostituire un disco rigido (HDD) con un disco a stato solido (SSD). Allo stesso modo, se si sta sostituendo un disco sicuro, assicurarsi che anche il disco sostitutivo sia sicuro.

3. Se necessario, utilizzare Gestore di sistema di SANtricity per individuare il disco all'interno dello storage array.

   a. Se lo shelf è dotato di una cornice, rimuovetela per vedere i LED.

   b. Dal menu di scelta rapida del disco, selezionare **attiva indicatore di posizione**.

      Il LED di attenzione del cassetto dell'unità (ambra) lampeggia per consentire l'apertura del cassetto dell'unità corretto e identificare l'unità da sostituire.



(1) *LED attenzione*

   c. Sganciare il cassetto dell'unità tirando entrambe le leve.

   d. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta.

   e. Controllare la parte superiore del cassetto dell'unità per individuare il LED di attenzione davanti a ciascun disco.

(1) *LED attenzione acceso per l'unità in alto a destra*

I LED attenzione cassetto unità si trovano sul lato sinistro davanti a ciascun disco, con un'icona di attenzione sulla maniglia del disco appena dietro il LED.

(1) *icona attenzione*

(2) *LED attenzione*

Fase 2: Rimozione del disco guasto (60 dischi)

Rimuovere un disco guasto per sostituirlo con uno nuovo.

Fasi

1. Disimballare l'unità sostitutiva e conservarla su una superficie piana e priva di elettricità statica vicino allo shelf.

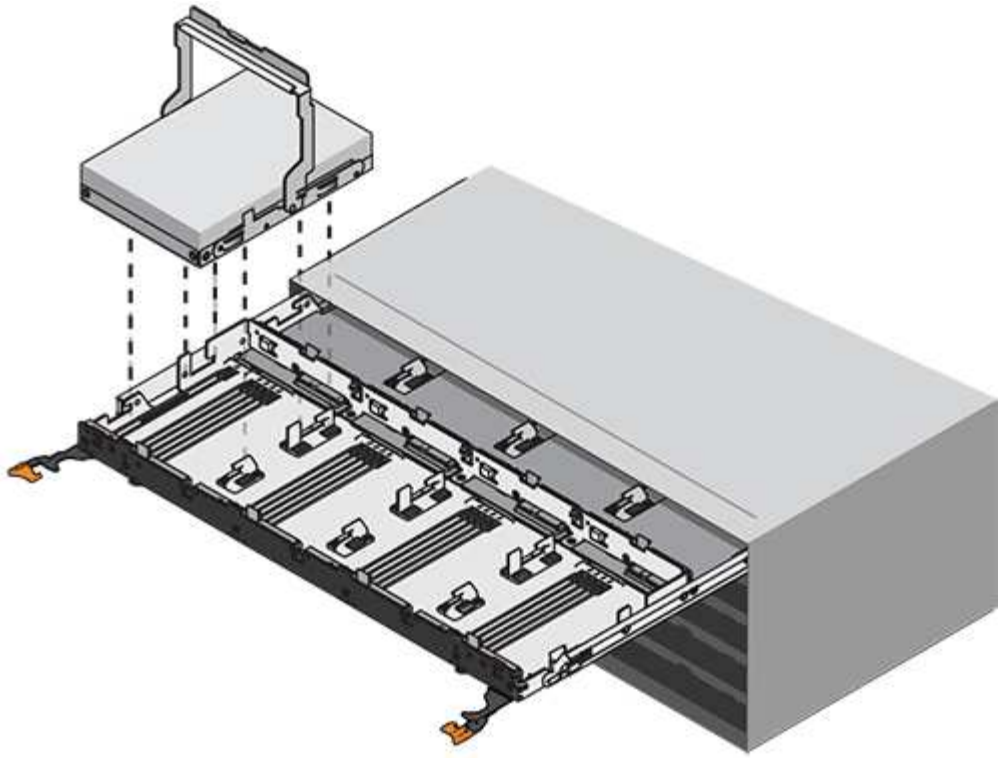
   Conservare tutti i materiali di imballaggio per la prossima volta che sarà necessario restituire un disco.

2. Rilasciare le leve del cassetto dell'unità dal centro del cassetto dell'unità appropriato, tirandole verso i lati del cassetto.
3. Tirare con cautela le leve del cassetto dell'unità esteso per estrarre il cassetto dell'unità fino alla sua estensione completa senza rimuoverlo dal contenitore.
4. Tirare delicatamente indietro il dispositivo di chiusura arancione che si trova davanti all'unità che si desidera rimuovere.

   La maniglia della camma sulle molle di azionamento si apre parzialmente e l'unità viene rilasciata dal cassetto.

(1) *dispositivo di chiusura arancione*

5. Aprire la maniglia della camma ed estrarre leggermente l’unità.
6. Attendere 30 secondi.
7. Utilizzare la maniglia della camma per sollevare l’unità dallo scaffale.



8. Posizionare l'unità su una superficie antistatica e imbottita, lontano dai campi magnetici.
9. Attendere 30 secondi affinché il software riconosca che l'unità è stata rimossa.

> Se si rimuove accidentalmente un disco attivo, attendere almeno 30 secondi, quindi reinstallarlo. Per la procedura di ripristino, fare riferimento al software di gestione dello storage.

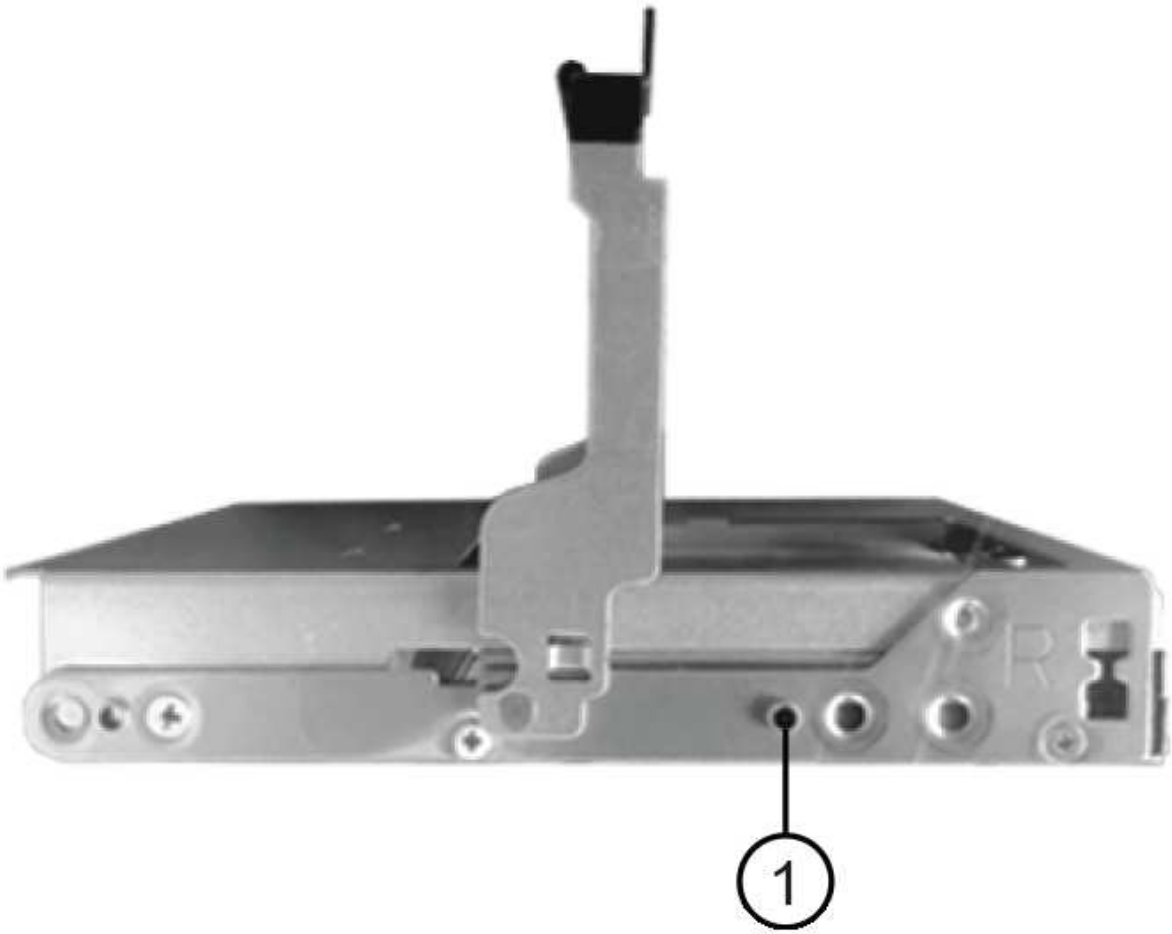
Fase 3: Installazione di un nuovo disco (60 dischi)

Installare un nuovo disco per sostituire quello guasto.

> **Possibile perdita di accesso ai dati** — quando si reinserisce il cassetto del disco nel contenitore, non chiudere mai il cassetto. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.

Fasi

1. Sollevare la maniglia della camma sul nuovo disco in verticale.
2. Allineare i due pulsanti rialzati su ciascun lato del supporto dell'unità con lo spazio corrispondente nel canale dell'unità sul cassetto dell'unità.



(1) *pulsante sollevato sul lato destro del supporto del disco*

3. Abbassare l'unità, quindi ruotare la maniglia della camma verso il basso fino a quando non scatta in posizione sotto il dispositivo di chiusura arancione.
4. Spingere con cautela il cassetto dell'unità all'interno del contenitore. Spingere lentamente il cassetto per evitare di strattonare il cassetto e danneggiare lo storage array.
5. Chiudere il cassetto dell'unità spingendo entrambe le leve verso il centro.

   Il LED di attività verde per l'unità sostituita nella parte anteriore del cassetto si accende quando l'unità è inserita correttamente.

   A seconda della configurazione, il controller potrebbe ricostruire automaticamente i dati nel nuovo disco. Se lo shelf utilizza dischi hot spare, il controller potrebbe dover eseguire una ricostruzione completa sull'hot spare prima di poter copiare i dati sull'unità sostituita. Questo processo di ricostruzione aumenta il tempo necessario per completare questa procedura.

Fase 4: Sostituzione completa del disco (60 dischi)

Verificare che il nuovo disco funzioni correttamente.

Fasi

1. Controllare il LED di alimentazione e il LED di attenzione sull'unità sostituita. (Quando si inserisce un disco per la prima volta, il LED attenzione potrebbe essere acceso. Tuttavia, il LED dovrebbe spegnersi entro un minuto.
   - Il LED di alimentazione è acceso o lampeggia e il LED attenzione è spento: Indica che il nuovo disco funziona correttamente.
   - LED di alimentazione spento: Indica che l'unità potrebbe non essere installata correttamente. Rimuovere l'unità, attendere 30 secondi, quindi reinstallarla.
   - LED attenzione acceso: Indica che il nuovo disco potrebbe essere difettoso. Sostituirlo con un altro disco nuovo.
2. Se il guru del ripristino in Gestione sistema di SANtricity continua a mostrare un problema, selezionare **ricontrollare** per assicurarsi che il problema sia stato risolto.
3. Se il Recovery Guru indica che la ricostruzione del disco non è stata avviata automaticamente, avviare la ricostruzione manualmente, come segue:

   Eseguire questa operazione solo se richiesto dal supporto tecnico o dal Recovery Guru.

   a. Selezionare **hardware**.
   b. Fare clic sull'unità sostituita.
   c. Dal menu di scelta rapida del disco, selezionare **Reconstruct** (ricostruzione).
   d. Confermare che si desidera eseguire questa operazione.

      Al termine della ricostruzione del disco, il gruppo di volumi si trova in uno stato ottimale.
4. Se necessario, reinstallare il pannello.
5. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

Quali sono le prossime novità?

La sostituzione del disco è completata. È possibile riprendere le normali operazioni.

Sostituire il cassetto unità E5700 (60 dischi)

È possibile sostituire un cassetto di dischi in un array E5700.

A proposito di questa attività

La procedura per sostituire un cassetto del disco guasto in uno shelf di controller E5760 o in uno shelf di dischi DE460C dipende dalla protezione dei volumi nel cassetto da parte della protezione contro la perdita di cassetto. Se tutti i volumi nel cassetto si trovano in pool di dischi o gruppi di volumi con protezione perdita cassetto, è possibile eseguire questa procedura online. In caso contrario, è necessario interrompere tutte le attività di i/o dell'host e spegnere lo shelf prima di sostituire il cassetto dell'unità.

Prima di iniziare

- Esaminare i requisiti di gestione dei dischi in "Requisiti per la sostituzione del disco E5700".
- Assicurarsi che lo shelf di dischi soddisfi tutte le seguenti condizioni:
  - Lo shelf di dischi non può essere troppo freddo.
  - Entrambe le ventole devono essere installate e avere uno stato ottimale.
  - Tutti i componenti dello shelf dei dischi devono essere in posizione.

- I volumi nel cassetto del disco non possono essere degradati.

> **Possibile perdita di accesso ai dati** — se un volume si trova già in uno stato degradato e si rimuovono le unità dal cassetto, il volume potrebbe non funzionare.

- Assicurarsi di disporre di quanto segue:
  - Un'unità sostitutiva supportata da NetApp per lo shelf di controller o lo shelf di dischi.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Una torcia.
  - Un indicatore permanente per annotare la posizione esatta di ciascuna unità durante la rimozione dell'unità dal cassetto.
  - Accesso all'interfaccia a riga di comando (CLI) dello storage array. Se non si dispone dell'accesso alla CLI, è possibile effettuare una delle seguenti operazioni:
    - **Per Gestore di sistema SANtricity (versione 11.60 e successive)** — Scarica il pacchetto CLI (file zip) da Gestore di sistema. Accedere al **Impostazioni › sistema › componenti aggiuntivi › interfaccia riga di comando**. È quindi possibile eseguire i comandi CLI da un prompt del sistema operativo, ad esempio il prompt di DOS C:.
    - **Per Gestione storage SANtricity/finestra di gestione aziendale (EMW)** — seguire le istruzioni nella guida rapida per scaricare e installare il software. È possibile eseguire i comandi CLI da EMW selezionando **Tools › Execute script** (Strumenti[Esegui script]).

Fase 1: Preparazione alla sostituzione del cassetto (60 dischi)

Preparare la sostituzione di un cassetto del disco determinando se è possibile eseguire la procedura di sostituzione mentre lo shelf del disco è online o se è necessario interrompere l'attività di i/o dell'host e spegnere uno degli shelf accesi. Se si sostituisce un cassetto in uno shelf con protezione perdita cassetto, non è necessario interrompere l'attività di i/o dell'host e spegnere uno degli shelf.

Fasi

1. Determinare se lo shelf di dischi è acceso.
   - Se l'alimentazione è spenta, non è necessario eseguire il comando CLI. Passare a. Fase 2: Rimuovere le catene di cavi.
   - Se l'alimentazione è accesa, passare alla fase successiva.
2. Digitare il seguente comando nella riga di comando e premere **Invio**:

```
SMcli <ctlr_IP1\> -p "array_password" -c "set tray [trayID] drawer
[drawerID]
serviceAllowedIndicator=on;"
```

   dove:

   - `<ctlr_IP1>` è l'identificatore del controller.
   - `array_password` è la password per lo storage array. È necessario racchiudere il valore di array_password tra virgolette doppie ("").
   - `[trayID]` è l'identificativo dello shelf di dischi che contiene il cassetto che si desidera sostituire. I

valori dell'ID dello shelf del disco vanno da 0 a 99. È necessario racchiudere il valore per `trayID` tra parentesi quadre.

- `[drawerID]` è l'identificativo del cassetto dell'unità che si desidera sostituire. I valori dell'ID cassetto sono da 1 (cassetto superiore) a 5 (cassetto inferiore). È necessario racchiudere il valore per `drawerID` tra parentesi quadre. Questo comando consente di rimuovere il cassetto più in alto nello shelf 10:

```
SMcli <ctlr_IP1\> -p "safety-1" -c "set tray [10] drawer [1]
serviceAllowedIndicator=forceOnWarning;"
```

3. Determinare se è necessario interrompere l'attività di i/o dell'host, come segue:
   - Se il comando ha esito positivo, non è necessario interrompere l'attività di i/o dell'host. Tutti i dischi nel cassetto sono in pool o gruppi di volumi con protezione perdita cassetto. Passare a. Fase 2: Rimuovere le catene di cavi.

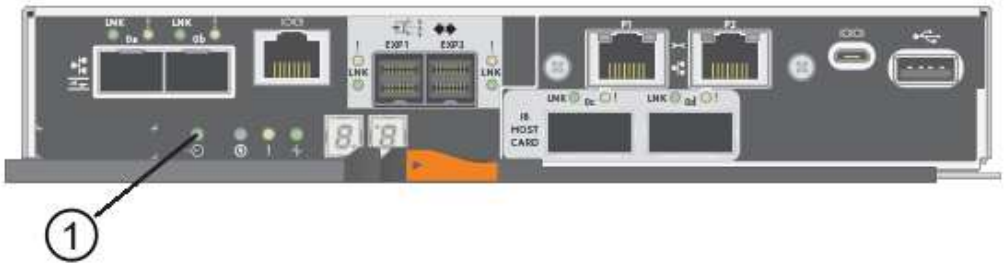
     Possibili danni ai dischi — attendere 30 secondi dopo il completamento del comando prima di aprire il cassetto del disco. L'attesa di 30 secondi consente lo spin down dei dischi, evitando possibili danni all'hardware.

   - Se viene visualizzato un avviso che indica che non è stato possibile completare questo comando, è necessario interrompere l'attività di i/o dell'host prima di rimuovere il cassetto. L'avviso viene visualizzato perché uno o più dischi nel cassetto interessato sono in pool o gruppi di volumi senza protezione perdita cassetto. Per evitare la perdita di dati, è necessario completare i passaggi successivi per interrompere l'attività di i/o dell'host e spegnere lo shelf di dischi e lo shelf di controller.
4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

     I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.
5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.

   Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere i dati perché lo storage array non sarà accessibile.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



(1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
8. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
9. Spegnere gli shelf come segue:
   - *Se stai sostituendo un cassetto in uno shelf **con** protezione perdita cassetto*:

     NON è necessario spegnere nessuno degli shelf.

   È possibile eseguire la procedura di sostituzione mentre il cassetto dell'unità è in linea, perché `Set Drawer Service Action Allowed Indicator` Comando CLI completato correttamente.

   - *Se stai sostituendo un cassetto in uno shelf **controller senza** protezione perdita cassetto*:
     i. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere che tutti i LED sullo shelf del controller si oscuri.
   - *Se si sostituisce un cassetto in uno shelf di dischi **espansione senza** protezione perdita cassetto*:
     i. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere che tutti i LED sullo shelf del controller si oscuri.
     iii. Spegnere entrambi gli interruttori di alimentazione sullo shelf di dischi.
     iv. Attendere due minuti per interrompere l'attività del disco.

Fase 2: Rimuovere le catene di cavi

Rimuovere entrambe le catene per cavi in modo da poter rimuovere e sostituire un cassetto del disco guasto. Le catene per cavi sinistra e destra consentono ai cassetti di scorrere verso l'interno e verso l'esterno.

A proposito di questa attività

Ciascun cassetto dispone di catene di cavi destra e sinistra. Le estremità metalliche delle catene per cavi scorrono nelle corrispondenti guide verticali e orizzontali all'interno del contenitore, come indicato di seguito:

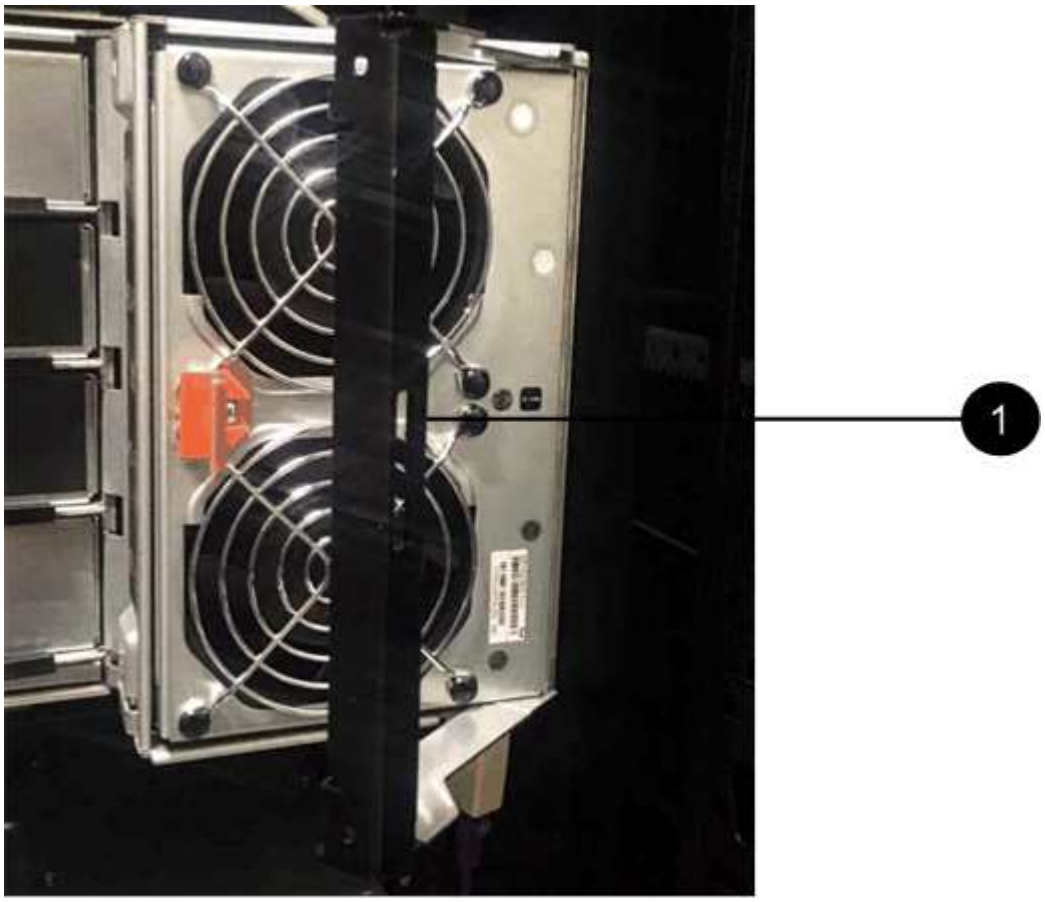
- Le guide verticali di destra e di sinistra collegano la catena di cavi alla scheda centrale del contenitore.
- Le guide orizzontali sinistra e destra collegano la catena di cavi al singolo cassetto.

> **Possibili danni all'hardware** — se il vassoio dell'unità è acceso, la catena di cavi viene eccitata fino a quando entrambe le estremità non vengono scollegate. Per evitare di mettere in corto circuito l'apparecchiatura, evitare che il connettore della catena di cavi scollegato tocchi il telaio metallico se l'altra estremità della catena di cavi è ancora collegata.

Fasi

1. Assicurarsi che l'attività di i/o dell'host sia stata interrotta e che lo shelf di dischi o lo shelf di controller sia spento, oppure eseguire il `Set Drawer Attention Indicator` Comando CLI.
2. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola di destra:
   a. Premere la linguetta arancione per rilasciare la maniglia del filtro a carboni attivi della ventola.

      La figura mostra la maniglia del filtro a carboni attivi della ventola estesa e rilasciata dalla linguetta arancione a sinistra.



(1) *maniglia del filtro della ventola*

   a. Utilizzando la maniglia, estrarre il contenitore della ventola dal vassoio dell'unità e metterlo da parte.
   b. Se il vassoio è acceso, assicurarsi che la ventola sinistra sia alla massima velocità.

> **Possibili danni all'apparecchiatura dovuti al surriscaldamento** — se il vassoio è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

3. Determinare la catena di cavi da scollegare:
   - Se l'alimentazione è accesa, il LED di attenzione di colore ambra sulla parte anteriore del cassetto indica la catena di cavi da scollegare.
   - Se l'alimentazione è spenta, è necessario determinare manualmente quale delle cinque catene di cavi scollegare. La figura mostra il lato destro dello shelf del disco con il contenitore della ventola rimosso. Una volta rimosso il contenitore della ventola, è possibile vedere le cinque catene di cavi e i connettori

verticali e orizzontali per ciascun cassetto.

La catena di cavi superiore è collegata al cassetto dell’unità 1. La catena dei cavi inferiore è collegata al cassetto dell’unità 5. Vengono fornite le didascalie per il cassetto unità 1.


2
1
3

(1) *catena di cavi*

(2) *connettore verticale (collegato alla scheda intermedia)*

(3) *connettore orizzontale (collegato al cassetto)*

4. Per un facile accesso, spostare la catena di cavi sul lato destro verso sinistra con un dito.
5. Scollegare una delle catene di cavi di destra dalla relativa guida verticale.

   a. Utilizzando una torcia, individuare l’anello arancione all’estremità della catena di cavi collegata alla guida verticale del contenitore.

(1) *anello arancione su guida verticale*

(2) *catena di cavi, parzialmente rimossa*

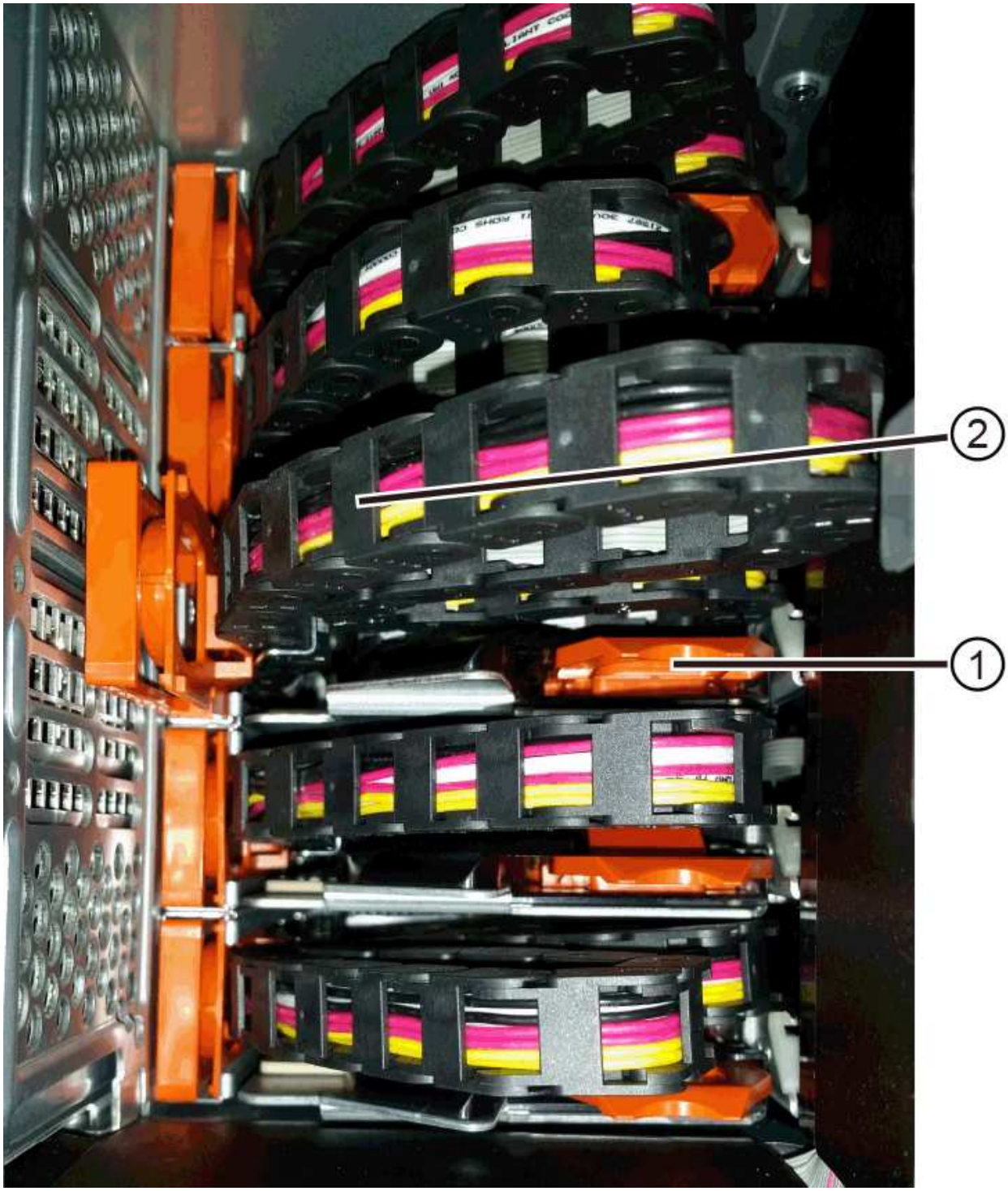
a. Per sganciare la catena di cavi, inserire il dito nell'anello arancione e premere verso il centro del sistema.

b. Per scollegare la catena di cavi, tirare con cautela il dito verso di sé circa 2.5 cm (1 pollice). Lasciare il connettore della catena di cavi all'interno della guida verticale. (Se il vassoio dell'unità è acceso, evitare che il connettore della catena di cavi tocchi il telaio metallico).

6. Scollegare l'altra estremità della catena portacavi:

   a. Utilizzando una torcia, individuare l'anello arancione all'estremità della catena di cavi collegata alla guida orizzontale del contenitore.

      La figura mostra il connettore orizzontale a destra e la catena dei cavi scollegata e parzialmente estratta sul lato sinistro.



(1) *anello arancione sulla guida orizzontale*

(2) *catena di cavi, parzialmente rimossa*

a. Per sganciare la catena di cavi, inserire delicatamente il dito nell'anello arancione e premere verso il basso.

   La figura mostra l'anello arancione sulla guida orizzontale (vedere l'elemento 1 nella figura precedente), in quanto viene spinto verso il basso in modo da poter estrarre il resto della catena di cavi dal contenitore.

b. Tirare il dito verso di sé per scollegare la catena di cavi.

7. Estrarre con cautela l'intera catena di cavi dallo shelf del disco.
8. Sostituire il filtro a carboni attivi della ventola destra:

   a. Far scorrere il contenitore della ventola fino in fondo nello scaffale.
   b. Spostare la maniglia del filtro a carboni attivi della ventola fino a quando non si blocca con la linguetta arancione.
   c. Se lo shelf del disco è alimentato, verificare che il LED di attenzione ambra sul retro della ventola non sia acceso e che l'aria stia uscendo dal retro della ventola.

      Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

   Se l'alimentazione è spenta, le ventole non funzionano e il LED non è acceso.

9. Dal retro dello shelf del disco, rimuovere il contenitore della ventola sinistro.
10. Se lo shelf di dischi riceve alimentazione, assicurarsi che la ventola giusta passi alla velocità massima.

> **Possibili danni all'apparecchiatura dovuti al surriscaldamento** — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

11. Scollegare la catena portacavi sinistra dalla relativa guida verticale:

    a. Utilizzando una torcia, individuare l'anello arancione all'estremità della catena di cavi collegata alla guida verticale.
    b. Per sganciare la catena di cavi, inserire il dito nell'anello arancione.
    c. Per scollegare la catena di cavi, tirare verso di sé circa 2.5 cm (1 poll.). Lasciare il connettore della catena di cavi all'interno della guida verticale.

> **Possibili danni all'hardware** — se il vassoio dell'unità è acceso, la catena di cavi viene eccitata fino a quando entrambe le estremità non vengono scollegate. Per evitare di mettere in corto circuito l'apparecchiatura, evitare che il connettore della catena di cavi scollegato tocchi il telaio metallico se l'altra estremità della catena di cavi è ancora collegata.

12. Scollegare la catena di cavi sinistra dalla guida orizzontale ed estrarre l'intera catena di cavi dallo shelf del disco.

    Se si esegue questa procedura con l'alimentazione accesa, tutti i LED si spengono quando si scollega l'ultimo connettore della catena di cavi, compreso il LED di attenzione di colore ambra.

13. Sostituire il filtro a carboni attivi della ventola sinistra. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola non sia acceso e che l'aria fuoriuscito dal retro della ventola.

    Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

Fase 3: Rimozione del cassetto del disco guasto (60 dischi)

Rimuovere un cassetto del disco guasto per sostituirlo con uno nuovo.

> **Possibile perdita di accesso ai dati** — i campi magnetici possono distruggere tutti i dati sul disco e causare danni irreparabili ai circuiti del disco. Per evitare la perdita di accesso ai dati e danni ai dischi, tenere i dischi sempre lontani da dispositivi magnetici.

Fasi

1. Assicurarsi che:
    - Le catene dei cavi destra e sinistra vengono rimosse dal cassetto dell'unità.
    - I contenitori delle ventole lato destro e sinistro vengono sostituiti.
2. Rimuovere il pannello frontale dallo shelf del disco.
3. Sganciare il cassetto dell'unità estraendo entrambe le leve.
4. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta. Non rimuovere completamente il cassetto dal ripiano del disco.
5. Se i volumi sono già stati creati e assegnati, utilizzare un indicatore permanente per annotare la posizione esatta di ciascun disco. Ad esempio, utilizzando il seguente disegno come riferimento, scrivere il numero di slot appropriato sulla parte superiore di ciascun disco.

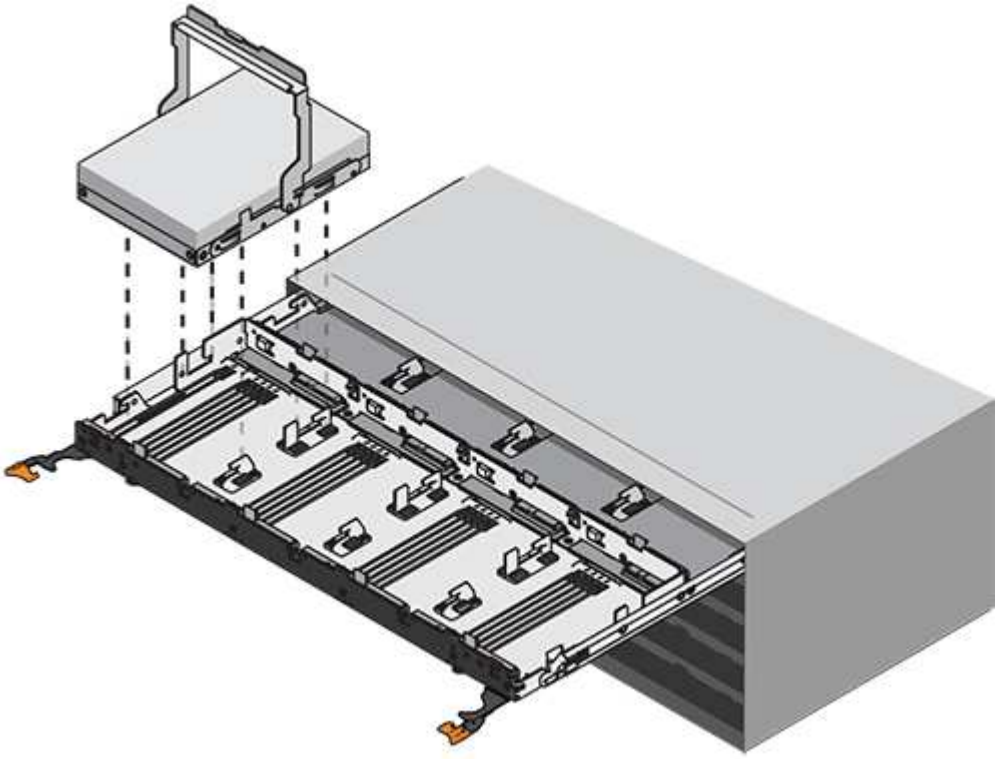
> **Possibile perdita di accesso ai dati** — assicurarsi di registrare la posizione esatta di ciascun disco prima di rimuoverlo.

6. Rimuovere le unità dal cassetto:
    a. Tirare delicatamente indietro il dispositivo di chiusura arancione visibile al centro della parte anteriore

di ciascun disco.

b. Sollevare la maniglia dell'unità in verticale.

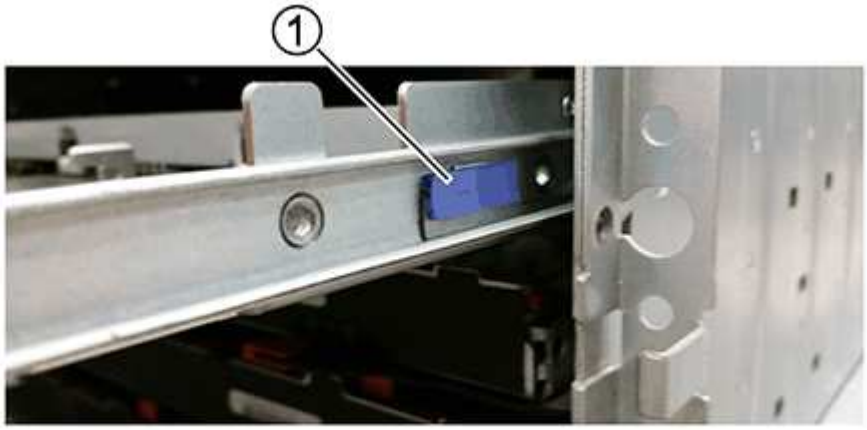
c. Utilizzare la maniglia per sollevare l'unità dal cassetto dell'unità.



d. Posizionare l'unità su una superficie piana, priva di scariche elettrostatiche e lontano da dispositivi magnetici.

7. Rimuovere il cassetto dell'unità:

a. Individuare la leva di rilascio in plastica su ciascun lato del cassetto dell'unità.



(1) *leva di rilascio cassetto unità*

a. Sganciare entrambe le leve di rilascio tirando i fermi verso di sé.

b. Tenendo entrambe le leve di rilascio, tirare il cassetto dell'unità verso di sé.

c. Rimuovere il cassetto del disco dallo shelf del disco.

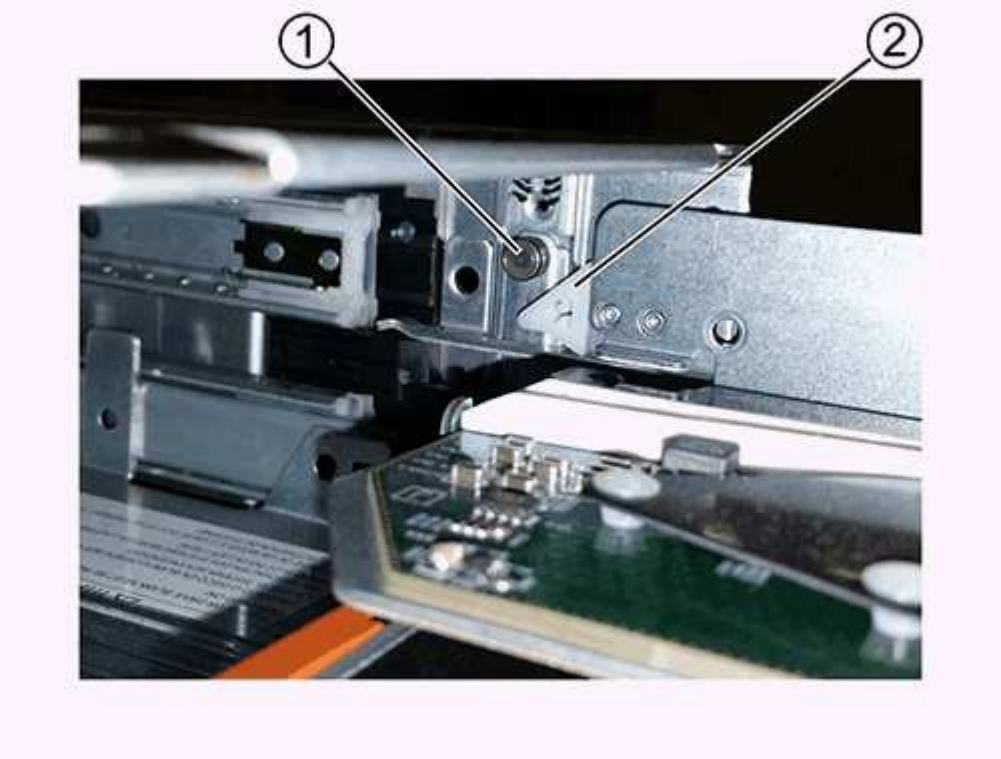
Fase 4: Installazione di un nuovo cassetto (60 dischi)

Installare un nuovo cassetto per sostituire quello guasto.

Fasi

1. Determinare la posizione in cui installare ciascun disco.
2. Dalla parte anteriore dello shelf del disco, far passare una torcia nello slot vuoto del cassetto e individuare il cilindretto di blocco dello slot.

   Il gruppo di blocco è una funzione di sicurezza che impedisce l'apertura di più cassetti per disco alla volta.



   (1) *Tumbler Lock-out*

   (2) *Guida cassetto*

3. Posizionare il cassetto dell'unità sostitutivo davanti allo slot vuoto e leggermente a destra rispetto al centro.

   Posizionando leggermente il cassetto a destra del centro, si garantisce che il nottolino di blocco e la guida del cassetto siano inseriti correttamente.

4. Far scorrere il cassetto dell'unità nello slot e assicurarsi che la guida del cassetto scorra sotto il nottolino di blocco.

   Rischio di danni all'apparecchiatura — si verifica un danno se la guida del cassetto non scorre sotto l'interruttore a levetta di blocco.

5. Spingere con cautela il cassetto dell'unità fino a quando il fermo non si aggancia completamente.

   Quando si chiude il cassetto per la prima volta, si verifica un livello di resistenza più elevato.

Rischio di danni all'apparecchiatura — interrompere la pressione del cassetto dell'unità se si ritiene che sia bloccato. Utilizzare le leve di rilascio nella parte anteriore del cassetto per far scorrere il cassetto all'indietro. Quindi, reinserire il cassetto nello slot, assicurarsi che il cilindretto si trovi sopra la guida e che le guide siano allineate correttamente.

Fase 5: Collegare le catene di cavi

Collegare le catene per cavi in modo da poter reinstallare in sicurezza le unità nel cassetto.

Quando si collega una catena di cavi, invertire l'ordine utilizzato per scollegare la catena di cavi. Inserire il connettore orizzontale della catena nella guida orizzontale del contenitore prima di inserire il connettore verticale della catena nella guida verticale del contenitore.

Fasi

1. Assicurarsi che:
   - La fase di installazione del nuovo cassetto unità è stata completata.
   - Sono presenti due catene di cavi sostitutive, contrassegnate come SINISTRA e DESTRA (sul connettore orizzontale accanto al cassetto dell'unità).
2. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola sul lato destro e metterlo da parte.
3. Se lo shelf è acceso, assicurarsi che la ventola sinistra sia alla massima velocità.

   Possibili danni all'apparecchiatura dovuti al surriscaldamento — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

4. Collegare la catena di cavi corretta:

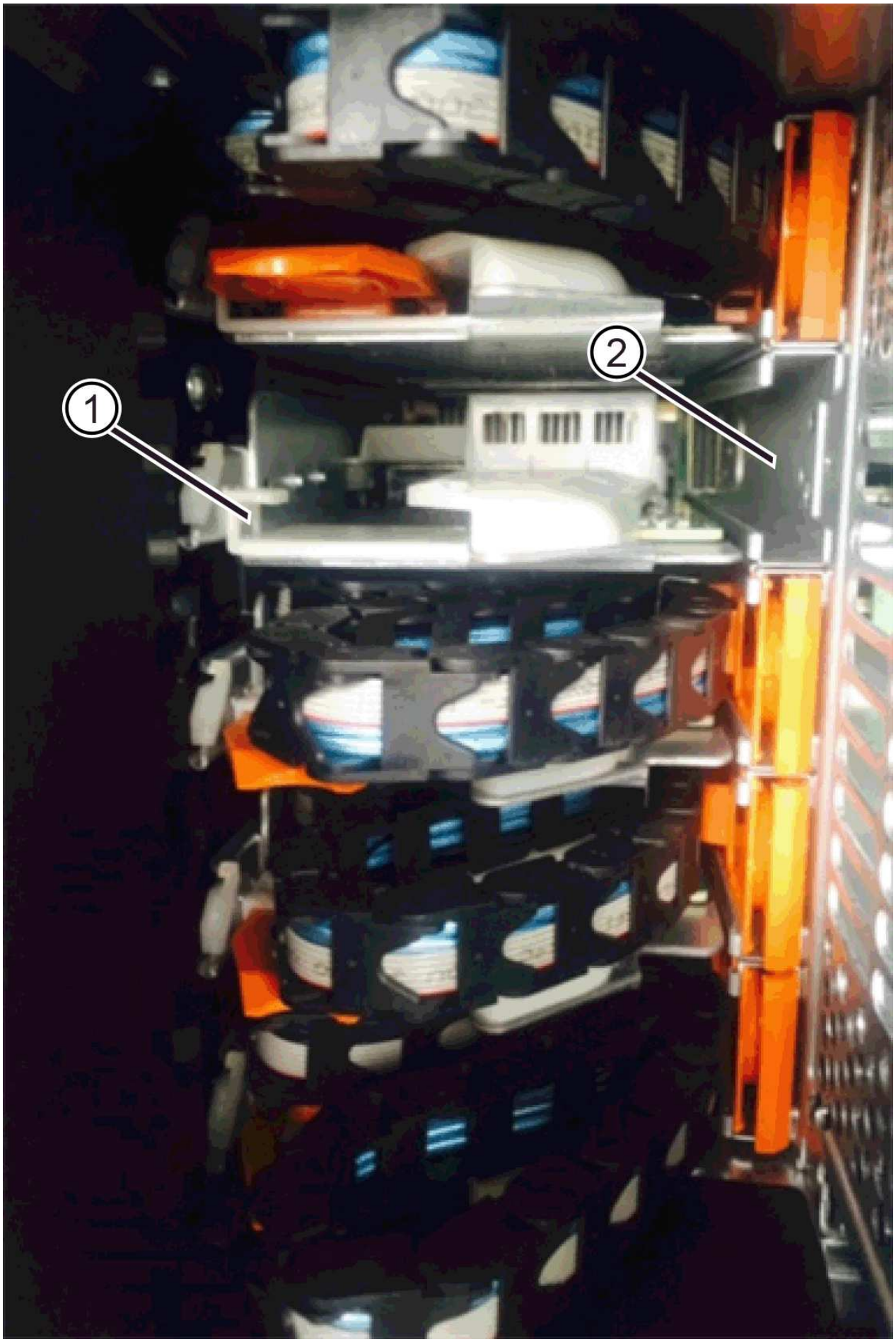
   a. Individuare i connettori orizzontali e verticali sulla catena destra e la guida orizzontale e verticale corrispondenti all'interno del contenitore.

   b. Allineare entrambi i connettori delle catene di cavi con le guide corrispondenti.

   c. Far scorrere il connettore orizzontale della catena di cavi sulla guida orizzontale e spingerlo fino in fondo.

      Rischio di malfunzionamento dell'apparecchiatura — assicurarsi di far scorrere il connettore nella guida. Se il connettore si trova sulla parte superiore della guida, potrebbero verificarsi problemi quando il sistema è in funzione.

      La figura mostra le guide orizzontali e verticali per il secondo cassetto del disco nel contenitore.


1
2

(1) *guida orizzontale*

(2) *guida verticale*

a. Far scorrere il connettore verticale sulla catena portacavi destra nella guida verticale.

b. Dopo aver ricollegato entrambe le estremità della catena, tirare con cautela la catena per verificare che entrambi i connettori siano bloccati.

> **Rischio di malfunzionamento dell'apparecchiatura** — se i connettori non sono bloccati, la catena dei cavi potrebbe allentarsi durante il funzionamento del cassetto.

5. Rimontare il filtro a carboni attivi della ventola lato destro. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola sia spento e che l'aria stia uscendo dal retro.

   Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola mentre la ventola si trova alla velocità corretta.

6. Dalla parte posteriore dello shelf del disco, rimuovere il contenitore della ventola sul lato sinistro dello shelf.
7. Se lo shelf è acceso, assicurarsi che la ventola giusta passi alla velocità massima.

> **Possibili danni all'apparecchiatura dovuti al surriscaldamento** — se lo shelf è acceso, non rimuovere entrambe le ventole contemporaneamente. In caso contrario, l'apparecchiatura potrebbe surriscaldarsi.

8. Ricollegare la catena del cavo sinistro:

   a. Individuare i connettori orizzontali e verticali sulla catena dei cavi e le relative guide orizzontali e verticali all'interno del contenitore.

   b. Allineare entrambi i connettori delle catene di cavi con le guide corrispondenti.

   c. Far scorrere il connettore orizzontale della catena nella guida orizzontale e spingerlo fino in fondo.

   > **Rischio di malfunzionamento dell'apparecchiatura** — assicurarsi di far scorrere il connettore all'interno della guida. Se il connettore si trova sulla parte superiore della guida, potrebbero verificarsi problemi quando il sistema è in funzione.

   d. Far scorrere il connettore verticale sulla catena sinistra nella guida verticale.

   e. Dopo aver ricollegato entrambe le estremità della catena, tirare con cautela la catena per verificare che entrambi i connettori siano bloccati.

   > **Rischio di malfunzionamento dell'apparecchiatura** — se i connettori non sono bloccati, la catena dei cavi potrebbe allentarsi durante il funzionamento del cassetto.

9. Rimontare il filtro a carboni attivi della ventola lato sinistro. Se lo shelf del disco riceve alimentazione, verificare che il LED ambra sul retro della ventola sia spento e che l'aria stia uscendo dal retro.

   Il LED potrebbe rimanere acceso per un minuto dopo aver reinstallato la ventola, mentre entrambe le ventole si posizionano alla velocità corretta.

Fase 6: Sostituzione completa del cassetto del disco (60 dischi)

Completare la sostituzione del cassetto dell'unità reinserendo le unità e riposizionando il pannello anteriore nell'ordine corretto.

> **Possibile perdita di accesso ai dati** — è necessario installare ciascun disco nella posizione originale nel cassetto.

Fasi

1. Reinstallare le unità nel cassetto:

   a. Sbloccare il cassetto dell'unità estraendo entrambe le leve nella parte anteriore del cassetto.

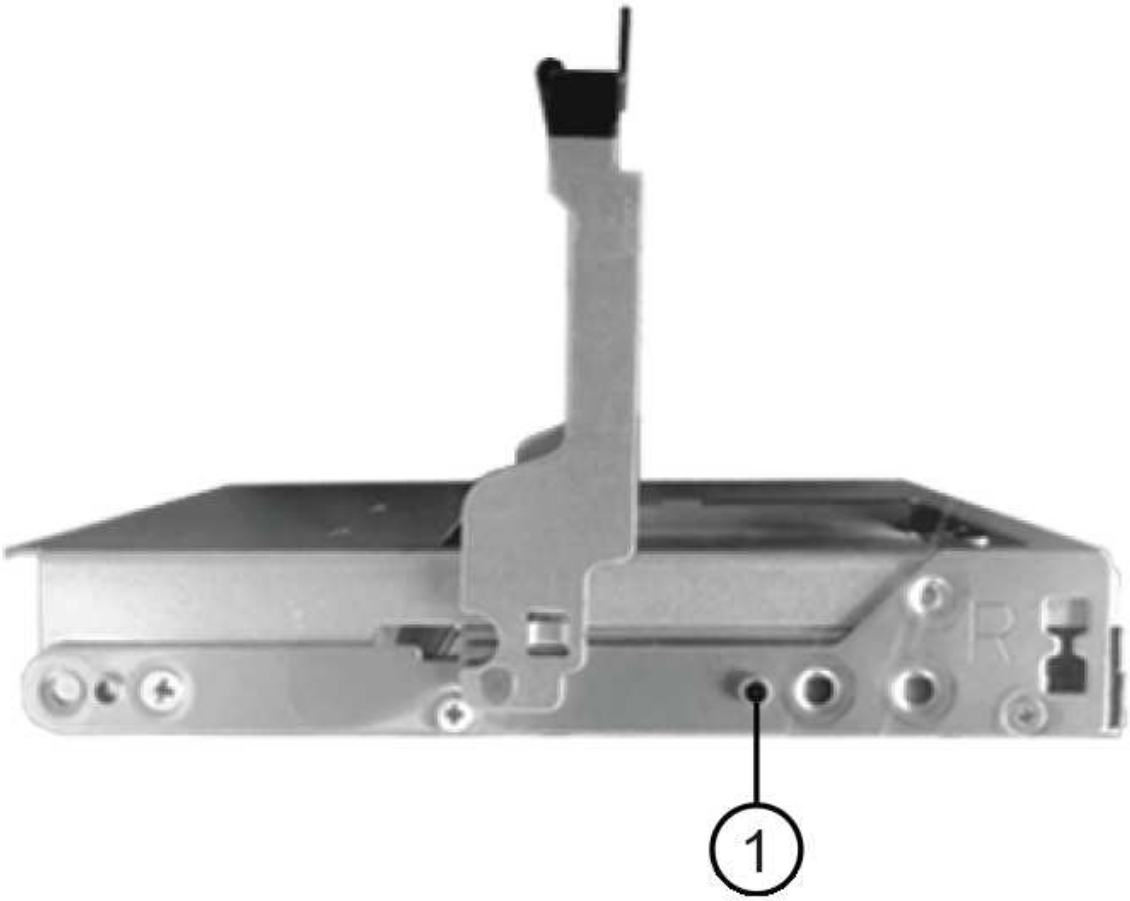
   b. Utilizzando le leve estese, estrarre con cautela il cassetto dell'unità fino a quando non si arresta. Non rimuovere completamente il cassetto dal ripiano del disco.

   c. Determinare il disco da installare in ogni slot utilizzando le note create durante la rimozione dei dischi.

   d. Sollevare la maniglia dell'unità in verticale.

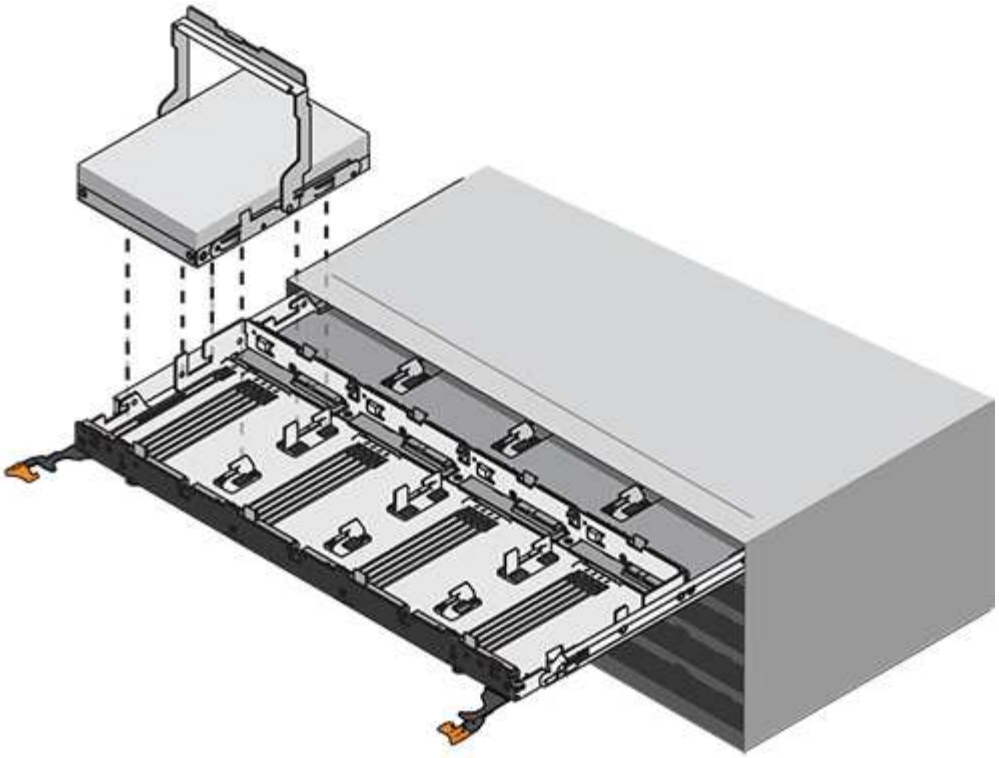
   e. Allineare i due pulsanti rialzati su ciascun lato dell'unità con le tacche del cassetto.

      La figura mostra la vista laterale destra di un'unità, che mostra la posizione dei pulsanti sollevati.



(1) *pulsante sollevato sul lato destro del disco*

a. Abbassare l'unità, accertandosi che sia premuta fino in fondo nell'alloggiamento, quindi ruotare la maniglia dell'unità verso il basso fino a farla scattare in posizione.



b. Ripetere questa procedura per installare tutti i dischi.

2. Far scorrere nuovamente il cassetto nello shelf dell'unità spingendolo dal centro e chiudendo entrambe le leve.

> **Rischio di malfunzionamento dell'apparecchiatura** — assicurarsi di chiudere completamente il cassetto dell'unità premendo entrambe le leve. Chiudere completamente il cassetto dell'unità per consentire un flusso d'aria adeguato ed evitare il surriscaldamento.

3. Fissare il pannello frontale alla parte anteriore dello shelf del disco.
4. Se si sono spenti uno o più shelf, riapplicare l'alimentazione:
   - **Se è stato sostituito un cassetto dischi in uno shelf *controller* senza protezione perdita cassetto**:
     i. Accendere entrambi gli interruttori di alimentazione sullo shelf del controller.
     ii. Attendere 10 minuti per il completamento del processo di accensione.
     iii. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.
   - **Se è stato sostituito un cassetto dischi in uno shelf di dischi *expansion* senza protezione perdita cassetto**:
     i. Accendere entrambi gli interruttori di alimentazione sullo shelf di dischi.
     ii. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.
     iii. Attendere due minuti prima di alimentare lo shelf del controller.
     iv. Accendere entrambi gli interruttori di alimentazione sullo shelf del controller.
     v. Attendere 10 minuti per il completamento del processo di accensione.

vi. Verificare che entrambe le ventole si accendano e che il LED ambra sul retro delle ventole sia spento.

Quali sono le prossime novità?

La sostituzione del cassetto dell'unità è stata completata. È possibile riprendere le normali operazioni.

Aggiunta a caldo di uno shelf di dischi

È possibile aggiungere un nuovo shelf di dischi mentre gli altri componenti del sistema di storage sono ancora in funzione. È possibile configurare, riconfigurare, aggiungere o spostare la capacità del sistema storage senza interrompere l'accesso degli utenti ai dati.

Prima di iniziare

A causa della complessità di questa procedura, si consiglia quanto segue:

- Leggere tutti i passaggi prima di iniziare la procedura.
- Assicurarsi che l'aggiunta a caldo di uno shelf di dischi sia la procedura necessaria.

A proposito di questa attività

Questa procedura si applica all'aggiunta a caldo di uno shelf di dischi DE212C, DE224C o DE460C a E2800, E2800, EF280, E5700, E5700B, Shelf di controller EF570, EF300 o EF600.

Questa procedura si applica agli shelf di dischi IOM12 e IOM12B.

> I moduli IOM12B sono supportati solo da SANtricity OS 11.70.2 in poi. Assicurarsi che il firmware del controller sia stato aggiornato prima di installare o eseguire l'aggiornamento a IOM12B.

> Questa procedura si applica a sostituzioni o sostituzioni IOM di shelf simili. Ciò significa che è possibile sostituire solo un modulo IOM12 con un altro modulo IOM12 o un modulo IOM12B con un altro modulo IOM12B. (Lo shelf può avere due moduli IOM12 o due moduli IOM12B).

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

> Per mantenere l'integrità del sistema, seguire la procedura esattamente nell'ordine suggerito.

Fase 1: Preparazione all'aggiunta dello shelf di dischi

Per prepararsi all'aggiunta a caldo di uno shelf di dischi, è necessario verificare la presenza di eventi critici e lo stato degli IOM.

Prima di iniziare

- La fonte di alimentazione del sistema storage deve essere in grado di soddisfare i requisiti di alimentazione del nuovo shelf di dischi. Per le specifiche di alimentazione dello shelf di dischi, consultare "Hardware Universe".
- Lo schema di cablaggio per il sistema storage esistente deve corrispondere a uno degli schemi applicabili illustrati in questa procedura.

Fasi

1. In Gestore di sistema di SANtricity, selezionare **supporto** > **Centro di supporto** > **Diagnostica**.
2. Selezionare **Collect Support Data**.

   Viene visualizzata la finestra di dialogo Collect Support Data (raccolta dati di supporto).

3. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome support-data.7z. I dati non vengono inviati automaticamente al supporto tecnico.

4. Selezionare **supporto** > **Registro eventi**.

   La pagina Registro eventi visualizza i dati dell'evento.

5. Selezionare l'intestazione della colonna **priorità** per ordinare gli eventi critici all'inizio dell'elenco.
6. Esaminare gli eventi critici di sistema per gli eventi che si sono verificati nelle ultime due o tre settimane e verificare che gli eventi critici recenti siano stati risolti o altrimenti risolti.

   > Se si sono verificati eventi critici non risolti nelle due o tre settimane precedenti, interrompere la procedura e contattare il supporto tecnico. Continuare la procedura solo dopo aver risolto il problema.

7. Selezionare **hardware**.
8. Selezionare l'icona **IOM (ESM)**.

   Viene visualizzata la finestra di dialogo Shelf Component Settings (Impostazioni componenti shelf) con la scheda **IOM (ESM)** selezionata.

9. Assicurarsi che lo stato visualizzato per ogni IOM/ESM sia *ottimale*.
10. Fare clic su **Mostra altre impostazioni**.
11. Verificare che sussistano le seguenti condizioni:
    - Il numero di ESM/IOM rilevati corrisponde al numero di ESM/IOM installati nel sistema e a quello di ogni shelf di dischi.
    - Entrambi gli ESM/IOM mostrano che la comunicazione è corretta.
    - La velocità di trasferimento dati è di 12 GB/s per gli shelf di dischi DE212C, DE224C e DE460C o di 6 GB/s per gli altri tray di dischi.

Fase 2: Installare lo shelf di dischi e alimentare

Si installa un nuovo shelf di dischi o uno shelf di dischi precedentemente installato, si accende l'alimentazione e si verifica la presenza di eventuali LED che richiedono attenzione.

Fasi

1. Se si sta installando uno shelf di dischi precedentemente installato in un sistema storage, rimuovere i dischi. I dischi devono essere installati uno alla volta più avanti in questa procedura.

   Se la cronologia di installazione dello shelf di dischi che si sta installando non è nota, si deve presumere che sia stato precedentemente installato in un sistema storage.

2. Installare lo shelf di dischi nel rack che contiene i componenti del sistema di storage.

> Consultare le istruzioni di installazione del modello in uso per la procedura completa per l'installazione fisica e il cablaggio di alimentazione. Le istruzioni di installazione del modello in uso includono note e avvisi da tenere in considerazione per installare in sicurezza uno shelf di dischi.

3. Accendere il nuovo shelf di dischi e verificare che sullo shelf non siano accesi LED di attenzione color ambra. Se possibile, risolvere eventuali condizioni di guasto prima di continuare con questa procedura.

Fase 3: Collegare il sistema via cavo

Selezionare una delle seguenti opzioni:

- Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700
- Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

Se si sta cablando uno shelf di controller meno recente a DE212C, DE224C o DE460, vedere "Aggiunta di shelf di dischi IOM a uno shelf di controller E27XX, E56XX o EF560 esistente".

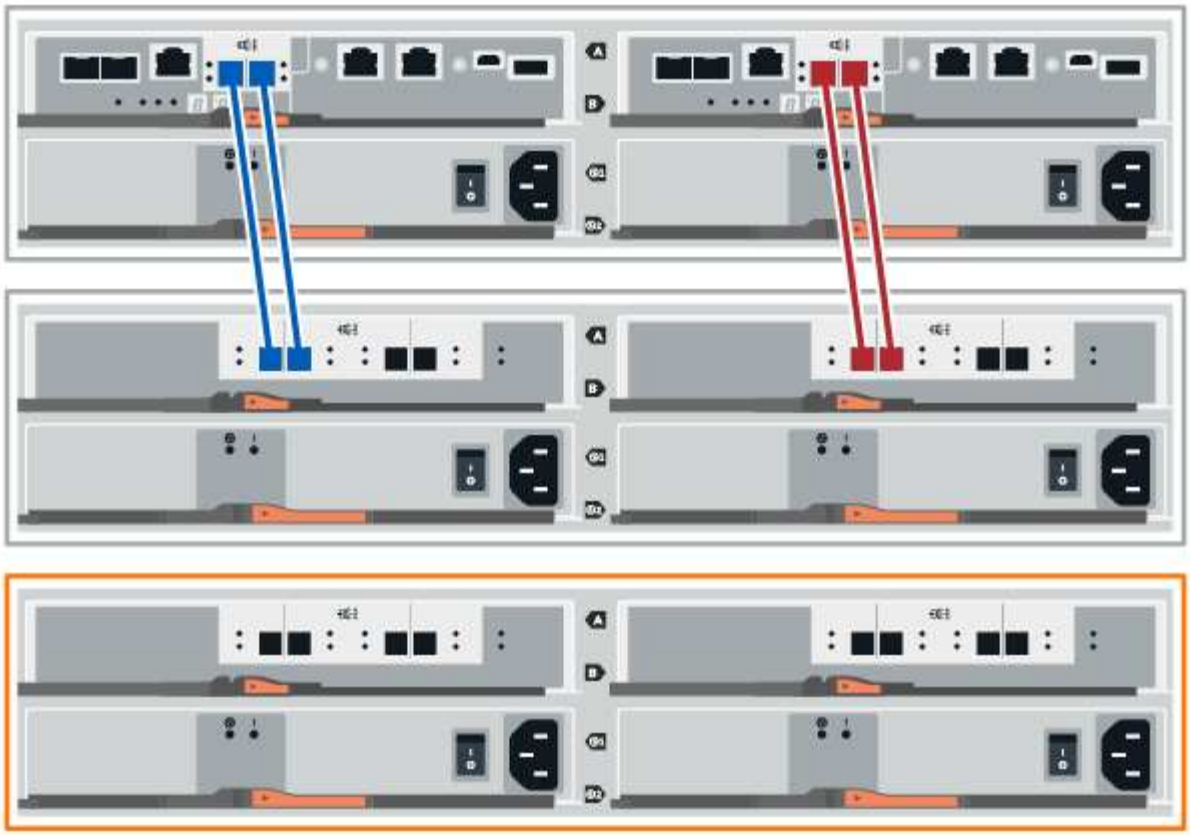
Opzione 1: Collegamento dello shelf di dischi per E2800 o E5700

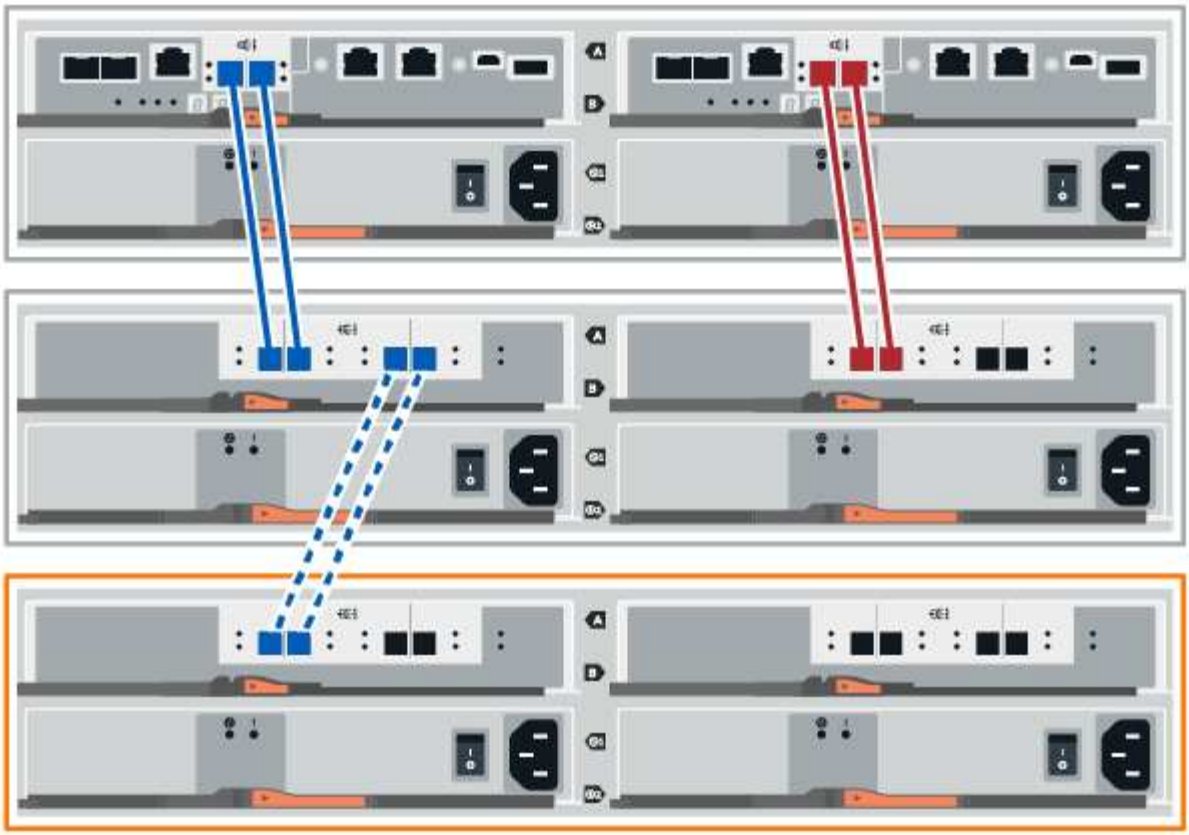
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Fasi

1. Collegare lo shelf di dischi al controller A.

   La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller A. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".





2. In Gestione sistema di SANtricity, fare clic su **hardware**.

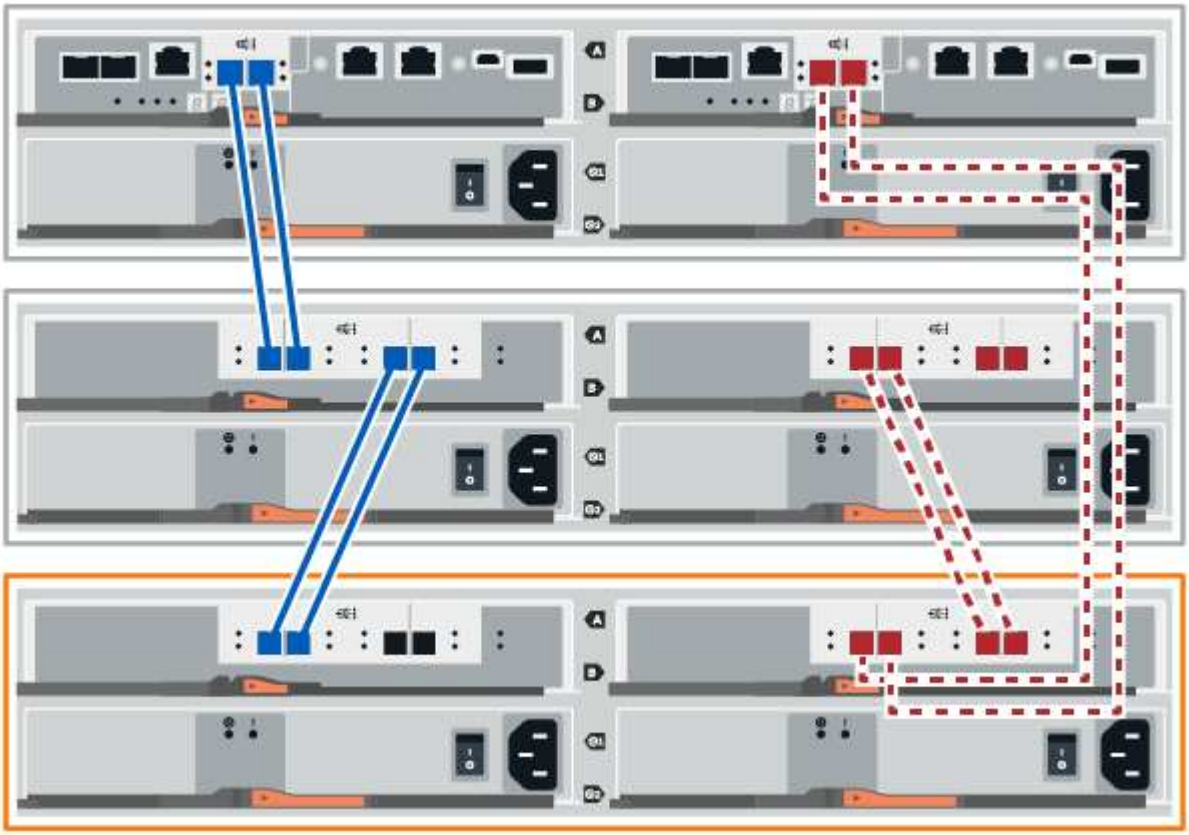
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

3. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
4. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

   Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

5. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
6. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
7. Scollegare tutti i cavi di espansione dal controller B.
8. Collegare lo shelf di dischi al controller B.

La figura seguente mostra un esempio di connessione tra un ulteriore shelf di dischi e il controller B. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



9. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Opzione 2: Collegare lo shelf di dischi per EF300 o EF600

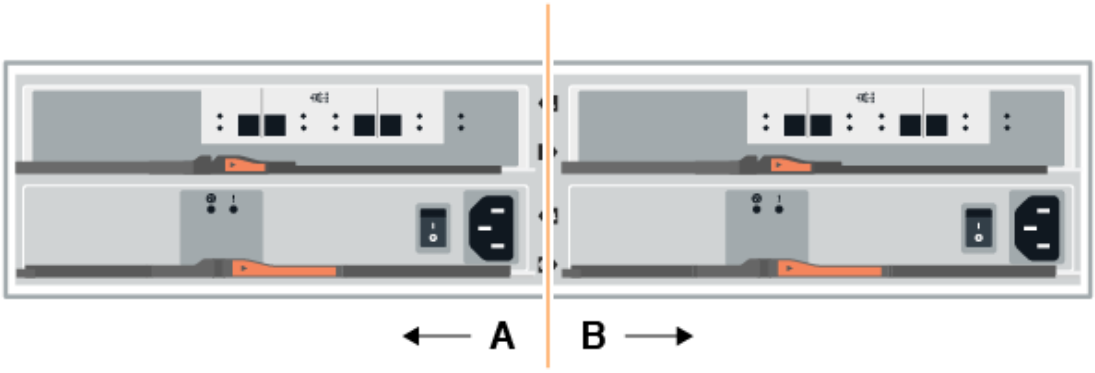
Collegare lo shelf di dischi al controller A, confermare lo stato IOM, quindi collegare lo shelf di dischi al controller B.

Prima di iniziare

- Il firmware è stato aggiornato alla versione più recente. Per aggiornare il firmware, seguire le istruzioni in "Aggiornamento del sistema operativo SANtricity".

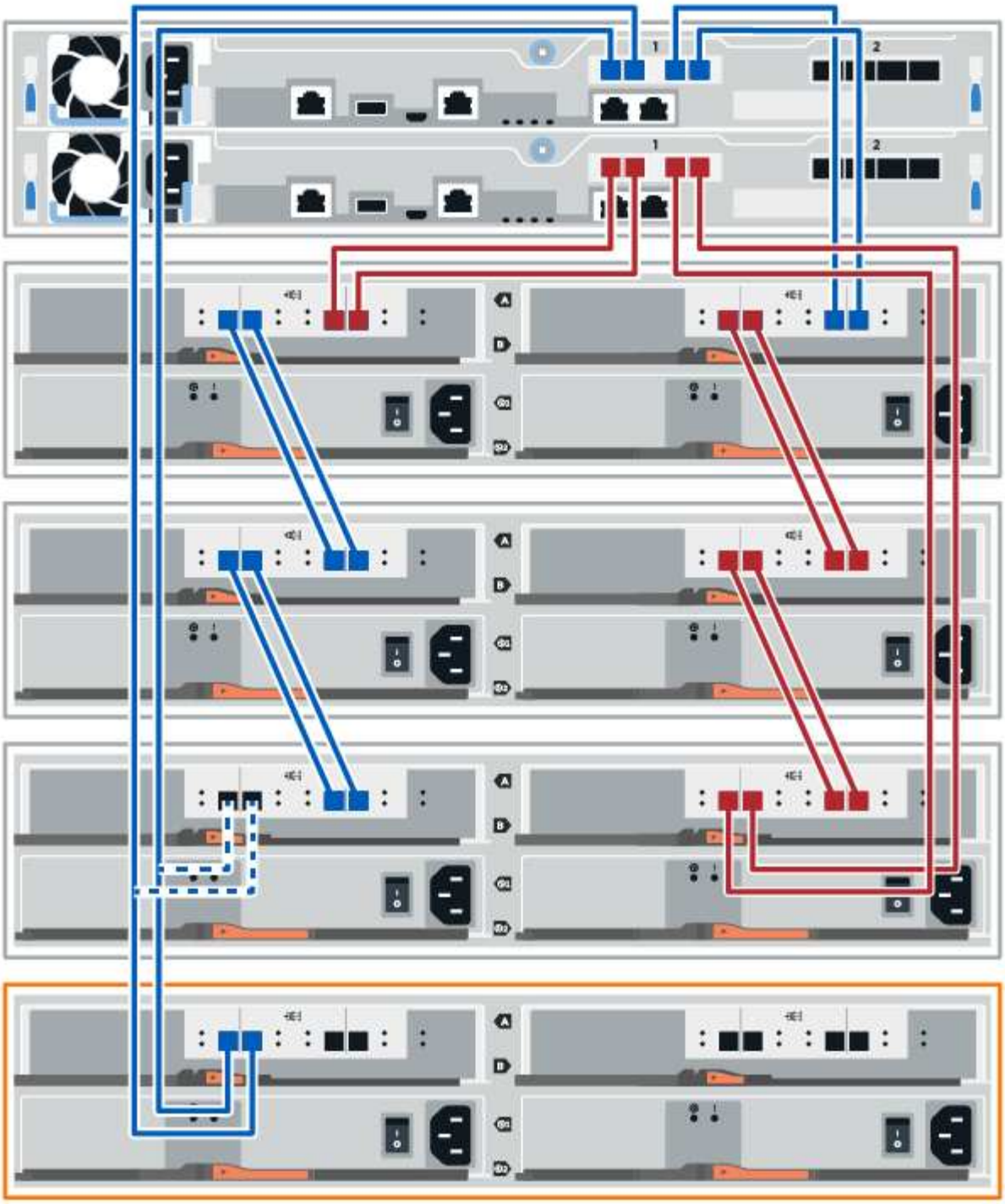
Fasi

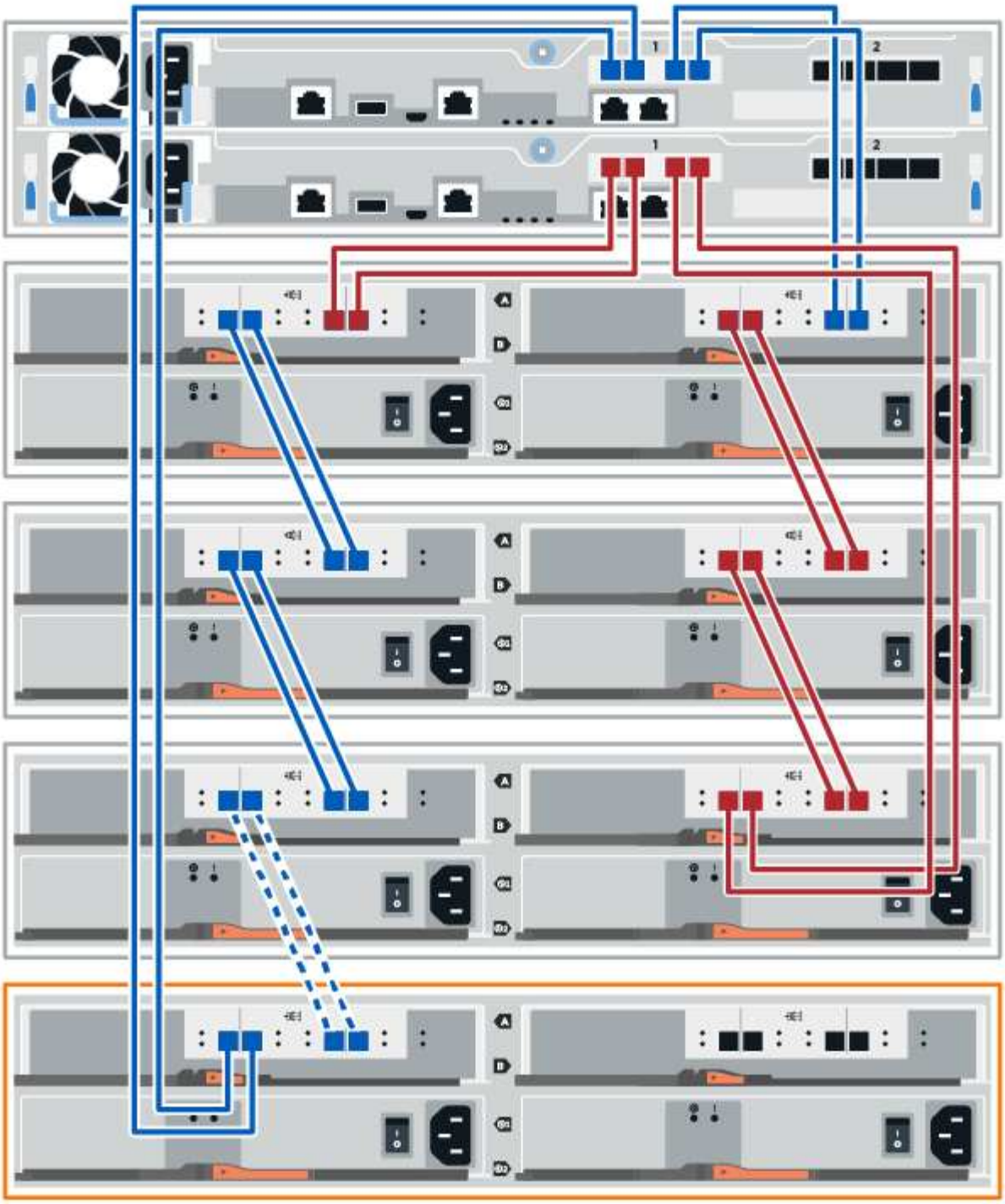
1. Scollegare entrambi i cavi del controller Lato A dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.



2. Collegare i cavi alle porte IOM12 lato A tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di connessione per un lato tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".


1
2
1
2
A
B



3. In Gestione sistema di SANtricity, fare clic su **hardware**.

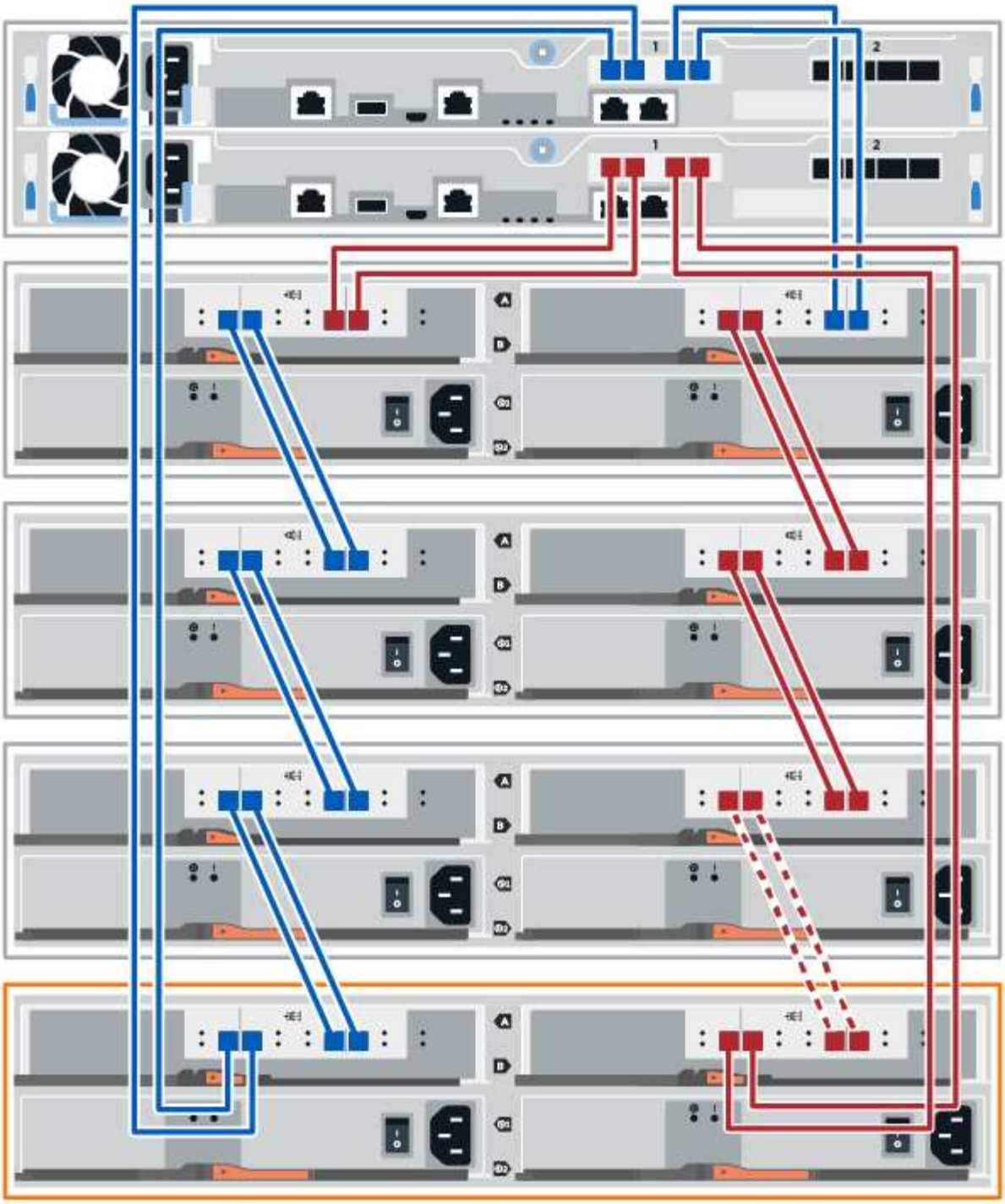
> A questo punto della procedura, si dispone di un solo percorso attivo per lo shelf del controller.

4. Scorrere verso il basso, se necessario, per visualizzare tutti gli shelf di dischi nel nuovo sistema storage. Se il nuovo shelf di dischi non viene visualizzato, risolvere il problema di connessione.
5. Selezionare l'icona **ESM/IOM** per il nuovo shelf di dischi.

Viene visualizzata la finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).

6. Selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings** (Impostazioni componenti shelf).
7. Selezionare **Mostra altre opzioni** e verificare quanto segue:
   - IOM/ESM A è elencato.
   - La velocità attuale dei dati è di 12 Gbps per uno shelf di dischi SAS-3.
   - Le comunicazioni con la scheda sono corrette.
8. Scollegare entrambi i cavi del controller lato B dalle porte IOM12 una e due dell'ultimo shelf precedente dello stack, quindi collegarli alle porte IOM12 del nuovo shelf una e due.
9. Collegare i cavi alle porte IOM12 lato B tre e quattro dal nuovo shelf alle porte IOM12 dell'ultimo shelf precedenti una e due.

   La figura seguente mostra un esempio di collegamento per il lato B tra un ulteriore shelf di dischi e l'ultimo shelf precedente. Per individuare le porte sul modello in uso, consultare la "Hardware Universe".



10. Se non è già selezionata, selezionare la scheda **ESM/IOM** nella finestra di dialogo **Shelf Component Settings**, quindi selezionare **Mostra altre opzioni**. Verificare che la scheda di comunicazione sia **sì**.

> Lo stato ottimale indica che l'errore di perdita di ridondanza associato al nuovo shelf di dischi è stato risolto e che il sistema di storage è stabilizzato.

Fase 4: Completare l'aggiunta a caldo

Per completare l'aggiunta a caldo, verificare la presenza di eventuali errori e confermare che lo shelf di dischi appena aggiunto utilizzi il firmware più recente.

Fasi

1. In Gestore di sistema di SANtricity, fare clic su **Home**.
2. Se il collegamento **Recover from Problems** (Ripristina da problemi) viene visualizzato al centro della pagina, fare clic sul collegamento e risolvere eventuali problemi indicati nel Recovery Guru.
3. In Gestione sistema di SANtricity, fare clic su **hardware** e scorrere verso il basso, se necessario, per visualizzare lo shelf di dischi appena aggiunto.
4. Per i dischi precedentemente installati in un sistema storage diverso, aggiungere un disco alla volta allo shelf di dischi appena installato. Attendere che ogni disco venga riconosciuto prima di inserire il disco successivo.

   Quando un disco viene riconosciuto dal sistema di storage, la rappresentazione dello slot nella pagina **hardware** viene visualizzata come un rettangolo blu.
5. Selezionare la scheda **Support** > **Support Center** > **Support Resources**.
6. Fare clic sul collegamento **Software and firmware Inventory** (inventario software e firmware) e verificare quali versioni del firmware IOM/ESM e del firmware del disco sono installate sul nuovo shelf di dischi.

   > Potrebbe essere necessario scorrere la pagina verso il basso per individuare questo collegamento.
7. Se necessario, aggiornare il firmware del disco.

   Il firmware IOM/ESM viene aggiornato automaticamente alla versione più recente, a meno che non sia stata disattivata la funzione di aggiornamento.

La procedura di aggiunta a caldo è stata completata. È possibile riprendere le normali operazioni.

Schede di interfaccia host

Requisiti per la sostituzione HIC E5700

Prima di aggiungere, aggiornare o sostituire una scheda di interfaccia host (HIC) in un E5700, esaminare i requisiti e le considerazioni.

Panoramica della procedura

È possibile aggiungere, aggiornare o sostituire un HIC nello shelf del controller E5724 e nello shelf del controller E5760.

Di seguito è riportata una panoramica dei passaggi per la sostituzione di un HIC in un controller E5700 (E5724 o E5760):

1. Portare il controller offline
2. Rimuovere il contenitore del controller
3. Sostituire la batteria

4. Sostituire il contenitore del controller
5. Portare il controller online

Requisiti per l'aggiunta, l'aggiornamento o la sostituzione di un HIC

Se si intende aggiungere, aggiornare o sostituire una scheda di interfaccia host (HIC), tenere presenti i seguenti requisiti.

- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).
- È necessario disporre di due HICS compatibili con i controller.

  Per le configurazioni duplex (due controller), l'HICS installato nei due contenitori del controller deve essere identico. La presenza di HICS non corrispondenti causa il blocco del controller con l'HIC sostitutivo quando lo si porta online.

- Sono disponibili tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host Bus Adapter) necessari per collegare le nuove porte host.

  Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

- Si dispone di un braccialetto ESD o si sono prese altre precauzioni antistatiche.
- Hai un cacciavite Phillips n. 1.
- Sono presenti etichette per identificare ciascun cavo collegato al contenitore del controller.
- Si dispone di una stazione di gestione con un browser in grado di accedere a Gestore di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Aggiunta della scheda di interfaccia host (HIC) E5700

È possibile aggiungere una scheda di interfaccia host (HIC) ai canister dei controller E5700 con porte host della scheda base. Questa aggiunta aumenta il numero di porte host nell'array di storage e fornisce protocolli host aggiuntivi.

A proposito di questa attività

Quando si aggiunge HICS, è necessario spegnere lo storage array, installare l'HIC e riapplicare l'alimentazione.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E5700".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).
- Assicurarsi di disporre di quanto segue:
  - Uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve

essere compatibile con i controller.

- Nuovo hardware host installato per le nuove porte host, ad esempio switch o HBA (host bus adapter).
- Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte host.

  Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" e a. "NetApp Hardware Universe".

- Etichette per identificare ciascun cavo collegato al contenitore del controller.
- Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
- Un cacciavite Phillips n. 1.
- Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione all'aggiunta di HIC

Preparare l'aggiunta di un HIC eseguendo il backup del database di configurazione dello storage array, raccogliendo i dati di supporto e interrompendo le operazioni di i/o dell'host. Quindi, è possibile spegnere lo shelf del controller.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il

problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
b. Selezionare **Collect Support Data**.
c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

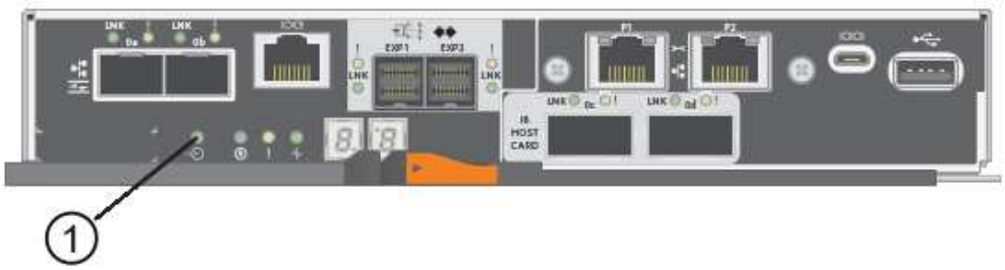
4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

   > I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

   > **Possibile perdita di dati** — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



(1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
8. Spegnere lo shelf del controller.
   a. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.

b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter aggiungere il nuovo HIC.

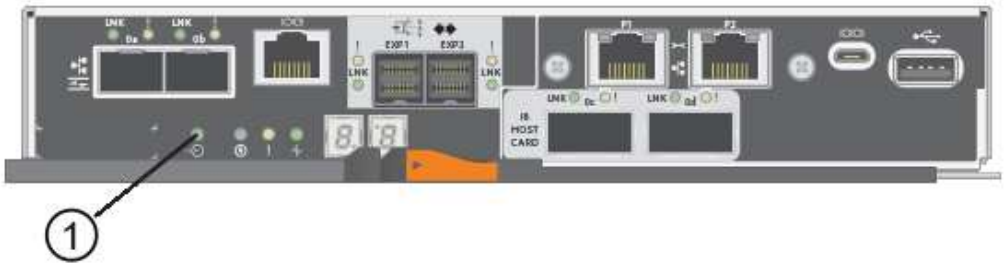
Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

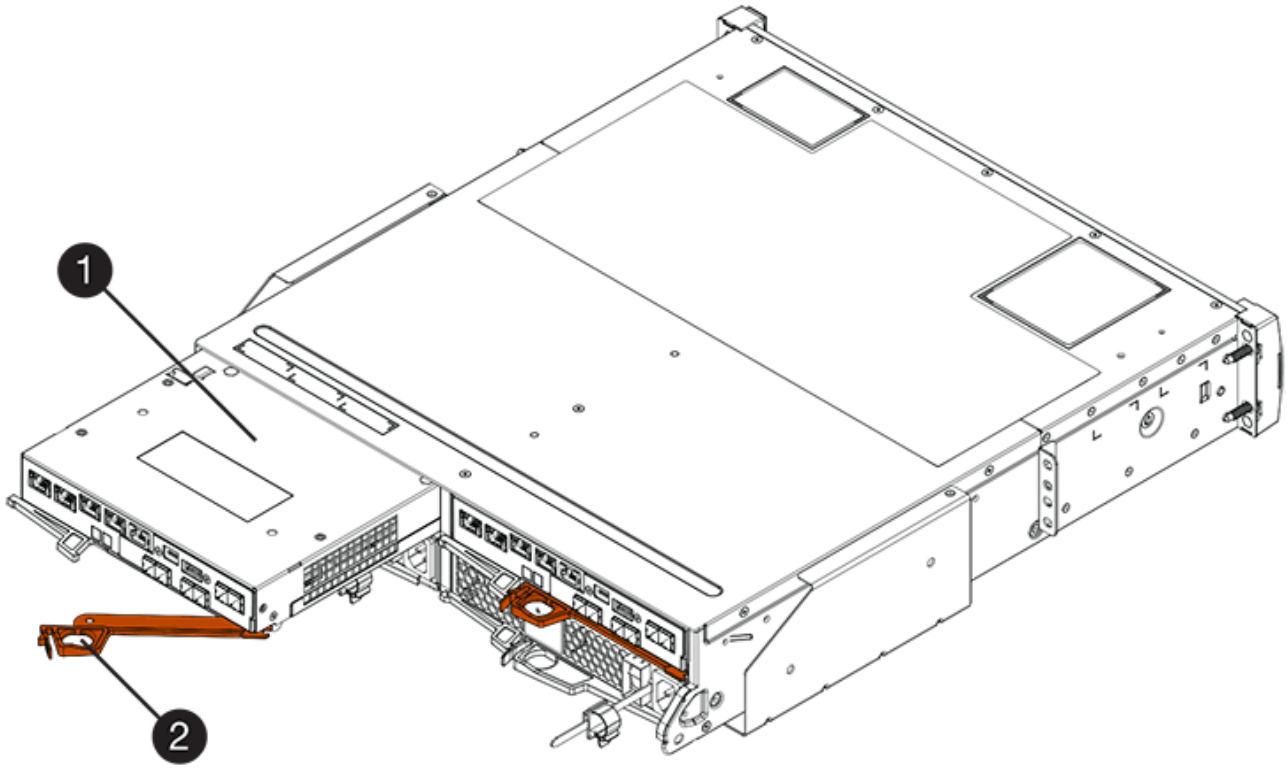
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



   (1) *LED cache attiva*

4. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

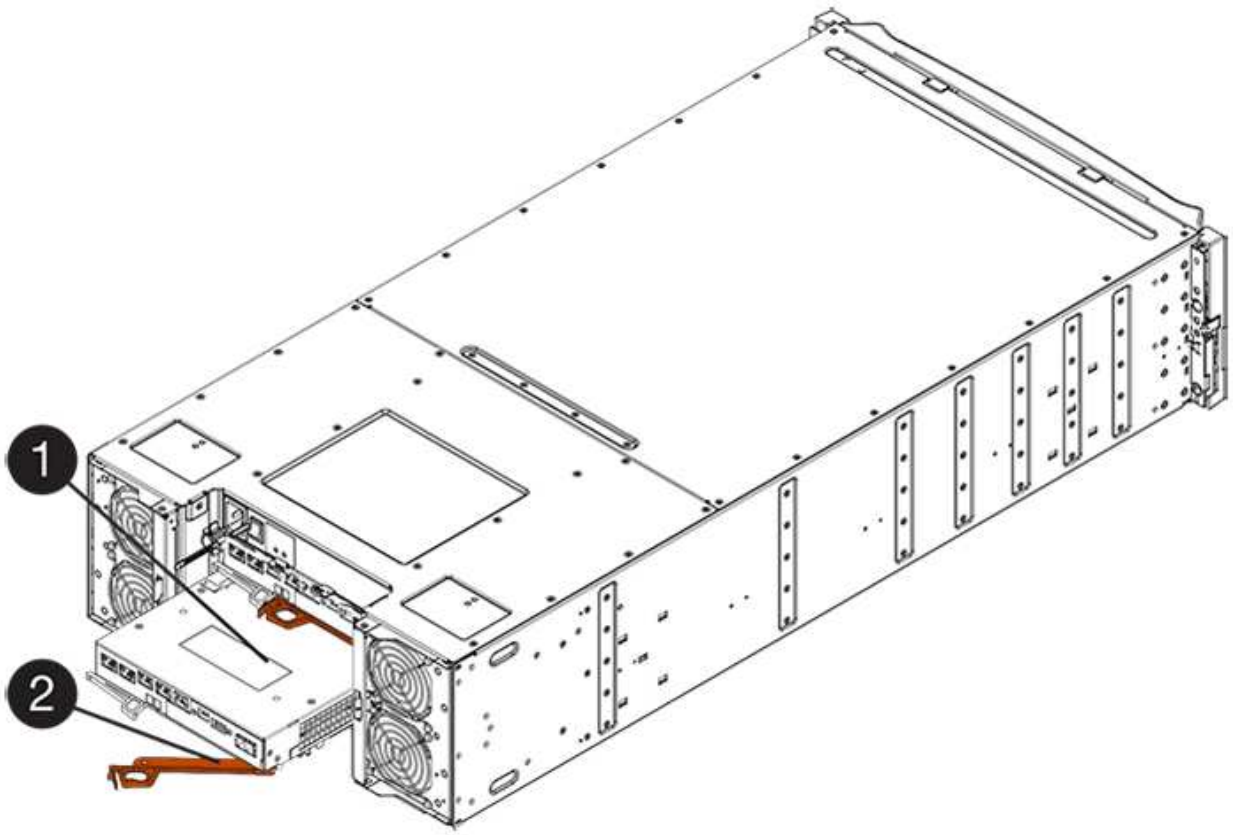
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

5. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf del controller E5724, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

6. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Installare un HIC

Installare la scheda di interfaccia host (HIC) per aumentare il numero di porte host nell'array di storage.

Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore del controller E5700 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Premere il pulsante sul coperchio del contenitore del controller ed estrarre il coperchio.

3. Verificare che il LED verde all'interno del controller (accanto ai DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

   (1) *cache interna attiva*

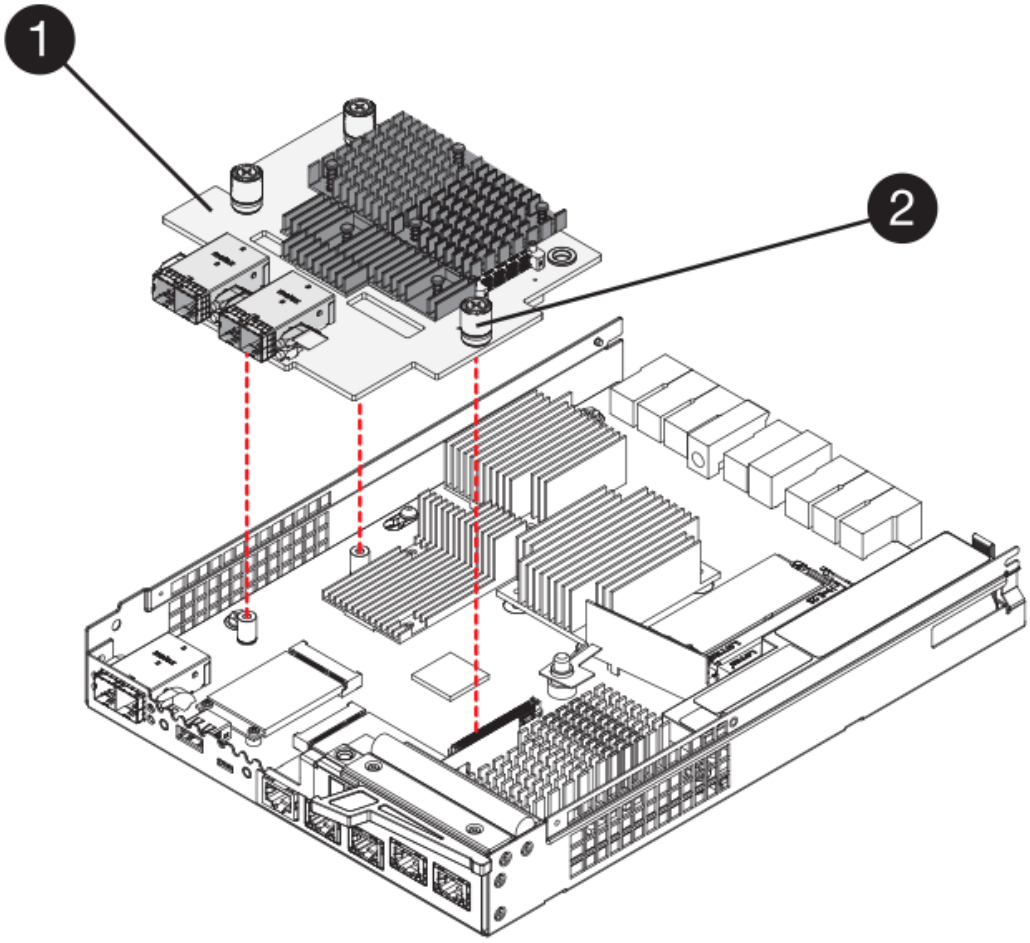
   (2) *batteria*

4. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller, quindi rimuovere la piastra frontale.
5. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

6. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



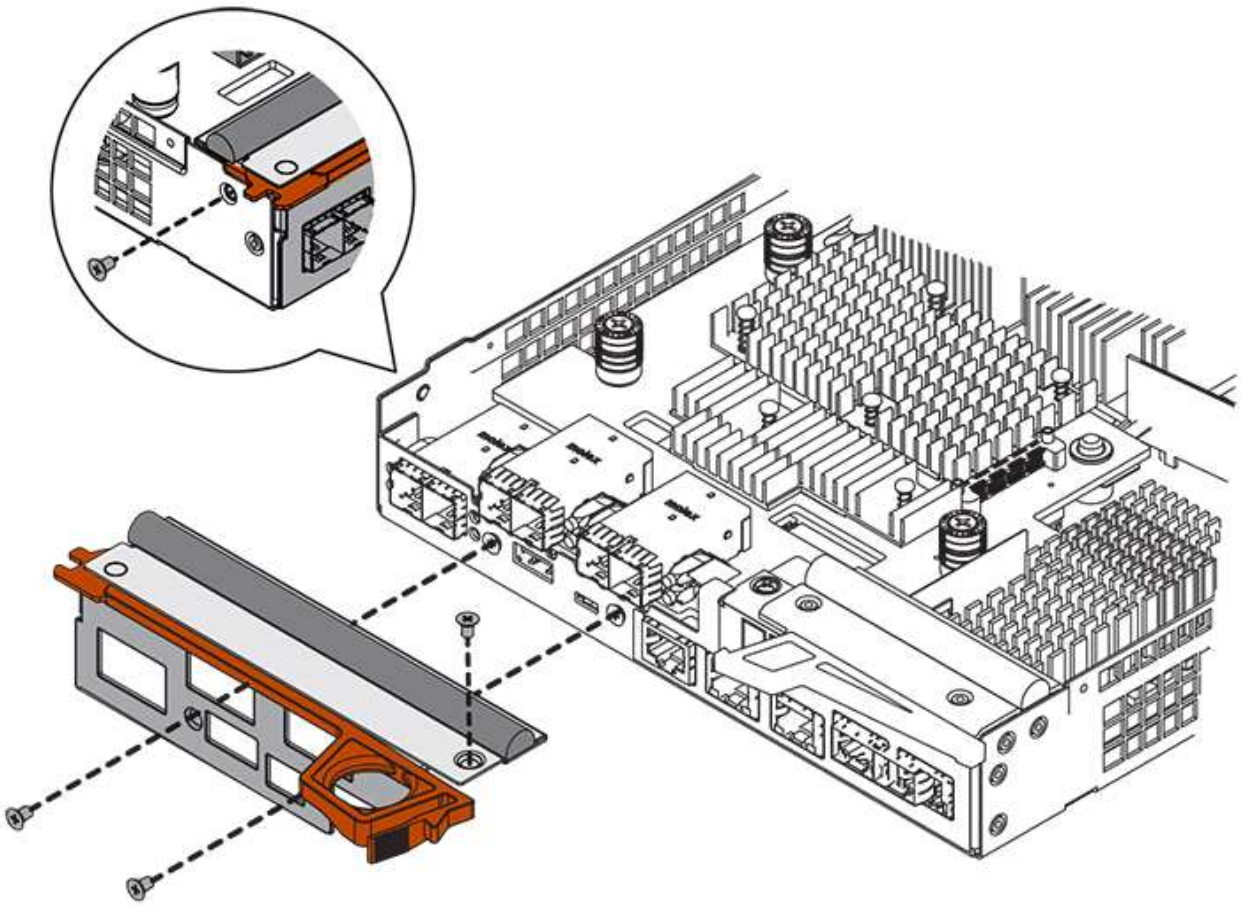
(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

7. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

8. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.



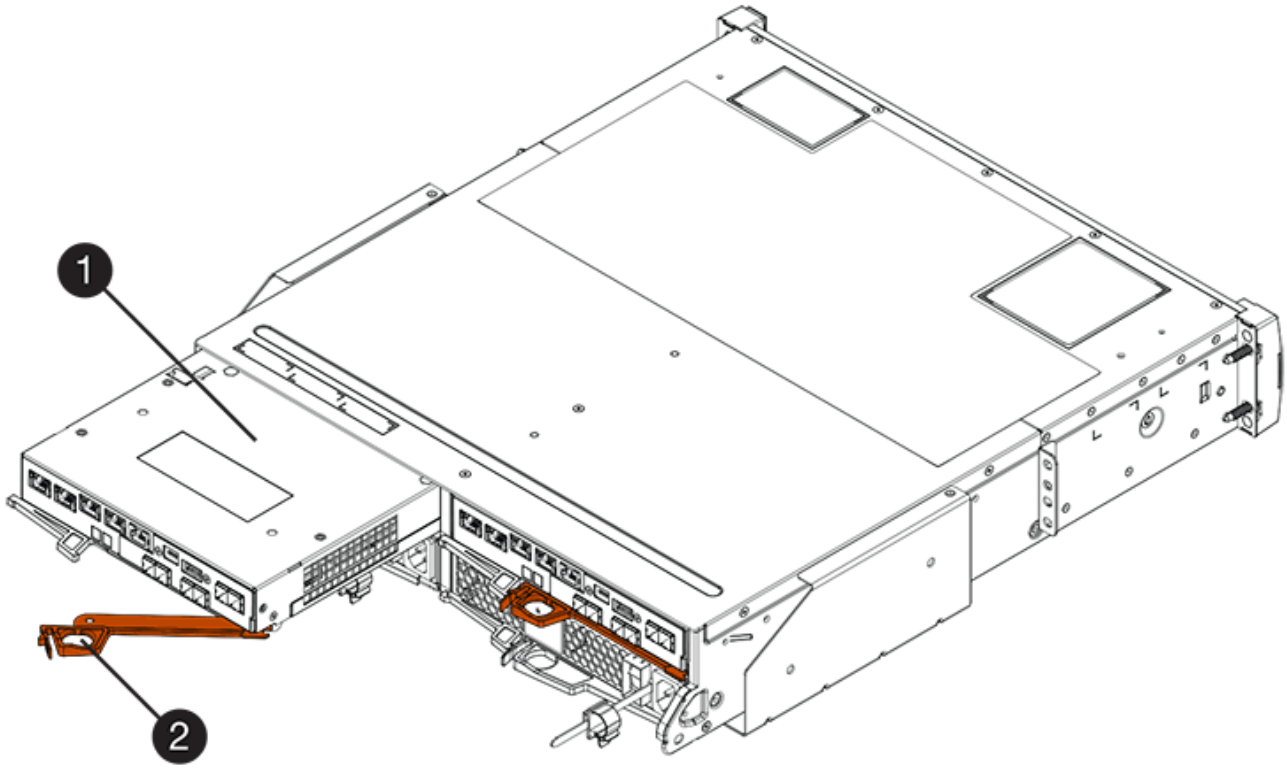
Fase 4: Reinstallare il contenitore del controller

Reinstallare il contenitore del controller nello shelf del controller dopo aver installato il nuovo HIC.

Fasi

1. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
2. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

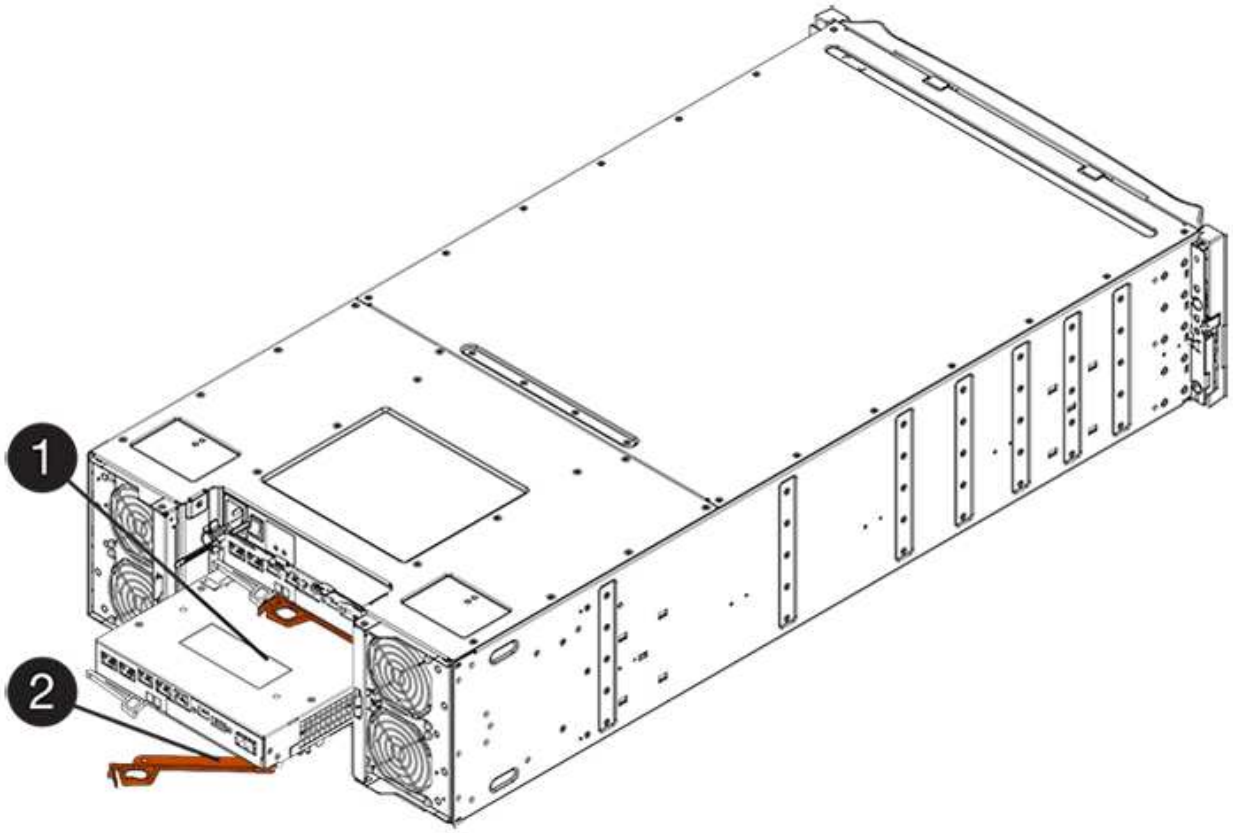
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

3. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
4. Ricollegare tutti i cavi rimossi.

   Non collegare i cavi dati alle nuove porte HIC in questo momento.

5. (Facoltativo) se si aggiunge HICS a una configurazione duplex, ripetere tutti i passaggi per rimuovere il secondo elemento filtrante del controller, installare il secondo HIC e reinstallare il secondo elemento filtrante del controller.

Fase 5: Completare l'aggiunta di HIC

Controllare i LED del controller e il display a sette segmenti, quindi verificare che lo stato del controller sia ottimale.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a

sette segmenti dovrebbe visualizzare l'ID del vassoio.

- Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
- I LED verdi del collegamento host rimangono spenti fino a quando non si collegano i cavi host.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

(1) *LED collegamento host*

(2) *LED di attenzione (ambra)*

(3) *Display a sette segmenti*

3. Da Gestore di sistema di SANtricity, verificare che lo stato del controller sia ottimale.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se le nuove porte HIC richiedono ricetrasmettitori SFP+, installarli.
5. Se è stato installato un HIC con porte SFP+ (ottiche), verificare che le nuove porte dispongano del protocollo host previsto.
   a. Da Gestione sistema di SANtricity, selezionare **hardware**.
   b. Se la figura mostra i dischi, fare clic su **Mostra retro dello shelf**.
   c. Selezionare l'immagine per Controller A o Controller B.
   d. Selezionare **Visualizza impostazioni** dal menu di scelta rapida.
   e. Selezionare la scheda **interfacce host**.
   f. Fare clic su **Mostra altre impostazioni**.
   g. Esaminare i dettagli mostrati per le porte HIC (le porte etichettate **e0*x*** o **0*x*** in posizione HIC **slot 1**) per determinare se si è pronti per collegare le porte host agli host dati:
      - *Se le nuove porte HIC dispongono del protocollo previsto*:

        Collegare le nuove porte HIC agli host dati; passare alla fase successiva.

- *Se le nuove porte HIC **non** hanno il protocollo previsto*:

  È necessario applicare un pacchetto di funzionalità software prima di poter collegare le nuove porte HIC agli host dati. Vedere "Modificare il protocollo host E5700". Quindi, collegare le porte host agli host dati e riprendere le operazioni.

6. Collegare i cavi dalle porte host del controller agli host dati.

   Per istruzioni sulla configurazione e l'utilizzo di un nuovo protocollo host, fare riferimento a. "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express".

Quali sono le prossime novità?

Il processo di aggiunta di una scheda di interfaccia host all'array di storage è completo. È possibile riprendere le normali operazioni.

Upgrade della scheda di interfaccia host (HIC) E5700

È possibile aggiornare una scheda di interfaccia host (HIC) in un array E5700 per aumentare il numero di porte host o modificare i protocolli host.

A proposito di questa attività

Quando si aggiorna l'HICS, è necessario spegnere lo storage array, rimuovere l'HIC esistente da ciascun controller, installare un nuovo HIC e riapplicare l'alimentazione.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E5700".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, questo perché entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).
- Assicurarsi di disporre di quanto segue:
  - Uno o due HICS, a seconda che si disponga di uno o due controller nell'array di storage. L'HICS deve essere compatibile con i controller.
  - Nuovo hardware host installato per le nuove porte host, ad esempio switch o HBA (host bus adapter).
  - Tutti i cavi, i ricetrasmettitori, gli switch e gli HBA (host bus adapter) necessari per collegare le nuove porte host.

    Per informazioni sull'hardware compatibile, fare riferimento a. "Matrice di interoperabilità NetApp" o il "NetApp Hardware Universe".

  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un cacciavite Phillips n. 1.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Preparazione all'aggiornamento di HICS

Preparare l'aggiornamento di un HIC eseguendo il backup del database di configurazione dello storage array, raccogliendo i dati di supporto e interrompendo le operazioni di i/o dell'host. Quindi, è possibile spegnere lo shelf del controller.

Fasi

1. Dalla home page di Gestore di sistema SANtricity, verificare che lo stato dello storage array sia ottimale.

   Se lo stato non è ottimale, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Non continuare con questa procedura.

2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.

   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

   Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:

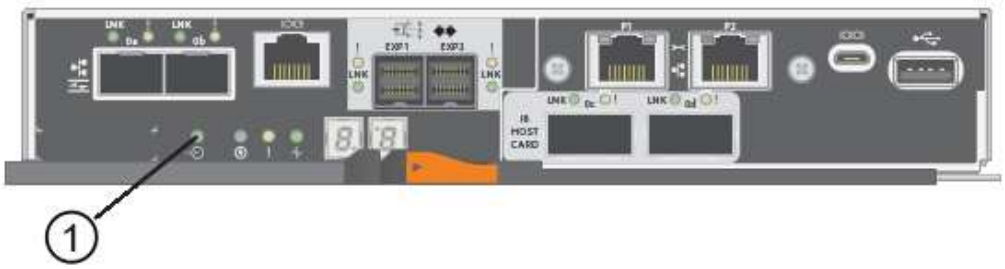
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull'array.

I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere l'accesso ai dati perché lo storage non è accessibile.

5. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
6. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



   (1) *LED cache attiva*

7. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.
8. Spegnere lo shelf del controller.
   a. Spegnere entrambi gli interruttori di alimentazione sullo shelf del controller.
   b. Attendere che tutti i LED sullo shelf del controller si spenga.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller per aggiornare il nuovo HIC.

Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

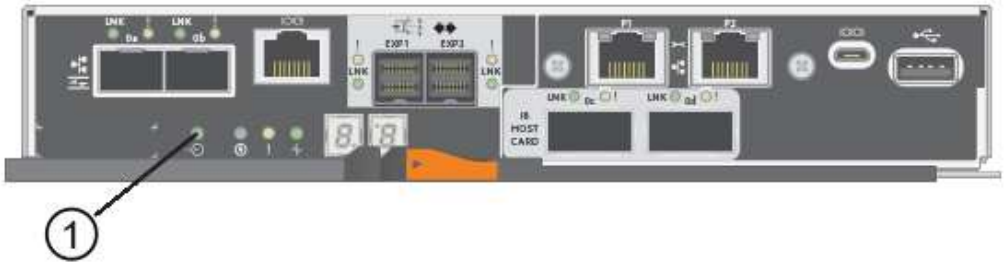
   Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Se le porte HIC utilizzano ricetrasmettitori SFP+, rimuoverli.

   A seconda del tipo di HIC a cui si esegue l'aggiornamento, potrebbe essere possibile riutilizzare questi SFP.

4. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

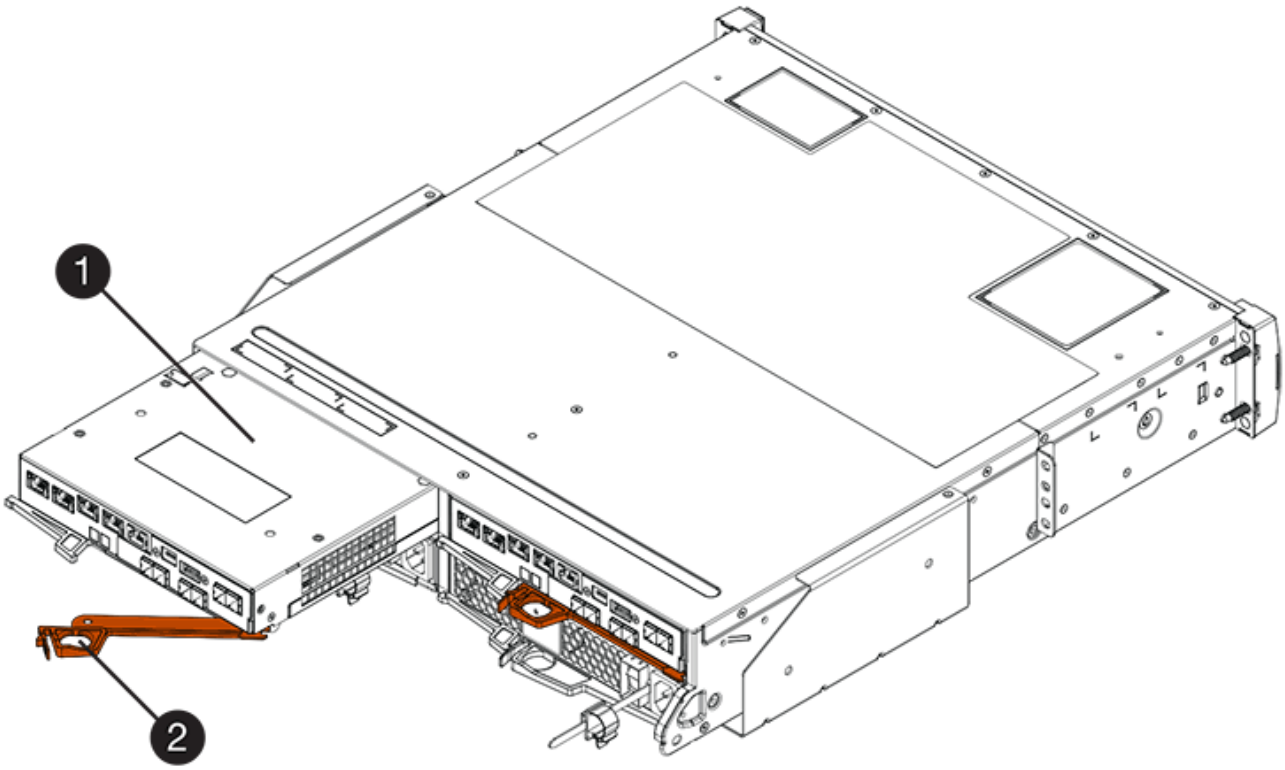
   Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



   (1) *LED cache attiva*

5. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

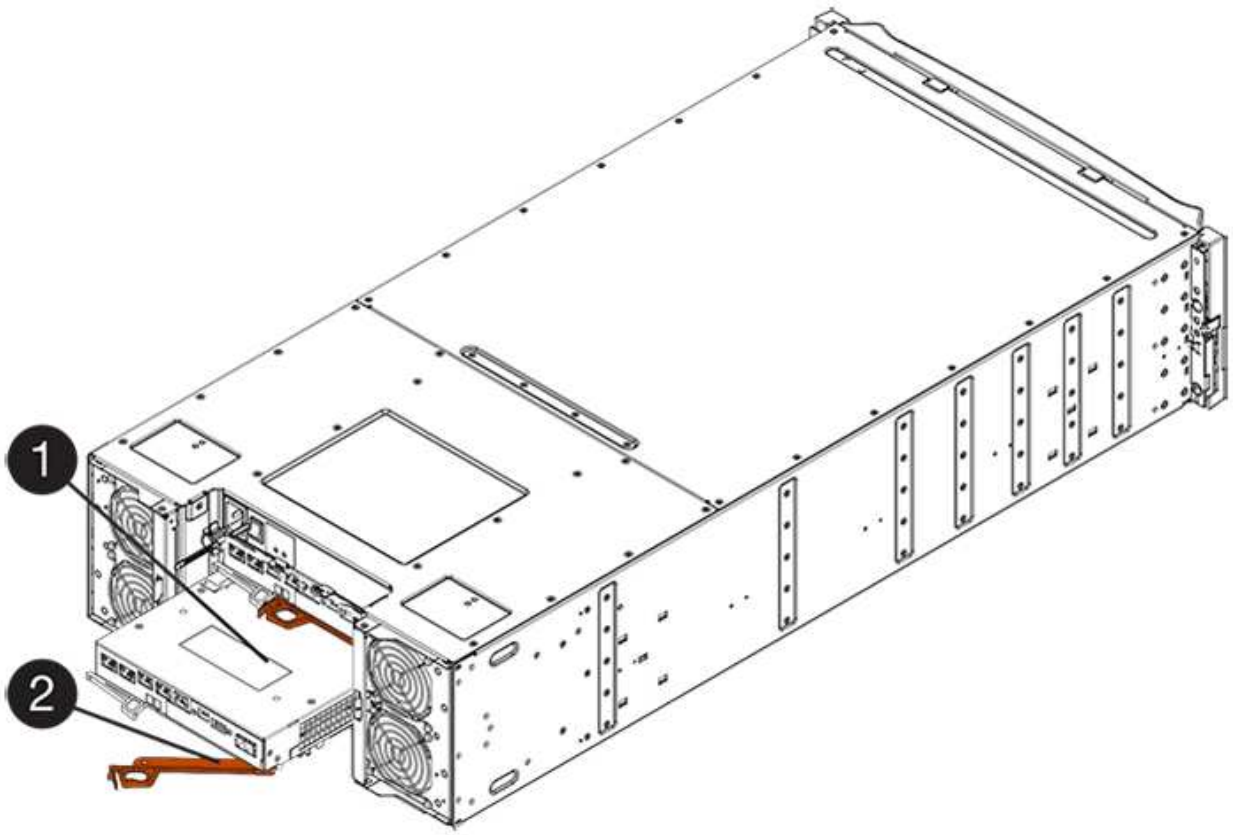
   La figura seguente è un esempio di shelf di controller E5724:



   (1) *contenitore controller*

   (2) *maniglia della camma*

   La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

6. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf del controller E5724, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

7. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
8. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Rimuovere un HIC

Rimuovere l'HIC originale in modo da poterlo sostituire con uno aggiornato.

Fasi

1. Rimuovere il coperchio del contenitore del controller premendo il pulsante e facendo scorrere il coperchio.
2. Verificare che il LED verde all'interno del controller (tra la batteria e i DIMM) sia spento.

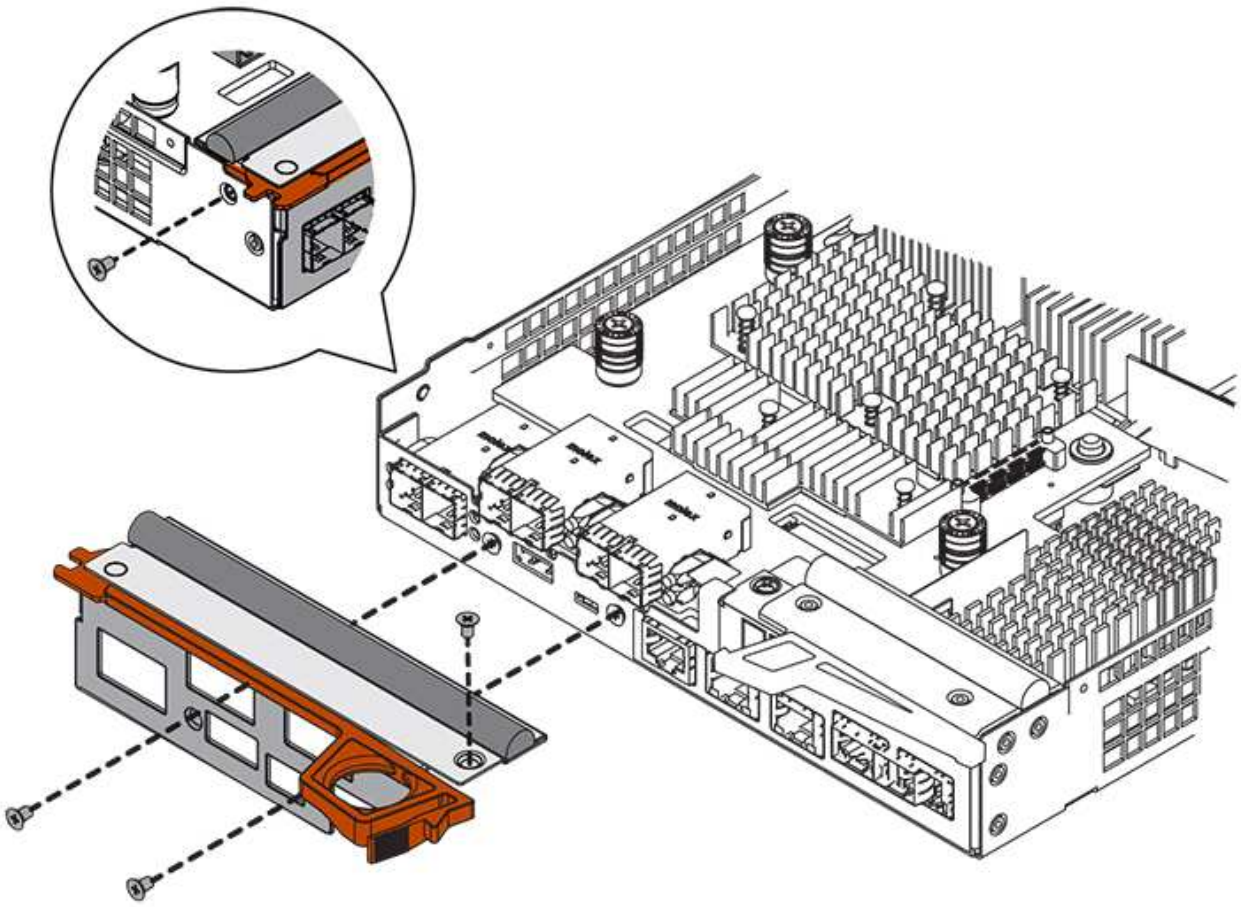
   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

(1) *LED cache attiva*

(2) *batteria*

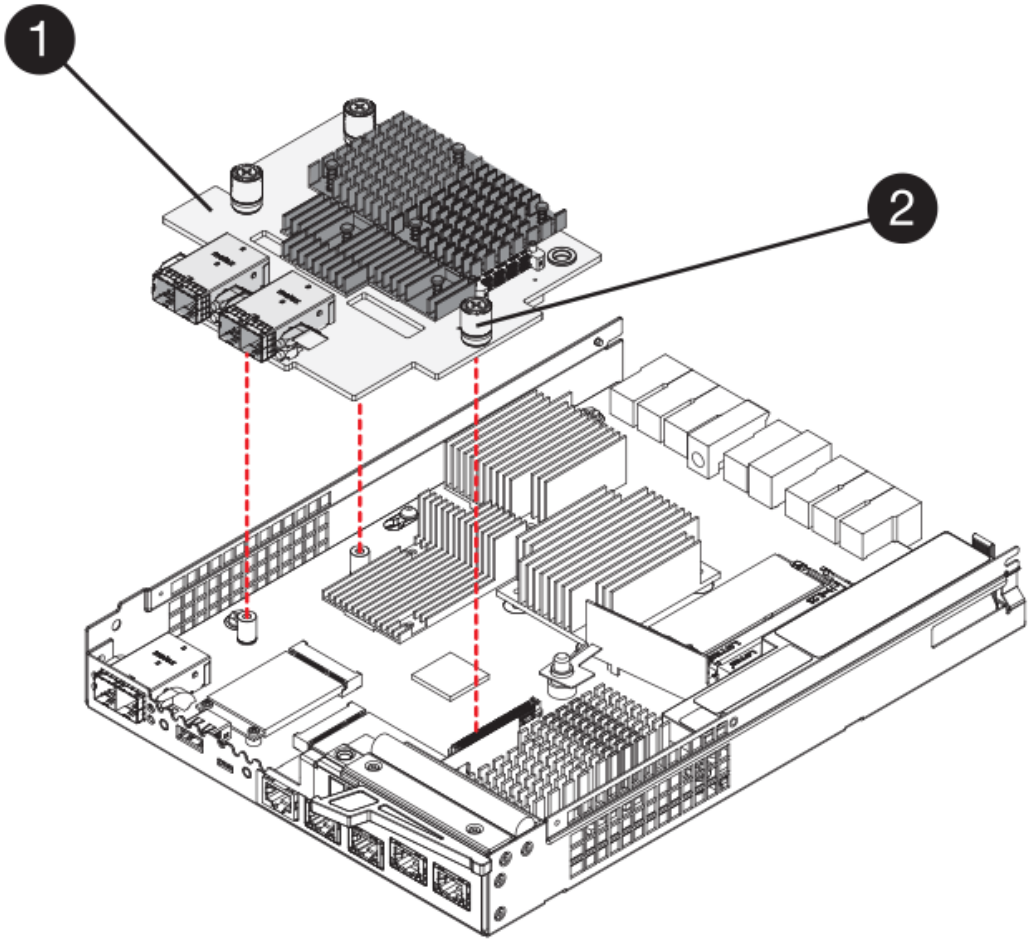
3. Utilizzando un cacciavite Phillips n. 1, rimuovere le viti che fissano la mascherina HIC al contenitore del controller.

   Sono presenti quattro viti: Una sulla parte superiore, una laterale e due sulla parte anteriore.



4. Rimuovere la piastra anteriore dell'HIC.
5. Utilizzando le dita o un cacciavite Phillips, allentare le tre viti a testa zigrinata che fissano l'HIC alla scheda del controller.
6. Scollegare con cautela l'HIC dalla scheda del controller sollevandola e facendola scorrere all'indietro.

> Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.



(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

7. Posizionare l'HIC su una superficie priva di elettricità statica.

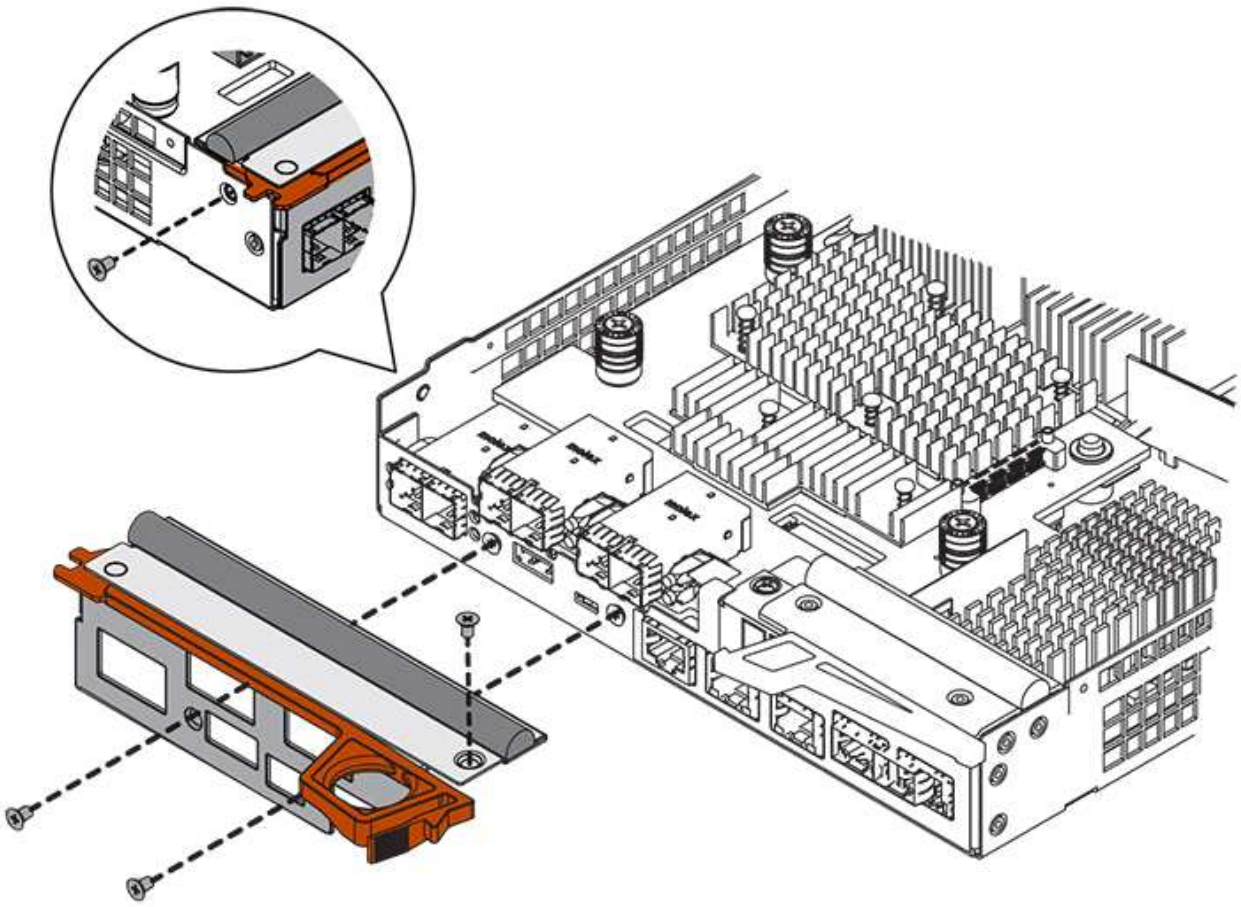
Fase 4: Installare il nuovo HIC

Installare il nuovo HIC host.

> **Possibile perdita di accesso ai dati** — non installare mai un HIC in un contenitore del controller E5700 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la piastra anteriore HIC al contenitore del controller, quindi rimuovere la piastra frontale.

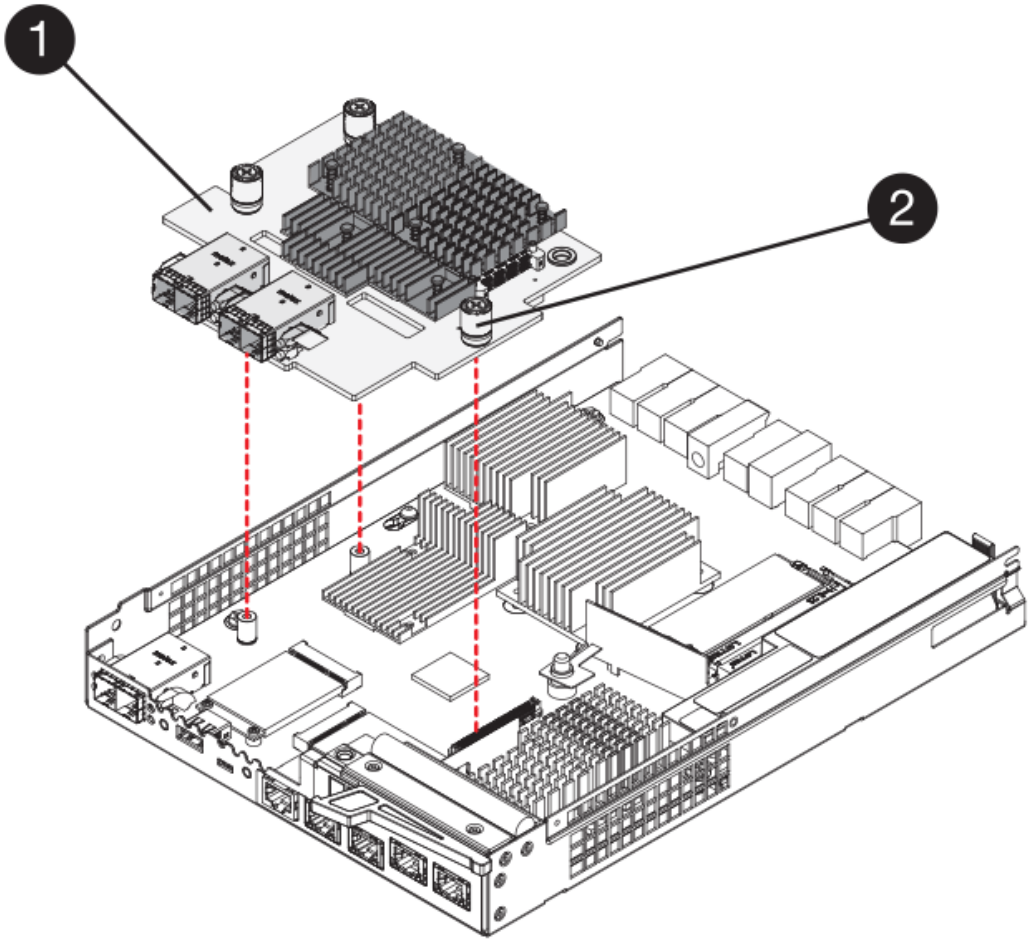


3. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

4. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

> **Possibili danni alle apparecchiature** — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



(1) *scheda di interfaccia host (HIC)*

(2) *viti a testa zigrinata*

5. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

6. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.

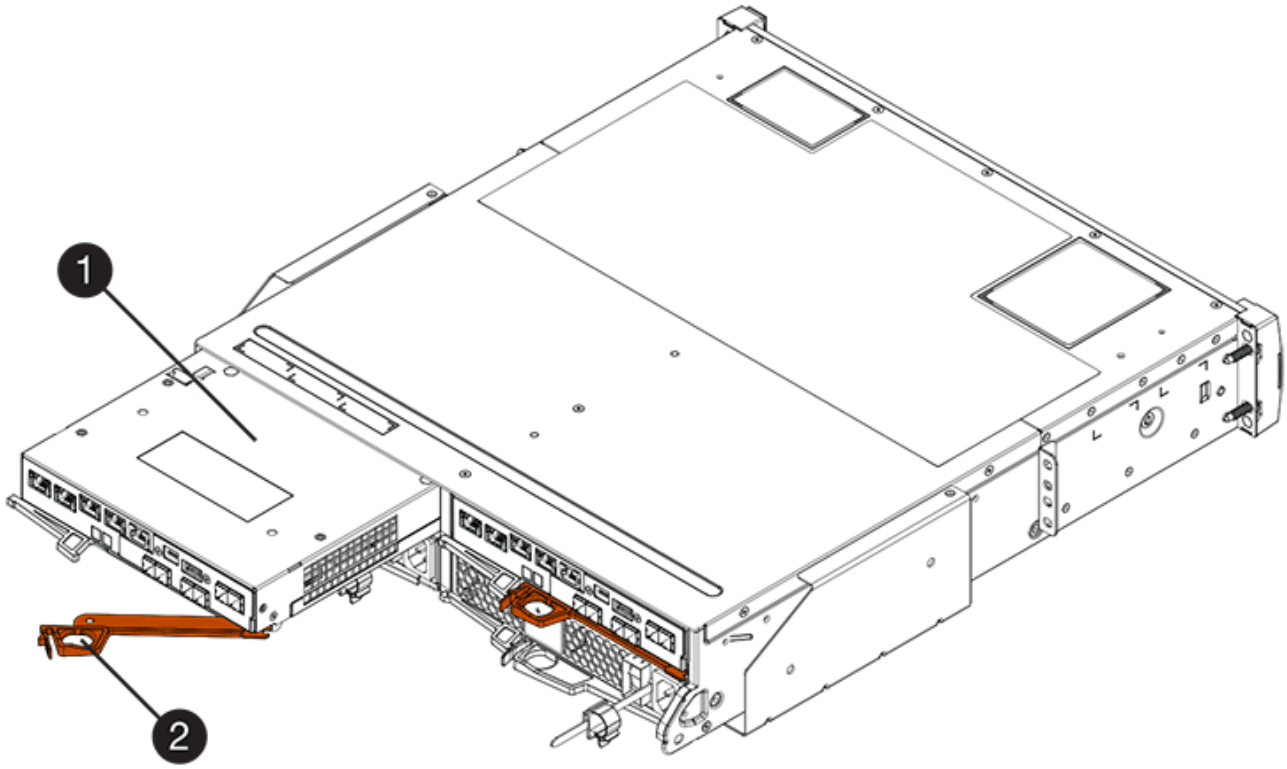
Fase 5: Reinstallare il contenitore del controller

Dopo aver installato il nuovo HIC, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Reinstallare il coperchio sul contenitore del controller facendo scorrere il coperchio dal retro verso la parte anteriore fino a quando il pulsante non scatta in posizione.
2. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
3. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

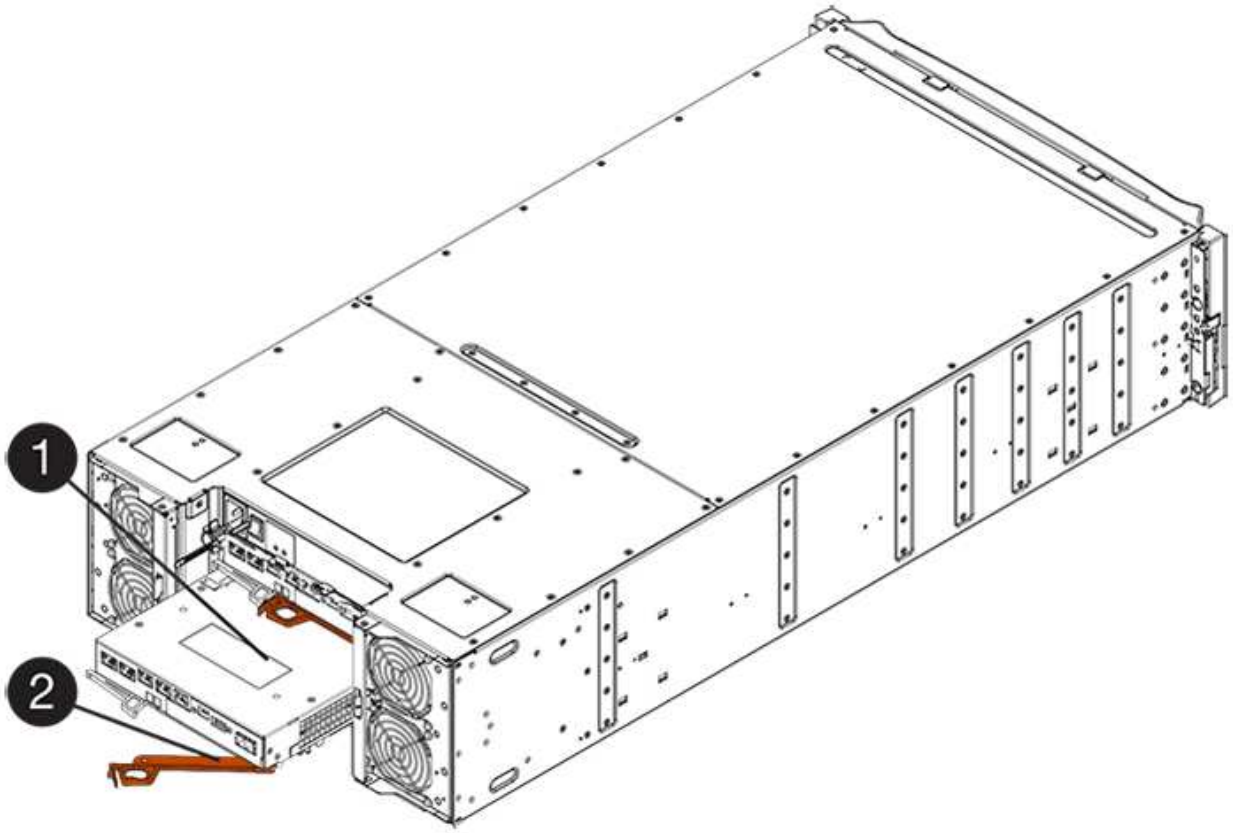
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

4. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
5. Ricollegare tutti i cavi rimossi.

> Non collegare i cavi dati alle nuove porte HIC in questo momento.

6. (Facoltativo) se si sta aggiornando HICS in una configurazione duplex, ripetere tutti i passaggi per rimuovere l'altro elemento filtrante del controller, rimuovere l'HIC, installare il nuovo HIC e sostituire il secondo elemento filtrante del controller.

Fase 6: Completare l'aggiornamento HIC

Controllare i LED del controller e il display a sette segmenti e verificare che lo stato del controller sia ottimale.

Fasi

1. Accendere i due interruttori di alimentazione sul retro dello shelf del controller.
   - Non spegnere gli interruttori di alimentazione durante il processo di accensione, che in genere richiede 90 secondi o meno.
   - Le ventole di ogni shelf sono molto rumorose al primo avvio. Il rumore forte durante l'avvio è normale.
2. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.
   - Il display a sette segmenti mostra la sequenza ripetuta **OS**, **SD**, ***blank*** per indicare che il controller sta eseguendo l'elaborazione SOD (Start-of-day). Una volta avviato correttamente un controller, il display a sette segmenti dovrebbe visualizzare l'ID del vassoio.

- Il LED di attenzione ambra sul controller si accende e poi si spegne, a meno che non si verifichi un errore.
- I LED verdi del collegamento host rimangono spenti fino a quando non si collegano i cavi host.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

(1) *LED link host (ambra)*

(2) *LED di attenzione (ambra)*

(3) *Display a sette segmenti*

3. Da Gestore di sistema di SANtricity, verificare che lo stato del controller sia ottimale.

   Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

   > Se non si riesce a risolvere il problema, contattare il supporto tecnico.

4. Se le nuove porte HIC richiedono ricetrasmettitori SFP+, installarli.
5. Collegare i cavi dalle porte host del controller agli host dati.

Quali sono le prossime novità?

Il processo di aggiornamento di una scheda di interfaccia host nell'array di storage è completo. È possibile riprendere le normali operazioni.

Sostituire la scheda di interfaccia host (HIC) E5700

È possibile sostituire una scheda di interfaccia host (HIC) guasta.

A proposito di questa attività

Quando si sostituisce un HIC, il controller viene scollegato (per le configurazioni duplex), viene rimosso il contenitore del controller, viene installato il nuovo HIC, quindi viene sostituito il contenitore del controller.

Prima di iniziare

- Revisione "Requisiti per la sostituzione HIC E5700".
- Pianificare una finestra di manutenzione dei tempi di inattività per questa procedura. Quando si installa

HICS, l'alimentazione deve essere spenta, in modo che non sia possibile accedere ai dati sullo storage array fino a quando non si è completata correttamente questa procedura. (In una configurazione duplex, entrambi i controller devono avere la stessa configurazione HIC quando vengono accesi).

- Verificare che non siano in uso volumi o che su tutti gli host che utilizzano questi volumi sia installato un driver multipath.
- Da Gestore di sistema di SANtricity, verificare i dettagli nel guru del ripristino per confermare che si è verificato un errore HIC e per assicurarsi che non siano necessari altri elementi prima di poter rimuovere e sostituire l'HIC.
- Assicurarsi di disporre di quanto segue:
  - Due HICS compatibili con i controller.

    Per le configurazioni duplex (due controller), l'HICS installato nei due contenitori del controller deve essere identico. La presenza di HICS non corrispondenti causa il blocco del controller con l'HIC sostitutivo quando lo si porta online.
  - Un braccialetto antistatico o sono state adottate altre precauzioni antistatiche.
  - Un cacciavite Phillips n. 1.
  - Etichette per identificare ciascun cavo collegato al contenitore del controller.
  - Stazione di gestione con un browser che può accedere a Gestione di sistema SANtricity per il controller. Per aprire l'interfaccia di System Manager, puntare il browser sul nome di dominio o sull'indirizzo IP del controller.

Fase 1: Posizionare il controller offline (duplex)

Se si dispone di una configurazione duplex, è necessario posizionare il controller interessato offline in modo da poter rimuovere in sicurezza l'HIC guasto.

Fasi

1. Dall'area Details (Dettagli) del Recovery Guru, determinare quale dei controller canister presenta l'HIC guasto.
2. Eseguire il backup del database di configurazione dello storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per ripristinare la configurazione. Il sistema salva lo stato corrente del database di configurazione RAID, che include tutti i dati per i gruppi di volumi e i pool di dischi sul controller.

   - Da System Manager:
     i. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
     ii. Selezionare **Collect Configuration Data** (raccolta dati di configurazione).
     iii. Fare clic su **Collect**.

     Il file viene salvato nella cartella Download del browser con il nome **configurationData-<arrayName>-<dateTime>.7z**.
   - In alternativa, è possibile eseguire il backup del database di configurazione utilizzando il seguente comando CLI:

     ```
     save storageArray dbmDatabase sourceLocation=onboard contentType=all
     file="filename";
     ```

3. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.

   Se si verifica un problema durante questa procedura, è possibile utilizzare il file salvato per risolvere il problema. Il sistema salva i dati di inventario, stato e performance relativi all'array di storage in un singolo file.

   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

4. Se il controller non è già offline, portalo offline usando Gestione di sistema di SANtricity.

   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf** per visualizzare i controller.
     iii. Selezionare il controller che si desidera mettere offline.
     iv. Dal menu di scelta rapida, selezionare **posiziona offline** e confermare che si desidera eseguire l'operazione.

     > Se si accede a Gestore di sistema di SANtricity utilizzando il controller che si sta tentando di mettere offline, viene visualizzato il messaggio Gestione di sistema di SANtricity non disponibile. Selezionare **connessione a una connessione di rete alternativa** per accedere automaticamente a Gestione di sistema SANtricity utilizzando l'altro controller.

   - In alternativa, è possibile disattivare i controller utilizzando i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=offline`

   Per il controller B: `set controller [b] availability=offline`

5. Attendere che Gestore di sistema di SANtricity aggiorni lo stato del controller su offline.

   > Non iniziare altre operazioni fino a quando lo stato non è stato aggiornato.

Fase 2: Rimuovere il contenitore del controller

Rimuovere il contenitore del controller in modo da poter aggiungere il nuovo HIC.

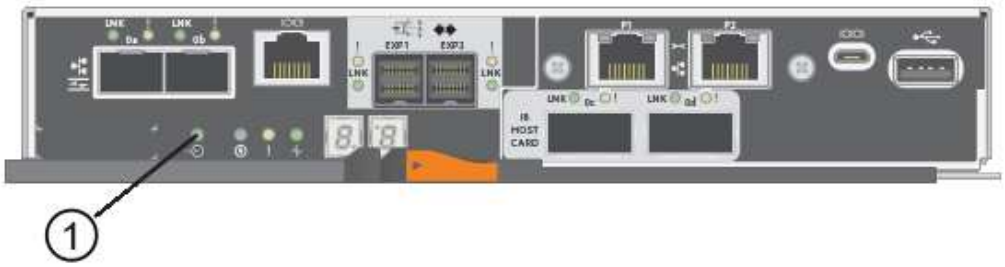
Fasi

1. Etichettare ciascun cavo collegato al contenitore del controller.
2. Scollegare tutti i cavi dal contenitore del controller.

   > Per evitare prestazioni degradate, non attorcigliare, piegare, pizzicare o salire sui cavi.

3. Verificare che il LED cache Active (cache attiva) sul retro del controller sia spento.

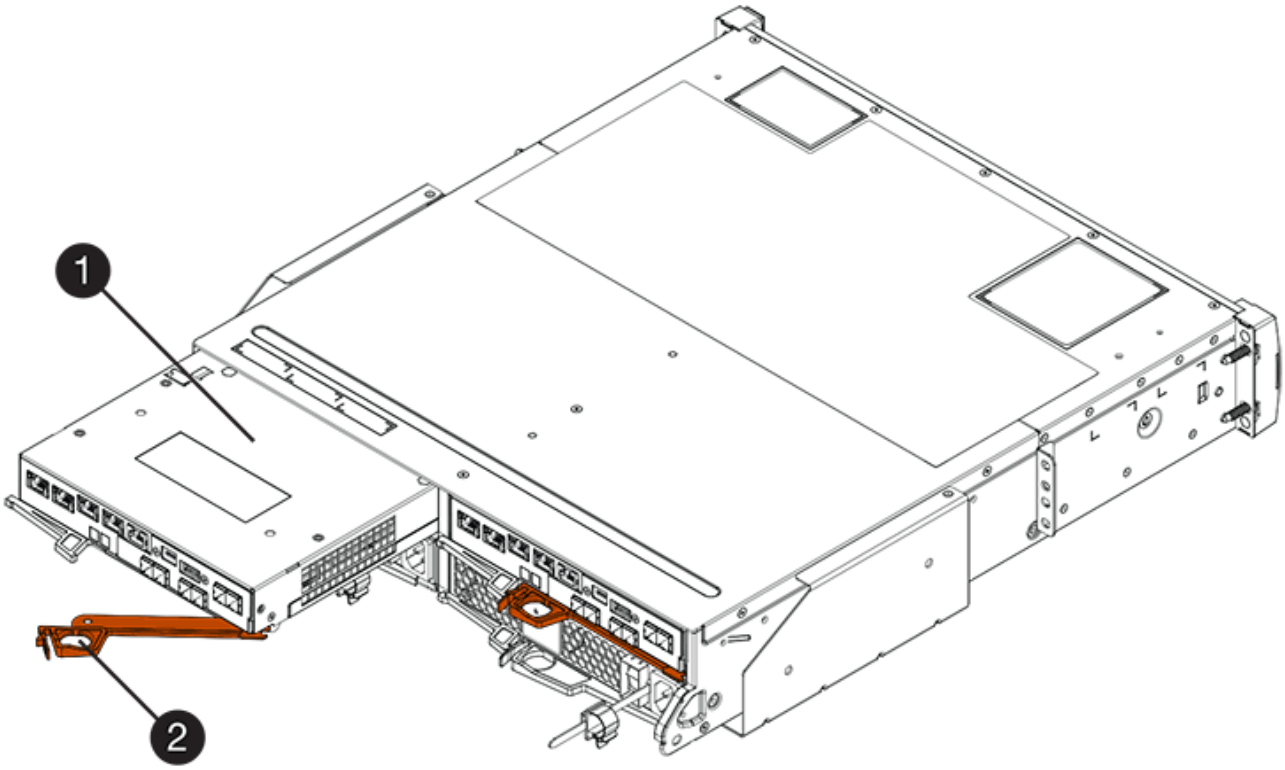
Il LED verde cache Active (cache attiva) sul retro del controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di rimuovere il contenitore del controller, è necessario attendere che questo LED si spenga.



(1) *LED cache attiva*

4. Premere il fermo sull'impugnatura della camma fino a quando non si rilascia, quindi aprire l'impugnatura della camma a destra per rilasciare l'elemento filtrante del controller dallo scaffale.

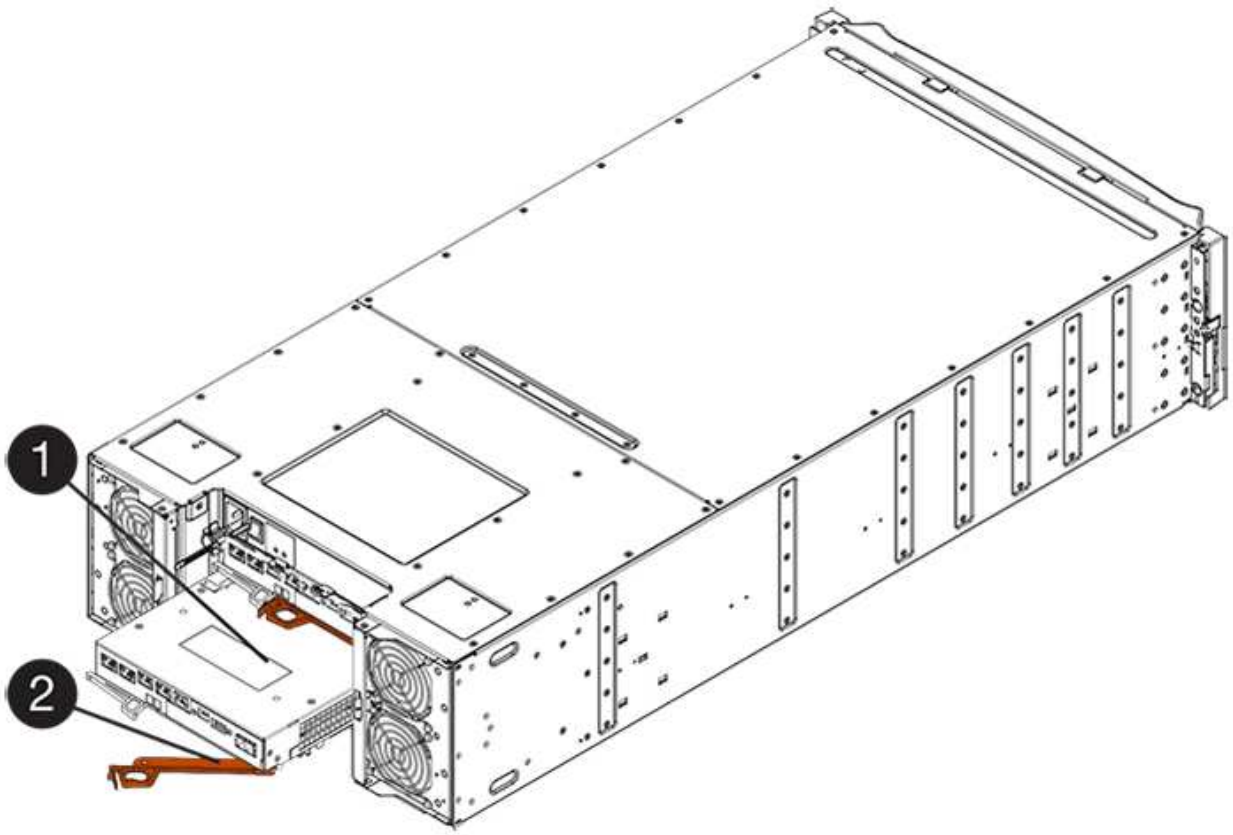
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

5. Utilizzando due mani e l'impugnatura della camma, estrarre il contenitore del controller dallo scaffale.

   Utilizzare sempre due mani per sostenere il peso di un contenitore del controller.

   Se si rimuove il contenitore del controller da uno shelf del controller E5724, un'aletta si sposta in posizione per bloccare l'alloggiamento vuoto, contribuendo a mantenere il flusso d'aria e il raffreddamento.

6. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso l'alto.
7. Posizionare il contenitore del controller su una superficie piana e priva di elettricità statica.

Fase 3: Installare un HIC

Installare un nuovo HIC per sostituire quello guasto.

Possibile perdita di accesso ai dati — non installare mai un HIC in un contenitore del controller E5700 se tale HIC è stato progettato per un altro controller e-Series. Inoltre, se si dispone di una configurazione duplex, entrambi i controller e gli HICS devono essere identici. La presenza di HICS incompatibili o non corrispondenti causa il blocco dei controller quando si applica l'alimentazione.

Fasi

1. Disimballare il nuovo HIC e la nuova mascherina HIC.
2. Premere il pulsante sul coperchio del contenitore del controller ed estrarre il coperchio.

3. Verificare che il LED verde all'interno del controller (accanto ai DIMM) sia spento.

   Se questo LED verde è acceso, il controller sta ancora utilizzando l'alimentazione a batteria. Prima di rimuovere qualsiasi componente, è necessario attendere che il LED si spenga.

   (1) *LED cache interna attiva*

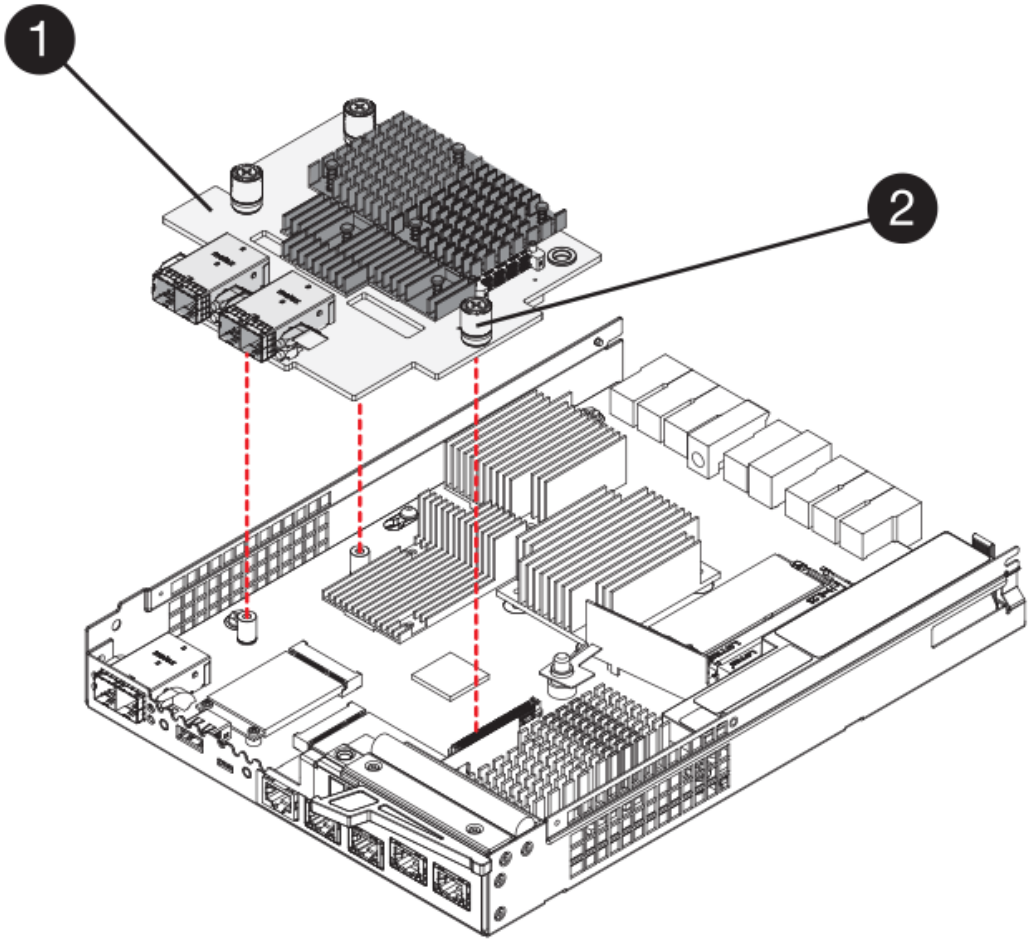
   (2) *batteria*

4. Utilizzando un cacciavite Phillips n. 1, rimuovere le quattro viti che fissano la mascherina vuota al contenitore del controller, quindi rimuovere la piastra frontale.
5. Allineare le tre viti a testa zigrinata sull'HIC con i fori corrispondenti sul controller e allineare il connettore sulla parte inferiore dell'HIC con il connettore di interfaccia HIC sulla scheda del controller.

   Fare attenzione a non graffiare o urtare i componenti sul fondo dell'HIC o sulla parte superiore della scheda del controller.

6. Abbassare con cautela l'HIC in posizione e inserire il connettore HIC premendo delicatamente sull'HIC.

   Possibili danni alle apparecchiature — fare molta attenzione a non stringere il connettore a nastro dorato dei LED del controller tra l'HIC e le viti a testa zigrinata.



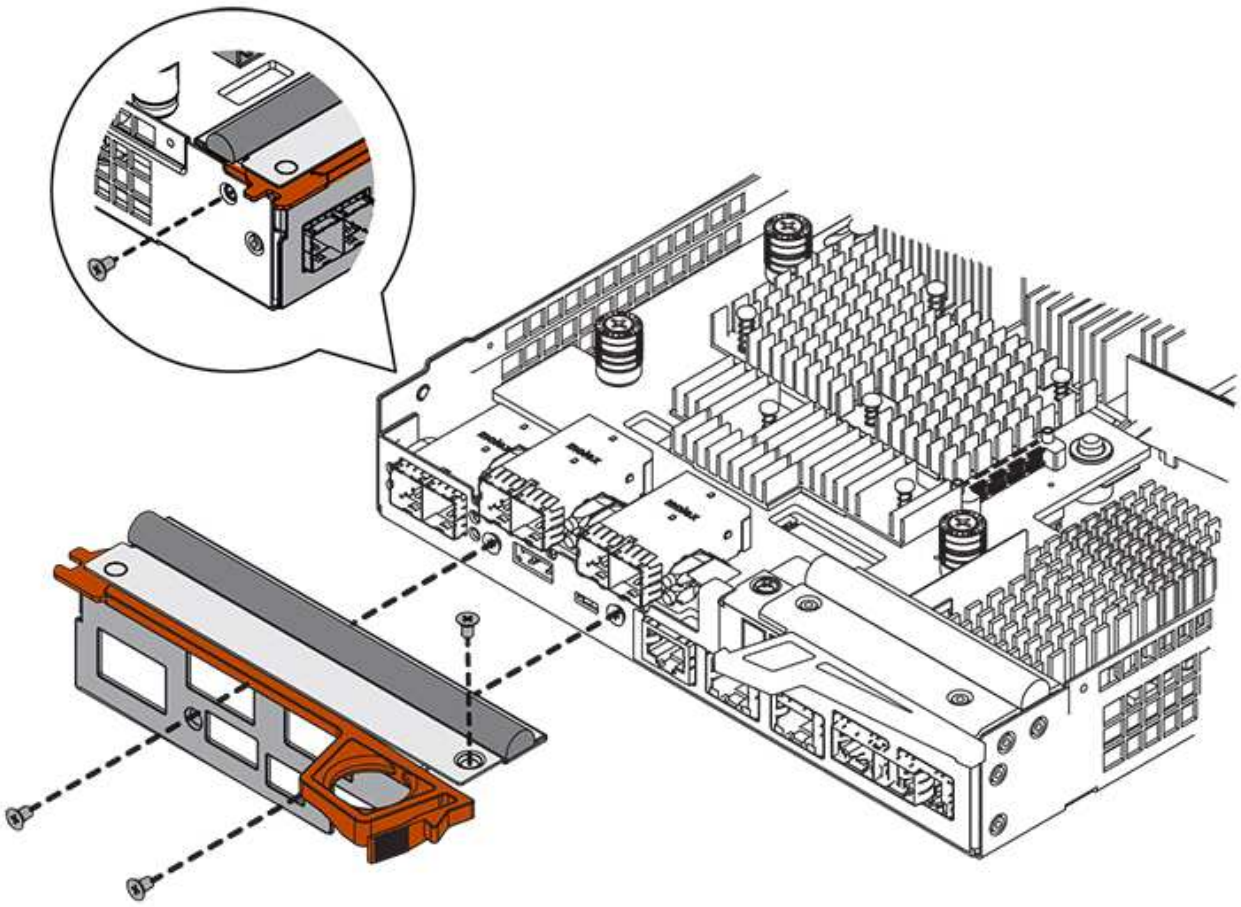
(1) *scheda di interfaccia host*

(2) *viti a testa zigrinata*

7. Serrare manualmente le viti a testa zigrinata HIC.

   Non utilizzare un cacciavite per evitare di serrare eccessivamente le viti.

8. Utilizzando un cacciavite Phillips n. 1, fissare la nuova piastra anteriore HIC al contenitore del controller con le quattro viti rimosse in precedenza.



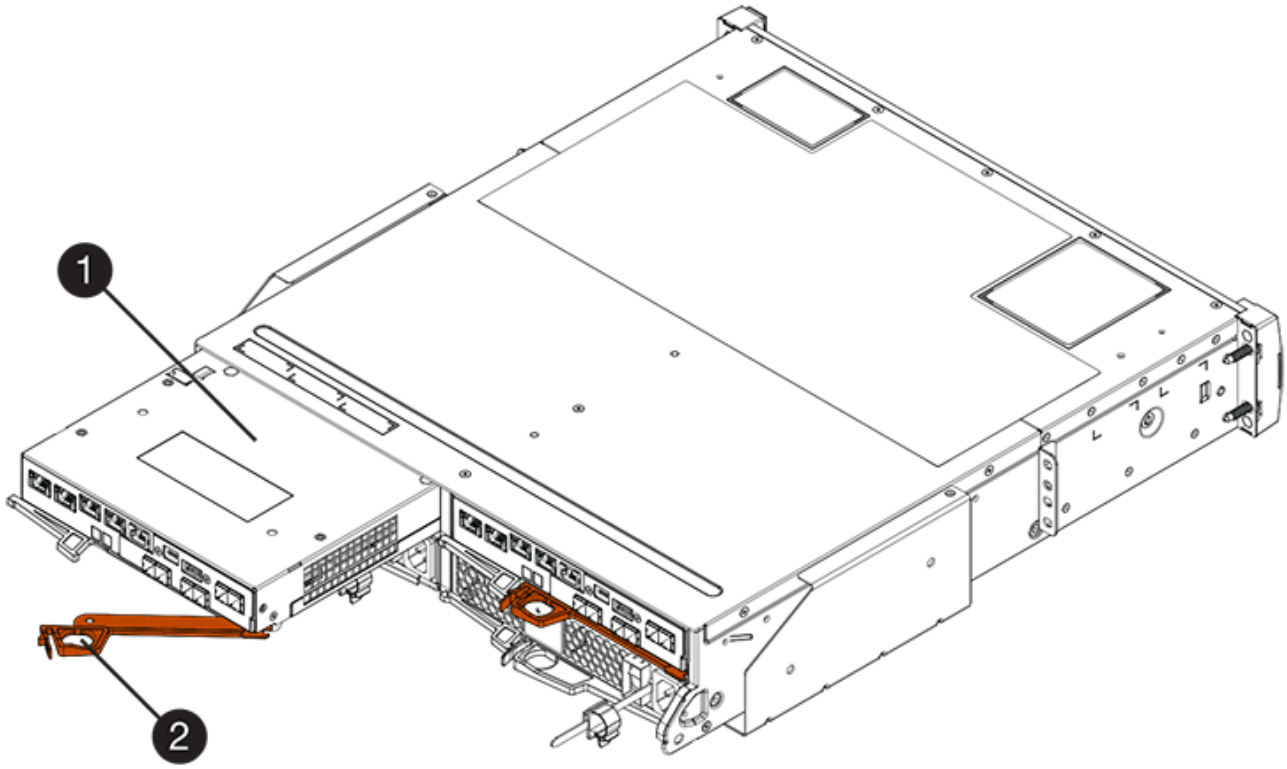
Fase 4: Reinstallare il contenitore del controller

Dopo aver installato l'HIC, reinstallare il contenitore del controller nello shelf del controller.

Fasi

1. Capovolgere il contenitore del controller, in modo che il coperchio rimovibile sia rivolto verso il basso.
2. Con la maniglia della camma in posizione aperta, far scorrere il contenitore del controller fino in fondo nello shelf del controller.

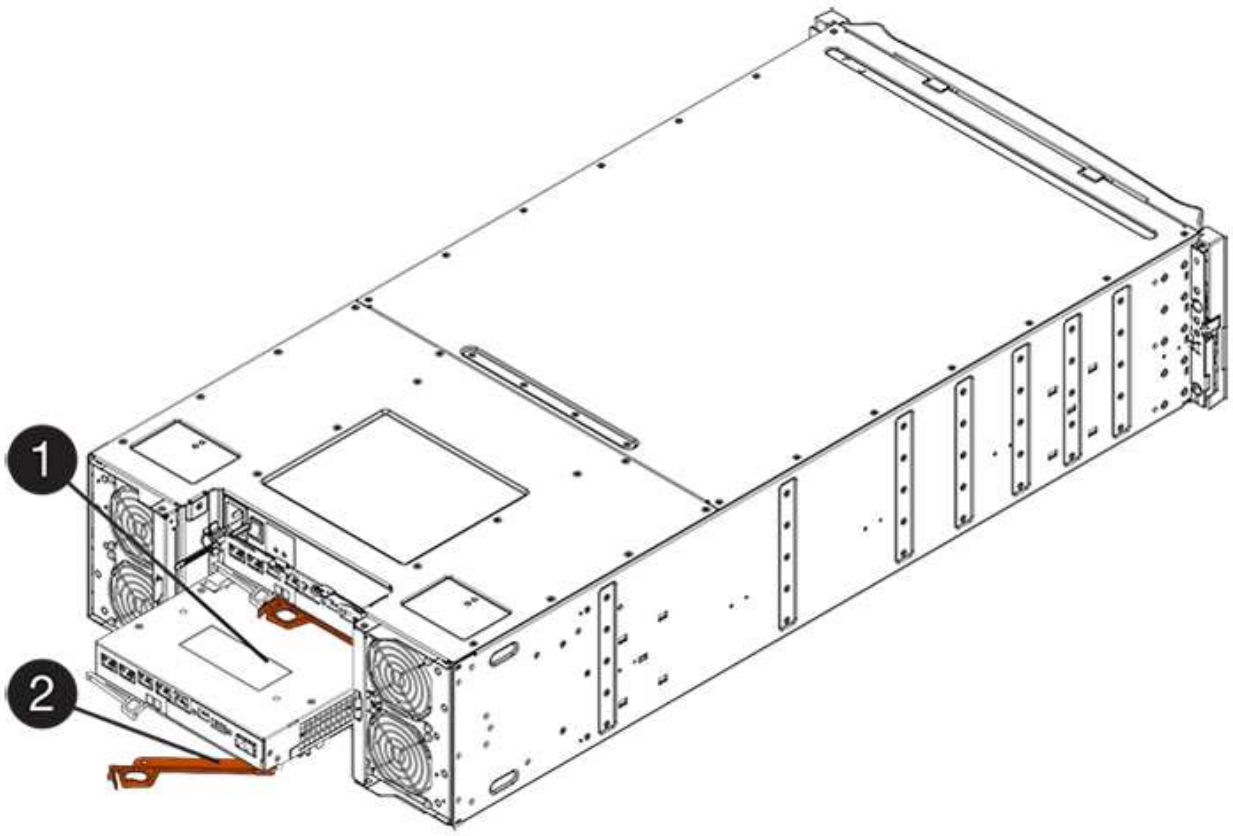
   La figura seguente è un esempio di shelf di controller E5724:



(1) *contenitore controller*

(2) *maniglia della camma*

La figura seguente è un esempio di shelf di controller E5760:



(1) *contenitore controller*

(2) *maniglia della camma*

3. Spostare la maniglia della camma verso sinistra per bloccare il contenitore del controller in posizione.
4. Ricollegare tutti i cavi rimossi.

> Non collegare i cavi dati alle nuove porte HIC in questo momento.

5. (Facoltativo) se si aggiunge HICS a una configurazione duplex, ripetere tutti i passaggi per rimuovere il secondo elemento filtrante del controller, installare il secondo HIC e reinstallare il secondo elemento filtrante del controller.

Fase 5: Posizionamento del controller online (duplex)

Se si dispone di una configurazione duplex, portare il controller online per verificare che lo storage array funzioni correttamente, raccogliere i dati di supporto e riprendere le operazioni.

> Eseguire questa operazione solo se lo storage array dispone di due controller.

Fasi

1. All'avvio del controller, controllare i LED del controller e il display a sette segmenti.

> La figura mostra un esempio di contenitore del controller. Il controller potrebbe avere un numero diverso e un tipo diverso di porte host.

Quando la comunicazione con l'altro controller viene ristabilita:

- Il display a sette segmenti mostra la sequenza ripetuta **OS**, **OL**, ***blank*** per indicare che il controller è offline.
- Il LED di attenzione di colore ambra rimane acceso.
- I LED del collegamento host potrebbero essere accesi, lampeggianti o spenti, a seconda dell'interfaccia
  host.

(1) *LED link host*

(2) *LED di attenzione (ambra)*

(3) *Display a sette segmenti*

2. Portare il controller online utilizzando Gestione di sistema di SANtricity.
   - Da Gestore di sistema di SANtricity:
     i. Selezionare **hardware**.
     ii. Se la figura mostra i dischi, selezionare **Mostra retro dello shelf**.
     iii. Selezionare il controller che si desidera mettere in linea.
     iv. Selezionare **Place Online** (Esegui online) dal menu di scelta rapida e confermare che si desidera eseguire l'operazione.

     Il sistema mette il controller in linea.
   - In alternativa, è possibile utilizzare i seguenti comandi CLI:

     Per il controller A: `set controller [a] availability=online;`

   Per il controller B: `set controller [b] availability=online;`

3. Controllare i codici sul display a sette segmenti del controller quando torna online. Se sul display viene visualizzata una delle seguenti sequenze di ripetizione, rimuovere immediatamente il controller.
   - **OE**, **L0**, ***blank*** (controller non corrispondenti)
   - **OE**, **L6**, ***blank*** (HIC non supportato) **attenzione: possibile perdita di accesso ai dati** — se il controller appena installato mostra uno di questi codici e l'altro controller viene ripristinato per qualsiasi motivo, anche il secondo controller potrebbe bloccarsi.
4. Quando il controller torna in linea, verificare che lo stato sia ottimale e controllare i LED di attenzione dello shelf di controller.

Se lo stato non è ottimale o se uno dei LED attenzione è acceso, verificare che tutti i cavi siano inseriti correttamente e che l'HIC e il contenitore del controller siano installati correttamente. Se necessario, rimuovere e reinstallare il contenitore del controller e l'HIC.

> Se non si riesce a risolvere il problema, contattare il supporto tecnico.

5. Raccogliere i dati di supporto per lo storage array utilizzando Gestione di sistema di SANtricity.
   a. Selezionare **Support › Support Center › Diagnostics** (supporto tecnico > Diagnostica).
   b. Selezionare **Collect Support Data**.
   c. Fare clic su **Collect**.

      Il file viene salvato nella cartella Download del browser con il nome **support-data.7z**.

6. Restituire la parte guasta a NetApp, come descritto nelle istruzioni RMA fornite con il kit.

   Contattare il supporto tecnico all'indirizzo "Supporto NetApp", 888-463-8277 (Nord America), 00-800-44-638277 (Europa) o +800-800-80-800 (Asia/Pacifico) se è necessario il numero RMA.

Quali sono le prossime novità?

La sostituzione dell'HIC è completata. È possibile riprendere le normali operazioni.

Protocollo della porta host

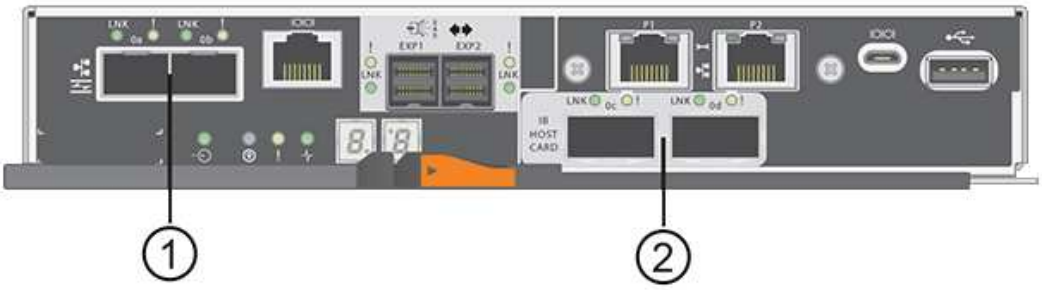
Requisiti per la modifica del protocollo della porta host E5700

Prima di convertire il protocollo della porta host in E5700, esaminare i requisiti.

Porte host modificabili

> È possibile convertire solo le porte della base ottica di un controller E5700.

La figura seguente mostra l'E5700 con le porte host SFP+ (ottiche) della scheda base **(1)** e le due porte IB HIC opzionali **(2)**.



Requisiti

- È necessario pianificare una finestra di manutenzione dei tempi di inattività per questa procedura.

- Quando si esegue la conversione, è necessario interrompere le operazioni di i/o dell'host e non sarà possibile accedere ai dati sull'array di storage fino a quando la conversione non sarà stata completata correttamente.
- È necessario utilizzare la gestione out-of-band. Non è possibile utilizzare la gestione in-band per completare questa procedura.
- Hai ottenuto l'hardware necessario per la conversione. Il tuo rappresentante commerciale NetApp può aiutarti a determinare l'hardware di cui hai bisogno e a ordinare le parti corrette.
- Se si tenta di modificare le porte host della scheda base dell'array di storage e attualmente si utilizzano ricetrasmettitori SFP a doppio protocollo (denominati anche *unificati*) acquistati da NetApp, non è necessario cambiare i ricetrasmettitori SFP.
- Assicurarsi che i ricetrasmettitori SFP a doppio protocollo supportino sia FC (a 4 Gbps o 16 Gbps) che iSCSI (a 10 Gbps), ma non supportano iSCSI a 1 Gbps. Vedere "Fase 1: Determinare se si dispone di SFP a doppio protocollo" Per determinare il tipo di ricetrasmettitori SFP installati.

Considerazioni per la modifica del protocollo host

Le considerazioni per la modifica del protocollo host dipendono dai protocolli iniziali e finali delle porte host della scheda base e delle porte HIC.

Se si utilizza una funzione di mirroring o la funzione Data Assurance (da), è necessario comprendere cosa accade a queste funzioni quando si modifica il protocollo della porta host.

> Le seguenti considerazioni si applicano solo se si sta convertendo un array di storage già in uso. Queste considerazioni non si applicano se si sta convertendo un nuovo array di storage che non ha ancora host e volumi definiti.

Conversione da FC a iSCSI

- Il mirroring asincrono richiede che sia lo storage array locale che quello remoto utilizzino lo stesso protocollo.
  - Se si utilizza attualmente il mirroring asincrono tramite la scheda base, è necessario disattivare le relazioni di mirroring asincrono utilizzando tali porte prima di applicare il Feature Pack.
  - Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per eliminare tutti i gruppi di coerenza dei mirror e rimuovere tutte le coppie mirrorate dagli array di storage locali e remoti. Inoltre, seguire le istruzioni della guida in linea per disattivare il mirroring asincrono.

> Se la configurazione contiene host DI avvio SAN collegati alle porte della scheda base FC, controllare "Matrice di interoperabilità NetApp" Per garantire che la configurazione sia supportata su iSCSI. In caso contrario, non è possibile convertire il protocollo host in iSCSI.

- La funzione di mirroring sincrono non è supportata per iSCSI.
  - Se si utilizzano attualmente relazioni di mirroring sincrono tramite le porte baseboard, è necessario disattivare tali relazioni di mirroring sincrono.
  - Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per rimuovere tutte le coppie di mirroring sincrono, che rimuove le relazioni di mirroring sull'array di storage locale e sull'array di storage remoto. Inoltre, seguire le istruzioni della guida in linea per disattivare Synchronous Mirroring.

> Se non si disattivano le relazioni di mirroring sincrono prima della conversione in iSCSI, il sistema perde l'accesso ai dati e potrebbe verificarsi una perdita di dati.

Conversione da iSCSI a FC

- Il mirroring asincrono richiede che sia lo storage array locale che quello remoto utilizzino lo stesso protocollo. Se si utilizza attualmente il mirroring asincrono con le porte della scheda base, è necessario disattivare il mirroring asincrono prima di modificare il protocollo.
- Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per eliminare tutti i gruppi di coerenza dei mirror e rimuovere tutte le coppie mirrorate dagli array di storage locali e remoti. Inoltre, seguire le istruzioni della guida in linea per disattivare il mirroring asincrono.

Conversione di IB-iSER in/da IB-SRP

- Non è necessario apportare modifiche all'hardware quando si effettua la conversione da/a iSER in SRP.
- La funzione Data Assurance (da) non è supportata per SRP.
- La funzione da non è supportata per IB-SRP. Se si utilizza questa funzione tramite IB-HIC e si desidera convertire tali porte da iSER a SRP, è necessario disattivare in modo permanente da su tutti i volumi. Fare riferimento alla guida in linea di Gestore di sistema di SANtricity per modificare le impostazioni di un volume per disattivare in modo permanente l'impostazione di data assurance.

  > Una volta disattivato, il da non può essere riattivato sul volume.

- Confermare quanto segue:
  - È possibile accedere a Gestore di sistema di SANtricity tramite un browser Web.
  - Il sistema storage esegue SANtricity OS (firmware del controller) versione 08.40.11.00 o successiva.

Le operazioni di mirroring richiedono lo stesso protocollo host

Le operazioni di mirroring non vengono influenzate se le porte host utilizzate per il mirroring mantengono lo stesso protocollo dopo l'applicazione del Feature Pack. Tuttavia, prima di applicare il Feature Pack, è necessario verificare che tutti i gruppi di coerenza mirror siano sincronizzati. Dopo aver applicato il Feature Pack, è necessario verificare la comunicazione tra lo storage array locale e lo storage array remoto. In caso di domande su come eseguire questa operazione, consultare la guida in linea di Gestore di sistema di SANtricity.

> Il mirroring asincrono e sincrono non è supportato per NVMe su fabric. Per disattivare il mirroring asincrono e sincrono, è possibile utilizzare `disable storageArray feature=asyncMirror` oppure `disable storageArray feature=syncMirror` comandi tramite l'interfaccia della riga di comando. Fare riferimento a. "Disattivare la funzione di array di storage" Comandi di mirroring nella Guida in linea di riferimento ai comandi CLI per ulteriori informazioni su come disattivare il mirroring.

Modificare il protocollo host E5700

Per un array di storage E5700, è possibile convertire le porte host della scheda base come segue:

- Da Fibre Channel (FC) a iSCSI
- Da iSCSI a FC

- Da IB a InfiniBand
- Da SRP a IB
- Da NVMe a IB
- Da NVMe a RoCE

Fase 1: Determinare se si dispone di SFP a doppio protocollo

Utilizzare Gestore di sistema SANtricity per determinare il tipo di ricetrasmettitori SFP in uso. Poiché questi SFP possono essere utilizzati con protocolli FC e iSCSI, vengono definiti come *dual-Protocol* o *Unified* SFP.

Se gli SFP attuali supportano velocità di trasferimento dati di 16 Gbps e 10 Gbps, è possibile continuare a utilizzarli dopo la conversione del protocollo della porta host.

Fasi

1. Da Gestore di sistema di SANtricity, selezionare **supporto**.
2. Selezionare il riquadro **Support Center**.
3. Nella scheda Support Resources (risorse di supporto), individuare e selezionare il collegamento **Storage Array Profile** (Profilo array di storage).
4. Digitare **SFP** nella casella di testo e fare clic su **Find** (trova).
5. Per ogni SFP elencato nel profilo dell'array di storage, individuare la voce **velocità dati supportata**.

```
SFP status:                Optimal
Attached to:               Host-side of controller B
Location:                  Unknown
Supported data rate(s):    16 Gbps, 10 Gbps, 8 Gbps, 4 Gbps
Link length:               Short
Connector:                 LC
Transmitter type:          Shortwave Laser w/o OFC
Transmission media:        TM Multi-mode 62.5m(M6)
IEEE company ID:           00 17 6a
Revision:                  Not Available
Part number:               AFBR-57F5UMZ
Serial number:             AA1317J14X7
Vendor:                    AVAGO
Date of manufacture:       4/28/13
```

6. Fare riferimento alla tabella per determinare se è possibile riutilizzare gli SFP, come indicato di seguito:

Velocità di trasferimento dati supportata	Tipo di SFP	Protocollo supportato
16 Gbps, 10 Gbps, 4 Gbps	Protocollo doppio	• **FC:** 16 Gbps, 4 Gbps • **ISCSI:**10 Gbps
10 Gbps	10 Gbps	Solo iSCSI
16 Gbps, 8 Gbps, 4 Gbps	16 Gbps	Solo FC

- Se si dispone di SFP a doppio protocollo, è possibile continuare a utilizzarli dopo aver convertito il protocollo.

> Gli SFP a doppio protocollo non supportano iSCSI da 1 GB. Se si stanno convertendo le porte host in iSCSI, tenere presente che gli SFP a doppio protocollo supportano solo un collegamento da 10 GB alla porta connessa.

- Se si utilizzano SFP a 16 Gbps e si stanno convertendo le porte host in iSCSI, è necessario rimuovere gli SFP e sostituirli con SFP a doppio protocollo o a 10 Gbps dopo la conversione del protocollo. In base alle esigenze, è anche possibile utilizzare il rame iSCSI a 10 Gbps utilizzando uno speciale cavo Twin-Ax con SFP.

> Gli SFP FC a 8 Gbps NON sono supportati nei controller E28xx o E57xx. Sono supportati SOLO SFP FC a 16 Gbps e 32 Gbps.

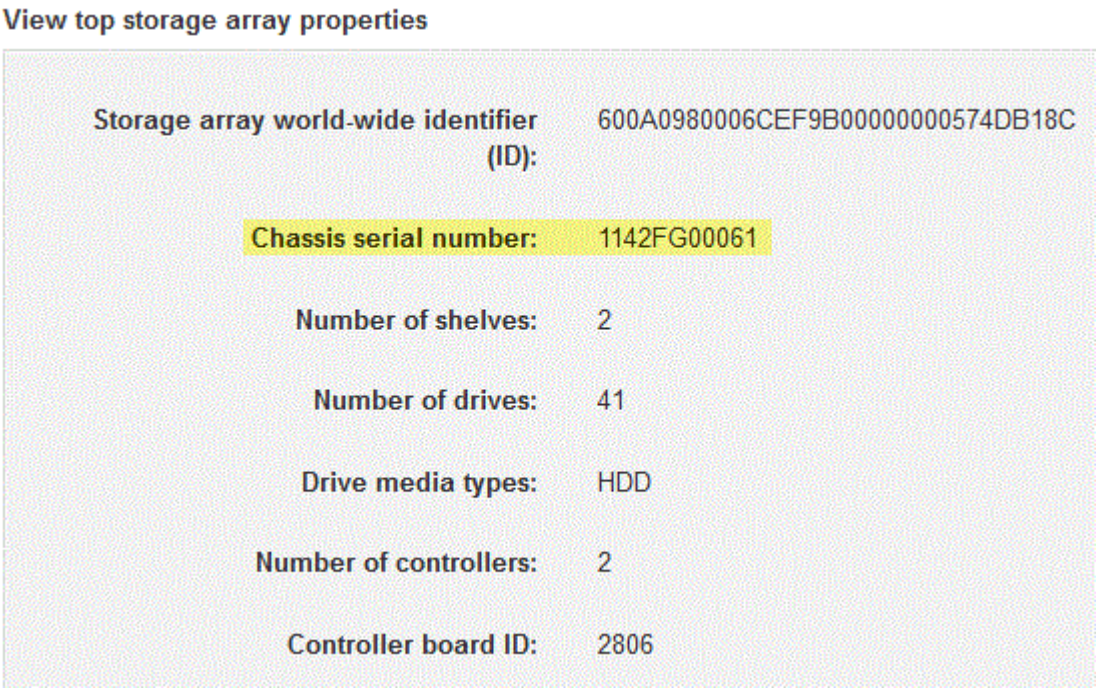
- Se si utilizzano SFP a 10 Gbps e si stanno convertendo le porte host in FC, è necessario rimuovere gli SFP da queste porte e sostituirli con SFP a doppio protocollo o a 16 Gbps dopo aver convertito il protocollo.

Fase 2: Ottenere il Feature Pack

Per ottenere il Feature Pack, è necessario il numero di serie dallo shelf del controller, un codice di attivazione delle funzioni e l'identificatore di abilitazione delle funzioni per lo storage array.

Fasi

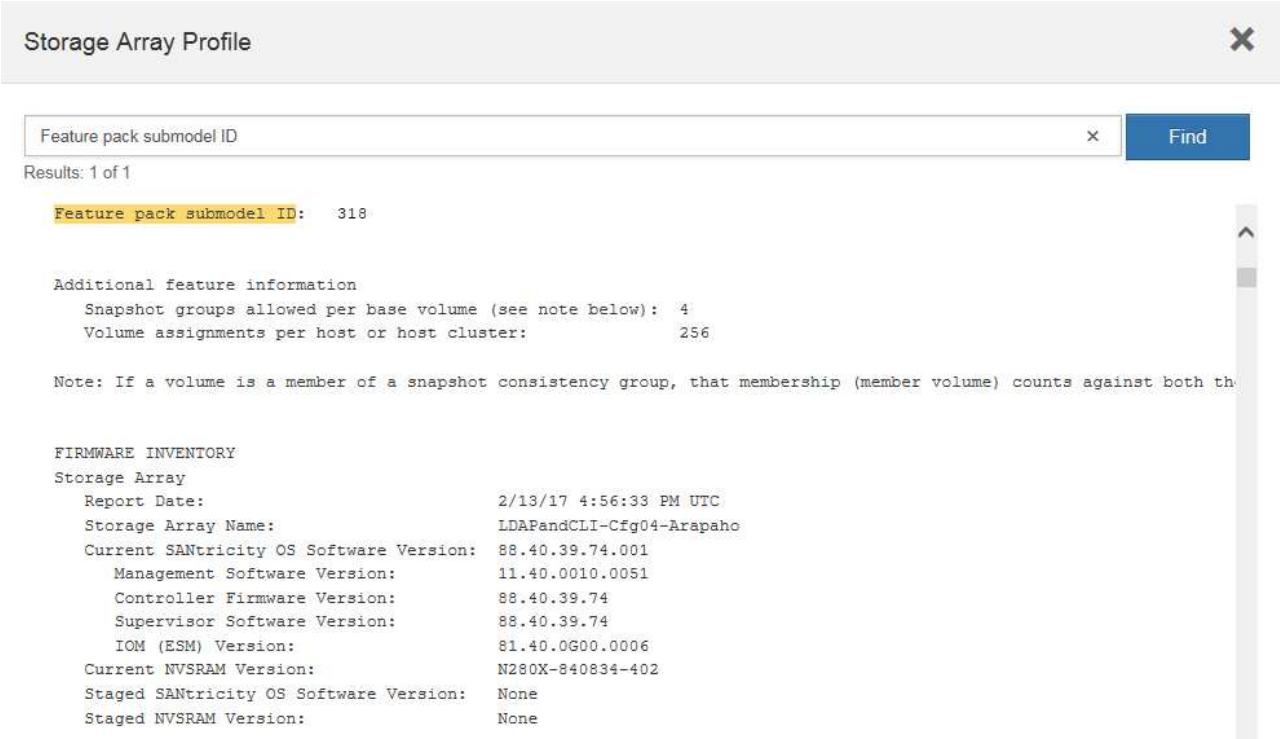
1. Individuare il numero di serie.
   a. Da Gestore di sistema di SANtricity, selezionare **supporto › Centro di supporto**.
   b. Con la scheda **Support Resources** (risorse di supporto) selezionata, scorrere fino alla sezione **View top storage array properties** (Visualizza proprietà principali storage array).
   c. Individuare **chassis Serial Number** (numero di serie chassis) e copiare questo valore in un file di testo.



2. Individuare l'ID del sottomodello **Feature Pack**.
   a. In Gestione sistema di SANtricity, selezionare **supporto**.
   b. Selezionare il riquadro **Support Center**.
   c. Nella scheda Support Resources (risorse di supporto), individuare e selezionare il collegamento **Storage Array Profile** (Profilo array di storage).
   d. Digitare **Feature Pack submodel ID** nella casella di testo e fare clic su **Find** (trova).

      Il "modello secondario" può anche essere scritto come "modello secondario".

   e. Individuare l'ID del sottomodello del Feature Pack per la configurazione iniziale.



3. Utilizzando l'ID del sottomodello del Feature Pack, individuare l'ID del sottomodello del controller corrispondente per la configurazione iniziale e individuare il codice di attivazione della funzione per la configurazione finale desiderata all'interno della tabella riportata di seguito. Quindi, copiare il codice di attivazione della funzione in un file di testo.

   Le porte della scheda base sono disattivate quando si esegue un protocollo NVMe sull'HIC.

   Se non si utilizza IB HIC, è possibile ignorare la colonna *HIC Ports* nelle seguenti tabelle:

Codici di attivazione delle funzioni compatibili con la crittografia (conversioni solo porta baseboard)				
Avvio della configurazione		Fine della configurazione		
ID del sottomodello del controller	Porte da convertire	ID del sottomodello del controller	Porte convertite in	Codice di attivazione della funzione

Codici di attivazione delle funzioni compatibili con la crittografia (conversioni solo porta baseboard)				
360	Porte per scheda base FC	362	Porte per scheda base iSCSI	SGL-2SB-ZEX13
362	Porte per scheda base iSCSI	360	Porte per scheda base FC	5GI-4 TB-ZW3HL

Codici di attivazione delle funzioni compatibili con la crittografia						
Avvio della configurazione			Fine della configurazione			
ID del sottomodello del controller	Porte della scheda base	Porte HIC	ID del sottomodello del controller	Porte della scheda base	Porte HIC	Codice di attivazione della funzione
360	FC	Er	361	FC	SRP	UTG-XSB-ZCZKU
362	ISCSI	Er	SGL-2SB-ZEX13	363	ISCSI	SRP
VGN-LTB-ZGFCT	382	Non disponibile	NVMe/IB	KGI-ISB-ZDHQF	403	Non disponibile
NVMe/RoCE o NVMe/FC	YGH-BHK-Z8EKB	361	FC	SRP	360	FC
Er	JGS-0TB-ZID1V	362	ISCSI	Er	UGX-RTB-ZLBPV	363
ISCSI	SRP	2G1-BTB-ZMRYN	382	Non disponibile	NVMe/IB	TGV-8TB-ZKTH6
403	Non disponibile	NVMe/RoCE o NVMe/FC	JGM-EIK-ZAC6Q	362	ISCSI	Er
360	FC	Er	5GI-4 TB-ZW3HL	361	FC	SRP
EGL-NTB-ZXKQ4	363	ISCSI	SRP	HGP-QUB-Z1ICJ	383	Non disponibile
NVMe/IB	BGS-AUB-Z2YNG	403	Non disponibile	NVMe/RoCE o NVMe/FC	1 GW-LIK-ZG9HN	363
ISCSI	SRP	360	FC	Er	SGU-VASCA-Z3G2U	361

Codici di attivazione delle funzioni compatibili con la crittografia						
FC	SRP	FGX-DUB-Z5WF7	362	ISCSI	SRP	LG3-GUB-Z7V17
383	Non disponibile	NVMe/IB	NG5-ZUB-Z8C8J	403	Non disponibile	NVMe/RoCE o NVMe/FC
WG2-0IK-ZI75U	382	Non disponibile	NVMe/IB	360	FC	Er
QG6-ETB-ZPPPT	361	FC	SRP	XG8-XTB-ZQ7XS	362	ISCSI
Er	SGB-HTB-ZS0AH	363	ISCSI	SRP	TGD-1TB-ZT5TL	403
Non disponibile	NVMe/RoCE o NVMe/FC	IGR-IIK-ZDBRB	383	Non disponibile	NVMe/IB	360
FC	Er	LG8-JUB-ZATLD	361	FC	SRP	LGA-3UB-ZBAX1
362	ISCSI	Er	NGF-7UB-ZE8KX	363	ISCSI	SRP
3GI-QUB-ZFP1Y	403	Non disponibile	NVMe/RoCE o NVMe/FC	5G7-RIK-ZL5PE	403	Non disponibile
NVMe/RoCE o NVMe/FC	360	FC	Er	BGC-UIK-Z03GR	361	FC
SRP	LGF-EIK-ZPJRX	362	ISCSI	Er	PGJ-HIK-ZSIDZ	363
ISCSI	SRP	1GM-1JK-ZTYQX	382	Non disponibile	NVMe/IB	JGH-XIK-ZQ142

Codici di attivazione delle funzioni non di crittografia (conversioni solo porta baseboard)				
Avvio della configurazione		Fine della configurazione		
ID del sottomodello del controller	Porte da convertire	ID del sottomodello del controller	Porte convertite in	Codice di attivazione della funzione
365	Porte per scheda base FC	367	Porte per scheda base iSCSI	BGU-GVB-ZM3KW

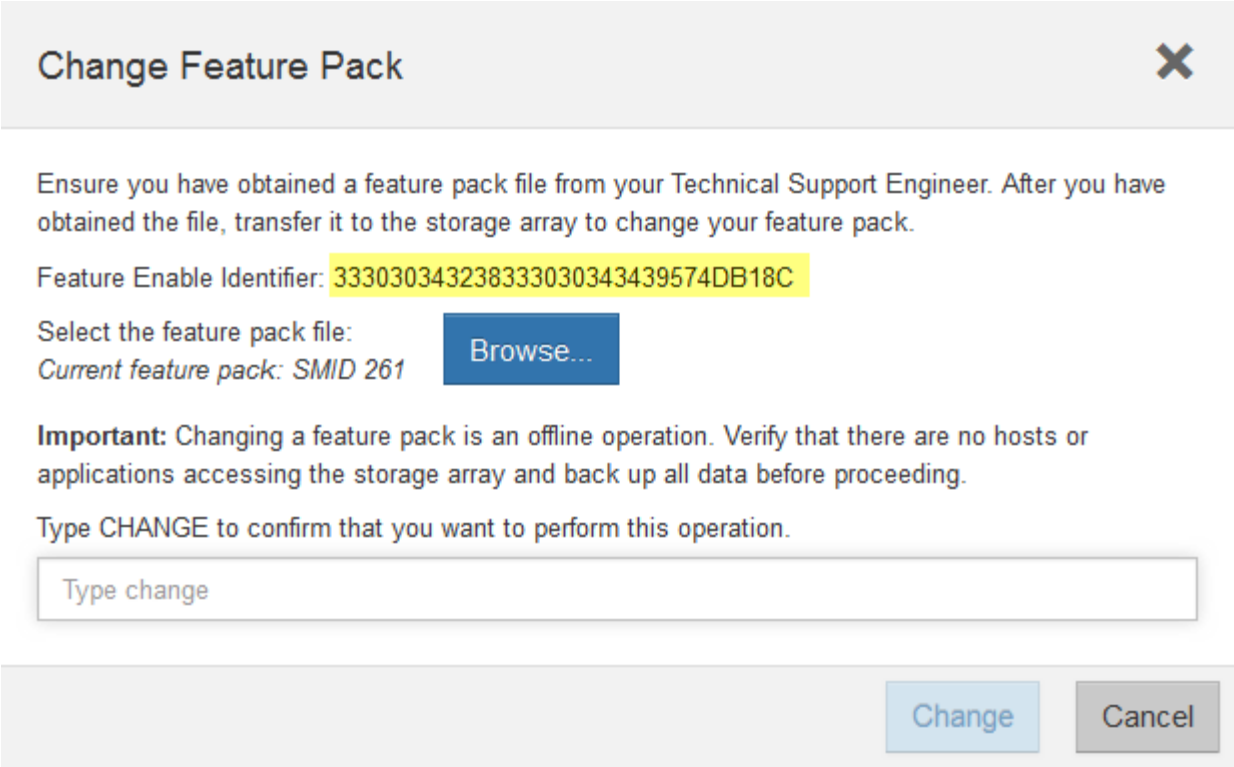
Codici di attivazione delle funzioni non di crittografia (conversioni solo porta baseboard)				
367	Porte per scheda base iSCSI	366	Porte per scheda base FC	9GU-2WB-Z503D

Codici di attivazione delle funzioni non di crittografia						
Avvio della configurazione			Fine della configurazione			
ID del sottomodello del controller	Porte baseboard	Porte HIC	ID del sottomodello del controller	Porte baseboard	Porte HIC	Codice di attivazione della funzione
365	FC	Er	366	FC	SRP	BGP-DVB-ZJ4YC
367	ISCSI	Er	BGU-GVB-ZM3KW	368	ISCSI	SRP
4GX-ZVB-ZNJVD	384	Non disponibile	NVMe/IB	TGS-WVB-ZKL9T	405	Non disponibile
NVMe/RoCE o NVMe/FC	WGC-GJK-Z7PU2	366	FC	SRP	365	FC
Er	WG2-3VB-ZQHLF	367	ISCSI	Er	QG7-6VB-ZSF8M	368
ISCSI	SRP	PGA-PVB-ZUWMX	384	Non disponibile	NVMe/IB	CG5-MVB-ZRYW1
405	Non disponibile	NVMe/RoCE o NVMe/FC	3GH-JJK-ZANJQ	367	ISCSI	Er
365	FC	Er	PGR-IWB-Z48PC	366	FC	SRP
9GU-2WB-Z503D	368	ISCSI	SRP	SGJ-IWB-ZJFE4	385	Non disponibile
NVMe/IB	UGM-2XB-ZKV0B	405	Non disponibile	NVMe/RoCE o NVMe/FC	8GR-QKK-ZFJTP	368
ISCSI	SRP	365	FC	Er	YG0-LXB-ZLD26	366
FC	SRP	SGR-5XB-ZNTFB	367	ISCSI	SRP	PGZ-5WB-Z8M0N

Codici di attivazione delle funzioni non di crittografia						
385	Non disponibile	NVMe/IB	KG2-0WB-Z9477	405	Non disponibile	NVMe/RoCE o NVMe/FC
2GV-TKK-ZIHI6	384	Non disponibile	NVMe/IB	365	FC	Er
SGF-SVB-ZWU9M	366	FC	SRP	7GH-CVB-ZYBGV	367	ISCSI
Er	6GK-VVB-ZSRN	368	ISCSI	SRP	RGM-FWB-Z195H	405
Non disponibile	NVMe/RoCE o NVMe/FC	VGM-NKK-ZDLDK	385	Non disponibile	NVMe/IB	365
FC	Er	GG5-8WB-ZBKEM	366	FC	SRP	KG7-RWB-ZC2RZ
367	ISCSI	Er	NGC-VWB-ZFZEN	368	ISCSI	SRP
4GE-FWB-ZGGQJ	405	Non disponibile	NVMe/RoCE o NVMe/FC	NG1-WKK-ZLFAI	405	Non disponibile
NVMe/RoCE o NVMe/FC	365	FC	Er	MG6-ZKK-ZNDVC	366	FC
SRP	WG9-JKK-ZPUAR	367	ISCSI	Er	NGE-MKK-ZRSW9	368
ISCSI	SRP	TGG-6KK-ZT9BU	384	Non disponibile	NVMe/IB	AGB-3KK-ZQBLR

Se l'ID del sottomodello del controller non è presente nell'elenco, contattare "Supporto NetApp".

4. In System Manager, individuare Feature Enable Identifier.
   a. Accedere al **Impostazioni › sistema**.
   b. Scorrere verso il basso fino a **componenti aggiuntivi**.
   c. In **Change Feature Pack**, individuare **Feature Enable Identifier**.
   d. Copiare e incollare questo numero di 32 cifre in un file di testo.



5. Passare a. "Attivazione della licenza NetApp: Attivazione della funzionalità Premium dello storage Array"e immettere le informazioni necessarie per ottenere il feature pack.
   - Numero di serie dello chassis
   - Codice di attivazione della funzione
   - Identificatore di abilitazione della funzione

> Il sito Web di attivazione delle funzionalità Premium include un collegamento a “istruzioni di attivazione delle funzioni Premium”. Non tentare di seguire queste istruzioni per questa procedura.

6. Scegliere se ricevere il file delle chiavi per il Feature Pack in un’e-mail o scaricarlo direttamente dal sito.

Fase 3: Arrestare l’i/o host

Interrompere tutte le operazioni di i/o dall’host prima di convertire il protocollo delle porte host. Non è possibile accedere ai dati sull’array di storage fino a quando la conversione non viene completata correttamente.

Questa attività si applica solo se si sta convertendo un array di storage già in uso.

Fasi

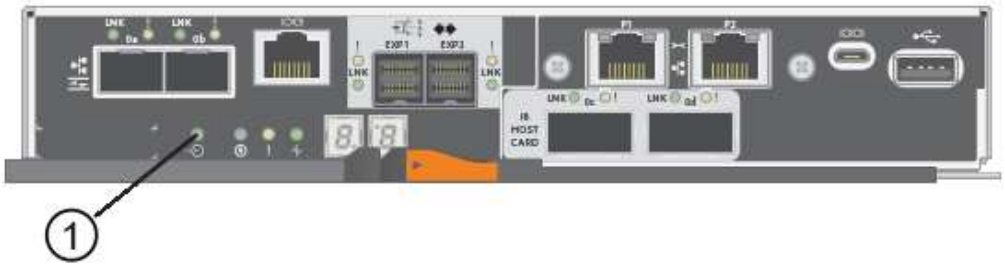
1. Assicurarsi che non si verifichino operazioni di i/o tra lo storage array e tutti gli host connessi. Ad esempio, è possibile eseguire le seguenti operazioni:
   - Arrestare tutti i processi che coinvolgono le LUN mappate dallo storage agli host.
   - Assicurarsi che nessuna applicazione stia scrivendo dati su tutte le LUN mappate dallo storage agli host.
   - Smontare tutti i file system associati ai volumi sull’array.

I passaggi esatti per interrompere le operazioni di i/o dell'host dipendono dal sistema operativo dell'host e dalla configurazione, che esulano dall'ambito di queste istruzioni. Se non si è sicuri di come interrompere le operazioni di i/o host nell'ambiente, è consigliabile arrestare l'host.

Possibile perdita di dati — se si continua questa procedura mentre si verificano le operazioni di i/o, l'applicazione host potrebbe perdere i dati perché lo storage array non sarà accessibile.

2. Se l'array di storage partecipa a una relazione di mirroring, interrompere tutte le operazioni di i/o dell'host sull'array di storage secondario.
3. Attendere che i dati presenti nella memoria cache vengano scritti sui dischi.

   Il LED verde cache Active (cache attiva) **(1)** sul retro di ciascun controller è acceso quando i dati memorizzati nella cache devono essere scritti sui dischi. Attendere che il LED si spenga.



4. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
5. Attendere il completamento di tutte le operazioni prima di passare alla fase successiva.

Fase 4: Modificare il Feature Pack

Modificare il Feature Pack per convertire il protocollo host delle porte host della scheda base, delle porte IB HIC o di entrambi i tipi di porte.

Fasi

1. Da Gestore di sistema di SANtricity, selezionare **Impostazioni › sistema**.
2. In **componenti aggiuntivi**, selezionare **Cambia Feature Pack**.

3. Fare clic su **Sfoglia**, quindi selezionare il Feature Pack che si desidera applicare.
4. Digitare **CHANGE** nel campo.
5. Fare clic su **Cambia**.

   Viene avviata la migrazione dei Feature Pack. Entrambi i controller si riavviano automaticamente due volte per rendere effettivo il nuovo Feature Pack. Una volta completato il riavvio, lo storage array torna allo stato di risposta.

6. Verificare che le porte host dispongano del protocollo previsto.
   a. Da Gestione sistema di SANtricity, selezionare **hardware**.
   b. Fare clic su **Mostra retro dello shelf**.
   c. Selezionare l'immagine per Controller A o Controller B.
   d. Selezionare **Visualizza impostazioni** dal menu di scelta rapida.
   e. Selezionare la scheda **interfacce host**.
   f. Fare clic su **Mostra altre impostazioni**.
   g. Esaminare i dettagli mostrati per le porte della scheda base e le porte HIC (etichettate "slotto 1") e verificare che ciascun tipo di porta disponga del protocollo previsto.

Quali sono le prossime novità?

Passare a. "Completa la conversione del protocollo host".

Conversione completa del protocollo host E5700

Dopo aver convertito il protocollo delle porte host, eseguire ulteriori operazioni per utilizzare il nuovo protocollo.

I passaggi da completare dipendono dai protocolli iniziali e finali delle porte host della scheda base e delle porte HIC.

Conversione completa da FC a iSCSI

Se in precedenza si disponevano di porte host FC e si erano convertiti in iSCSI, potrebbe essere necessario modificare la configurazione esistente per supportare iSCSI. La seguente procedura è applicabile solo se non è presente iSCSI HIC.

A proposito di questa attività

Questa attività si applica solo se si sta convertendo un array di storage già in uso.

Questa attività non si applica se si sta convertendo un nuovo array di storage che non ha ancora host e volumi definiti. Se è stato convertito il protocollo host-port di un nuovo array di storage, consultare "Procedure di cablaggio" Per installare cavi e SFP. Quindi, seguire le istruzioni in "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express" per completare la configurazione di ciascun protocollo.

Fasi

1. Configurare gli switch.

   È necessario configurare gli switch utilizzati per il trasporto del traffico iSCSI in base alle raccomandazioni del vendor per iSCSI. Questi consigli possono includere sia direttive di configurazione che aggiornamenti del codice.

2. Da Gestore di sistema di SANtricity, selezionare **hardware › Configura porte iSCSI**.
3. Selezionare le impostazioni della porta.

   È possibile configurare la rete iSCSI in diversi modi. Rivolgersi all'amministratore di rete per suggerimenti sulla scelta della configurazione migliore per l'ambiente in uso.

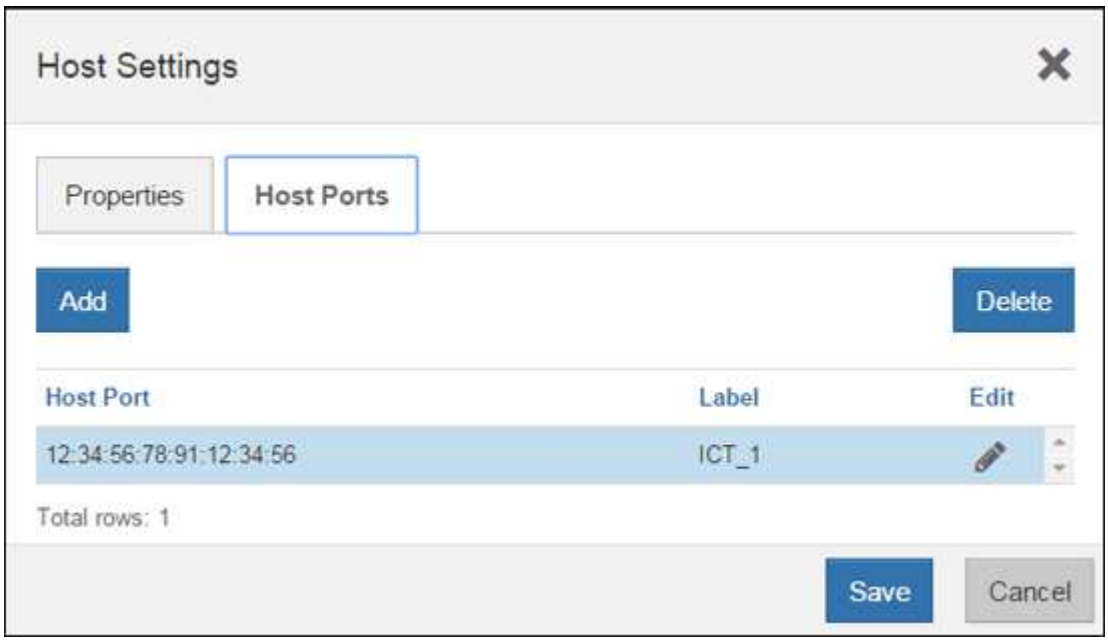
4. Aggiornare le definizioni degli host in Gestore di sistema di SANtricity.

   Per istruzioni sull'aggiunta di host o cluster di host, consultare la guida in linea di Gestione di sistema di SANtricity.

   a. Selezionare **Storage › Hosts** (Storage[host]).
   b. Selezionare l'host a cui associare la porta e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

      Viene visualizzata la finestra di dialogo host Settings (Impostazioni host).

   c. Fare clic sulla scheda **host Ports** (Porte host).



d. Fare clic su **Add** (Aggiungi) e utilizzare la finestra di dialogo **Add host Port** (Aggiungi porta host) 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 FC 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.

e. Fare clic su **Delete** (Elimina) e utilizzare la finestra di dialogo **Delete host Port** (Elimina porta host) per rimuovere (annullare l'associazione) un identificatore di porta host.

   L'opzione **Delete** 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.

f. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni dell'identificatore della porta host.

g. Ripetere questa procedura per aggiungere e rimuovere eventuali identificatori di porta host aggiuntivi.

5. Riavviare l'host o eseguire una nuova scansione in modo che l'host scopra correttamente le LUN.
6. Eseguire il remount dei volumi o iniziare a utilizzare il volume a blocchi.

Quali sono le prossime novità?

La conversione del protocollo host è stata completata. È possibile riprendere le normali operazioni.

Conversione completa da iSCSI a FC

Se in precedenza si disponevano di porte host iSCSI e si erano convertiti in FC, potrebbe essere necessario modificare la configurazione esistente per supportare FC. La seguente procedura è applicabile solo se non è presente FC HIC.

Questa attività si applica solo se si sta convertendo un array di storage già in uso.

Questa attività non si applica se si sta convertendo un nuovo array di storage che non ha ancora host e volumi definiti. Se è stato convertito il protocollo host-port di un nuovo array di storage, consultare "Procedure di cablaggio" Per installare cavi e SFP. Quindi, seguire le istruzioni in "Configurazione di Linux Express", "Configurazione di Windows Express", o. "Configurazione di VMware Express" per completare la configurazione di ciascun protocollo.

Fasi

1. Installare l'utility HBA e determinare le WWPN dell'iniziatore.
2. Fare una zona tra gli switch.

   Lo zoning degli switch consente agli host di connettersi allo storage e limita il numero di percorsi. Gli switch vengono posizionati in zone utilizzando l'interfaccia di gestione degli switch.

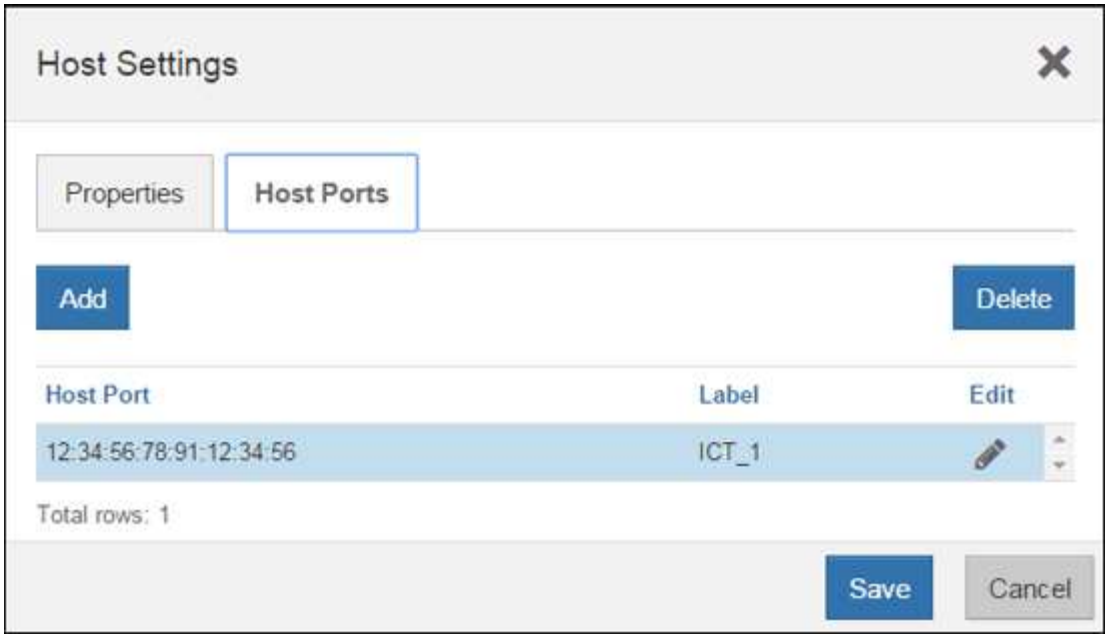
3. Aggiornare le definizioni degli host in Gestore di sistema di SANtricity.

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

   b. Selezionare l'host a cui associare la porta e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

      Viene visualizzata la finestra di dialogo host Settings (Impostazioni host).

   c. Fare clic sulla scheda **host Ports** (Porte host).



d. Fare clic su **Add** (Aggiungi) e utilizzare la finestra di dialogo **Add host Port** (Aggiungi porta host) 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 FC 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.

e. Fare clic su **Delete** (Elimina) e utilizzare la finestra di dialogo **Delete host Port** (Elimina porta host) per rimuovere (annullare l'associazione) un identificatore di porta host.

   L'opzione **Delete** 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.

f. Fare clic su **Save** (Salva) per applicare le modifiche alle impostazioni dell'identificatore della porta host.

g. Ripetere questa procedura per aggiungere e rimuovere eventuali identificatori di porta host aggiuntivi.

4. Riavviare l'host o eseguire una nuova scansione in modo che l'host scopra correttamente lo storage mappato.
5. Eseguire il remount dei volumi o iniziare a utilizzare il volume a blocchi.

Quali sono le prossime novità?

La conversione del protocollo host è stata completata. È possibile riprendere le normali operazioni.

Conversione completa per IB-iSER a/da IB-SRP, NVMe su IB, NVMe su RoCE o NVMe su FC

Dopo aver applicato la chiave Feature Pack per convertire il protocollo utilizzato dalla porta InfiniBand iSER HIC in/da SRP, NVMe su InfiniBand, NVMe su RoCE o NVMe su Fibre Channel, è necessario configurare l'host per utilizzare il protocollo appropriato.

Fasi

1. Configurare l'host per l'utilizzo del protocollo SRP, iSER o NVMe.

   Per istruzioni dettagliate su come configurare l'host per l'utilizzo di SRP, iSER o NVMe, consultare

"Configurazione di Linux Express".

2. Per collegare l'host allo storage array per una configurazione SRP, è necessario attivare lo stack di driver InfiniBand con le opzioni appropriate.

   Impostazioni specifiche possono variare a seconda delle distribuzioni Linux. Controllare "Matrice di interoperabilità NetApp" per istruzioni specifiche e impostazioni aggiuntive consigliate per la soluzione.

Quali sono le prossime novità?

La conversione del protocollo host è stata completata. È possibile riprendere le normali operazioni.

Gestire lo storage

Utilizzare i collegamenti riportati di seguito per accedere alla documentazione che descrive come configurare, gestire e monitorare gli oggetti di storage e i sistemi di storage e-Series. I collegamenti consentono di accedere a un altro sito di documentazione.

Guida in linea di System Manager 11.7

Accedere a. "Guida in linea di Gestore di sistema di SANtricity 11.7", dove è possibile trovare informazioni su come pianificare, configurare, gestire e risolvere i problemi del proprio array di storage.

Guida in linea di Unified Manager 5

Accedere a. "Guida in linea di SANtricity Unified Manager 5", dove è possibile apprendere come eseguire comandi di gestione dello storage su più array di storage di rete.

Riferimento al comando

Accedere a. "Riferimento al comando", Dove è possibile apprendere come configurare e monitorare gli array di storage utilizzando i comandi dell'interfaccia a riga di comando (CLI).

Utilizzare le soluzioni SANtricity

Proxy dei servizi Web

Panoramica dei proxy dei servizi web SANtricity

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

Panoramica dell'installazione

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

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

Trova ulteriori informazioni

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

Scopri di più sui servizi Web

Panoramica dei servizi Web e di Unified Manager

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

Servizi Web

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

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

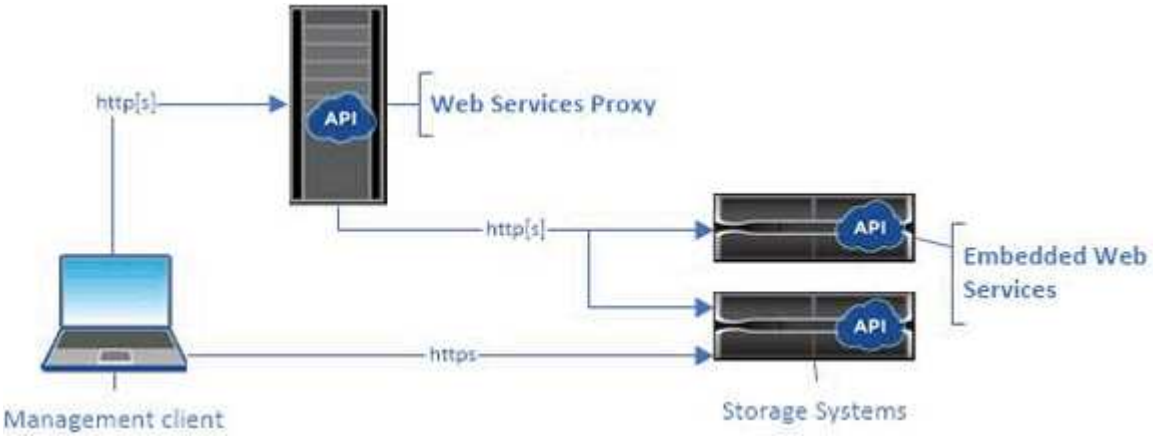
Quando si utilizza l'API dei servizi Web per gestire i sistemi storage, è necessario avere familiarità con quanto segue:

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

I servizi Web sono disponibili in due implementazioni:

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

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



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

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

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

Unified Manager

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

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

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

Compatibilità e limitazioni

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

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

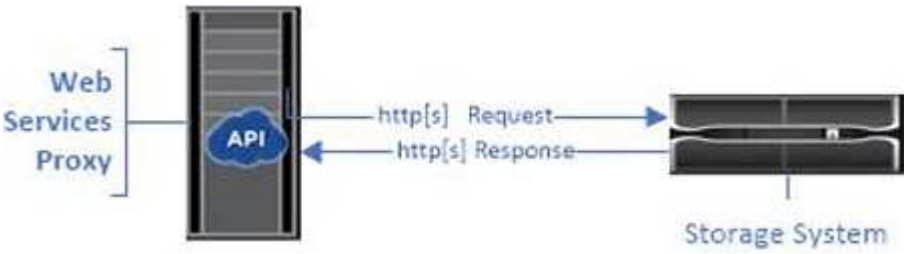
Considerazione	Compatibilità o restrizione
Supporto IP	Il proxy dei servizi Web supporta il protocollo IPv4 o IPv6. Il protocollo IPv6 potrebbe non funzionare quando il proxy dei servizi Web tenta di rilevare automaticamente l'indirizzo di gestione dalla configurazione del controller. Le possibili cause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

Nozioni di base sulle API

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

Elementi URL nelle richieste

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



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

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

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

Verbi HTTP supportati

I verbi HTTP supportati includono GET, POST ed DELETE:

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

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

Accettare le intestazioni

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

Risposte

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

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

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

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

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

Script di esempio

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

Termini e concetti

I seguenti termini si applicano al proxy dei servizi Web.

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

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

Installare e configurare

Verifica dei requisiti di installazione e aggiornamento

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

Requisiti di installazione

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

L'installazione del proxy include i seguenti requisiti.

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

Considerazioni sull'upgrade

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

conservati o rimossi.

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

Installare o aggiornare il file proxy dei servizi Web

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

Scaricare i file proxy dei servizi Web

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

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

Fasi

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

Installazione su server Windows o Linux

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

Prima di iniziare

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

Installazione in modalità grafica

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

Fasi

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

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

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

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

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

3. Seguire le istruzioni a schermo.

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

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

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

   Viene visualizzata la finestra di dialogo Installazione completata.

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

Installazione in modalità console

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

Fasi

1. Eseguire il seguente comando: `<install filename> -i console`

   Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   Per annullare l'installazione in qualsiasi momento durante il processo di installazione, digitare `QUIT` al prompt dei comandi.

   Viene avviato il processo di installazione e viene visualizzato il messaggio Avvio del programma di installazione — Introduzione.

2. Seguire le istruzioni a schermo.

   Durante l'installazione, viene richiesto di attivare diverse funzioni e di inserire alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.

   Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

3. Una volta completata l'installazione, premere **Invio** per uscire dal programma di installazione.

Installazione in modalità silenziosa

È possibile eseguire l'installazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Eseguire il seguente comando: `<install filename> -i silent`

   Nel comando precedente, `<install filename>` rappresenta il nome del file di installazione del proxy scaricato (ad esempio: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Premere **Invio**.

   Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Installazione del comando RPM (solo Linux)

Per i sistemi Linux compatibili con il sistema di gestione dei pacchetti RPM, è possibile installare il proxy dei servizi Web utilizzando un file RPM opzionale.

Fasi

1. Scaricare il file RPM sul server in cui si desidera installare il proxy e Unified Manager.
2. Aprire una finestra terminale.
3. Immettere il seguente comando:

   ```
   rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   > Nel comando precedente, `nn.nn.nn.nnnn` rappresenta il numero di versione.

   Il completamento del processo di installazione può richiedere alcuni minuti. Una volta completata l'installazione, viene visualizzato un prompt dei comandi nella finestra del terminale.

Accedere a API e Unified Manager

I servizi Web includono la documentazione API, che consente di interagire direttamente con L'API REST. Include inoltre Unified Manager, un'interfaccia basata su browser per la gestione di più sistemi storage e-Series.

Accedere all'API dei servizi Web

Dopo aver installato Web Services Proxy, è possibile accedere alla documentazione API interattiva in un browser.

La documentazione API viene eseguita con ogni istanza dei servizi Web ed è disponibile anche in formato PDF statico dal sito del supporto NetApp. Per accedere alla versione interattiva, aprire un browser e immettere l'URL che indica la posizione dei servizi Web (un controller per la versione incorporata o un server per il proxy).

> L'API dei servizi Web implementa la specifica OpenAPI (originariamente chiamata specifica Swagger).

Per l'accesso iniziale, utilizzare le credenziali "admin". "Admin" è considerato un super amministratore con accesso a tutte le funzioni e i ruoli.

Fasi

1. Aprire un browser.
2. Inserire l'URL per l'implementazione del proxy o incorporato:

   - Integrato: `https://<controller>:<port>/devmgr/docs/`

     In questo URL, `<controller>` È l'indirizzo IP o FQDN del controller, e. `<port>` è il numero della porta di gestione del controller (il valore predefinito è 8443).

   - Proxy: `http[s]://<server>:<port>/devmgr/docs/`

     In questo URL, `<server>` È l'indirizzo IP o FQDN del server in cui è installato il proxy, e. `<port>` È il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o 8443 per HTTPS).

     > Se la porta di ascolto è già in uso, il proxy rileva il conflitto e richiede di scegliere un'altra porta di ascolto.

   La documentazione API viene aperta nel browser.

3. Una volta aperta la documentazione API interattiva, accedere al menu a discesa in alto a destra della pagina e selezionare **utils**.
4. Fare clic sulla categoria **Login** per visualizzare gli endpoint disponibili.
5. Fare clic sull'endpoint **POST: /Login**, quindi fare clic su **Provalo**.
6. Per il primo accesso, immettere admin come nome utente e password.
7. Fare clic su **Execute** (Esegui).
8. Per accedere agli endpoint per la gestione dello storage, andare al menu a discesa in alto a destra e selezionare **v2**.

   Vengono visualizzate le categorie di alto livello per gli endpoint. È possibile esplorare la documentazione API come descritto nella tabella.

Area	Descrizione
Menu a discesa	Nella parte superiore destra della pagina, un menu a discesa fornisce le opzioni per passare dalla versione 2 della documentazione API (V2), all'interfaccia dei simboli (Symbol V2) e alle utility API (utils) per l'accesso. Poiché la versione 1 della documentazione API era una versione preliminare e generalmente non disponibile, V1 non è incluso nel menu a discesa.

Area	Descrizione
Categorie	La documentazione API è organizzata in base a categorie di alto livello (ad esempio, amministrazione, configurazione). Fare clic su una categoria per visualizzare gli endpoint correlati.
Endpoint	Selezionare un endpoint per visualizzare i percorsi URL, i parametri richiesti, i corpi di risposta e i codici di stato che gli URL potrebbero restituire.
Provalo	Interagire direttamente con l'endpoint facendo clic su **Provalo**. Questo pulsante viene fornito in ciascuna vista espansa per gli endpoint. Quando si fa clic sul pulsante, vengono visualizzati i campi per l'immissione dei parametri (se applicabile). Immettere i valori e fare clic su **Esegui**. La documentazione interattiva utilizza JavaScript per inviare la richiesta direttamente all'API; non si tratta di una richiesta di test.

Accedere a Unified Manager

Dopo aver installato Web Services Proxy, è possibile accedere a Unified Manager per gestire più sistemi storage in un'interfaccia basata su web.

Per accedere a Unified Manager, aprire un browser e immettere l'URL che indica la posizione in cui è installato il proxy. Sono supportati i seguenti browser e versioni.

Browser	Versione minima
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

Fasi

1. Aprire un browser e immettere il seguente URL:

   ```
   http[s]://<server>:<port>/um
   ```

   In questo URL, `<server>` Rappresenta l'indirizzo IP o FQDN del server in cui è installato Web Services Proxy, e. `<port>` Rappresenta il numero della porta di ascolto (il valore predefinito è 8080 per HTTP o

8443 per HTTPS).

Viene visualizzata la pagina di accesso a Unified Manager.

2. Per il primo accesso, immettere `admin` specificare il nome utente, quindi impostare e confermare una password per l'utente amministratore.

   La password può contenere fino a 30 caratteri. Per ulteriori informazioni su utenti e password, consultare la sezione Gestione degli accessi della guida in linea di Unified Manager.

Configurare il proxy dei servizi Web

È possibile modificare le impostazioni di Web Services Proxy per soddisfare i requisiti operativi e di performance specifici per il proprio ambiente.

Arrestare o riavviare il server Web

Il servizio Webserver viene avviato durante l'installazione e viene eseguito in background. Durante alcune attività di configurazione, potrebbe essere necessario arrestare o riavviare il servizio Webserver.

Fasi

1. Effettuare una delle seguenti operazioni:

   - Per Windows, accedere al menu **Avvio**, selezionare **Strumenti di amministrazione › servizi**, individuare **servizi Web NetApp SANtricity** e selezionare **Interrompi** o **Riavvia**.
   - Per Linux, scegliere il metodo per arrestare e riavviare il server Web per la versione del sistema operativo in uso. Durante l'installazione, una finestra di dialogo a comparsa indica quale demone è stato avviato. Ad esempio:

     ```
     web_services_proxy webserver installed and started. You can interact with it
     using systemctl start|stop|restart|status web_services_proxy.service
     ```

   Il metodo più comune per interagire con il servizio è l'utilizzo di `systemctl` comandi.

Risolvere i conflitti di porta

Se il proxy dei servizi Web è in esecuzione mentre un'altra applicazione è disponibile all'indirizzo o alla porta definiti, è possibile risolvere il conflitto di porte nel file wsconfig.xml.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere la seguente riga al file wsconfig.xml, in cui *n* è il numero della porta:

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   La tabella seguente mostra gli attributi che controllano le porte HTTP e le porte HTTPS.

Nome	Descrizione	Nodo padre	Attributi	Obbligatorio
config	Il nodo root per la configurazione	Nullo	Versione - la versione dello schema di configurazione è attualmente 1.0.	Sì
slport	La porta TCP in attesa delle richieste SSL. Il valore predefinito è 8443.	config	Clientauth	No
porta	La porta TCP in attesa della richiesta HTTP, per impostazione predefinita, è 8080.	config	-	No

3. Salvare e chiudere il file.
4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare il bilanciamento del carico e/o l'alta disponibilità

Per utilizzare il proxy dei servizi Web in una configurazione ad alta disponibilità (ha), è possibile configurare il bilanciamento del carico. In una configurazione ha, in genere, un singolo nodo riceve tutte le richieste mentre le altre sono in stand-by oppure le richieste sono bilanciate in base al carico su tutti i nodi.

Il proxy dei servizi Web può esistere in un ambiente ad alta disponibilità (ha), con la maggior parte delle API che funzionano correttamente indipendentemente dal destinatario della richiesta. I tag e le cartelle dei metadati sono due eccezioni, perché i tag e le cartelle vengono memorizzati in un database locale e non vengono condivisi tra le istanze di Web Services Proxy.

Tuttavia, in una piccola percentuale di richieste si verificano alcuni problemi di tempistica noti. In particolare, un'istanza del proxy può avere dati più recenti più velocemente di una seconda istanza per una piccola finestra. Il proxy dei servizi Web include una configurazione speciale che elimina questo problema di tempistica. Questa opzione non è attivata per impostazione predefinita, perché aumenta il tempo necessario per le richieste di servizio (per la coerenza dei dati). Per attivare questa opzione, è necessario aggiungere una proprietà a un file .INI (per Windows) o .SH (per Linux).

Fasi

1. Effettuare una delle seguenti operazioni:
   - Windows: Aprire il file appserver64.ini, quindi aggiungere `Dload-balance.enabled=true` proprietà.

     Ad esempio: `vmarg.7=-Dload-balance.enabled=true`
   - Linux: Aprire il file webserver.sh, quindi aggiungere `Dload-balance.enabled=true` proprietà.

     Ad esempio: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Salvare le modifiche.
3. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Disattiva il simbolo HTTPS

È possibile disattivare i comandi dei simboli (impostazione predefinita) e inviare comandi tramite una chiamata di procedura remota (RPC). Questa impostazione può essere modificata nel file wsconfig.xml.

Per impostazione predefinita, il proxy dei servizi Web invia i comandi dei simboli tramite HTTPS per tutti i sistemi storage della serie E2800 e E5700 con SANtricity OS versione 08.40 o successiva. I comandi Symbol inviati tramite HTTPS vengono autenticati nel sistema di storage. Se necessario, è possibile disattivare il supporto dei simboli HTTPS e inviare comandi tramite RPC. Ogni volta che viene configurato Symbol over RPC, tutti i comandi passivi al sistema di storage vengono abilitati senza autenticazione.

> Quando viene utilizzato Symbol over RPC, il proxy dei servizi Web non può connettersi ai sistemi con la porta di gestione dei simboli disattivata.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. In `devicemgt.symbolclientstrategy` sostituire `httpsPreferred` valore con `rpcOnly`.

   Ad esempio:

   ```
   <env key="devicemgt.symbolclientstrategy">rpcOnly</env>
   ```

3. Salvare il file.

Configurare la condivisione delle risorse tra origini

È possibile configurare la condivisione delle risorse tra origini (CORS), un meccanismo che utilizza intestazioni HTTP aggiuntive per fornire un'applicazione Web in esecuzione su un'origine per avere l'autorizzazione ad accedere a risorse selezionate da un server di origine diversa.

Il CORS viene gestito dal file cors.cfg che si trova nella directory di lavoro. La configurazione CORS è aperta per impostazione predefinita, pertanto l'accesso tra domini non è limitato.

Se non è presente alcun file di configurazione, CORS è aperto. Ma se il file cors.cfg è presente, viene utilizzato. Se il file cors.cfg è vuoto, non è possibile effettuare una richiesta CORS.

Fasi

1. Aprire il file cors.cfg che si trova nella directory di lavoro.
2. Aggiungere le righe desiderate al file.

   Ogni riga nel file di configurazione CORS è un modello di espressione regolare da abbinare. L'intestazione di origine deve corrispondere a una riga nel file cors.cfg. Se un modello di riga corrisponde all'intestazione di origine, la richiesta è consentita. Viene confrontata l'origine completa, non solo l'elemento host.

3. Salvare il file.

Le richieste vengono associate sull'host e in base al protocollo, ad esempio:

- Associare localhost a qualsiasi protocollo — `*localhost*`
- Corrispondenza localhost solo per HTTPS — `https://localhost*`

Disinstallare il proxy dei servizi Web

Per rimuovere Web Services Proxy e Unified Manager, è possibile utilizzare qualsiasi modalità (file grafico, console, silenzioso o RPM), indipendentemente dal metodo utilizzato per installare il proxy.

Disinstallazione della modalità grafica

È possibile eseguire la disinstallazione in modalità grafica per Windows o Linux. In modalità grafica, i prompt vengono visualizzati in un'interfaccia di tipo Windows.

Fasi

1. Avviare la disinstallazione per Windows o Linux, come indicato di seguito:
   - Windows — accedere alla directory che contiene il file di disinstallazione uninstall_web_Services_proxy. La directory predefinita si trova nel seguente percorso: C:/Program Files/NetApp/SANtricity Web Services Proxy/. Fare doppio clic `uninstall_web_services_proxy.exe`.

     In alternativa, è possibile accedere a **pannello di controllo › programmi › Disinstalla un programma**, quindi selezionare "Proxy dei servizi web NetApp SANtricity".

   - Linux — accedere alla directory che contiene il file di disinstallazione di Web Services Proxy. La directory predefinita si trova nella seguente posizione: `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i gui
   ```

   Viene visualizzata la schermata iniziale del proxy dei servizi Web di SANtricity.

3. Nella finestra di dialogo Disinstalla, fare clic su **Disinstalla**.

   Viene visualizzata la barra di avanzamento del programma di disinstallazione che mostra lo stato di avanzamento.

4. Quando viene visualizzato il messaggio Uninstall complete (disinstallazione completata), fare clic su **Done** (fine).

Disinstallazione della modalità console

È possibile eseguire la disinstallazione in modalità Console per Windows o Linux. In modalità Console, i prompt vengono visualizzati nella finestra del terminale.

Fasi

1. Accedere alla directory uninstall_web_Services_proxy.
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i console
   ```

Viene avviato il processo di disinstallazione.

3. Una volta completata la disinstallazione, premere **Invio** per uscire dal programma di installazione.

Disinstallazione in modalità silenziosa

È possibile eseguire la disinstallazione in modalità silenziosa per Windows o Linux. In modalità silenziosa, nella finestra del terminale non vengono visualizzati messaggi o script di ritorno.

Fasi

1. Accedere alla directory uninstall_web_Services_proxy.
2. Eseguire il seguente comando:

   ```
   uninstall_web_services_proxy -i silent
   ```

   Il processo di disinstallazione viene eseguito, ma nella finestra del terminale non vengono visualizzati messaggi o script di ritorno. Una volta disinstallato Web Services Proxy, viene visualizzato un prompt dei comandi nella finestra del terminale.

Disinstallazione del comando RPM (solo Linux)

È possibile utilizzare un comando RPM per disinstallare il proxy dei servizi Web da un sistema Linux.

Fasi

1. Aprire una finestra terminale.
2. Immettere la seguente riga di comando:

   ```
   rpm -e santricity_webservices
   ```

   > Il processo di disinstallazione potrebbe lasciare file che non facevano parte dell'installazione originale. Eliminare manualmente questi file per rimuovere completamente il proxy dei servizi Web.

Gestire l'accesso degli utenti in Web Services Proxy

È possibile gestire l'accesso degli utenti alle API dei servizi Web e a Unified Manager per motivi di sicurezza.

Panoramica della gestione degli accessi

La gestione degli accessi include accessi in base al ruolo, crittografia delle password, autenticazione di base e integrazione LDAP.

Accesso in base al ruolo

RBAC (role-based access control) associa gli utenti predefiniti ai ruoli. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità.

La tabella seguente descrive ciascun ruolo.

Ruolo	Descrizione
security.admin	SSL e gestione dei certificati.
storage.admin	Accesso completo in lettura/scrittura alla configurazione del sistema storage.
storage.monitor	Accesso in sola lettura per visualizzare i dati del sistema di storage.
support.admin	Accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).

Gli account utente predefiniti sono definiti nel file users.properties. È possibile modificare gli account utente modificando direttamente il file users.properties o utilizzando le funzioni di gestione degli accessi di Unified Manager.

La tabella seguente elenca gli accessi utente disponibili per il proxy dei servizi Web.

Accesso utente predefinito	Descrizione
amministratore	Un super amministratore che ha accesso a tutte le funzioni e include tutti i ruoli. Per Unified Manager, è necessario impostare la password al primo accesso.
storage	L'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
sicurezza	L'utente responsabile della configurazione della sicurezza. Questo utente include i seguenti ruoli: Security.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
supporto	L'utente responsabile delle risorse hardware, dei dati di guasto e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
monitorare	Un utente con accesso di sola lettura al sistema. Questo utente include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.
rw (legacy per gli array meno recenti)	L'utente rw (lettura/scrittura) include i seguenti ruoli: Storage.admin, support.admin e storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Accesso utente predefinito	Descrizione
ro (legacy per gli array meno recenti)	L'utente ro (sola lettura) include solo il ruolo storage.monitor. Questo account viene disattivato fino a quando non viene impostata una password.

Crittografia della password

Per ciascuna password, è possibile applicare un ulteriore processo di crittografia utilizzando la codifica della password SHA256 esistente. Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.

> Prima della versione 3.0 di Web Services Proxy, le password venivano crittografate solo tramite l'hashing SHA256. Tutte le password crittografate SHA256 esistenti con solo hash mantengono questa codifica e sono ancora valide nel file users.properties. Tuttavia, le password crittografate SHA256 solo con hash non sono sicure come quelle con crittografia SARTed SHA256.

Autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Questa impostazione può essere modificata nel file wsconfig.xml.

LDAP

Il protocollo LDAP (Lightweight Directory Access Protocol), un protocollo applicativo per l'accesso e la manutenzione dei servizi informativi di directory distribuiti, è abilitato per il proxy dei servizi Web. L'integrazione LDAP consente l'autenticazione dell'utente e il mapping dei ruoli ai gruppi.

Per informazioni sulla configurazione della funzionalità LDAP, fare riferimento alle opzioni di configurazione nell'interfaccia di Unified Manager o nella sezione LDAP della documentazione API interattiva.

Configurare l'accesso dell'utente

È possibile gestire l'accesso degli utenti applicando una crittografia aggiuntiva alle password, impostando l'autenticazione di base e definendo l'accesso in base al ruolo.

Applicare crittografia aggiuntiva alle password

Per ottenere il massimo livello di sicurezza, è possibile applicare una crittografia aggiuntiva alle password utilizzando la codifica password SHA256 esistente.

Questo processo di crittografia aggiuntivo applica un set casuale di byte a ciascuna password (SALT) per ogni crittografia hash SHA256. La crittografia SARTed SHA256 viene applicata a tutte le password appena create.

Fasi

1. Aprire il file users.properties all'indirizzo:
   - (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Immettere nuovamente la password crittografata come testo normale.
3. Eseguire `securepasswds` Utilità della riga di comando per crittografare nuovamente la password o

semplicemente riavviare il proxy dei servizi Web. Questa utility viene installata nella directory di installazione principale del proxy dei servizi Web.

> In alternativa, è possibile utilizzare le password utente locali e cancellarle ogni volta che vengono modificate le password tramite Unified Manager.

Configurare l'autenticazione di base

Per impostazione predefinita, l'autenticazione di base è attivata, il che significa che il server restituisce una sfida di autenticazione di base. Se lo si desidera, è possibile modificare tale impostazione nel file wsconfig.xml.

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Modificare la riga seguente nel file specificando false (non abilitato) o true (abilitato).

   Ad esempio: `<env key="enable-basic-auth">true</env>`
3. Salvare il file.
4. Riavviare il servizio Webserver in modo che la modifica abbia effetto.

Configurare l'accesso in base al ruolo

Per limitare l'accesso degli utenti a funzioni specifiche, è possibile modificare i ruoli specificati per ciascun account utente.

Web Services Proxy include RBAC (role-based access control), in cui i ruoli sono associati a utenti predefiniti. Ogni ruolo concede le autorizzazioni a un livello specifico di funzionalità. È possibile modificare i ruoli assegnati agli account utente modificando direttamente il file users.properties.

> È inoltre possibile modificare gli account utente utilizzando Access Management in Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Fasi

1. Aprire il file users.properties, che si trova in:
   - (Windows) — C: File di programma/Proxy servizi Web NetApp/SANtricity/data/config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Individuare la riga dell'account utente che si desidera modificare (storage, sicurezza, monitor, supporto, rw, o ro).

   > Non modificare l'utente admin. Si tratta di un super utente con accesso a tutte le funzioni.
3. Aggiungere o rimuovere i ruoli specificati, come desiderato.

   I ruoli includono:

   - Security.admin — SSL e gestione dei certificati.
   - Storage.admin — accesso completo in lettura/scrittura alla configurazione del sistema storage.

- Storage.monitor — accesso in sola lettura per visualizzare i dati del sistema di storage.
- Support.admin — accesso a tutte le risorse hardware sui sistemi storage e operazioni di supporto come il recupero ASUP (AutoSupport).

> Il ruolo storage.monitor è necessario per tutti gli utenti, incluso l'amministratore.

4. Salvare il file.

Gestire la sicurezza e i certificati in Web Services Proxy

Per motivi di sicurezza in Web Services Proxy, è possibile specificare una designazione della porta SSL ed è possibile gestire i certificati. I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server.

Abilitare SSL

Il proxy dei servizi Web utilizza Secure Sockets Layer (SSL) per la protezione, che viene attivata durante l'installazione. È possibile modificare la designazione della porta SSL nel file wsconfig.xml.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere o modificare il numero della porta SSL, in modo simile all'esempio seguente:

```
<sslport clientauth="request">8443</sslport>
```

Risultato

Quando il server viene avviato con SSL configurato, il server cerca i file keystore e truststore.

- Se il server non trova un keystore, utilizza l'indirizzo IP del primo indirizzo IPv4 non loopback rilevato per generare un keystore e aggiungere un certificato autofirmato al keystore.
- Se il server non trova un truststore o non viene specificato, il server utilizza il keystore come truststore.

Ignora la convalida del certificato

Per supportare connessioni sicure, il proxy dei servizi Web convalida i certificati` dei sistemi di storage rispetto ai propri certificati attendibili. Se necessario, è possibile specificare che il proxy eluderà la convalida prima di connettersi ai sistemi di storage.

Prima di iniziare

- Tutte le connessioni del sistema di storage devono essere sicure.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy

- (Linux) — /opt/netapp/santricity_web_Services_proxy

2. Invio `true` in `trust.all.arrays` come mostrato nell'esempio:

```
<env key="trust.all.arrays">true</env>
```

3. Salvare il file.

Generare e importare un certificato di gestione host

I certificati identificano i proprietari dei siti Web per connessioni sicure tra client e server. Per generare e importare certificati CA (Certificate Authority) per il sistema host in cui è installato Web Services Proxy, è possibile utilizzare endpoint API.

Per gestire i certificati per il sistema host, eseguire le seguenti attività utilizzando l'API:

- Creare una richiesta di firma del certificato (CSR) per il sistema host.
- Inviare il file CSR a una CA, quindi attendere l'invio dei file di certificato.
- Importare i certificati firmati nel sistema host.

> È inoltre possibile gestire i certificati nell'interfaccia di Unified Manager. Per ulteriori informazioni, consultare la guida in linea disponibile in Unified Manager.

Fasi

1. Accedere a. "Documentazione API interattiva".
2. Andare al menu a discesa in alto a destra e selezionare **v2**.
3. Espandere il collegamento **Administration** e scorrere verso il basso fino agli endpoint **/certificates**.
4. Generare il file CSR:
   a. Selezionare **POST:/certificates**, quindi selezionare **Try it out**.

      Il server Web rigenera un certificato autofirmato. È quindi possibile inserire informazioni nei campi per definire il nome comune, l'organizzazione, l'unità organizzativa, l'ID alternativo e altre informazioni utilizzate per generare la CSR.

   b. Aggiungere le informazioni richieste nel riquadro **Example Values** (valori di esempio) per generare un certificato CA valido, quindi eseguire i comandi.

      > Non chiamare di nuovo **POST:/certificates** o **POST:/certificates/reset**, altrimenti è necessario rigenerare la CSR. Quando si chiama **POST:/certificates** o **POST:/certificates/reset**, si sta generando un nuovo certificato autofirmato con una nuova chiave privata. Se si invia una CSR generata prima dell'ultimo ripristino della chiave privata sul server, il nuovo certificato di protezione non funziona. È necessario generare una nuova CSR e richiedere un nuovo certificato CA.

   c. Eseguire l'endpoint **GET:/certificates/server** per confermare che lo stato corrente del certificato è il certificato autofirmato con le informazioni aggiunte dal comando **POST:/certificates**.

      Il certificato del server (indicato dall'alias `jetty`) è ancora autofirmato a questo punto.

d. Espandere l'endpoint **POST:/certificates/export**, selezionare **provalo**, immettere un nome di file per il file CSR, quindi fare clic su **Esegui**.

5. Copiare e incollare `fileUrl` In una nuova scheda del browser per scaricare il file CSR, quindi inviare il file CSR a una CA valida per richiedere una nuova catena di certificati del server Web.
6. Quando la CA emette una nuova catena di certificati, utilizzare uno strumento di gestione dei certificati per suddividere i certificati server root, intermedi e Web, quindi importarli nel server proxy dei servizi Web:
   a. Espandere l'endpoint **POST:/sslconfig/server** e selezionare **Provalo**.
   b. Immettere un nome per il certificato CA root nel campo **alias**.
   c. Selezionare **false** nel campo **replaceMainServerCertificate**.
   d. Individuare e selezionare il nuovo certificato CA principale.
   e. Fare clic su **Execute** (Esegui).
   f. Verificare che il caricamento del certificato sia riuscito.
   g. Ripetere la procedura di caricamento del certificato CA per il certificato intermedio CA.
   h. Ripetere la procedura di caricamento del certificato per il nuovo file di certificato di sicurezza del server Web, ad eccezione di questa fase, selezionare **true** nell'elenco a discesa **replaceMainServerCertificate**.
   i. Verificare che l'importazione del certificato di sicurezza del server Web sia riuscita.
   j. Per confermare che i nuovi certificati root, intermedi e server web sono disponibili nel keystore, eseguire **GET:/certificates/server**.
7. Selezionare ed espandere l'endpoint **POST:/certificates/reload**, quindi selezionare **Try it out**. Quando richiesto, se si desidera riavviare entrambi i controller, selezionare **false**. ("vero" si applica solo nel caso di controller a doppio array). Fare clic su **Execute** (Esegui).

   L'endpoint **/certificates/reload** in genere restituisce una risposta http 202 corretta. Tuttavia, il ricaricamento dei certificati truststore e keystore del server Web crea una race condition tra il processo API e il processo di ricarica dei certificati del server Web. In rari casi, il ricaricamento del certificato del server Web può superare l'elaborazione dell'API. In questo caso, il ricaricamento sembra non riuscire anche se è stato completato correttamente. In tal caso, passare comunque alla fase successiva. Se il ricaricamento non è riuscito, anche il passaggio successivo non riesce.

8. Chiudere la sessione corrente del browser sul proxy dei servizi Web, aprire una nuova sessione del browser e verificare che sia possibile stabilire una nuova connessione sicura del browser al proxy dei servizi Web.

   Utilizzando una sessione di navigazione in incognito o privata, è possibile aprire una connessione al server senza utilizzare i dati salvati delle sessioni di navigazione precedenti.

Gestire i sistemi storage utilizzando Web Services Proxy

Per gestire i sistemi storage in rete, è necessario prima rilevarli e poi aggiungerli all'elenco di gestione.

Scopri i sistemi storage

È possibile impostare il rilevamento automatico o rilevare manualmente i sistemi storage.

Rilevare automaticamente i sistemi storage

È possibile specificare che i sistemi di storage vengano rilevati automaticamente in rete modificando le impostazioni nel file wsconfig.xml. Per impostazione predefinita, il rilevamento automatico IPv6 è disattivato e IPv4 è attivato.

Per aggiungere un sistema storage, è necessario fornire un solo indirizzo IP o DNS di gestione. Il server rileva automaticamente tutti i percorsi di gestione quando i percorsi non sono configurati o sono configurati e ruotabili.

> Se si tenta di utilizzare un protocollo IPv6 per rilevare automaticamente i sistemi storage dalla configurazione del controller dopo aver effettuato una connessione iniziale, il processo potrebbe non riuscire. Le possibili cause del guasto includono problemi durante l'inoltro dell'indirizzo IP o l'attivazione di IPv6 sui sistemi storage, ma non sul server.

Prima di iniziare

Prima di attivare le impostazioni di rilevamento IPv6, verificare che l'infrastruttura supporti la connettività IPv6 ai sistemi storage per mitigare eventuali problemi di connessione.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Nelle stringhe di ricerca automatica, modificare le impostazioni da `true` a. `false`, come desiderato. Vedere l'esempio seguente.

```
<env key="autodiscover.ipv6.enable">true</env>
```

> Quando i percorsi sono configurati, ma non configurati in modo che il server possa instradare verso gli indirizzi, si verificano errori di connessione intermittenti. Se non è possibile impostare gli indirizzi IP in modo che possano essere instradati dall'host, disattivare la funzione di rilevamento automatico (modificare le impostazioni su `false`).

3. Salvare il file.

Rilevare e aggiungere sistemi storage utilizzando endpoint API

È possibile utilizzare gli endpoint API per rilevare e aggiungere sistemi storage all'elenco gestito. Questa procedura crea una connessione di gestione tra il sistema di storage e l'API.

> Questa attività descrive come individuare e aggiungere sistemi storage utilizzando l'API REST, in modo da poter gestire questi sistemi nella documentazione API interattiva. Tuttavia, è possibile gestire i sistemi storage in Unified Manager, che offre un'interfaccia di facile utilizzo. Per ulteriori informazioni, consultare la guida in linea disponibile con Unified Manager.

Prima di iniziare

Per i sistemi storage con SANtricity versione 11.30 e successive, l'interfaccia di gestione legacy per Symbol deve essere attivata nell'interfaccia di Gestore di sistema di SANtricity. In caso contrario, gli endpoint di rilevamento non riescono. Per trovare questa impostazione, aprire Gestione sistema e accedere al

Impostazioni › sistema › Impostazioni aggiuntive › interfaccia di gestione delle modifiche.

Fasi

1. Accedere a. "Documentazione API interattiva".
2. Scopri i sistemi storage come segue:
   a. Nella documentazione API, assicurarsi che sia selezionato **V2** nell'elenco a discesa, quindi espandere la categoria **Storage-Systems**.
   b. Fare clic sull'endpoint **POST: /Discovery**, quindi fare clic su **Provalo**.
   c. Inserire i parametri come descritto nella tabella.

IP startup IP finale
Sostituire la stringa con l'intervallo di indirizzi IP iniziale e finale per uno o più sistemi di storage in rete.
UseAgents
Impostare questo valore su: • Vero = utilizza agenti in-band per la scansione di rete. • Falso = non utilizzare agenti in-band per la scansione di rete.
ConnectionTimeout
Inserire i secondi consentiti per la scansione prima che la connessione si esaurisca.
MaxPortsToUse
Immettere un numero massimo di porte utilizzate per la scansione di rete.

   d. Fare clic su **Execute** (Esegui).

   Le azioni API vengono eseguite senza richieste dell'utente.

   Il processo di rilevamento viene eseguito in background.

   a. Assicurarsi che il codice restituisca 202.
   b. In **Response Body**, individuare il valore restituito per l'ID richiesta. Per visualizzare i risultati nel passaggio successivo, è necessario l'ID richiesta.
3. Visualizzare i risultati del rilevamento come segue:
   a. Fare clic sull'endpoint **GET: /Discovery**, quindi fare clic su **Provalo**.
   b. Inserire l'ID richiesta dal passaggio precedente. Se si lascia vuoto **ID richiesta**, l'endpoint passa per impostazione predefinita all'ultimo ID richiesta eseguito.

c. Fare clic su **Execute** (Esegui).

d. Assicurarsi che il codice restituisca 200.

e. Nel corpo della risposta, individuare l'ID richiesta e le stringhe per i sistemi di storage. Le stringhe sono simili all'esempio seguente:

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Annotare i valori per wwn, Label e ipAddresses. Sono necessari per il passaggio successivo.

4. Aggiungere i sistemi storage come segue:

a. Fare clic sull'endpoint **POST: /Storage-system**, quindi fare clic su **Provalo**.

b. Inserire i parametri come descritto nella tabella.

id
Immettere un nome univoco per il sistema di storage. È possibile inserire l'etichetta (visualizzata nella risposta per GET: /Discovery), ma il nome può essere qualsiasi stringa scelta. Se non si specifica un valore per questo campo, i servizi Web assegnano automaticamente un identificatore univoco.
ControllerAddresses
Inserire gli indirizzi IP visualizzati nella risposta per GET: /Discovery. Per i controller doppi, separare gli indirizzi IP con una virgola. Ad esempio: `"IP address 1","IP address 2"`
validare
Invio `true`, In modo da poter ricevere la conferma che i servizi Web possono connettersi al sistema di storage.
password
Inserire la password amministrativa per il sistema di storage.

wwn
Inserire il WWN del sistema di storage (visualizzato nella risposta per GET: /Discovery).

c. Rimuovi tutte le stringhe dopo `"enableTrace": true`, in modo che l'intero set di stringhe sia simile all'esempio seguente:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Fare clic su **Execute** (Esegui).

e. Assicurarsi che la risposta del codice sia 201, che indica che l'endpoint è stato eseguito correttamente.

   L'endpoint **Post: /Storage-Systems** viene messo in coda. È possibile visualizzare i risultati utilizzando l'endpoint **GET: /Storage-Systems** nella fase successiva.

5. Confermare l'aggiunta dell'elenco, come segue:

   a. Fare clic sull'endpoint **GET: /Storage-system**.

      Non sono richiesti parametri.

   b. Fare clic su **Execute** (Esegui).

   c. Assicurarsi che la risposta del codice sia 200, che indica che l'endpoint è stato eseguito correttamente.

   d. Nel corpo della risposta, cercare i dettagli del sistema di storage. I valori restituiti indicano che è stato aggiunto correttamente all'elenco degli array gestiti, in modo simile all'esempio seguente:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


Scalare il numero di sistemi storage gestiti

Per impostazione predefinita, l'API può gestire fino a 100 sistemi storage. Se è necessario gestire di più, è necessario superare i requisiti di memoria per il server.

Il server è impostato per utilizzare 512 MB di memoria. Per ogni 100 sistemi storage aggiuntivi della rete, aggiungere 250 MB a tale numero. Non aggiungere più memoria di quella fisicamente disponibile. Consente di aggiungere un numero sufficiente di componenti aggiuntivi per il sistema operativo e altre applicazioni.

> La dimensione predefinita della cache è 8,192 eventi. L'utilizzo approssimativo dei dati per la cache degli eventi MEL è di 1 MB per ogni 8,192 eventi. Pertanto, mantenendo le impostazioni predefinite, l'utilizzo della cache dovrebbe essere di circa 1 MB per un sistema storage.

> Oltre alla memoria, il proxy utilizza le porte di rete per ciascun sistema di storage. Linux e Windows considerano le porte di rete come handle di file. Come misura di sicurezza, la maggior parte dei sistemi operativi limita il numero di handle di file aperti che un processo o un utente può avere aperto contemporaneamente. In particolare negli ambienti Linux, dove le connessioni TCP aperte sono considerate come handle di file, il proxy dei servizi Web può facilmente superare questo limite. Poiché la correzione dipende dal sistema, fare riferimento alla documentazione del sistema operativo per informazioni su come aumentare questo valore.

Fasi

1. Effettuare una delle seguenti operazioni:
   - In Windows, accedere al file appserver64.init. Individuare la linea, `vmarg.3=-Xmx512M`
   - Su Linux, andare al file webserver.sh. Individuare la linea, `JAVA_OPTIONS="-Xmx512M"`
2. Per aumentare la memoria, sostituire `512` Con la memoria desiderata in MB.
3. Salvare il file.

Gestire il polling automatico per le statistiche del proxy dei servizi Web

È possibile configurare il polling automatico per tutte le statistiche di dischi e volumi sui sistemi storage rilevati.

Panoramica delle statistiche

Le statistiche forniscono informazioni sui tassi di raccolta dei dati e sulle performance dei sistemi storage.

Il proxy dei servizi Web consente di accedere ai seguenti tipi di statistiche:

- Statistiche raw — contatori totali per i punti dati al momento della raccolta dei dati. Le statistiche raw possono essere utilizzate per operazioni di lettura totali o operazioni di scrittura totali.
- Statistiche analizzate — informazioni calcolate per un intervallo. Esempi di statistiche analizzate sono le operazioni di input/output in lettura (IOPS) al secondo o il throughput in scrittura.

Le statistiche raw sono lineari, in genere richiedono almeno due punti di dati raccolti per ricavare da essi i dati utilizzabili. Le statistiche analizzate sono una derivazione delle statistiche raw, che forniscono metriche importanti. Molti valori che possono essere derivati dalle statistiche raw vengono visualizzati in un formato point-in-time utilizzabile nelle statistiche analizzate per maggiore comodità.

È possibile recuperare le statistiche raw indipendentemente dal fatto che il polling automatico sia attivato o meno. È possibile aggiungere `usecache=true` Stringa di query alla fine dell'URL per recuperare le statistiche memorizzate nella cache dall'ultimo polling. L'utilizzo dei risultati memorizzati nella cache aumenta notevolmente le performance del recupero delle statistiche. Tuttavia, più chiamate a una velocità uguale o inferiore alla cache dell'intervallo di polling configurata recuperano gli stessi dati.

Funzionalità delle statistiche

Il proxy dei servizi Web fornisce endpoint API che consentono il recupero di statistiche di controller e interfacce raw e analizzate da modelli hardware e versioni software supportati.

API Raw Statistics

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API delle statistiche analizzate

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Questi URL recuperano le statistiche analizzate dall'ultimo polling e sono disponibili solo quando il polling è attivato. Questi URL includono i seguenti dati input-output:

- Operazioni al secondo
- Throughput in megabyte al secondo
- Tempi di risposta in millisecondi

I calcoli si basano sulle differenze tra le iterazioni di polling statistiche, che sono le misure più comuni delle performance dello storage. Queste statistiche sono preferibili alle statistiche non analizzate.

> All'avvio del sistema, non esiste alcuna raccolta di statistiche precedente da utilizzare per calcolare le varie metriche, pertanto le statistiche analizzate richiedono almeno un ciclo di polling dopo l'avvio per restituire i dati. Inoltre, se i contatori cumulativi vengono ripristinati, il ciclo di polling successivo avrà numeri imprevedibili per i dati.

Configurare gli intervalli di polling

Per configurare gli intervalli di polling, modificare il file wsconfig.xml in modo da specificare un intervallo di polling in secondi.

> Poiché le statistiche sono memorizzate nella cache, potrebbe verificarsi un aumento di circa 1.5 MB di utilizzo della memoria per ciascun sistema di storage.

Prima di iniziare

- I sistemi storage devono essere rilevati dal proxy.

Fasi

1. Aprire il file wsconfig.xml all'indirizzo:
   - (Windows) — C:/Program Files/NetApp/SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Aggiungere la seguente riga all'interno di `<env-entries>` tag, in cui `n` indica il numero di secondi dell'intervallo tra le richieste di polling:

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Ad esempio, se si inserisce 60, il polling inizia a intervalli di 60 secondi. Ovvero, il sistema richiede l'avvio del polling 60 secondi dopo il completamento del periodo di polling precedente (indipendentemente dalla durata del periodo di polling precedente). Tutte le statistiche sono contrassegnate con l'ora esatta in cui sono state recuperate. Il sistema utilizza l'indicatore orario o la differenza temporale su cui basare il calcolo di 60 secondi.
3. Salvare il file.

Gestire AutoSupport utilizzando il proxy dei servizi Web

È possibile configurare ASUP (AutoSupport), che raccoglie i dati e li invia automaticamente al supporto tecnico per la risoluzione dei problemi e l'analisi dei problemi in remoto.

Panoramica di ASUP (AutoSupport)

La funzione ASUP (AutoSupport) trasmette automaticamente i messaggi a NetApp in base a criteri manuali e basati su pianificazione.

Ogni messaggio AutoSupport è un insieme di file di log, dati di configurazione, dati di stato e metriche delle performance. Per impostazione predefinita, AutoSupport trasmette i file elencati nella tabella seguente al team di supporto NetApp una volta alla settimana.

Nome file	Descrizione
x-headers-data.txt	Un file .txt contenente le informazioni dell'intestazione X.
manifest.xml	Un file .xml che descrive il contenuto del messaggio.
arraydata.xml	Un file .xml contenente l'elenco dei dati persistenti del client.
appserver-config.txt	Un file .txt contenente i dati di configurazione dell'application server.
wsconfig.txt	Un file .txt contenente i dati di configurazione del servizio Web.
host-info.txt	Un file .txt contenente informazioni sull'ambiente host.
server-logs.7z	Un file .7z contenente tutti i file di log del webserver disponibili.
client-info.txt	Un file .txt con coppie chiave/valore arbitrarie per contatori specifici dell'applicazione, ad esempio accessi a metodi e pagine web.
webservices-profile.json	Questi file contengono i dati del profilo WebServices e i dati statistici di monitoraggio Jersey. Per impostazione predefinita, le statistiche di monitoraggio Jersey sono attivate. È possibile attivarle e disattivarle nel file wsconfig.xml, come indicato di seguito: • Abilitare: `<env key="enable.jersey.statistics">true</env>` • Disattiva: `<env key="enable.jersey.statistics">false</env>`

Configurare AutoSupport

AutoSupport è attivato per impostazione predefinita al momento dell'installazione; tuttavia, è possibile modificare tale impostazione o i tipi di consegna.

Attiva o disattiva AutoSupport

La funzione AutoSupport viene attivata o disattivata durante l'installazione iniziale del proxy dei servizi Web, ma è possibile modificarla nel file ASUPConfig.

È possibile attivare o disattivare AutoSupport tramite il file ASUPConfig.xml, come descritto di seguito. In alternativa, è possibile attivare o disattivare questa funzione tramite l'API utilizzando **Configuration** e

POST/asup, quindi immettendo "true" o "false".

1. Aprire il file ASUPConfig.xml nella directory di lavoro.
2. Individuare le linee per <asupdata enable="Boolean_value" timestamp="timestamp">
3. Invio `true` (attiva) o. `false` (disattiva). Ad esempio:

```
<asupdata enabled="false" timestamp="0">
```

> La voce relativa all'indicatore data e ora è superflua.

4. Salvare il file.

Configurare il metodo di erogazione AutoSupport

È possibile configurare la funzione AutoSupport in modo che utilizzi i metodi di consegna HTTPS, HTTP o SMTP. HTTPS è il metodo di consegna predefinito.

1. Accedere al file ASUPConfig.xml nella directory di lavoro.
2. Nella stringa, `<delivery type="n">`, inserire 1, 2 o 3 come descritto nella tabella:

Valore	Descrizione
1	**HTTPS** (impostazione predefinita) <delivery type="1">
2	**HTTP** <delivery type="2">

3	**SMTP** — per configurare correttamente il tipo di recapito AutoSupport su SMTP, è necessario includere l'indirizzo del server di posta SMTP, insieme ai messaggi di posta elettronica dell'utente mittente e destinatario, come nell'esempio seguente:
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

Mirroring remoto del volume

Panoramica dei volumi di storage remoto

Utilizzare la funzione volumi di storage remoto SANtricity® per importare i dati da un dispositivo di storage remoto direttamente in un volume e-Series locale. Questa funzione consente di ottimizzare il processo di upgrade delle apparecchiature e offre funzionalità di migrazione dei dati per spostare i dati da dispositivi non-e-Series a sistemi e-Series.

Panoramica della configurazione

La funzione volumi di storage remoto è disponibile con Gestore di sistema SANtricity per gli ID dei sottomodello selezionati. Per utilizzare questa funzione, è necessario configurare un sistema di storage remoto e un sistema di storage e-Series per comunicare tra loro.

Utilizzare il seguente flusso di lavoro:

1. "Esaminare requisiti e limitazioni".
2. "Configurare l'hardware".
3. "Importa storage remoto".

Trova ulteriori informazioni

- Guida in linea, disponibile nell'interfaccia utente di System Manager o in "Sito della documentazione del software SANtricity".
- Per ulteriori informazioni tecniche sulla funzione Remote Storage Volumes (volumi storage remoti), consultare la "Report tecnico sui volumi di storage remoto".

Requisiti e restrizioni per lo storage remoto

Prima di configurare la funzione Remote Storage Volumes, esaminare i seguenti requisiti e limitazioni.

Requisiti hardware

Protocolli supportati

Per la versione iniziale della funzione Remote Storage Volumes, il supporto è disponibile solo per i protocolli iSCSI e IPv4.

Fare riferimento a. "Tool di matrice di interoperabilità NetApp" Per informazioni aggiornate sul supporto e sulla configurazione tra l'host e l'array e-Series (destinazione) utilizzato per la funzione Remote Storage Volumes.

Requisiti di sistema per lo storage

Il sistema storage e-Series deve includere:

- Due controller (modalità duplex)
- Connessioni iSCSI per i controller e-Series per comunicare con il sistema di storage remoto attraverso una o più connessioni iSCSI

- SANtricity OS 11.71 o superiore
- Funzione di storage remoto attivata nell'ID modello secondario (SMID)

Il sistema remoto può essere un sistema storage e-Series o un sistema di un altro vendor. Deve includere interfacce compatibili con iSCSI.

Requisiti di volume

I volumi utilizzati per le importazioni devono soddisfare i requisiti di dimensione, stato e altri criteri.

Volume di storage remoto

Il volume di origine di un'importazione viene chiamato "volume di storage remoto". Questo volume deve soddisfare i seguenti criteri:

- Non può far parte di un'altra importazione
- Deve avere uno stato online

Una volta avviata l'importazione, il firmware del controller crea un volume di storage remoto in background. A causa di questo processo in background, il volume di storage remoto non è gestibile in System Manager e può essere utilizzato solo per l'operazione di importazione.

Una volta creato, il volume di storage remoto viene trattato come qualsiasi altro volume standard sul sistema e-Series con le seguenti eccezioni:

- Può essere utilizzato come proxy per il dispositivo di storage remoto.
- Non può essere utilizzato come candidato per altre copie di volumi o snapshot.
- Impossibile modificare l'impostazione Data Assurance durante l'importazione.
- Non può essere mappato ad alcun host, perché sono riservati esclusivamente per l'operazione di importazione.

Ogni volume di storage remoto è associato a un solo oggetto di storage remoto; tuttavia, un oggetto di storage remoto può essere associato a più volumi di storage remoto. Il volume di storage remoto viene identificato in modo univoco utilizzando una combinazione di quanto segue:

- Identificatore dell'oggetto storage remoto
- Numero LUN del dispositivo di storage remoto

Candidati al volume di destinazione

Il volume di destinazione è il volume di destinazione sul sistema e-Series locale.

Il volume di destinazione deve soddisfare i seguenti criteri:

- Deve essere un volume RAID/DDP.
- Deve avere una capacità uguale o superiore al volume di storage remoto.
- Deve avere una dimensione del blocco uguale a quella del volume di storage remoto.
- Deve avere uno stato valido (ottimale).
- Non è possibile avere alcuna delle seguenti relazioni: Copia del volume, copie Snapshot, mirroring asincrono o sincrono.

- Non è possibile eseguire operazioni di riconfigurazione: Espansione dinamica del volume, espansione dinamica della capacità, dimensione dinamica dei segmenti, migrazione dinamica del RAID, riduzione dinamica della capacità, O deframmentazione.
- Impossibile eseguire il mapping a un host prima dell'inizio dell'importazione (tuttavia, è possibile eseguire il mapping dopo l'avvio dell'importazione).
- Non è possibile attivare la funzione Flash Read cache (FRC).

System Manager verifica automaticamente questi requisiti nell'ambito della procedura guidata di importazione dello storage remoto. Per la selezione del volume di destinazione vengono visualizzati solo i volumi che soddisfano tutti i requisiti.

Restrizioni

La funzione di storage remoto presenta le seguenti restrizioni:

- Il mirroring deve essere disattivato.
- Il volume di destinazione sul sistema e-Series non deve disporre di snapshot.
- Il volume di destinazione sul sistema e-Series non deve essere mappato ad alcun host prima dell'avvio dell'importazione.
- Il provisioning delle risorse del volume di destinazione nel sistema e-Series deve essere disattivato.
- I mapping diretti del volume di storage remoto a uno o più host non sono supportati.
- Il proxy dei servizi Web non è supportato.
- I segreti CHAP iSCSI non sono supportati.
- SMcli non è supportato.
- VMware Datastore non è supportato.
- Quando è presente una coppia di importazione, è possibile aggiornare un solo sistema di storage alla volta nella coppia relazione/importazione.

Preparazione per le importazioni in produzione

È necessario eseguire un'importazione di test o "dry run" prima delle importazioni in produzione per verificare la corretta configurazione dello storage e del fabric.

Molte variabili possono influire sull'operazione di importazione e sui tempi di completamento. Per garantire che un'importazione in produzione sia riuscita e per ottenere una stima della durata, è possibile utilizzare queste importazioni di test per garantire che tutte le connessioni funzionino come previsto e che l'operazione di importazione venga completata in un periodo di tempo appropriato. È quindi possibile apportare modifiche per ottenere i risultati desiderati prima di avviare l'importazione in produzione.

Configurare l'hardware per i volumi di storage remoto

Il sistema storage e-Series deve essere configurato per comunicare con il sistema storage remoto attraverso il protocollo iSCSI supportato.

Configurare il dispositivo di storage remoto e l'array e-Series

Prima di passare a Gestione sistema di SANtricity per configurare la funzione volumi di storage remoto, procedere come segue:

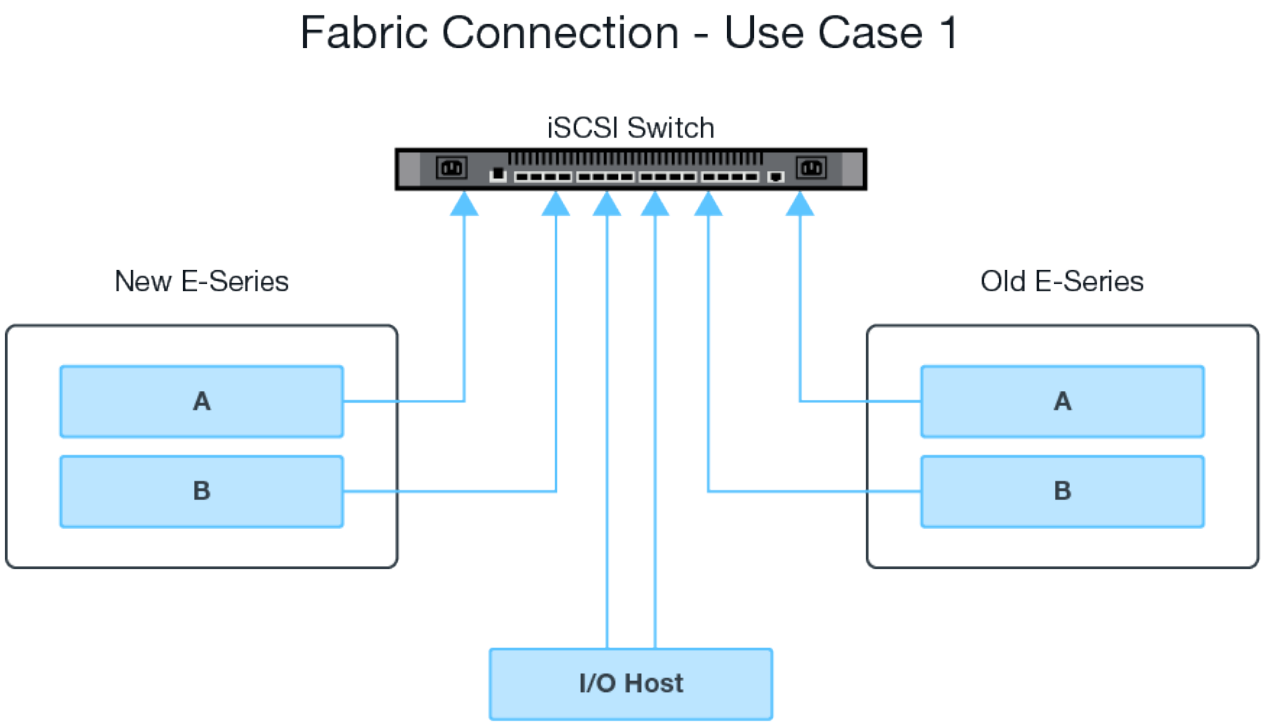
1. Stabilire manualmente una connessione cablata tra il sistema e-Series e il sistema di storage remoto in modo che i due sistemi possano essere configurati per comunicare tramite iSCSI.
2. Configurare le porte iSCSI in modo che il sistema e-Series e il sistema di storage remoto possano comunicare correttamente tra loro.
3. Ottenere l'IQN del sistema e-Series.
4. Rendere il sistema e-Series visibile al sistema di storage remoto. Se il sistema di storage remoto è un sistema e-Series, creare un host utilizzando l'IQN del sistema e-Series di destinazione come informazione di connessione per la porta host.
5. Se il dispositivo di storage remoto è in uso da un host/applicazione:
   - Arrestare i/o sul dispositivo di storage remoto.
   - Dismappare/smontare il dispositivo di storage remoto.
6. Mappare il dispositivo di storage remoto all'host definito per il sistema di storage e-Series.
7. Ottenere il numero LUN del dispositivo utilizzato per la mappatura.

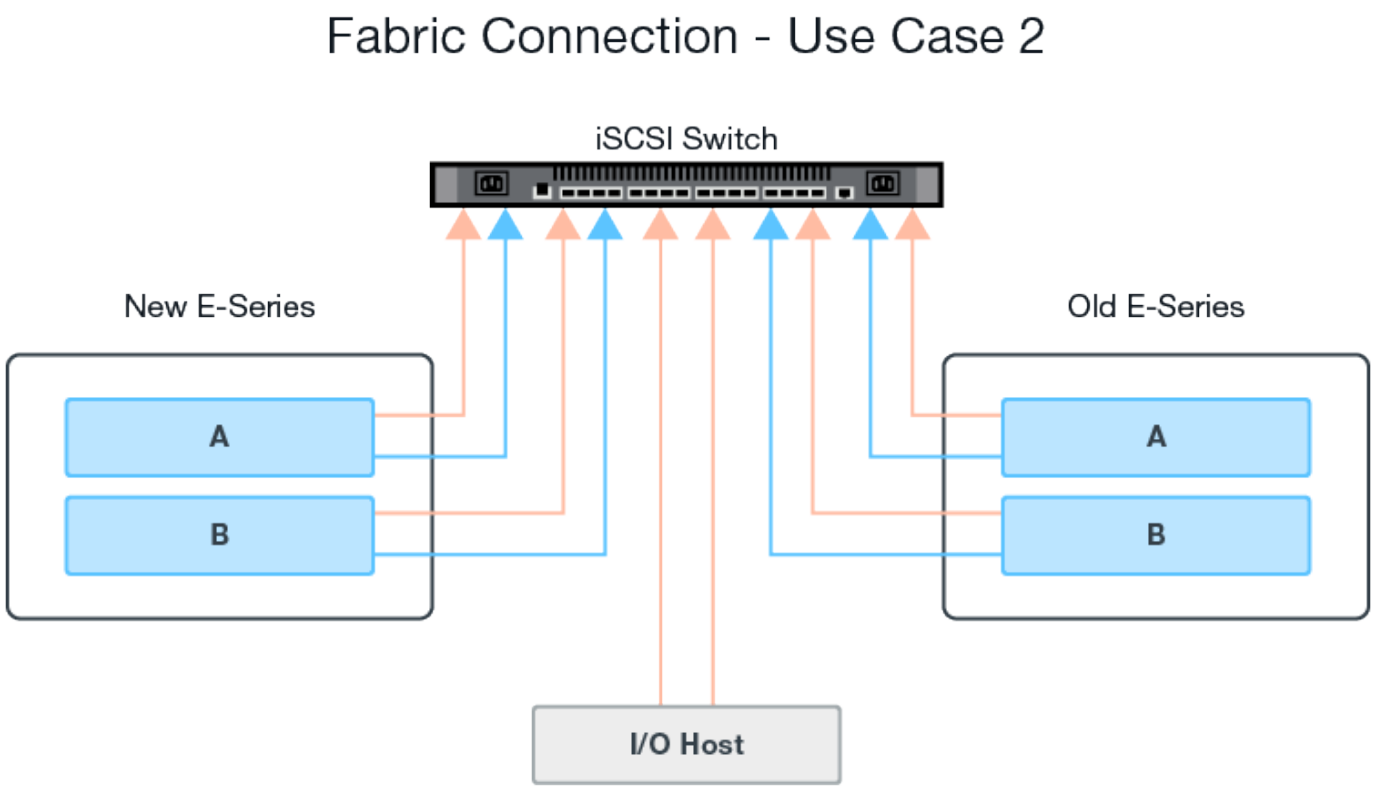
> Consigliato: Eseguire il backup del volume di origine remoto prima di avviare il processo di importazione.

Cablare gli array di storage

Nell'ambito del processo di configurazione, gli array di storage e l'host i/o devono essere cablati all'interfaccia compatibile con iSCSI.

I seguenti diagrammi forniscono esempi di come collegare i sistemi in modo che eseguano operazioni Remote Storage Volume su una connessione iSCSI.





Configurare le porte iSCSI

È necessario configurare le porte iSCSI per garantire la comunicazione tra la destinazione (array di storage locale e-Series) e l'origine (array di storage remoto).

Le porte iSCSI possono essere configurate in più modi in base alla subnet. Di seguito sono riportati alcuni esempi su come configurare le porte iSCSI per l'utilizzo con la funzione Remote Storage Volumes.

Fonte A.	Fonte B	Destinazione A	Destinazione B
10.10.1.100/22	10.10.2.100/22	10.10.1.101/22	10.10.2.101/22

Fonte A.	Fonte B	Destinazione A	Destinazione B
10.10.0.100/16	10.10.0.100/16	10.10.0.101/16	10.10.0.101/16

Importa storage remoto

Per avviare un'importazione dello storage da un sistema remoto a un sistema storage e-Series locale, utilizzare la procedura guidata di importazione dello storage remoto nell'interfaccia utente di Gestore di sistema di SANtricity.

Di cosa hai bisogno

- Il sistema storage e-Series deve essere configurato per comunicare con il sistema storage remoto. Vedere "Configurare l'hardware".

- Per il sistema di storage remoto, raccogliere le seguenti informazioni:
  - IQN iSCSI
  - Indirizzi IP iSCSI
  - Numero LUN del dispositivo di storage remoto (volume di origine)
- Per il sistema storage e-Series locale, creare o selezionare un volume da utilizzare per l'importazione dei dati. Il volume di destinazione deve soddisfare i seguenti requisiti:
  - Corrisponde alle dimensioni del blocco del dispositivo di storage remoto (il volume di origine).
  - Ha una capacità uguale o superiore al dispositivo di storage remoto.
  - Ha uno stato di ottimale ed è disponibile. Per un elenco completo dei requisiti, vedere "Requisiti e limitazioni".
- Consigliato: Eseguire il backup dei volumi sul sistema di storage remoto prima di avviare il processo di importazione.

A proposito di questa attività

In questa attività, viene creata una mappatura tra il dispositivo di storage remoto e un volume sul sistema di storage e-Series locale. Al termine della configurazione, viene avviata l'importazione.

> Poiché molte variabili possono influire sull'operazione di importazione e sui tempi di completamento, è necessario eseguire prima importazioni di "test" più piccole. Utilizzare questi test per assicurarsi che tutte le connessioni funzionino come previsto e che l'operazione di importazione venga completata in un intervallo di tempo appropriato.

Fasi

1. Da Gestione sistema di SANtricity, fare clic su **Storage > Storage remoto**.
2. Fare clic su **Importa storage remoto**.

   Viene visualizzata una procedura guidata per l'importazione dello storage remoto.

3. Nella fase 1a del pannello Configure Source (Configura origine), immettere le informazioni di connessione.

   a. Nel campo **Nome**, immettere il nome del dispositivo di storage remoto.

   b. Sotto **iSCSI Connection properties** (Proprietà connessione iSCSI), immettere quanto segue per il dispositivo di storage remoto: IQN, indirizzo IP e numero di porta (il valore predefinito è 3260).

      Se si desidera aggiungere un'altra connessione iSCSI, fare clic su **+Aggiungi un altro indirizzo IP** per includere un indirizzo IP aggiuntivo per lo storage remoto. Al termine, fare clic su **Avanti**.

   Dopo aver fatto clic su Next (Avanti), viene visualizzata la fase 1b del pannello Configure Source (Configura origine).

4. Nel campo **LUN**, selezionare il LUN di origine desiderato per il dispositivo di storage remoto, quindi fare clic su **Avanti**.

   Viene visualizzato il pannello Configure Target (Configura destinazione) che visualizza i volumi candidati da utilizzare come destinazione per l'importazione. Alcuni volumi non vengono visualizzati nell'elenco dei candidati a causa delle dimensioni dei blocchi, della capacità o della disponibilità dei volumi.

5. Dalla tabella, selezionare un volume di destinazione nel sistema storage e-Series. Se necessario, utilizzare il dispositivo di scorrimento per modificare la priorità di importazione. Fare clic su **Avanti**. Confermare

l'operazione nella finestra di dialogo successiva digitando `continue`, Quindi fare clic su **continua**.

Se il volume di destinazione ha una capacità superiore a quella del volume di origine, tale capacità aggiuntiva non viene segnalata all'host connesso al sistema e-Series. Per utilizzare la nuova capacità, è necessario eseguire un'operazione di espansione del file system sull'host dopo il completamento dell'operazione di importazione e la disconnessione.

Dopo aver confermato la configurazione nella finestra di dialogo, viene visualizzato il pannello Review (Revisione).

6. Dalla schermata Review (Revisione), verificare che le impostazioni relative al dispositivo di storage remoto, alla destinazione e all'importazione siano corrette. Fare clic su **fine** per completare la creazione dello storage remoto.

   Viene visualizzata un'altra finestra di dialogo che chiede se si desidera avviare un'altra importazione.

7. Se necessario, fare clic su **Sì** per creare un'altra importazione di storage remoto. Facendo clic su Yes (Sì) si torna alla fase 1a del pannello Configure Source (Configura origine), in cui è possibile selezionare la configurazione esistente o aggiungerne una nuova. Se non si desidera creare un'altra importazione, fare clic su **No** per uscire dalla finestra di dialogo.

   Una volta avviato il processo di importazione, l'intero volume di destinazione viene sovrascritto con i dati copiati. Se l'host scrive nuovi dati nel volume di destinazione durante questo processo, tali nuovi dati vengono propagati nuovamente al dispositivo remoto (volume di origine).

8. Visualizzare l'avanzamento dell'operazione nella finestra di dialogo View Operations (Visualizza operazioni) sotto il pannello Remote Storage (archiviazione remota).

   Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del sistema di storage remoto, dall'impostazione della priorità per l'importazione e dalla quantità di carico i/o su entrambi i sistemi storage e sui volumi associati. Una volta completata l'importazione, il volume locale è un duplicato del dispositivo di storage remoto.

9. Quando si è pronti a interrompere la relazione tra i due volumi, selezionare **Disconnect** nell'oggetto di importazione dalla vista Operations in Progress (operazioni in corso). Una volta disconnessa la relazione, le prestazioni del volume locale tornano alla normalità e non sono più influenzate dalla connessione remota.

Gestire l'avanzamento dell'importazione

Una volta avviato il processo di importazione, è possibile visualizzare e intraprendere azioni in merito.

Per ogni operazione di importazione, la pagina Operations in Progress (operazioni in corso) visualizza una percentuale di completamento e il tempo rimanente stimato. Le azioni includono la modifica della priorità di importazione, l'interruzione e la ripresa delle operazioni e la disconnessione dall'operazione.

> È inoltre possibile visualizzare le operazioni in corso dalla home page (**Home > Mostra operazioni in corso**).

Fasi

1. In Gestore di sistema di SANtricity, accedere alla pagina Storage remoto e selezionare **Visualizza operazioni**.

Viene visualizzata la finestra di dialogo Operations in Progress (operazioni in corso).

2. Se lo si desidera, utilizzare i collegamenti nella colonna Actions (azioni) per interrompere e riprendere, modificare la priorità o disconnettersi da un'operazione.
   - **Cambia priorità** – selezionare **Cambia priorità** per modificare la priorità di elaborazione di un'operazione in corso o in sospeso. Applicare una priorità all'operazione, quindi fare clic su **OK**.
   - **Stop** – selezionare **Stop** per sospendere la copia dei dati dal dispositivo di storage remoto. La relazione tra la coppia di importazione è ancora intatta ed è possibile selezionare **Riprendi** quando si è pronti per continuare l'operazione di importazione.
   - **Riprendi** – selezionare **Riprendi** per avviare un processo interrotto o non riuscito da dove è stato interrotto. Quindi, applicare una priorità all'operazione di ripresa, quindi fare clic su **OK**.

     L'operazione di ripresa **non** riavvia l'importazione dall'inizio. Se si desidera riavviare il processo dall'inizio, selezionare **Disconnect** (Disconnetti), quindi ricreare l'importazione mediante la procedura guidata di importazione dello storage remoto.
   - **Disconnect** – selezionare **Disconnect** per interrompere la relazione tra i volumi di origine e di destinazione per un'operazione di importazione interrotta, completata o non riuscita.

Modificare le impostazioni di connessione dello storage remoto

È possibile modificare, aggiungere o eliminare le impostazioni di connessione per qualsiasi configurazione di storage remoto tramite l'opzione View/Edit Settings (Visualizza/Modifica impostazioni).

Le modifiche apportate alle proprietà della connessione influiscono sulle importazioni in corso. Per evitare interruzioni, apportare modifiche alle proprietà della connessione solo quando le importazioni non sono in esecuzione.

Fasi

1. Dalla schermata archiviazione remota di Gestione sistema SANtricity, selezionare l'oggetto di archiviazione remota desiderato nella sezione Result list (elenco risultati).
2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la schermata Remote Storage Settings (Impostazioni storage remoto).
3. Fare clic sulla scheda **Connection Properties** (Proprietà connessione).

   Vengono visualizzati l'indirizzo IP configurato e le impostazioni della porta per l'importazione dello storage remoto.
4. Eseguire una delle seguenti operazioni:
   - **Edit** (Modifica) – fare clic su **Edit** (Modifica) accanto alla voce corrispondente per l'oggetto storage remoto. Inserire l'indirizzo IP e/o le informazioni sulla porta modificati nei campi.
   - **Aggiungi** – fare clic su **Aggiungi**, quindi inserire il nuovo indirizzo IP e le informazioni sulla porta nei campi forniti. Fare clic su **Aggiungi** per confermare, quindi la nuova connessione viene visualizzata nell'elenco degli oggetti di storage remoto.
   - **Delete** (Elimina) – selezionare la connessione desiderata dall'elenco, quindi fare clic su **Delete** (Elimina). Confermare l'operazione digitando `delete` Nel campo fornito, quindi fare clic su **Delete** (Elimina). La connessione viene rimossa dall'elenco degli oggetti di storage remoto.

5. Fare clic su **Save** (Salva).

   Le impostazioni di connessione modificate vengono applicate all'oggetto storage remoto.

Rimuovere l'oggetto storage remoto

Una volta completata l'importazione, è possibile rimuovere un oggetto di storage remoto se non si desidera più copiare i dati tra i dispositivi locali e remoti.

Fasi

1. Assicurarsi che nessuna importazione sia associata all'oggetto di storage remoto che si intende rimuovere.
2. Dalla schermata archiviazione remota di Gestione sistema SANtricity, selezionare l'oggetto di archiviazione remota desiderato nella sezione Result list (elenco risultati).
3. Fare clic su **Rimuovi**.

   Viene visualizzata la finestra di dialogo Conferma rimozione connessione storage remoto.

4. Confermare l'operazione digitando `remove` Quindi fare clic su **Rimuovi**.

   L'oggetto Remote Storage selezionato viene rimosso.

Plug-in di storage per vCenter

Panoramica dello Storage Plugin per vCenter

Il plug-in di storage SANtricity per vCenter offre una gestione integrata degli array di storage e-Series dall'interno di una sessione del client VMware vSphere.

Attività disponibili

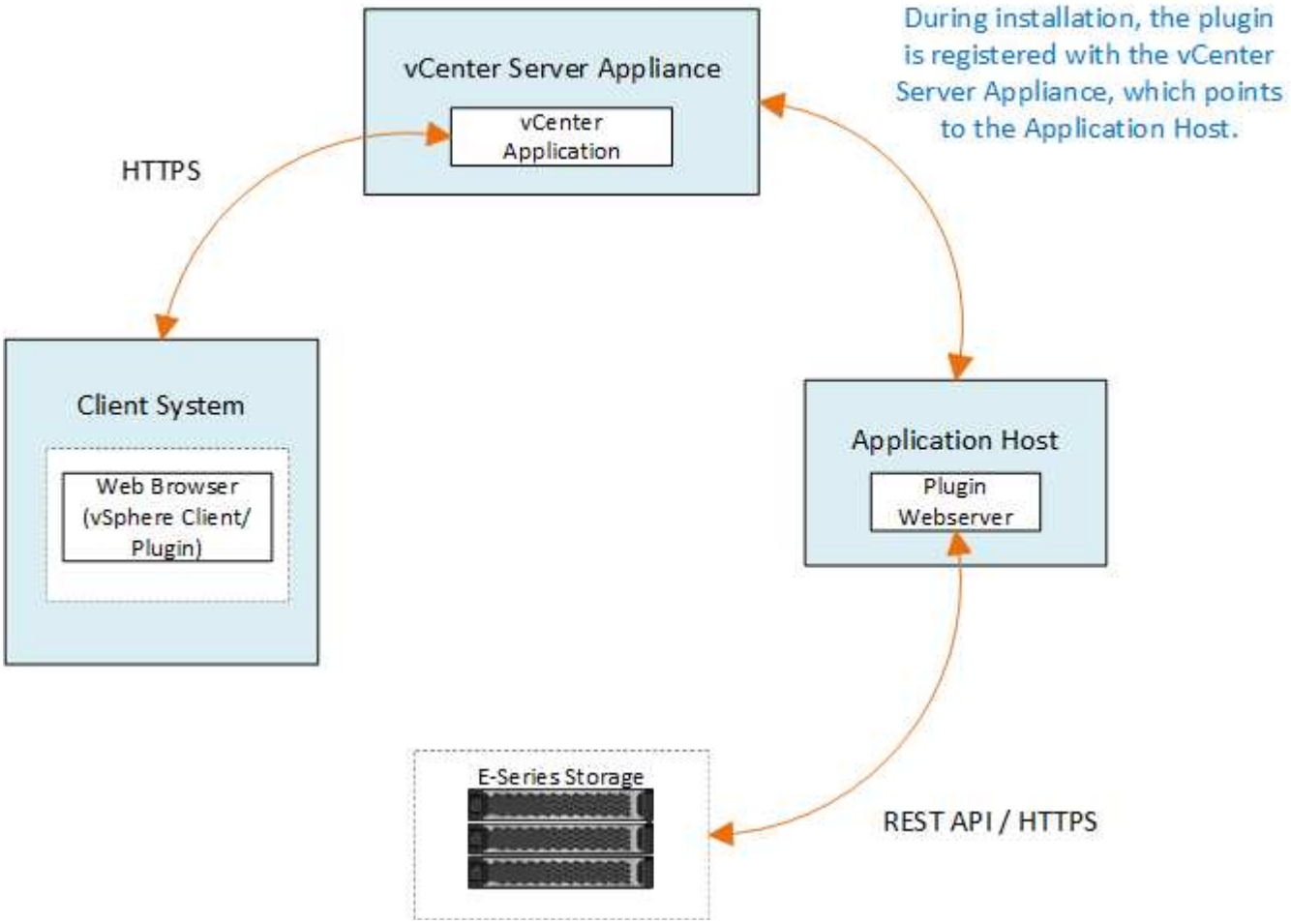
È possibile utilizzare il plug-in per eseguire le seguenti operazioni:

- Visualizzare e gestire gli array di storage rilevati in rete.
- Eseguire operazioni batch su gruppi di più array di storage.
- Eseguire gli aggiornamenti sul sistema operativo del software.
- Importare le impostazioni da uno storage array a un altro.
- Configurare volumi, cache SSD, host, cluster di host, pool, e gruppi di volumi.
- Avviare l'interfaccia di System Manager per ulteriori attività di gestione su un array.

> Il plug-in non sostituisce direttamente l'interfaccia di System Manager, integrata in ciascun controller per uno storage array. System Manager offre funzionalità di gestione aggiuntive; se lo si desidera, è possibile aprire System Manager selezionando un array di storage nella vista principale del plug-in e facendo clic su **Launch**.

Il plug-in richiede un'appliance VMware vCenter Server implementata nell'ambiente VMware e un host dell'applicazione per installare ed eseguire il webserver plug-in.

Fare riferimento alla figura seguente per ulteriori informazioni sulle comunicazioni nell'ambiente vCenter.



Panoramica dell'interfaccia

Quando si accede al plug-in, la pagina principale si apre su **Manage - All** (Gestisci - tutto). Da questa pagina è possibile visualizzare e gestire tutti gli array di storage rilevati nella rete.

Barra laterale di navigazione

La barra laterale di navigazione visualizza quanto segue:

- **Gestisci** — rileva gli array di storage nella tua rete, avvia System Manager per un array, importa le impostazioni da un array a più array, gestisci i gruppi di array, aggiorna il sistema operativo SANtricity ed esegui il provisioning dello storage.
- **Certificate Management** — Gestione dei certificati per l'autenticazione tra browser e client.
- **Operations** — consente di visualizzare l'avanzamento delle operazioni batch, ad esempio l'importazione di impostazioni da un array a un altro.

> Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.

- **Supporto** — Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

Browser supportati

È possibile accedere allo Storage Plugin per vCenter da diversi tipi di browser. Sono supportati i seguenti browser e versioni.

- Google Chrome 89 o versione successiva
- Mozilla Firefox 80 o versione successiva
- Microsoft Edge 90 o versione successiva

Ruoli e autorizzazioni degli utenti

Per accedere alle attività nel plug-in di storage per vCenter, l'utente deve disporre dei permessi di lettura/scrittura. Per impostazione predefinita, tutti gli ID utente VMware vCenter definiti non dispongono di autorizzazioni per eseguire le attività nel plug-in.

Panoramica della configurazione

La configurazione prevede i seguenti passaggi:

1. "Installare e registrare il plug-in".
2. "Configurare i permessi di accesso al plug-in".
3. "Accedere all'interfaccia del plug-in".
4. "Scopri gli array di storage".
5. "Eseguire il provisioning dello storage".

Trova ulteriori informazioni

Per ulteriori informazioni sulla gestione dei datastore nel client vSphere, vedere "Documentazione VMware vSphere".

Inizia subito

Verifica dei requisiti di installazione e aggiornamento

Prima di installare o aggiornare il plug-in di storage SANtricity per vCenter, esaminare i requisiti di installazione e le considerazioni sull'aggiornamento.

Requisiti di installazione

È possibile installare e configurare Storage Plugin per vCenter su un sistema host Windows. L'installazione del plug-in include i seguenti requisiti.

Requisito	Descrizione
Versioni supportate	• Versioni supportate di VMware vCenter Server Appliance: 6.7U3J, 7.0U1, 7.0U2, 7.0U3 e 8.0. • Versione del sistema operativo NetApp SANtricity: 11.60.2 o superiore • Versioni degli host delle applicazioni supportate: Windows 2016, Windows 2019, Windows 2022. Per ulteriori informazioni sulla compatibilità, consultare "Tool di matrice di interoperabilità NetApp".

Requisito	Descrizione
Istanze multiple	È possibile installare solo un'istanza di Storage Plugin per vCenter su un host Windows e registrarla solo su un vCSA.
Pianificazione della capacità	Storage Plugin per vCenter richiede uno spazio adeguato per l'esecuzione e la registrazione. Assicurarsi che il sistema soddisfi i seguenti requisiti di spazio disponibile su disco: • Spazio di installazione richiesto: 275 MB • Spazio di storage: 275 MB + 200 MB (registrazione) • Memoria di sistema: 1.5 GB
Licenza	Lo Storage Plugin per vCenter è un prodotto standalone gratuito che non richiede una chiave di licenza. Tuttavia, si applicano i copyright e i termini del servizio applicabili.

Considerazioni sull'upgrade

Se si esegue l'aggiornamento da una versione precedente, tenere presente che il plug-in deve essere disregistrato da vCSA prima dell'aggiornamento.

- Durante l'aggiornamento, la maggior parte delle impostazioni di configurazione precedenti del plug-in vengono mantenute. Queste impostazioni includono password utente, tutti i sistemi di storage rilevati, certificati server, certificati attendibili e configurazione del runtime del server.
- Il processo di aggiornamento non conserva i file **vcenter.properties**, pertanto è necessario annullare la registrazione del plug-in prima dell'aggiornamento. Una volta completato l'aggiornamento, è possibile registrare nuovamente il plug-in nella vCSA.
- Tutti i file SANtricity OS precedentemente caricati nel repository vengono rimossi durante l'aggiornamento.

Installare o aggiornare il plug-in di storage per vCenter

Per installare Storage Plugin per vCenter e verificare la registrazione del plug-in, procedere come segue. È anche possibile aggiornare il plug-in seguendo queste istruzioni.

Verificare i prerequisiti per l'installazione

Assicurarsi che i sistemi soddisfino i requisiti di "Verifica dei requisiti di installazione e aggiornamento".

> Il processo di aggiornamento non conserva i file **vcenter.properties**. Se si esegue l'aggiornamento, è necessario annullare la registrazione del plug-in prima dell'aggiornamento. Una volta completato l'aggiornamento, è possibile registrare nuovamente il plug-in nella vCSA.

Installare il software del plug-in

Per installare il software del plug-in:

1. Copiare il file del programma di installazione nell'host che verrà utilizzato come server applicazioni, quindi accedere alla cartella in cui è stato scaricato il programma di installazione.

2. Fare doppio clic sul file di installazione:

   ```
   santricity_storage_vcenterplugin-windows_x64-- nn.nn.nn.nnnn.exe
   ```

   Nel nome file sopra indicato, `nn.nn.nn.nnnn` rappresenta il numero di versione.

3. All'avvio dell'installazione, seguire le istruzioni visualizzate sullo schermo per attivare diverse funzioni e immettere alcuni parametri di configurazione. Se necessario, è possibile modificare una di queste selezioni in un secondo momento nei file di configurazione.

   Durante un aggiornamento, non vengono richiesti i parametri di configurazione.

   Durante l'installazione, viene richiesto di eseguire la convalida del certificato. Mantenere la casella di controllo selezionata se si desidera applicare la convalida del certificato tra il plug-in e gli array di storage. Con questa applicazione, i certificati dell'array di storage vengono verificati per essere considerati attendibili rispetto al plug-in. Se i certificati non sono attendibili, non è consentito aggiungerli al plug-in. Se si desidera eseguire l'override della convalida del certificato, deselezionare la casella di controllo in modo che tutti gli array di storage possano essere aggiunti al plug-in utilizzando certificati autofirmati. Per ulteriori informazioni sui certificati, consultare la guida in linea disponibile nell'interfaccia del plug-in.

4. Quando viene visualizzato il messaggio Webserver Started (Server Web avviato), fare clic su **OK** per completare l'installazione, quindi fare clic su **Done** (fine).
5. Verificare che il server applicazioni sia stato installato correttamente eseguendo il comando **Services.msc**.
6. Verificare che il servizio del server applicazioni (VCP), **plug-in storage NetApp SANtricity per vCenter**, sia stato installato e che il servizio sia stato avviato.

   Se necessario, è possibile modificare le impostazioni di convalida certificato e porta servizio Web dopo l'installazione. Dalla directory di installazione, aprire il file wsconfig.xml. Per rimuovere la convalida del certificato sugli array di storage, modificare `env` chiave, `trust.all.arrays`, a. `true`. Per modificare la porta dei servizi Web, modificare `sslport` valore sul valore della porta desiderato compreso tra 0 e 65535. Assicurarsi che il numero di porta utilizzato non sia vincolante per un altro processo. Al termine, salvare le modifiche e riavviare il server Web del plug-in. Se il valore della porta del webserver del plug-in viene modificato dopo la registrazione del plug-in in vCSA, è necessario annullare la registrazione e registrare nuovamente il plug-in in modo che vCSA stia comunicando al webserver del plug-in sulla porta modificata.

Registrare il plug-in con un'appliance vCenter Server

Una volta installato il software del plug-in, registrare il plug-in con un vCSA.

Il plug-in può essere registrato solo su una vCSA alla volta. Per effettuare la registrazione a un vCSA diverso, è necessario annullare la registrazione del plug-in dal vCSA corrente e disinstallarlo dall'host dell'applicazione. È quindi possibile reinstallare il plug-in e registrarlo sull'altro vCSA.

1. Aprire un prompt dalla riga di comando e accedere alla seguente directory:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Eseguire il file **vcenter-register.bat**:
```
vcenter-register.bat ^
-action registerPlugin ^
-vcenterHostname <vCenter FQDN> ^
-username <Administrator username> ^
```
3. Verificare che lo script sia stato eseguito correttamente.

I registri vengono salvati in `%install_dir%/working/logs/vc-registration.log`.

Verificare la registrazione del plug-in

Dopo aver installato il plug-in e aver eseguito lo script di registrazione, verificare che il plug-in sia stato registrato correttamente con vCenter Server Appliance.

1. Aprire il client vSphere sull'appliance vCenter Server.
2. Nella barra dei menu, selezionare **Administrator › Client Plugin**.
3. Assicurarsi che Storage Plugin per vCenter sia elencato come **Enabled**.

   Se il plug-in è elencato come Disabled (Disattivato) e viene visualizzato un messaggio di errore che indica che non è possibile comunicare con l'application server, verificare che il numero di porta definito per l'application server sia abilitato a passare attraverso eventuali firewall in uso. Il numero di porta TCP (Transmission Control Protocol) del server applicazioni predefinito è 8445.

Configurare i permessi di accesso al plug-in

È possibile configurare le autorizzazioni di accesso per lo Storage Plugin per vCenter, che include utenti, ruoli e privilegi.

Esaminare i privilegi vSphere richiesti

Per accedere al plug-in nel client vSphere, è necessario assegnare un ruolo con i privilegi vSphere appropriati. Gli utenti con il privilegio vSphere "Configura datastore" hanno accesso in lettura/scrittura al plug-in, mentre gli utenti con il privilegio "Sfoglia datastore" hanno accesso in sola lettura. Se un utente non dispone di questi privilegi, il plug-in visualizza il messaggio "privilegi insufficienti".

Tipo di accesso al plug-in	È richiesto il privilegio vSphere
Lettura/scrittura (configurazione)	Datastore.Configure
Sola lettura (visualizzazione)	Datastore.Browse

Configurare i ruoli di Storage Administrator

Per fornire privilegi di lettura/scrittura agli utenti dei plug-in, è possibile creare, clonare o modificare un ruolo. Per ulteriori informazioni sulla configurazione dei ruoli nel client vSphere, consultare il seguente argomento nel VMware Doc Center:

- "Creare un ruolo personalizzato"

Accedere alle azioni dei ruoli

1. Dalla home page di vSphere Client, selezionare **Administrator** dall'area di controllo degli accessi.

2. Fare clic su **Roles** nell'area di controllo degli accessi.
3. Eseguire una delle seguenti operazioni:
   - **Crea nuovo ruolo**: Fare clic sull'icona dell'azione **Crea ruolo**.
   - **Clone role**: Selezionare un ruolo esistente e fare clic sull'icona dell'azione **Clone role**.
   - **Modifica ruolo esistente**: Selezionare un ruolo esistente e fare clic sull'icona dell'azione **Modifica ruolo**.

> Il ruolo di amministratore non è modificabile.

Viene visualizzata la procedura guidata appropriata, a seconda della selezione precedente.

Creare un nuovo ruolo

1. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

2. Assegnare altri privilegi all'elenco, se necessario, quindi fare clic su **Avanti**.
3. Assegnare un nome al ruolo e fornire una descrizione.
4. Fare clic su **fine**.

Clonare un ruolo

1. Assegnare un nome al ruolo e fornire una descrizione.
2. Fare clic su **OK** per terminare la procedura guidata.
3. Selezionare il ruolo clonato dall'elenco, quindi fare clic su **Edit role** (Modifica ruolo).
4. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

5. Fare clic su **Avanti**.
6. Aggiornare il nome e la descrizione, se necessario.
7. Fare clic su **fine**.

Modificare un ruolo esistente

1. Nell'elenco dei privilegi, selezionare le autorizzazioni di accesso da assegnare a questo ruolo.

   Per consentire l'accesso in sola lettura al plug-in, selezionare **Archivio dati › Sfoglia archivio dati**. Per consentire l'accesso in lettura/scrittura, selezionare **datastore › Configure datastore**.

2. Fare clic su **Avanti**.
3. Aggiornare il nome o la descrizione, se necessario.
4. Fare clic su **fine**.

Impostare le autorizzazioni per vCenter Server Appliance

Dopo aver impostato i privilegi per un ruolo, è necessario aggiungere un'autorizzazione all'appliance vCenter Server. Questa autorizzazione consente a un determinato utente o gruppo di accedere al plug-in.

1. Dall'elenco a discesa del menu, selezionare **hosts and Clusters** (host e cluster).
2. Selezionare **vCenter Server Appliance** dall'area di controllo degli accessi.
3. Fare clic sulla scheda **Permissions**.
4. Fare clic sull'icona dell'azione **Add Permission**.
5. Selezionare il dominio e l'utente/gruppo appropriati.
6. Selezionare il ruolo creato che consente il privilegio del plug-in di lettura/scrittura.
7. Attivare l'opzione **propaga ai figli**, se necessario.
8. Fare clic su **OK**.

> È possibile selezionare un'autorizzazione esistente e modificarla per utilizzare il ruolo creato. **Tuttavia, tenere presente che il ruolo deve avere gli stessi privilegi insieme ai privilegi del plug-in di lettura/scrittura per evitare una regressione dei permessi.**

Per accedere al plug-in, è necessario accedere a vSphere Client con l'account utente che dispone dei privilegi di lettura/scrittura per il plug-in.

Per ulteriori informazioni sulla gestione delle autorizzazioni, consultare i seguenti argomenti in VMware Doc Center:

- "Gestione delle autorizzazioni per i componenti vCenter"
- "Best practice per ruoli e autorizzazioni"

Accedere e navigare nel plug-in di storage per vCenter

È possibile accedere allo Storage Plugin per vCenter per navigare nell'interfaccia utente.

1. Prima di accedere al plug-in, assicurarsi di utilizzare uno dei seguenti browser:
   - Google Chrome 89 o versione successiva
   - Mozilla Firefox 80 o versione successiva
   - Microsoft Edge 90 o versione successiva
2. Accedere al client vSphere con l'account utente che dispone dei privilegi di lettura/scrittura per il plug-in.
3. Dalla home page del client vSphere, fare clic su **plug-in di storage SANtricity per vCenter**.

   Il plug-in si apre all'interno di una finestra del client vSphere. La pagina principale del plugin si apre su **Manage-All**.

4. Accedi alle attività di gestione dello storage dalla barra laterale di navigazione a sinistra:
   - **Gestisci** – rileva gli array di storage nella tua rete, apri System Manager per un array, importa le impostazioni da un array a più array, gestisci i gruppi di array, aggiorna il software del sistema operativo e esegui il provisioning dello storage.
   - **Certificate Management** – Gestisci i certificati per l'autenticazione tra browser e client.
   - **Operazioni** – consente di visualizzare l'avanzamento delle operazioni batch, ad esempio

l'importazione di impostazioni da un array a un altro.

- **Supporto** – Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

> Alcune operazioni non sono disponibili quando uno storage array ha uno stato non ottimale.

Rilevare gli array di storage nel plug-in

Per visualizzare e gestire le risorse di storage, è necessario utilizzare l'interfaccia Storage Plugin for vCenter per rilevare gli indirizzi IP degli array nella rete.

Prima di iniziare

- È necessario conoscere gli indirizzi IP di rete (o l'intervallo di indirizzi) degli array controller.
- Gli array di storage devono essere configurati e configurati correttamente, nonché conoscere le credenziali di accesso (nome utente e password).

Fase 1: Inserire gli indirizzi di rete per il rilevamento

Fasi

1. Dalla pagina Gestisci, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Immetti intervallo indirizzi di rete.

2. Effettuare una delle seguenti operazioni:
   - Per rilevare un array, selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage), quindi immettere l'indirizzo IP di uno dei controller dell'array di storage.
   - Per rilevare più array di storage, selezionare il pulsante di opzione **Discover all storage array in a network range** (rileva tutti gli array di storage all'interno di un intervallo di rete), quindi immettere l'indirizzo di rete iniziale e l'indirizzo di rete finale per eseguire la ricerca nella sottorete locale.

3. Fare clic su **Avvia rilevamento**.

   All'inizio del processo di rilevamento, la finestra di dialogo visualizza gli array di storage rilevati. Il completamento del processo di rilevamento potrebbe richiedere alcuni minuti.

   Se non vengono rilevati array gestibili, verificare che gli array di storage siano collegati correttamente alla rete e che gli indirizzi assegnati rientrino nell'intervallo. Fare clic su **New Discovery Parameters** (nuovi parametri di rilevamento) per tornare alla pagina Add/Discover (Aggiungi/rileva).

4. Selezionare la casella di controllo accanto a qualsiasi array di storage che si desidera aggiungere al dominio di gestione.

   Il sistema esegue un controllo delle credenziali su ogni array che si sta aggiungendo al dominio di gestione. Prima di procedere, potrebbe essere necessario risolvere eventuali problemi relativi ai certificati non attendibili.

5. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

   Se gli array di storage dispongono di certificati validi, passare a. Fase 3: Fornire le password.

   Se gli array di storage non dispongono di certificati validi, viene visualizzata la finestra di dialogo Risolvi certificati autofirmati. Passare a. Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento.

   Se si desidera importare i certificati firmati dalla CA, annullare la procedura guidata di rilevamento e fare

clic su **Certificate Management** (Gestione certificati) nel pannello a sinistra. Per ulteriori informazioni, consultare la guida in linea.

Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento

È necessario risolvere eventuali problemi di certificato prima di procedere con il processo di rilevamento.

1. Se viene visualizzata la finestra di dialogo Risolvi certificati autofirmati, esaminare le informazioni visualizzate per i certificati non attendibili. Per ulteriori informazioni, fare clic sui puntini di sospensione all'estremità della tabella e selezionare **View** (Visualizza) dal menu a comparsa.
2. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, fare clic su **Avanti**, quindi su **Sì** per confermare e passare alla finestra di dialogo successiva della procedura guidata. I certificati autofirmati sono contrassegnati come attendibili e gli array di storage vengono aggiunti al plug-in.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una.
3. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.

Fase 3: Fornire le password

Come ultimo passaggio per il rilevamento, è necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

1. Per ogni array rilevato, inserire la password admin nei campi.
2. Fare clic su **fine**.

   Il sistema può impiegare diversi minuti per connettersi agli array di storage specificati. Al termine del processo, gli array di storage vengono aggiunti al dominio di gestione e associati al gruppo selezionato (se specificato).

Eseguire il provisioning dello storage nel plug-in

Per eseguire il provisioning dello storage, è necessario creare volumi, assegnare volumi agli host e assegnare volumi agli archivi dati.

Fase 1: Creazione di volumi

I volumi sono container di dati che gestiscono e organizzano lo spazio di storage sull'array di storage. È possibile creare volumi dalla capacità di storage disponibile sull'array di storage, che consente di organizzare le risorse del sistema. Il concetto di "volumi" è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso rapido.

I volumi sono l'unico livello di dati visibile agli host. In un ambiente SAN, i volumi vengono mappati ai LUN (Logical Unit Number). Queste LUN conservano i dati utente accessibili mediante uno o più protocolli di accesso host supportati dallo storage array.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › Volumes** (Crea[volumi]).

Viene visualizzata la finestra di dialogo Select host (Seleziona host).

4. Dall'elenco a discesa, selezionare un host o un cluster host specifico al quale assegnare i volumi oppure scegliere di assegnare l'host o il cluster host in un secondo momento.
5. Per continuare la sequenza di creazione del volume per l'host o il cluster host selezionato, fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro). Un carico di lavoro contiene volumi con caratteristiche simili, ottimizzati in base al tipo di applicazione supportata dal carico di lavoro. È possibile definire un carico di lavoro o selezionare i carichi di lavoro esistenti.

6. Effettuare una delle seguenti operazioni:
   - Selezionare l'opzione **Create Volumes for a existing workload** (Crea volumi per un carico di lavoro esistente), quindi selezionare il carico di lavoro dall'elenco a discesa.
   - Selezionare l'opzione **Create a new workload** (Crea nuovo carico di lavoro) per definire un nuovo carico di lavoro per un'applicazione supportata o per altre applicazioni, quindi attenersi alla seguente procedura:
     i. Dall'elenco a discesa, selezionare il nome dell'applicazione per cui si desidera creare il nuovo workload. Selezionare una delle "altre" voci se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.
     ii. Immettere un nome per il carico di lavoro che si desidera creare.
7. Fare clic su **Avanti**. Se il carico di lavoro è associato a un tipo di applicazione supportato, inserire le informazioni richieste; in caso contrario, passare alla fase successiva.

   Viene visualizzata la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi). In questa finestra di dialogo vengono creati volumi da pool o gruppi di volumi idonei. Per ciascun pool e gruppo di volumi idonei, vengono visualizzati il numero di dischi disponibili e la capacità libera totale. Per alcuni carichi di lavoro specifici dell'applicazione, ciascun pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e la capacità libera rimanente in GiB. Per gli altri carichi di lavoro, la capacità proposta viene visualizzata quando si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

8. Prima di iniziare ad aggiungere volumi, leggere le linee guida riportate nella seguente tabella.

Campo	Descrizione
Capacità libera	Poiché i volumi vengono creati da pool o gruppi di volumi, il pool o il gruppo di volumi selezionato deve disporre di capacità libera sufficiente.

Campo	Descrizione
Data Assurance (da)	Per creare un volume abilitato da, la connessione host che si intende utilizzare deve supportare da. • Se si desidera creare un volume abilitato da, selezionare un pool o un gruppo di volumi che supporti da (cercare **Sì** accanto a "da" nella tabella dei candidati del pool e del gruppo di volumi). • Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi. LA protezione DA verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. La selezione di un pool o di un gruppo di volumi da-capable per il nuovo volume garantisce il rilevamento e la correzione degli errori. • Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.
Sicurezza dei dischi	Per creare un volume abilitato alla protezione, è necessario creare una chiave di sicurezza per l'array di storage. • Se si desidera creare un volume abilitato alla protezione, selezionare un pool o un gruppo di volumi che supporti la protezione (cercare **Sì** accanto a "abilitato alla protezione" nella tabella dei candidati del gruppo di volumi e del pool). • Le funzionalità di sicurezza dei dischi vengono presentate a livello di pool e gruppo di volumi. I dischi con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Un disco abilitato alla sicurezza crittografa i dati durante la scrittura e decrta i dati durante la lettura utilizzando una chiave di crittografia univoca. • Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
Provisioning delle risorse	Per creare un volume con provisioning di risorse, tutti i dischi devono essere dischi NVMe con l'opzione Deallocated o Unwritten Logical Block Error (DULBE).

9. Scegliere una di queste azioni a seconda che sia stato selezionato "Altro" o un carico di lavoro specifico dell'applicazione nella fase precedente:

   - **Altro** – fare clic su **Aggiungi nuovo volume** in ciascun pool o gruppo di volumi che si desidera utilizzare per creare uno o più volumi.
   - **Carico di lavoro specifico dell'applicazione** – fare clic su **Avanti** per accettare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato.

     Vengono visualizzati i seguenti campi.

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. La capacità in un pool viene allocata in incrementi di 4-GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Tipo di volume	Se si seleziona "carico di lavoro specifico dell'applicazione", viene visualizzato il campo Volume Type (tipo di volume). Indica il tipo di volume creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • da 512 a 512 byte • 4K – 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** – il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi con cache SSD**: È possibile specificare una dimensione dei segmenti 4 KiB per i volumi con cache SSD. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** – il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi del pool o del gruppo di volumi sono compatibili con la crittografia. Drive Security impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione Drive Security è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

10. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti**.
11. Nell'ultimo passaggio, esaminare un riepilogo dei volumi che si intende creare e apportare le modifiche necessarie. Per apportare modifiche, fare clic su **Indietro**. Quando si è soddisfatti della configurazione del volume, fare clic su **fine**.

Fase 2: Creazione dell'accesso host e assegnazione dei volumi

È possibile creare un host automaticamente o manualmente:

- **Automatico** — la creazione automatica dell'host per gli host basati su SCSI (non NVMe-of) viene avviata dall'HCA (host Context Agent). HCA è un'utility che è possibile installare su ciascun host collegato allo storage array. Ogni host su cui è installato l'HCA invia le informazioni di configurazione ai controller degli array di storage attraverso il percorso i/O. In base alle informazioni sull'host, i controller creano automaticamente l'host e le porte host associate e impostano il tipo di host. Se necessario, è possibile apportare ulteriori modifiche alla configurazione dell'host. Dopo che l'HCA ha eseguito il rilevamento automatico, l'host viene configurato automaticamente con i seguenti attributi:
  - Il nome host derivato dal nome di sistema dell'host.
  - Le porte di identificazione host associate all'host.
  - Il tipo di sistema operativo host dell'host.

> Il software host Context Agent per Linux e Windows è disponibile all'interno del sito "Supporto NetApp - Download".

> Gli host vengono creati come host standalone; l'HCA non crea o aggiunge automaticamente ai cluster di host.

- **Manuale** – durante la creazione manuale dell'host, è possibile associare gli identificatori delle porte host selezionandoli da un elenco o inserendoli manualmente. Dopo aver creato un host, è possibile assegnarvi dei volumi o aggiungerlo a un cluster host se si intende condividere l'accesso ai volumi.

Utilizzo di HCA per rilevare automaticamente l'host

È possibile consentire all'HCA (host Context Agent) di rilevare automaticamente gli host, quindi verificare che le informazioni siano corrette.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare **Storage › Hosts** (Storage[host]).

   La tabella elenca gli host creati automaticamente.

4. Verificare che le informazioni fornite dall'HCA siano corrette (nome, tipo di host, identificatori della porta host).
5. Per modificare le informazioni, selezionare l'host, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

Creazione manuale dell'host

Prima di iniziare

Leggi le seguenti linee guida:

- È necessario aver già aggiunto o rilevato gli array di storage all'interno dell'ambiente.
- È necessario definire le porte di identificazione host associate all'host.
- Assicurarsi di fornire lo stesso nome del nome di sistema assegnato all'host.
- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Fare clic sul **Create › host** (Crea[host]).

   Viene visualizzata la finestra di dialogo Create host (Crea host).

4. Selezionare le impostazioni per l'host in base alle esigenze.

Campo	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare il sistema operativo in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia host	(Facoltativo) se si dispone di più tipi di interfaccia host supportati sull'array di storage, selezionare il tipo di interfaccia host che si desidera utilizzare.

Campo	Descrizione
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare l'interfaccia i/o** — in genere, le porte host devono essere state registrate ed essere disponibili dall'elenco a discesa. È possibile selezionare gli identificatori della porta host dall'elenco. • **Aggiunta manuale** — se un identificatore di porta host non viene visualizzato nell'elenco, significa che la porta host non ha effettuato l'accesso. È possibile utilizzare un'utility HBA o l'utility iSCSI Initiator per individuare gli identificatori delle porte host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dall'utility (uno alla volta) nel campo host ports (Porte host). È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori associati all'host. Ciascun identificatore viene visualizzato nel campo host ports (Porte host). Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto.
Impostare CHAP Initiator secret	(Facoltativo) se si seleziona o si immette manualmente una porta host con un IQN iSCSI e si desidera richiedere a un host che tenta di accedere all'array di storage per l'autenticazione mediante il protocollo CHAP (Challenge Handshake Authentication Protocol), selezionare la casella di controllo **Set CHAP Initiator secret** (Imposta CHAP initiator secret). Per ogni porta host iSCSI selezionata o inserita manualmente, procedere come segue: • Immettere lo stesso segreto CHAP impostato su ciascun iniziatore host iSCSI per l'autenticazione CHAP. Se si utilizza l'autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di validarsi nell'array di storage e a un array di storage di validarsi nell'host), è necessario impostare anche il segreto CHAP per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lasciare vuoto il campo se non si richiede l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato è CHAP.

5. Fare clic su **Create** (Crea).
6. Per aggiornare le informazioni sull'host, selezionare l'host dalla tabella e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Una volta creato correttamente l'host, il sistema crea un nome predefinito per ciascuna porta host configurata per l'host (etichetta utente). L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per l'host IPT è `IPT_1`.

7. Quindi, è necessario assegnare un volume a un host o a un cluster di host in modo che possa essere utilizzato per le operazioni di i/O. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

8. Selezionare l'host o il cluster host a cui si desidera assegnare i volumi, quindi fare clic su **Assign Volumes**

(Assegna volumi).

Viene visualizzata una finestra di dialogo che elenca tutti i volumi che è possibile assegnare. È possibile ordinare qualsiasi colonna o digitare qualcosa nella casella Filter (filtro) per semplificare la ricerca di volumi specifici.

9. Selezionare la casella di controllo accanto a ciascun volume che si desidera assegnare oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
10. Fare clic su **Assegna** per completare l'operazione.

    Il sistema esegue le seguenti operazioni:

    - Il volume assegnato riceve il successivo numero LUN disponibile. L'host utilizza il numero LUN per accedere al volume.
    - Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host. Se applicabile, il volume di accesso configurato in fabbrica viene visualizzato anche negli elenchi dei volumi associati all'host.

Fase 3: Creazione di un datastore in vSphere Client

Per creare un datastore nel client vSphere, vedere "Creare un datastore VMFS nel client vSphere" Argomento di VMware Doc Center.

Aumentare la capacità del datastore esistente aumentando la capacità del volume

È possibile aumentare la capacità riportata (la capacità riportata agli host) di un volume utilizzando la capacità libera disponibile nel pool o nel gruppo di volumi.

Prima di iniziare

Assicurarsi che:

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associati al volume.
- Il volume è ottimale e non in alcun stato di modifica.
- Nel volume non sono in uso dischi hot spare. (Si applica solo ai volumi nei gruppi di volumi).

> L'aumento della capacità di un volume è supportato solo su alcuni sistemi operativi. Se si aumenta la capacità del volume su un sistema operativo host che non supporta l'espansione LUN, la capacità espansa non è utilizzabile e non è possibile ripristinare la capacità del volume originale.

Fasi

1. Accedere al plug-in in vSphere Client.
2. All'interno del plug-in, selezionare l'array di storage desiderato.
3. Fare clic su **Provisioning** e selezionare **Manage Volumes** (Gestisci volumi).
4. Selezionare il volume per il quale si desidera aumentare la capacità, quindi selezionare **aumenta capacità**.

   Viene visualizzata la finestra di dialogo Conferma aumento capacità.

5. Selezionare **Sì** per continuare.

Viene visualizzata la finestra di dialogo aumenta capacità riportata.

Questa finestra di dialogo visualizza la capacità corrente del volume riportata e la capacità libera disponibile nel gruppo di volumi o pool associato al volume.

6. Utilizzare la casella **aumenta capacità segnalata aggiungendo…** per aggiungere capacità alla capacità corrente disponibile indicata. È possibile modificare il valore della capacità in modo che venga visualizzato in megibyte (MiB), gibibyte (GiB) o tebibyte (TIB).
7. Fare clic su **aumenta**.
8. Visualizzare il pannello Recent Tasks (attività recenti) per l'avanzamento dell'operazione di aumento della capacità attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.
9. Una volta completata la capacità del volume, è necessario aumentare manualmente le dimensioni VMFS in modo che corrispondano come descritto nella "Aumentare la capacità del datastore VMFS nel client vSphere" Argomento di VMware Doc Center.

Aumentare la capacità del datastore esistente aggiungendo volumi

1. È possibile aumentare la capacità di un datastore aggiungendo volumi. Seguire la procedura descritta in Fase 1: Creazione di volumi.
2. Quindi, assegnare i volumi all'host desiderato per aumentare la capacità del datastore.

   Vedere "Aumentare la capacità del datastore VMFS nel client vSphere" Per ulteriori informazioni, consultare l'argomento di VMware Doc Center.

Visualizzare lo stato

È possibile visualizzare lo stato del sistema dal plugin Storage per vCenter o dal client vSphere.

1. Aprire il plug-in dal client vSphere.
2. Visualizzare lo stato dai seguenti pannelli:
   - **Stato array di storage** — Vai al pannello **Gestisci-tutto**. Per ogni array rilevato, la riga fornisce una colonna Status (Stato).
   - **Operazioni in corso** — fare clic su **operazioni** sul pannello laterale per visualizzare tutte le attività in esecuzione a lungo, ad esempio l'importazione delle impostazioni. È inoltre possibile visualizzare le operazioni a esecuzione prolungata dall'elenco a discesa Provisioning. Per ciascuna operazione elencata nella finestra di dialogo Operations in Progress (operazioni in corso), vengono visualizzate una percentuale di completamento e il tempo stimato rimanente per completare l'operazione. In alcuni casi, è possibile interrompere un'operazione o posizionarla con priorità più alta o più bassa. Se lo si desidera, utilizzare i collegamenti nella colonna Actions (azioni) per interrompere o modificare la priorità di un'operazione.

> Leggere tutto il testo di avviso fornito nelle finestre di dialogo, in particolare quando si interrompe un'operazione.

Le operazioni che potrebbero essere visualizzate per il plug-in sono elencate nella seguente tabella. È possibile che nell'interfaccia di System Manager vengano visualizzate operazioni aggiuntive.

Operazione	Stato possibile dell'operazione	Azioni da intraprendere
Creazione di volumi (solo volumi thick pool superiori a 64 TiB)	In corso	nessuno
Eliminazione del volume (solo volumi thick pool superiori a 64 TiB)	In corso	nessuno
Aggiungere capacità al pool o al gruppo di volumi	In corso	nessuno
Modificare un livello RAID per un volume	In corso	nessuno
Ridurre la capacità di un pool	In corso	nessuno
Verificare il tempo rimanente per un'operazione con formato di disponibilità istantanea (IAF) per i volumi del pool	In corso	nessuno
Controllare la ridondanza dei dati di un gruppo di volumi	In corso	nessuno
Inizializzare un volume	In corso	nessuno
Aumentare la capacità di un volume	In corso	nessuno
Modificare le dimensioni dei segmenti di un volume	In corso	nessuno

Gestire i certificati

Panoramica dei certificati

Gestione dei certificati nel plug-in di storage per vCenter consente di creare richieste di firma dei certificati (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I certificati sono file digitali che identificano entità online, come siti Web e server, per comunicazioni sicure su Internet. Garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privatamente e inalterate, solo tra il server e il client specificati. Utilizzando Storage Plugin per vCenter, è possibile gestire i certificati per il browser su un sistema di gestione host e i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità attendibile o autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e determinato che i loro dispositivi possono essere affidabili.

Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. È possibile continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati dalla CA per una connessione più sicura tra i controller e i sistemi host.

Sebbene i certificati firmati dalla CA forniscano una migliore protezione di sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), richiedono anche tariffe che possono essere costose se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

Certificati firmati

Un certificato firmato viene convalidato da un'autorità di certificazione (CA), un'organizzazione di terze parti fidata. I certificati firmati includono i dettagli sul proprietario dell'entità (in genere, un server o un sito Web), la data di emissione e scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando si apre un browser e si inserisce un indirizzo Web, il sistema esegue un processo di verifica dei certificati in background per determinare se si sta effettuando la connessione a un sito Web che include un certificato valido firmato dalla CA. In genere, un sito protetto con un certificato firmato include un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se si tenta di connettersi a un sito Web che non contiene un certificato firmato dalla CA, il browser visualizza un avviso che indica che il sito non è sicuro.

La CA esegue le operazioni necessarie per verificare l'identità dell'utente durante il processo dell'applicazione. Potrebbero inviare un'e-mail all'azienda registrata, verificare l'indirizzo aziendale ed eseguire una verifica HTTP o DNS. Una volta completato il processo applicativo, la CA invia i file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di attendibilità, come segue:

- **Root** — nella parte superiore della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. La directory principale identifica un'organizzazione CA specifica. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedio** — i certificati intermedi si disconnettono dalla radice. La CA emette uno o più certificati intermedi per fungere da intermediario tra certificati di server e root protetti.
- **Server** — nella parte inferiore della catena si trova il certificato del server, che identifica l'entità specifica dell'utente, ad esempio un sito Web o un altro dispositivo. Ogni controller di uno storage array richiede un certificato server separato.

Certificati autofirmati

Ogni controller dell'array di storage include un certificato preinstallato e autofirmato. Un certificato autofirmato è simile a un certificato firmato dalla CA, ad eccezione del fatto che è convalidato dal proprietario dell'entità anziché da una terza parte. Come un certificato firmato dalla CA, un certificato autofirmato contiene una propria chiave privata e garantisce inoltre che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client.

I certificati autofirmati non sono "attendibili" dai browser. Ogni volta che si tenta di connettersi a un sito Web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di accedere al sito Web; in questo modo, si accetta essenzialmente il certificato autofirmato.

Certificato di gestione

Quando si apre il plug-in, il browser tenta di verificare che l'host di gestione sia un'origine attendibile verificando la presenza di un certificato digitale. Se il browser non individua un certificato firmato dalla CA, viene visualizzato un messaggio di avviso. Da qui, è possibile accedere al sito Web per accettare il certificato autofirmato per la sessione. È inoltre possibile ottenere certificati digitali firmati da una CA, in modo da non visualizzare più il messaggio di avviso.

Certificati attendibili

Durante una sessione di plug-in, potrebbero essere visualizzati ulteriori messaggi di sicurezza quando si tenta di accedere a un controller che non dispone di un certificato firmato dalla CA. In questo caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati dalla CA per i controller in modo che il plug-in possa autenticare le richieste dei client in entrata da questi controller.

USA certificati firmati dalla CA

È possibile ottenere e importare certificati con firma CA per un accesso sicuro al sistema di gestione che ospita lo Storage Plugin per vCenter.

L'utilizzo dei certificati firmati dalla CA è una procedura in tre fasi:

- Fase 1: Completare un file CSR.
- Fase 2: Inviare il file CSR.
- Fase 3: Importazione dei certificati di gestione.

Fase 1: Completare un file CSR

È necessario innanzitutto generare un file CSR (Certificate Signing Request) che identifichi l'organizzazione e il sistema host in cui è in esecuzione il plug-in. In alternativa, è possibile generare un file CSR utilizzando uno strumento come OpenSSL e passare a. Fase 2: Inviare il file CSR.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **completa CSR**.
3. Inserire le seguenti informazioni, quindi fare clic su **Avanti**:
   - **Organizzazione** — il nome completo e legale della tua azienda o organizzazione. Includere i suffissi, ad esempio Inc. O Corp.
   - **Unità organizzativa (opzionale)** — la divisione dell'organizzazione che gestisce il certificato.
   - **Città/Località** — la città in cui si trova il sistema host o l'azienda.
   - **Stato/Regione (opzionale)** — Stato o regione in cui si trova il sistema host o l'azienda.
   - **Codice ISO del Paese** — Codice ISO (International Organization for Standardization) a due cifre del Paese, ad esempio USA.
4. Immettere le seguenti informazioni sul sistema host in cui è in esecuzione il plug-in:
   - **Nome comune** — l'indirizzo IP o il nome DNS del sistema host in cui è in esecuzione il plug-in. Assicurarsi che questo indirizzo sia corretto; deve corrispondere esattamente a quello immesso per accedere al plug-in nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi** — se il nome comune è un indirizzo IP, è possibile inserire eventuali indirizzi IP o alias aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole.
   - **Nomi DNS alternativi** — se il nome comune è un nome DNS, immettere eventuali nomi DNS aggiuntivi per il sistema host. Per più voci, utilizzare un formato delimitato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato immesso un nome DNS nel primo campo, copiarlo qui. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurarsi che le informazioni sull'host siano corrette. In caso contrario, i certificati restituiti dalla CA non avranno esito positivo quando si tenta di importarli.

6. Fare clic su **fine**.

Fase 2: Inviare il file CSR

Dopo aver creato un file CSR (Certificate Signing Request), il file CSR generato viene inviato a una CA per ricevere certificati di gestione firmati per il sistema che ospita il plug-in.

I sistemi e-Series richiedono il formato PEM (codifica ASCII Base64) per i certificati firmati, che include i seguenti tipi di file: .Pem, .crt, .cer o .key.

Fasi

1. Individuare il file CSR scaricato.

   La posizione della cartella del download dipende dal browser in uso.

2. Inviare il file CSR a una CA (ad esempio, VeriSign o DigiCert) e richiedere certificati firmati in formato PEM.

   Dopo aver inviato un file CSR alla CA, NON rigenerare un altro file CSR.

Ogni volta che si genera una CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte della CSR, mentre la chiave privata viene conservata nell'archivio chiavi del sistema. Quando si ricevono i certificati firmati e li si importano, il sistema garantisce che sia la chiave privata che la chiave pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno ed è necessario richiedere nuovi certificati alla CA.

Fase 3: Importazione dei certificati di gestione

Una volta ricevuti i certificati firmati dall'autorità di certificazione (CA), importare i certificati nel sistema host in cui è installato il plug-in.

Prima di iniziare

- È necessario disporre dei certificati firmati dalla CA. Questi file includono il certificato di origine, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di certificato concatenato (ad esempio, un file .p7b), è necessario decomprimere il file concatenato in singoli file: Il certificato root, uno o più certificati intermedi e il certificato del server. È possibile utilizzare l'utility Windows certmgr per decomprimere i file (fare clic con il pulsante destro del mouse e selezionare **All Tasks › Export**). Si consiglia la codifica base-64. Una volta completate le esportazioni, viene visualizzato un file CER per ciascun file di certificato nella catena.
- È necessario copiare i file dei certificati nel sistema host in cui è in esecuzione il plug-in.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Gestione**, selezionare **Importa**.

   Viene visualizzata una finestra di dialogo per l'importazione dei file dei certificati.

3. Fare clic su **Browse** (Sfoglia) per selezionare prima i file dei certificati root e intermedi, quindi selezionare il certificato del server. Se la CSR è stata generata da uno strumento esterno, è necessario importare anche il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fare clic su **Importa**.

Risultato

I file vengono caricati e validati. Le informazioni sul certificato vengono visualizzate nella pagina Gestione certificati.

Reimpostare i certificati di gestione

Per il sistema di gestione che ospita lo Storage Plugin per vCenter, è possibile riportare il certificato di gestione allo stato originale autofirmato.

A proposito di questa attività

Questa attività elimina il certificato di gestione corrente dal sistema host in cui è in esecuzione Storage Plugin per vCenter. Una volta ripristinato il certificato, il sistema host torna a utilizzare il certificato autofirmato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Dalla scheda **Management**, selezionare **Reset**.

   Viene visualizzata la finestra di dialogo Conferma ripristino certificato di gestione.

3. Digitare reset nel campo, quindi fare clic su **Reset**.

   Dopo l'aggiornamento del browser, il browser potrebbe bloccare l'accesso al sito di destinazione e segnalare che il sito utilizza HTTP Strict Transport Security. Questa condizione si verifica quando si torna ai certificati autofirmati. Per eliminare la condizione che sta bloccando l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultato

Il sistema torna a utilizzare il certificato autofirmato dal server. Di conseguenza, il sistema richiede agli utenti di accettare manualmente il certificato autofirmato per le sessioni.

Importare certificati per gli array

Se necessario, è possibile importare i certificati per gli array di storage in modo che possano autenticarsi con il sistema che ospita lo Storage Plugin per vCenter. I certificati possono essere firmati da un'autorità di certificazione (CA) o autofirmati.

Prima di iniziare

Se si importano certificati attendibili, è necessario importarli per i controller degli array di storage utilizzando System Manager.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

   Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.

4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato e fare clic su **Importa**.

   Il certificato viene caricato e validato.

Visualizzare i certificati

È possibile visualizzare informazioni riepilogative per un certificato, che includono l'organizzazione che utilizza il certificato, l'autorità che ha emesso il certificato, il periodo di validità e le impronte digitali (identificatori univoci).

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Per visualizzare ulteriori informazioni su un certificato, selezionare la relativa riga, selezionare i puntini di sospensione alla fine della riga, quindi fare clic su **Visualizza** o **Esporta**.

Esportare i certificati

È possibile esportare un certificato per visualizzarne i dettagli completi.

Prima di iniziare

Per aprire il file esportato, è necessario disporre di un'applicazione per il visualizzatore dei certificati.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il plugin. Un certificato di gestione può essere autofirmato o approvato da un'autorità di certificazione (CA). Consente un accesso sicuro al plug-in.
   - **Trusted** — Mostra i certificati ai quali il plug-in può accedere per gli array di storage e altri server remoti, come un server LDAP. I certificati possono essere emessi da un'autorità di certificazione (CA) o autofirmati.
3. Selezionare un certificato dalla pagina, quindi fare clic sui puntini di sospensione alla fine della riga.
4. Fare clic su **Esporta**, quindi salvare il file del certificato.
5. Aprire il file nell'applicazione di visualizzazione dei certificati.

Eliminare i certificati attendibili

È possibile eliminare uno o più certificati non più necessari, ad esempio un certificato

scaduto.

Prima di iniziare

Importare il nuovo certificato prima di eliminarlo.

> Tenere presente che l'eliminazione di un certificato root o intermedio può influire su più array di storage, poiché questi array possono condividere gli stessi file di certificato.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.
3. Selezionare uno o più certificati nella tabella, quindi fare clic su **Elimina**.

   > La funzione Elimina non è disponibile per i certificati preinstallati.

   Viene visualizzata la finestra di dialogo Conferma eliminazione certificato attendibile.

4. Confermare l'eliminazione, quindi fare clic su **Delete** (Elimina).

   Il certificato viene rimosso dalla tabella.

Risolvi i certificati non attendibili

Dalla pagina Certificate (certificato), è possibile risolvere i certificati non attendibili importando un certificato autofirmato dall'array di storage o importando un certificato dell'autorità di certificazione (CA) emesso da una terza parte attendibile.

Prima di iniziare

Se si intende importare un certificato firmato dalla CA, assicurarsi che:

- È stata generata una richiesta di firma del certificato (file CSR) per ciascun controller nell'array di storage e inviata alla CA.
- La CA ha restituito file di certificato attendibili.
- I file dei certificati sono disponibili nel sistema locale.

A proposito di questa attività

I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura al plug-in, ma la connessione non viene confermata come sicura. Potrebbe essere necessario installare altri certificati CA attendibili se si verifica una delle seguenti condizioni:

- Di recente è stato aggiunto uno storage array.
- Uno o entrambi i certificati sono scaduti o revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Fasi

1. Selezionare **Certificate Management** (Gestione certificati).
2. Selezionare la scheda **Trusted**.

Questa pagina mostra tutti i certificati segnalati per gli array di storage.

3. Selezionare il **Importa › certificati** per importare un certificato CA oppure il **Importa › certificati array storage autofirmati** per importare un certificato autofirmato.
4. Per limitare la visualizzazione, è possibile utilizzare il campo di filtraggio **Mostra certificati…** oppure ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.
5. Nella finestra di dialogo, selezionare il certificato, quindi fare clic su **Importa**.

   Il certificato viene caricato e validato.

Gestire gli array

Panoramica sulla gestione degli array

Utilizzare la funzione Add/Discover per trovare e aggiungere gli array di storage che si desidera gestire nel plug-in Storage per vCenter. Dalla pagina Manage (Gestione), è possibile rinominare, rimuovere e fornire nuove password per gli array rilevati.

Considerazioni per il rilevamento degli array

Affinché il plug-in visualizzi e gestisca le risorse di storage, è necessario individuare gli array di storage che si desidera gestire nella rete aziendale. È possibile rilevare e aggiungere un singolo array o più array.

Array di storage multipli

Se si sceglie di rilevare più array, immettere un intervallo di indirizzi IP di rete e il sistema tenta di stabilire connessioni individuali a ciascun indirizzo IP dell'intervallo. Qualsiasi array di storage raggiunto correttamente viene visualizzato nel plug-in ed è possibile aggiungerlo al dominio di gestione.

Singolo storage array

Se si sceglie di rilevare un singolo array, immettere l'indirizzo IP singolo per uno dei controller nell'array di storage e aggiungerlo al dominio di gestione.

> Il plug-in rileva e visualizza solo il singolo indirizzo IP o indirizzo IP all'interno di un intervallo assegnato a un controller. Se a questi controller sono assegnati controller alternativi o indirizzi IP che non rientrano in questo singolo indirizzo IP o intervallo di indirizzi IP, il plug-in non li rileva o li visualizza. Tuttavia, una volta aggiunto lo storage array, tutti gli indirizzi IP associati vengono rilevati e visualizzati nella vista Manage (Gestione).

Credenziali dell'utente

Specificare la password di amministratore per ciascun array di storage che si desidera aggiungere.

Certificati

Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage rilevati stiano utilizzando certificati da un'origine attendibile. Il sistema utilizza due tipi di autenticazione basata su certificati per tutte le connessioni stabilite con il browser:

- **Certificati attendibili** — potrebbe essere necessario installare altri certificati attendibili forniti dall'autorità di certificazione se uno o entrambi i certificati del controller sono scaduti, revocati o mancanti nella relativa

catena.

- **Certificati autofirmati** — gli array possono anche utilizzare certificati autofirmati. Se si tenta di rilevare gli array senza importare certificati firmati, il plug-in fornisce un'ulteriore fase che consente di accettare il certificato autofirmato. Il certificato autofirmato dell'array di storage viene contrassegnato come attendibile e l'array di storage viene aggiunto al plug-in. Se le connessioni all'array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia del certificato di sicurezza dell'array di storage prima di aggiungere l'array di storage al plug-in.

Stato dello storage array

Quando si apre Storage Plugin per vCenter, viene stabilita la comunicazione con ciascun array di storage e viene visualizzato lo stato di ciascun array di storage.

Dalla pagina **Gestisci - tutto**, è possibile visualizzare lo stato dello storage array e lo stato della connessione dello storage array.

Stato	Indica
Ottimale	Lo storage array si trova in uno stato ottimale. Non ci sono problemi di certificato e la password è valida.
Password non valida	È stata fornita una password dello storage array non valida.
Certificato non attendibile	Una o più connessioni con lo storage array non sono attendibili perché il certificato HTTPS è autofirmato e non è stato importato oppure il certificato è firmato dalla CA e i certificati CA principali e intermedi non sono stati importati.
Richiede attenzione	Si è verificato un problema con lo storage array che richiede l'intervento dell'utente per correggerlo.
Blocco	Lo storage array si trova in uno stato bloccato.
Sconosciuto	Lo storage array non è mai stato contattato. Questo può accadere quando il plug-in si avvia e non è ancora entrato in contatto con lo storage array, oppure lo storage array non è in linea e non è mai stato contattato dall'avvio del plug-in.
Offline	Il plug-in aveva precedentemente contattato lo storage array, ma ora ha perso tutte le connessioni.

Interfaccia plug-in rispetto a System Manager

È possibile utilizzare Storage Plugin per vCenter per le attività operative di base sull'array di storage; tuttavia, in alcuni casi potrebbe essere necessario avviare System Manager per eseguire attività non disponibili nel plug-in.

System Manager è un'applicazione integrata nel controller dello storage array, collegata alla rete tramite una porta di gestione Ethernet. System Manager include tutte le funzioni basate su array.

La seguente tabella consente di decidere se utilizzare l'interfaccia del plug-in o l'interfaccia di System Manager per una specifica attività di array di storage.

Funzione	Interfaccia del plugin	Interfaccia di System Manager
Operazioni in batch su gruppi di array storage multipli	Sì	No Le operazioni vengono eseguite su un singolo array.
Aggiornamenti per il firmware del sistema operativo SANtricity	Sì. Uno o più array in un'operazione batch.	Sì. Solo array singolo.
Importa le impostazioni da un array a più array	Sì	No
Gestione dei cluster host e host (creazione, assegnazione di volumi, aggiornamento ed eliminazione)	Sì	Sì
Gestione di pool e gruppi di volumi (creazione, aggiornamento, attivazione della protezione ed eliminazione)	Sì	Sì
Gestione dei volumi (creazione, ridimensionamento, aggiornamento ed eliminazione)	Sì	Sì
Gestione della cache SSD (creazione, aggiornamento ed eliminazione)	Sì	Sì
Mirroring e gestione delle snapshot	No	Sì
Gestione dell'hardware (visualizzare lo stato del controller, configurare le connessioni delle porte, portare il controller offline, abilitare le hot spare, cancellare i dischi, ecc.)	No	Sì
Gestire gli avvisi (e-mail, SNMP e syslog)	No	Sì
Gestione delle chiavi di sicurezza	No	Sì
Gestione dei certificati per i controller	No	Sì
Gestione degli accessi per controller (LDAP, SAML, ecc.)	No	Sì
Gestione di AutoSupport	No	Sì

Scopri gli array di storage

Per visualizzare e gestire le risorse di storage nel plug-in Storage per vCenter, è necessario individuare gli indirizzi IP degli array nella rete.

Prima di iniziare

- È necessario conoscere gli indirizzi IP di rete (o l'intervallo di indirizzi) degli array controller.

- Gli array di storage devono essere configurati e configurati correttamente.
- Le password degli array di storage devono essere impostate utilizzando il riquadro Access Management di System Manager.

A proposito di questa attività

Il rilevamento degli array è una procedura a più fasi:

- Fase 1: Inserire gli indirizzi di rete per il rilevamento
- Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento
- Fase 3: Fornire le password

Fase 1: Inserire gli indirizzi di rete per il rilevamento

Come primo passo per il rilevamento degli array di storage, immettere un singolo indirizzo IP o un intervallo di indirizzi IP per la ricerca nella sottorete locale. La funzione Aggiungi/rileva consente di aprire una procedura guidata che guida l'utente nel processo di rilevamento.

Fasi

1. Dalla pagina **Gestisci**, selezionare **Aggiungi/rileva**.

   Viene visualizzata la finestra di dialogo Immetti intervallo indirizzi di rete.

2. Effettuare una delle seguenti operazioni:
   - Per rilevare un array, selezionare il pulsante di opzione **Discover a single storage array** (rileva un singolo array di storage), quindi immettere l'indirizzo IP di uno dei controller dell'array di storage.
   - Per rilevare più array di storage, selezionare il pulsante di opzione **Discover all storage array in a network range** (rileva tutti gli array di storage all'interno di un intervallo di rete), quindi immettere l'indirizzo di rete iniziale e l'indirizzo di rete finale per eseguire la ricerca nella sottorete locale.
3. Fare clic su **Avvia rilevamento**.

   All'inizio del processo di rilevamento, la finestra di dialogo visualizza gli array di storage rilevati. Il completamento del processo di rilevamento potrebbe richiedere alcuni minuti.

   > Se non vengono rilevati array gestibili, verificare che gli array di storage siano collegati correttamente alla rete e che gli indirizzi assegnati rientrino nell'intervallo. Fare clic su **New Discovery Parameters** (nuovi parametri di rilevamento) per tornare alla pagina Add/Discover (Aggiungi/rileva).

4. Selezionare la casella di controllo accanto a qualsiasi array di storage che si desidera aggiungere al dominio di gestione.

   Il sistema esegue un controllo delle credenziali su ogni array che si sta aggiungendo al dominio di gestione. Prima di procedere, potrebbe essere necessario risolvere eventuali problemi relativi ai certificati non attendibili.

5. Fare clic su **Avanti** per passare alla fase successiva della procedura guidata.
6. Se gli array di storage dispongono di certificati validi, passare a. Fase 3: Fornire le password. Se uno degli array di storage non dispone di certificati validi, viene visualizzata la finestra di dialogo Risolvi certificati autofirmati; passare a. Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento. Se si desidera importare i certificati firmati dalla CA, annullare le finestre di dialogo di rilevamento e accedere a. "Importare certificati per gli array".

Fase 2: Risoluzione dei certificati non attendibili durante il rilevamento

Se necessario, è necessario risolvere eventuali problemi di certificato prima di procedere con il processo di rilevamento.

Durante il rilevamento, se uno degli array di storage mostra lo stato "certificati non attendibili", viene visualizzata la finestra di dialogo Risolvi certificati autofirmati. In questa finestra di dialogo è possibile risolvere i certificati non attendibili oppure importare i certificati CA (vedere "Importare certificati per gli array").

Fasi

1. Se viene visualizzata la finestra di dialogo Risolvi certificati autofirmati, esaminare le informazioni visualizzate per i certificati non attendibili. Per ulteriori informazioni, fare clic sui puntini di sospensione all'estremità della tabella e selezionare **View** (Visualizza) dal menu a comparsa.
2. Effettuare una delle seguenti operazioni:
   - Se le connessioni agli array di storage rilevati sono attendibili, fare clic su **Avanti**, quindi su **Sì** per confermare e passare alla scheda successiva della procedura guidata. I certificati autofirmati verranno contrassegnati come attendibili e gli array di storage verranno aggiunti al plug-in.
   - Se le connessioni agli array di storage non sono attendibili, selezionare **Annulla** e convalidare la strategia di certificato di sicurezza di ciascun array di storage prima di aggiungerne una al plug-in.

Fase 3: Fornire le password

Come ultimo passaggio per il rilevamento, è necessario immettere le password per gli array di storage che si desidera aggiungere al dominio di gestione.

Fasi

1. Se in precedenza sono stati configurati gruppi per gli array, è possibile utilizzare il menu a discesa per selezionare un gruppo per gli array rilevati.
2. Per ogni array rilevato, inserire la password admin nei campi.
3. Fare clic su **fine**.

> Il sistema può impiegare diversi minuti per connettersi agli array di storage specificati.

Risultato

Gli array di storage vengono aggiunti al dominio di gestione e associati al gruppo selezionato (se specificato).

> È possibile utilizzare l'opzione Launch per aprire System Manager basato su browser per uno o più array di storage quando si desidera eseguire operazioni di gestione.

Rinominare l'array di storage

È possibile modificare il nome dello storage array visualizzato nella pagina Manage (Gestione) del plug-in Storage per vCenter.

Fasi

1. Nella pagina **Manage** (Gestisci), selezionare la casella di controllo a sinistra del nome dello storage array.
2. Selezionare i puntini di sospensione all'estrema destra della riga, quindi selezionare **Rename storage array** dal menu a comparsa.
3. Inserire il nuovo nome e fare clic su **Save** (Salva).

Modificare le password degli array di storage

È possibile aggiornare le password utilizzate per visualizzare e accedere agli array di storage nel plug-in Storage per vCenter.

Prima di iniziare

È necessario conoscere la password corrente per lo storage array, impostata in System Manager.

A proposito di questa attività

In questa attività, immettere la password corrente per un array di storage in modo da potervi accedere nel plug-in. Questo potrebbe essere necessario se la password dell'array è stata modificata in System Manager.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare uno o più array di storage.
2. Selezionare **operazioni non comuni › fornire password array di storage**.
3. Immettere la password o le password per ciascun array di storage, quindi fare clic su **Save** (Salva).

Rimuovere gli array di storage

È possibile rimuovere uno o più array di storage se non si desidera più gestirli dallo Storage Plugin per vCenter.

A proposito di questa attività

Non è possibile accedere a nessuno degli array di storage rimossi. Tuttavia, è possibile stabilire una connessione a uno degli array di storage rimossi puntando direttamente un browser all'indirizzo IP o al nome host.

La rimozione di uno storage array non influisce in alcun modo sullo storage array o sui relativi dati. Se uno storage array viene rimosso accidentalmente, può essere aggiunto di nuovo.

Fasi

1. Dalla pagina **Manage** (Gestione), selezionare uno o più array di storage da rimuovere.
2. Selezionare **operazioni non comuni › Rimuovi array di storage**.

   Lo storage array viene rimosso da tutte le viste dell'interfaccia del plugin.

Avviare System Manager

Per gestire un singolo array, utilizzare l'opzione di avvio per aprire Gestione di sistema di SANtricity in una nuova finestra del browser.

System Manager è un'applicazione integrata nel controller dello storage array, collegata alla rete tramite una porta di gestione Ethernet. System Manager include tutte le funzioni basate su array. Per accedere a System Manager, è necessario disporre di una connessione out-of-band a un client di gestione della rete con un browser Web.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare uno o più array di storage che si desidera gestire.
2. Fare clic su **Avvia**.

Il sistema apre una nuova scheda nel browser, quindi visualizza la pagina di accesso di System Manager.

3. Immettere il nome utente e la password, quindi fare clic su **Log in** (Accedi).

Importare le impostazioni

Panoramica delle impostazioni di importazione

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che consente di replicare le impostazioni di un singolo array di storage (l'origine) in più array (le destinazioni) nel plug-in Storage per vCenter.

Impostazioni disponibili per l'importazione

È possibile importare le seguenti configurazioni da un array a un altro:

- **Alerts** — metodi di avviso per inviare eventi importanti agli amministratori utilizzando la posta elettronica, un server syslog o un server SNMP.
- **AutoSupport** — funzionalità che monitora lo stato di salute di uno storage array e invia automaticamente i dispatches al supporto tecnico.
- **Servizi di directory** — metodo di autenticazione dell'utente gestito tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, ad esempio Active Directory di Microsoft.
- **Impostazioni di sistema** — configurazioni relative a:
  - Impostazioni di scansione dei supporti per un volume
  - Impostazioni SSD
  - Bilanciamento automatico del carico (non include il reporting sulla connettività host)
- **Configurazione dello storage** — configurazioni relative a:
  - Volumi (solo volumi thick e non repository)
  - Gruppi di volumi e pool
  - Assegnazioni dei dischi hot spare

Workflow di configurazione

Per importare le impostazioni, seguire questo flusso di lavoro:

1. Su uno storage array da utilizzare come origine, configurare le impostazioni utilizzando System Manager.
2. Sugli array di storage da utilizzare come destinazione, eseguire il backup della configurazione utilizzando System Manager.
3. Dall'interfaccia del plugin, accedere alla pagina **Manage** e importare le impostazioni.
4. Dalla pagina Operations (operazioni), esaminare i risultati dell'operazione Import Settings (Impostazioni di importazione).

Requisiti per la replica delle configurazioni di storage

Prima di importare una configurazione dello storage da uno storage array a un altro, esaminare i requisiti e le linee guida.

Shelf

- Gli shelf in cui risiedono i controller devono essere identici sugli array di origine e di destinazione.
- Gli shelf ID devono essere identici sugli array di origine e di destinazione.
- Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità (se il disco viene utilizzato nella configurazione, la posizione dei dischi inutilizzati non è importante).

Controller

- Il tipo di controller può essere diverso tra gli array di origine e di destinazione, ma il tipo di enclosure RBOD deve essere identico.
- L'HICS, incluse le funzionalità da dell'host, deve essere identico tra gli array di origine e di destinazione.
- L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
- Le impostazioni FDE non sono incluse nel processo di importazione.

Stato

- Gli array di destinazione devono essere nello stato ottimale.
- Non è necessario che l'array di origine sia nello stato ottimale.

Storage

- La capacità del disco può variare tra gli array di origine e di destinazione, a condizione che la capacità del volume sulla destinazione sia superiore a quella dell'origine. (Un array di destinazione potrebbe disporre di unità più recenti e di capacità maggiore che non sarebbero completamente configurate nei volumi dall'operazione di replica).
- Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.

Importare le impostazioni degli avvisi

È possibile importare configurazioni di avviso da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Gli avvisi vengono configurati in System Manager (**Impostazioni › Avvisi**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

È possibile selezionare avvisi e-mail, SNMP o syslog per l'operazione di importazione:

- **Avvisi via email** — Indirizzo del server di posta e indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — Nome di comunità e indirizzo IP per il server SNMP.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Email alerts** (Avvisi email), **SNMP alerts** (Avvisi SNMP) o **Syslog alerts** (Avvisi Syslog), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati per inviare avvisi agli amministratori tramite e-mail, SNMP o syslog.

Importa impostazioni AutoSupport

È possibile importare una configurazione AutoSupport da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- AutoSupport è configurato in Gestione sistema (**supporto › Centro di supporto**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Seleziona impostazioni, selezionare **AutoSupport**, quindi fare clic su **Avanti**.

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni AutoSupport dell'array di origine.

Importare le impostazioni dei servizi di directory

È possibile importare una configurazione di servizi di directory da un array di storage ad altri array di storage. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- I servizi di directory sono configurati in System Manager (**Impostazioni › Gestione accessi**) per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono il nome di dominio e l'URL di un server LDAP (Lightweight Directory

Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Directory Services** (servizi directory), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con gli stessi servizi di directory dell'array di origine.

Importare le impostazioni di sistema

È possibile importare le impostazioni di sistema da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Le impostazioni di sistema sono configurate in System Manager per lo storage array che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".

A proposito di questa attività

Le impostazioni importate includono le impostazioni di scansione dei supporti per un volume, le impostazioni SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **System** (sistema), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con le stesse impostazioni di sistema dell'array di origine.

Importare le impostazioni di configurazione dello storage

È possibile importare la configurazione dello storage da uno storage array ad altri storage array. Questa operazione batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

Assicurarsi che:

- Lo storage viene configurato in System Manager per l'array di storage che si desidera utilizzare come origine.
- Il backup della configurazione esistente per gli array di storage di destinazione viene eseguito in System Manager (**Impostazioni › sistema › Salva configurazione array di storage**).
- Sono stati esaminati i requisiti per la replica delle configurazioni di storage in "Panoramica delle impostazioni di importazione".
- Gli array di origine e di destinazione devono soddisfare i seguenti requisiti:
  - Gli shelf in cui risiedono i controller devono essere identici.
  - Gli ID degli shelf devono essere identici.
  - Gli shelf di espansione devono essere inseriti negli stessi slot con gli stessi tipi di unità.

- Il tipo di enclosure RBOD deve essere identico.
- L'HICS, incluse le funzionalità di Data Assurance dell'host, deve essere identico.
- Gli array di destinazione devono essere nello stato ottimale.
- La capacità del volume sull'array di destinazione è maggiore della capacità dell'array di origine.

- Hai compreso le seguenti restrizioni:
  - L'importazione da una configurazione duplex a una facciata singola non è supportata; tuttavia, è consentita l'importazione da una facciata singola a una facciata fronte/retro.
  - Volumi di pool di dischi di almeno 64 TB sull'array di origine impediranno il processo di importazione sulle destinazioni.

A proposito di questa attività

Le impostazioni importate includono volumi configurati (solo volumi thick e non di repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.

Fasi

1. Dalla pagina Manage (Gestione), fare clic su **Actions › Import Settings** (azioni[Impostazioni importazione]).

   Viene visualizzata la procedura guidata Import Settings (Impostazioni importazione).

2. Nella finestra di dialogo Select Settings (Seleziona impostazioni), selezionare **Storage Configuration** (Configurazione archiviazione), quindi fare clic su **Next** (Avanti).

   Viene visualizzata una finestra di dialogo per la selezione dell'array di origine.

3. Nella finestra di dialogo Select Source (Seleziona origine), selezionare l'array con le impostazioni che si desidera importare, quindi fare clic su **Next** (Avanti).
4. Nella finestra di dialogo Select targets (Seleziona destinazioni), selezionare uno o più array per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se il plug-in non è in grado di comunicare con tale array (ad esempio, se non è in linea o se presenta problemi di certificato, password o rete).

5. Fare clic su **fine**.

   La pagina Operations (operazioni) visualizza i risultati dell'operazione di importazione. Se l'operazione non riesce, fare clic sulla relativa riga per visualizzare ulteriori informazioni.

Risultato

Gli array di storage di destinazione sono ora configurati con la stessa configurazione dello storage dell'array di origine.

Gestire i gruppi di array

Panoramica dei gruppi di array

È possibile gestire l'infrastruttura fisica e virtualizzata nel plug-in di storage per vCenter

raggruppando un set di array di storage. È possibile raggruppare gli array di storage per semplificare l'esecuzione dei processi di monitoraggio o reporting.

Tipi di gruppi di array di storage:

- **Tutti i gruppi** — il gruppo tutti è il gruppo predefinito e include tutti gli array di storage rilevati nell'organizzazione. È possibile accedere al gruppo All dalla vista principale.
- **User-created group** — Un gruppo creato dall'utente include gli array di storage che si selezionano manualmente per aggiungere a quel gruppo. È possibile accedere ai gruppi creati dall'utente dalla vista principale.

Creare un gruppo di array di storage

È possibile creare gruppi di storage e quindi aggiungere array di storage ai gruppi. Il gruppo di storage definisce quali dischi forniscono lo storage che costituisce il volume.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Create storage array group** (Crea gruppo array di storage).
2. Nel campo **Nome**, digitare un nome per il nuovo gruppo.
3. Selezionare gli array di storage che si desidera aggiungere al nuovo gruppo.
4. Fare clic su **Create** (Crea).

Aggiungere array di storage al gruppo

È possibile aggiungere uno o più array di storage a un gruppo creato dall'utente.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo a cui si desidera aggiungere gli array di storage.
2. Selezionare **Manage Groups › Add storage array to group** (Gestisci gruppi[Aggiungi array di storage al gruppo]).
3. Selezionare gli array di storage che si desidera aggiungere al gruppo.
4. Fare clic su **Aggiungi**.

Rinominare il gruppo di array di storage

È possibile modificare il nome di un gruppo di array di storage quando il nome corrente non è più significativo o applicabile.

A proposito di questa attività

Tenere presenti queste linee guida.

- Un nome può essere composto da lettere, numeri e caratteri speciali come sottolineatura (_), trattino (-) e cancelletto (n.). Se si sceglie un altro carattere, viene visualizzato un messaggio di errore. Viene richiesto di scegliere un altro nome.
- Limitare il nome a 30 caratteri. Gli spazi iniziali e finali del nome vengono cancellati.

- Utilizzare un nome univoco e significativo, facile da comprendere e ricordare.
- Evitare nomi o nomi arbitrari che perderebbero rapidamente il loro significato in futuro.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare il gruppo di array di storage che si desidera rinominare.
2. Selezionare **Manage Groups › Rename storage array group** (Gestisci gruppi[Rinomina gruppo array di storage])
3. Nel campo **Nome gruppo**, digitare un nuovo nome per il gruppo.
4. Fare clic su **Rinomina**.

Rimuovere gli array di storage dal gruppo

È possibile rimuovere uno o più array di storage gestiti da un gruppo se non si desidera più gestirli da un gruppo di storage specifico.

A proposito di questa attività

La rimozione degli array di storage da un gruppo non influisce in alcun modo sull'array di storage o sui relativi dati. Se lo storage array è gestito da System Manager, è comunque possibile gestirlo utilizzando il browser. Se uno storage array viene accidentalmente rimosso da un gruppo, può essere aggiunto di nuovo.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare il **Manage Groups (Gestisci gruppi) › Remove storage array from group** (Rimuovi array di storage dal gruppo).
2. Dal menu a discesa, selezionare il gruppo che contiene gli array di storage che si desidera rimuovere, quindi fare clic sulla casella di controllo accanto a ciascun array di storage che si desidera rimuovere dal gruppo.
3. Fare clic su **Rimuovi**.

Eliminare il gruppo di array di storage

È possibile rimuovere uno o più gruppi di array di storage non più necessari.

A proposito di questa attività

Questa operazione elimina solo il gruppo di array di storage. Gli array di storage associati al gruppo cancellato rimangono accessibili tramite la vista Manage All (Gestisci tutti) o qualsiasi altro gruppo a cui è associato.

Fasi

1. Dalla pagina Manage (Gestisci), selezionare **Manage Groups (Gestisci gruppi) › Delete storage array group** (Elimina gruppo array di storage).
2. Selezionare uno o più gruppi di array di storage che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).

Aggiornare il software del sistema operativo

Panoramica sull'aggiornamento

Nel plug-in di storage per vCenter, è possibile gestire il software SANtricity e gli

aggiornamenti DI NVSRAM per più array di storage dello stesso tipo.

Workflow di upgrade

I seguenti passaggi forniscono un workflow di alto livello per l'esecuzione degli aggiornamenti software:

1. È possibile scaricare il file SANtricity OS più recente dal sito di supporto (un collegamento è disponibile nella pagina di supporto). Salvare il file sul sistema host di gestione (l'host in cui si accede al plug-in in un browser), quindi decomprimere il file.
2. Nel plug-in, è possibile caricare il file del software SANtricity OS e IL file NVSRAM nel repository (un'area del server in cui sono memorizzati i file).
3. Una volta caricati i file nel repository, è possibile selezionare il file da utilizzare nell'aggiornamento. Dalla pagina Aggiorna software SANtricity OS, selezionare il file del software del sistema operativo e IL file NVSRAM. Dopo aver selezionato un file software, in questa pagina viene visualizzato un elenco di array di storage compatibili. Selezionare quindi gli array di storage che si desidera aggiornare con il nuovo software. (Non è possibile selezionare array incompatibili).
4. È quindi possibile avviare un trasferimento e un'attivazione software immediati oppure scegliere di preparare i file per l'attivazione in un secondo momento. Durante il processo di aggiornamento, il plug-in esegue le seguenti operazioni:
   - Esegue un controllo dello stato degli array di storage per determinare se esistono condizioni che potrebbero impedire il completamento dell'aggiornamento. Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.
   - Trasferisce i file di aggiornamento a ciascun controller.
   - Riavvia i controller e attiva il nuovo software del sistema operativo, un controller alla volta. Durante l'attivazione, il file del sistema operativo esistente viene sostituito con il nuovo file.

> È inoltre possibile specificare che il software venga attivato in un secondo momento.

Considerazioni sull'upgrade

Prima di eseguire l'upgrade di più array di storage, esaminare le considerazioni chiave come parte della pianificazione.

Versioni correnti

È possibile visualizzare le versioni correnti del software SANtricity OS dalla pagina Gestione del plug-in di storage per vCenter per ciascun array di storage rilevato. La versione viene visualizzata nella colonna Software SANtricity OS. Il firmware del controller e LE informazioni SU NVSRAM sono disponibili in una finestra di dialogo a comparsa quando si fa clic sulla versione del sistema operativo in ciascuna riga.

Altri componenti che richiedono l'aggiornamento

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare il driver multipath/failover dell'host o il driver HBA in modo che l'host possa interagire correttamente con i controller. Per informazioni sulla compatibilità, fare riferimento a. "Tool di matrice di interoperabilità".

Controller doppi

Se uno storage array contiene due controller e si dispone di un driver multipath installato, lo storage array può continuare a elaborare l'i/o durante l'aggiornamento. Durante l'aggiornamento, si verifica la seguente

procedura:

1. Il controller A esegue il failover di tutti i LUN verso il controller B.
2. L'aggiornamento avviene sul controller A.
3. Il controller A riprende i LUN e tutti i LUN del controller B.
4. L'aggiornamento avviene sul controller B.

Al termine dell'aggiornamento, potrebbe essere necessario ridistribuire manualmente i volumi tra i controller per garantire che i volumi tornino al controller proprietario corretto.

Eseguire un controllo dello stato di salute prima dell'aggiornamento

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare. Il controllo dello stato di salute valuta i componenti dello storage array per assicurarsi che l'aggiornamento possa continuare.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › controllo stato pre-aggiornamento**.

   Viene visualizzata la finestra di dialogo Pre-Upgrade Health Check (verifica dello stato di salute pre-aggiornamento) che elenca tutti i sistemi storage rilevati.

2. Se necessario, filtrare o ordinare i sistemi storage nell'elenco, in modo da poter visualizzare tutti i sistemi che non sono attualmente nello stato ottimale.
3. Selezionare le caselle di controllo relative ai sistemi storage che si desidera eseguire attraverso il controllo dello stato di salute.
4. Fare clic su **Start**.

   L'avanzamento viene visualizzato nella finestra di dialogo durante l'esecuzione del controllo dello stato di salute.

5. Una volta completato il controllo dello stato di salute, fare clic sui puntini di sospensione (…) a destra di ciascuna riga per visualizzare ulteriori informazioni ed eseguire altre attività.

> Se un array non supera il controllo dello stato di salute, è possibile saltare tale array e continuare l'aggiornamento per gli altri oppure interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il test.

Aggiornare il sistema operativo SANtricity

Aggiorna uno o più storage array con il software più recente e NVSRAM per assicurarti di disporre di tutte le funzionalità più recenti e delle correzioni dei bug. Controller NVSRAM è un file controller che specifica le impostazioni predefinite per i controller.

Prima di iniziare

Assicurarsi che:

- I file più recenti del sistema operativo SANtricity sono disponibili sul sistema host in cui è in esecuzione il plug-in.
- Si sa se si desidera attivare l'aggiornamento software ora o in una versione successiva. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:
  - **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. Il failover dei controller durante l'attivazione potrebbe risultare inferiore al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — si consiglia di testare il nuovo software del sistema operativo su un array di storage prima di aggiornare i file su altri array di storage.

> **Rischio di perdita di dati o rischio di danni allo storage array** — non apportare modifiche allo storage array durante l'aggiornamento. Mantenere l'alimentazione dello storage array.

Fasi

1. Se l'array di storage contiene un solo controller o un driver multipath non è in uso, interrompere l'attività i/o dell'array di storage per evitare errori dell'applicazione. Se lo storage array dispone di due controller e si dispone di un driver multipath installato, non è necessario interrompere l'attività di i/O.
2. Dalla vista principale, selezionare **Gestisci**, quindi uno o più array di storage da aggiornare.
3. Selezionare **Upgrade Center › Upgrade › SANtricity OS › Software**.

   Viene visualizzata la pagina aggiornamento del software SANtricity OS.

4. Scaricare il pacchetto software SANtricity OS più recente dal sito del supporto sul computer locale.
   a. Fare clic su Aggiungi nuovo file al repository software
   b. Fare clic sul collegamento per trovare i download più recenti di SANtricity OS.
   c. Fare clic sul collegamento **Download Latest Release** (Scarica ultima versione).
   d. Seguire le istruzioni rimanenti per scaricare il file del sistema operativo e IL file NVSRAM sul computer locale.

   > Il firmware con firma digitale è richiesto nella versione 8.42 e successive. Se si tenta di scaricare il firmware senza firma, viene visualizzato un errore e il download viene interrotto.

5. Selezionare il file del software del sistema operativo e IL file NVSRAM che si desidera utilizzare per aggiornare i controller:

   a. Dal menu a discesa, selezionare il file del sistema operativo scaricato sul computer locale.

      Se sono disponibili più file, i file vengono ordinati dalla data più recente alla data più vecchia.

      > Il repository software elenca tutti i file software associati al plug-in. Se il file che si desidera utilizzare non viene visualizzato, fare clic sul collegamento **Add new file to software repository** (Aggiungi nuovo file al repository software) per accedere alla posizione in cui si trova il file del sistema operativo che si desidera aggiungere.

   a. Dal menu a discesa **Select an NVSRAM file** (Seleziona un file NVSRAM), selezionare il file del controller che si desidera utilizzare.

      Se sono presenti più file, i file vengono ordinati dalla data più recente alla data più vecchia.

6. Nella tabella Compatible Storage Array (matrice di storage compatibile), esaminare gli array di storage compatibili con il file software del sistema operativo selezionato, quindi selezionare gli array da aggiornare.
   - Gli array di storage selezionati nella vista Manage (Gestione) e compatibili con il file del firmware selezionato vengono selezionati per impostazione predefinita nella tabella Compatible Storage Array (array di storage compatibile).
   - Gli array di storage che non possono essere aggiornati con il file del firmware selezionato non sono selezionabili nella tabella degli array di storage compatibili, come indicato dallo stato **incompatibile**.
7. (Facoltativo) per trasferire il file software agli array di storage senza attivarli, selezionare la casella di controllo **trasferire il software del sistema operativo agli array di storage, contrassegnarlo come staged e attivarlo in un secondo momento**.
8. Fare clic su **Start**.
9. A seconda che si sia scelto di attivare ora o successivamente, eseguire una delle seguenti operazioni:
   - Tipo `TRANSFER` Per confermare che si desidera trasferire le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Transfer** (trasferimento). Per attivare il software trasferito, selezionare **Centro di aggiornamento › attiva software SANtricity OS a fasi**.
   - Tipo `UPGRADE` Per confermare che si desidera trasferire e attivare le versioni software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fare clic su **Upgrade** (Aggiorna).

     Il sistema trasferisce il file software a ciascun array di storage selezionato per l'aggiornamento, quindi attiva il file avviando un riavvio.

   Durante l'operazione di aggiornamento si verificano le seguenti azioni:

   - Durante il processo di aggiornamento viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa continuare.
   - Se un controllo dello stato di salute non riesce per un array di storage, l'aggiornamento si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'aggiornamento.
   - È possibile annullare l'operazione di aggiornamento dopo il controllo dello stato di salute prima dell'aggiornamento.
10. (Facoltativo) una volta completato l'aggiornamento, è possibile visualizzare un elenco degli aggiornamenti per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

    Il file viene salvato nella cartella Download del browser con il nome `upgrade_log-<date>. json`.

Attivare il software del sistema operativo in fasi

È possibile scegliere di attivare il file software immediatamente o attendere fino a un momento più comodo. Questa procedura presuppone che l'utente abbia scelto di attivare il file software in un secondo momento.

A proposito di questa attività

È possibile trasferire i file del firmware senza attivarli. È possibile scegliere di eseguire l'attivazione in un secondo momento per i seguenti motivi:

- **Ora del giorno** — l'attivazione del software può richiedere molto tempo, quindi potrebbe essere necessario attendere che i carichi di i/o siano più leggeri. I controller si riavviano e si eseguono il failover durante l'attivazione, pertanto le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — si consiglia di testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri array di storage.

> Non è possibile interrompere il processo di attivazione dopo l'avvio.

Fasi

1. Dalla vista principale, selezionare **Gestisci**. Se necessario, fare clic sulla colonna **Status** per ordinare, nella parte superiore della pagina, tutti gli array di storage con stato "OS Upgrade (waiting activation)" (aggiornamento del sistema operativo (in attesa di attivazione).
2. Selezionare uno o più array di storage per i quali si desidera attivare il software, quindi selezionare **Centro di aggiornamento › attiva software Staged SANtricity**.

   Durante l'operazione di aggiornamento si verificano le seguenti azioni:

   - Nell'ambito del processo di attivazione viene eseguito un controllo dello stato di salute prima dell'aggiornamento. Il controllo dello stato di salute prima dell'aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'attivazione possa continuare.
   - Se un controllo dello stato di salute non riesce per un array di storage, l'attivazione si interrompe. È possibile fare clic sui puntini di sospensione (…) E selezionare **Save Log** (Salva registro) per esaminare gli errori. È inoltre possibile scegliere di ignorare l'errore di controllo dello stato di salute e fare clic su **continua** per procedere con l'attivazione.
   - È possibile annullare l'operazione di attivazione dopo il controllo dello stato di salute pre-aggiornamento.

     Una volta completato correttamente il controllo dello stato di salute prima dell'aggiornamento, si verifica l'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dello storage array e dai componenti che si stanno attivando.

3. (Facoltativo) una volta completata l'attivazione, è possibile visualizzare un elenco degli elementi attivati per uno specifico array di storage facendo clic sui puntini di sospensione (…) E quindi selezionando **Save Log** (Salva registro).

   Il file viene salvato nella cartella Download del browser con il nome `activate_log-<date>. json`.

Software per sistemi operativi chiari e staged

È possibile rimuovere il software del sistema operativo in fasi per assicurarsi che una versione in sospeso non venga attivata inavvertitamente in un secondo momento. La rimozione del software del sistema operativo in fasi non influisce sulla versione corrente in esecuzione sugli array di storage.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi selezionare **Centro di aggiornamento › Cancella software SANtricity in fasi**.

   Viene visualizzata la finestra di dialogo Cancella software SANtricity a fasi che elenca tutti i sistemi storage

rilevati con software o NVSRAM in sospeso.

2. Se necessario, filtrare o ordinare i sistemi di storage nell'elenco, in modo da poter visualizzare tutti i sistemi che dispongono di software in fasi.
3. Selezionare le caselle di controllo relative ai sistemi storage con software in sospeso che si desidera eliminare.
4. Fare clic su **Cancella**.

   Lo stato dell'operazione viene visualizzato nella finestra di dialogo.

Gestire il repository software

È possibile visualizzare e gestire un repository software, che elenca tutti i file software associati allo Storage Plugin per vCenter.

Prima di iniziare

Se si utilizza il repository per aggiungere file SANtricity OS, assicurarsi che i file del sistema operativo siano disponibili sul sistema locale.

A proposito di questa attività

È possibile utilizzare l'opzione Gestisci repository software SANtricity OS per importare uno o più file del sistema operativo nel sistema host in cui è in esecuzione il plug-in. Puoi anche scegliere di eliminare uno o più file del sistema operativo disponibili nel repository software.

Fasi

1. Dalla vista principale, selezionare **Gestisci**, quindi **Centro di aggiornamento › Gestisci repository software SANtricity**.

   Viene visualizzata la finestra di dialogo Gestisci repository software SANtricity OS.

2. Eseguire una delle seguenti operazioni:
   - **Importazione:**
     i. Fare clic su **Importa**.
     ii. Fare clic su **Browse** (Sfoglia), quindi individuare il percorso in cui si trovano i file del sistema operativo che si desidera aggiungere. I file del sistema operativo hanno un nome file simile a. `N2800-830000-000.dlp`.
     iii. Selezionare uno o più file del sistema operativo da aggiungere, quindi fare clic su **Importa**.
   - **Elimina:**
     i. Selezionare uno o più file del sistema operativo che si desidera rimuovere dal repository software.
     ii. Fare clic su **Delete** (Elimina).

Risultato

Se è stata selezionata l'opzione di importazione, i file vengono caricati e validati. Se si seleziona Delete (Elimina), i file vengono rimossi dal repository software.

Eseguire il provisioning dello storage

Panoramica sul provisioning

Nel plug-in Storage per vCenter, è possibile creare container di dati, chiamati volumi, in modo che l'host possa accedere allo storage sull'array.

Tipi di volume e caratteristiche

I volumi sono container di dati che gestiscono e organizzano lo spazio di storage sull'array di storage.

È possibile creare volumi dalla capacità di storage disponibile sull'array di storage, che consente di organizzare le risorse del sistema. Il concetto di "volumi" è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso rapido.

I volumi sono l'unico livello di dati visibile agli host. In un ambiente SAN, i volumi vengono mappati ai LUN (Logical Unit Number). Queste LUN conservano i dati utente accessibili mediante uno o più protocolli di accesso host supportati dallo storage array, tra cui FC, iSCSI e SAS.

Ciascun volume di un pool o di un gruppo di volumi può avere le proprie caratteristiche individuali in base al tipo di dati che verranno memorizzati in esso. Alcune di queste caratteristiche includono:

- **Dimensione segmento** — Un segmento è la quantità di dati in kilobyte (KiB) che viene memorizzata su un disco prima che lo storage array passi al disco successivo nello stripe (gruppo RAID). La dimensione del segmento è uguale o inferiore alla capacità del gruppo di volumi. La dimensione del segmento è fissa e non può essere modificata per i pool.
- **Capacità** — consente di creare un volume dalla capacità libera disponibile in un pool o in un gruppo di volumi. Prima di creare un volume, il pool o il gruppo di volumi deve già esistere e disporre di capacità libera sufficiente per creare il volume.
- **Controller ownership** — tutti gli storage array possono avere uno o due controller. Su un array a controller singolo, il carico di lavoro di un volume viene gestito da un singolo controller. Su un array a controller doppio, un volume avrà un controller preferito (A o B) che "possiede" il volume. In una configurazione a controller doppio, la proprietà del volume viene regolata automaticamente utilizzando la funzione di bilanciamento automatico del carico per correggere eventuali problemi di bilanciamento del carico quando i carichi di lavoro si spostano tra i controller. Il bilanciamento automatico del carico fornisce il bilanciamento automatizzato del carico di lavoro i/o e garantisce che il traffico i/o in entrata dagli host sia gestito dinamicamente e bilanciato tra entrambi i controller.
- **Assegnazione del volume** — è possibile consentire agli host di accedere a un volume sia quando si crea il volume che in un secondo momento. Tutti gli accessi host vengono gestiti tramite un numero di unità logica (LUN). Gli host rilevano le LUN che, a loro volta, sono assegnate ai volumi. Se si assegna un volume a più host, utilizzare il software di clustering per assicurarsi che il volume sia disponibile per tutti gli host.

  Il tipo di host può avere limiti specifici sul numero di volumi a cui l'host può accedere. Tenere presente questa limitazione quando si creano volumi per l'utilizzo da parte di un determinato host.

- **Resource provisioning** — per gli array storage EF600 o EF300, è possibile specificare che i volumi vengano utilizzati immediatamente senza alcun processo di inizializzazione in background. Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati).
- **Descrivi name** — puoi assegnare un nome a un volume qualsiasi, ma ti consigliamo di renderlo descrittivo.

Durante la creazione del volume, a ciascun volume viene allocata la capacità e viene assegnato un nome, una

dimensione del segmento (solo gruppi di volumi), una proprietà del controller e un'assegnazione volume-a-host. I dati dei volumi vengono automaticamente bilanciati in base alle esigenze dei controller.

Capacità per i volumi

I dischi dell'array di storage forniscono la capacità fisica dello storage per i dati. Prima di iniziare a memorizzare i dati, è necessario configurare la capacità allocata in componenti logici noti come pool o gruppi di volumi. Questi oggetti storage vengono utilizzati per configurare, memorizzare, gestire e conservare i dati sull'array di storage.

Capacità di creare ed espandere volumi

È possibile creare volumi dalla capacità non assegnata o dalla capacità libera in un pool o un gruppo di volumi.

- Quando si crea un volume dalla capacità non assegnata, è possibile creare contemporaneamente un pool o un gruppo di volumi e il volume.
- Quando si crea un volume dalla capacità libera, si crea un volume aggiuntivo su un pool o un gruppo di volumi già esistente.dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere una corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

> L'interfaccia del plug-in non fornisce un'opzione per creare volumi thin.

Capacità dei volumi riportata

La capacità del volume riportata è uguale alla quantità di capacità dello storage fisico allocata. Deve essere presente l'intera quantità di capacità dello storage fisico. Lo spazio fisicamente allocato è uguale allo spazio riportato all'host.

Di norma, si imposta la capacità del volume indicata come capacità massima a cui si pensa che il volume crescerà. I volumi offrono performance elevate e prevedibili per le applicazioni, soprattutto perché tutta la capacità dell'utente viene riservata e allocata al momento della creazione.

Limiti di capacità

La capacità minima di un volume è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità dei dischi nel pool o nel gruppo di volumi.

Quando si aumenta la capacità di un volume segnalata, tenere presenti le seguenti linee guida:

- È possibile specificare fino a tre cifre decimali (ad esempio, 65.375 GiB).
- La capacità deve essere inferiore o uguale al massimo disponibile nel gruppo di volumi. Quando si crea un volume, viene preallocata una certa capacità aggiuntiva per la migrazione DSS (Dynamic Segment Size). La migrazione DSS è una funzione del software che consente di modificare le dimensioni dei segmenti di un volume.
- Alcuni sistemi operativi host supportano volumi superiori a 2 TIB (la capacità massima indicata è determinata dal sistema operativo host). Infatti, alcuni sistemi operativi host supportano fino a 128 volumi TIB. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Carichi di lavoro specifici dell'applicazione

Quando si crea un volume, si seleziona un carico di lavoro per personalizzare la configurazione dell'array di

storage per un'applicazione specifica.

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

Durante la creazione del volume, il sistema richiede di rispondere alle domande sull'utilizzo di un carico di lavoro. Ad esempio, se si creano volumi per Microsoft Exchange, viene chiesto quante cassette postali sono necessarie, quali sono i requisiti medi di capacità delle caselle postali e quante copie del database si desidera. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze. In alternativa, è possibile saltare questo passaggio nella sequenza di creazione del volume.

Tipi di carichi di lavoro

È possibile creare due tipi di carichi di lavoro: Specifici dell'applicazione e altri.

- **Specifico dell'applicazione** — quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.
  - Microsoft SQL Server
  - Server Microsoft Exchange
  - Applicazioni di videosorveglianza
  - VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

    È possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).
- **Altri (o applicazioni senza supporto specifico per la creazione di volumi)** — Altri carichi di lavoro utilizzano una configurazione del volume che è necessario specificare manualmente quando si desidera creare un carico di lavoro non associato a un'applicazione specifica o se il sistema non dispone di ottimizzazione integrata per l'applicazione che si intende utilizzare sull'array di storage. Specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Viste delle applicazioni e dei workload

Per visualizzare applicazioni e carichi di lavoro, avviare System Manager. Da questa interfaccia è possibile visualizzare le informazioni associate a un carico di lavoro specifico dell'applicazione in due modi diversi:

- È possibile selezionare la scheda Applications & workload (applicazioni e carichi di lavoro) nel riquadro Volumes (volumi) per visualizzare i volumi dell'array di storage raggruppati per carico di lavoro e il tipo di applicazione a cui è associato il carico di lavoro.
- È possibile selezionare la scheda applicazioni e carichi di lavoro nel riquadro prestazioni per visualizzare le metriche delle performance (latenza, IOPS e MB) per gli oggetti logici. Gli oggetti sono raggruppati in base all'applicazione e al carico di lavoro associato. Raccogliendo questi dati sulle performance a intervalli

regolari, è possibile stabilire misurazioni di riferimento e analizzare i trend, che possono aiutare a indagare i problemi relativi alle performance di i/O.

Creare storage

Nel plug-in di storage per vCenter, è possibile creare lo storage creando prima un carico di lavoro per un tipo di applicazione specifico. In seguito, è possibile aggiungere capacità di storage al carico di lavoro creando volumi con caratteristiche di volume sottostanti simili.

Fase 1: Creazione di carichi di lavoro

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione.

A proposito di questa attività

Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

Il sistema consiglia una configurazione del volume ottimizzata solo per i seguenti tipi di applicazione:

- Microsoft SQL Server
- Server Microsoft Exchange
- Videosorveglianza
- VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › workload** (Crea[carico di lavoro]).

   Viene visualizzata la finestra di dialogo Create Application workload (Crea carico di lavoro applicazione).

4. Utilizzare l'elenco a discesa per selezionare il tipo di applicazione per cui si desidera creare il carico di lavoro, quindi digitare un nome per il carico di lavoro.
5. Fare clic su **Create** (Crea).

Fase 2: Creazione di volumi

È possibile creare volumi per aggiungere capacità di storage a un carico di lavoro specifico dell'applicazione e rendere visibili i volumi creati a un host o a un cluster host specifico.

A proposito di questa attività

La maggior parte dei tipi di applicazioni utilizza per impostazione predefinita una configurazione di volume definita dall'utente, mentre altri tipi hanno una configurazione smart applicata alla creazione di un volume. Ad esempio, se si creano volumi per un'applicazione Microsoft Exchange, viene chiesto quante cassette postali sono necessarie, quali sono i requisiti medi di capacità delle caselle postali e quante copie del database si

desidera. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze.

È possibile creare volumi dal **Provisioning › Gestisci volumi › Crea › volumi** o dal **Provisioning › Configura pool e gruppi di volumi › Crea › volumi**. La procedura è la stessa per entrambe le selezioni.

Il processo di creazione di un volume è una procedura a più fasi.

Fase 2a: Selezionare l'host per un volume

Nella prima fase, è possibile selezionare un host o un cluster host specifico per il volume oppure scegliere di assegnare l'host in un secondo momento.

Prima di iniziare

Assicurarsi che:

- Sono stati definiti host o cluster di host validi (andare al **Provisioning › Configure hosts**).
- Sono stati definiti gli identificatori delle porte host per l'host.
- La connessione host deve supportare Data Assurance (da) se si intende creare volumi abilitati da. Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

A proposito di questa attività

Tenere presenti queste linee guida quando si assegnano i volumi:

- Il sistema operativo di un host può avere limiti specifici sul numero di volumi a cui l'host può accedere. Tenere presente questa limitazione quando si creano volumi per l'utilizzo da parte di un determinato host.
- È possibile definire un'assegnazione per ciascun volume nell'array di storage.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un LUN univoco.
- Se si desidera accelerare il processo di creazione dei volumi, è possibile saltare la fase di assegnazione dell'host in modo che i volumi appena creati vengano inizializzati offline.

> L'assegnazione di un volume a un host non riesce se si tenta di assegnare un volume a un cluster di host che è in conflitto con un'assegnazione stabilita per un host nei cluster di host.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare **Create › Volumes** (Crea[volumi]).

   Viene visualizzata la finestra di dialogo Select host (Seleziona host).

4. Dall'elenco a discesa, selezionare un host o un cluster host specifico al quale assegnare i volumi oppure scegliere di assegnare l'host o il cluster host in un secondo momento.
5. Per continuare la sequenza di creazione del volume per l'host o il cluster host selezionato, fare clic su **Avanti.**

Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

Fase 2b: Selezionare un carico di lavoro per un volume

Nella seconda fase, selezionare un workload per personalizzare la configurazione dello storage array per un'applicazione specifica, ad esempio VMware.

A proposito di questa attività

Questa attività descrive come creare volumi per un carico di lavoro. In genere, un carico di lavoro contiene volumi con caratteristiche simili, ottimizzati in base al tipo di applicazione supportata dal carico di lavoro. È possibile definire un workload in questa fase oppure selezionare i workload esistenti.

Tenere presenti le seguenti linee guida:

- Quando si utilizza un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. È possibile rivedere la configurazione del volume consigliata, quindi modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi) (disponibile nella fase successiva).
- Quando si utilizzano altri tipi di applicazioni, è possibile specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi) (disponibile nella fase successiva).

Fasi

1. Effettuare una delle seguenti operazioni:
    - Selezionare l'opzione **Create Volumes for a existing workload** (Crea volumi per un carico di lavoro esistente), quindi selezionare il carico di lavoro dall'elenco a discesa.
    - Selezionare l'opzione **Create a new workload** (Crea nuovo carico di lavoro) per definire un nuovo carico di lavoro per un'applicazione supportata o per "altre" applicazioni, quindi attenersi alla seguente procedura:
        - Dall'elenco a discesa, selezionare il nome dell'applicazione per cui si desidera creare il nuovo workload. Selezionare una delle "altre" voci se l'applicazione che si desidera utilizzare su questo array di storage non è elencata.
        - Immettere un nome per il carico di lavoro che si desidera creare.
2. Fare clic su **Avanti**.
3. Se il carico di lavoro è associato a un tipo di applicazione supportato, inserire le informazioni richieste; in caso contrario, passare alla fase successiva.

Fase 2c: Aggiunta o modifica di volumi

Nel terzo passaggio, definire la configurazione del volume.

Prima di iniziare

- I pool o i gruppi di volumi devono disporre di capacità libera sufficiente.
- Il numero massimo di volumi consentito in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello di sistema di storage:
    - 2,048 volumi (serie EF600 ed E5700)
    - 1,024 volumi (EF300)

    - 512 volumi (serie E2800)
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.
    - Se si desidera creare un volume abilitato da, selezionare un pool o un gruppo di volumi che supporti da (cercare **Sì** accanto a "da" nella tabella dei candidati del pool e del gruppo di volumi).
    - Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi. LA protezione DA verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. La selezione di un pool o di un gruppo di volumi da-capable per il nuovo volume garantisce il rilevamento e la correzione degli errori.
    - Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.
- Per creare un volume abilitato alla protezione, è necessario creare una chiave di sicurezza per l'array di storage.
    - Se si desidera creare un volume abilitato per la protezione, selezionare un pool o un gruppo di volumi che supporti la protezione (cercare Sì accanto a "abilitato per la protezione" nella tabella dei candidati del pool e del gruppo di volumi).
    - Le funzionalità di sicurezza dei dischi vengono presentate a livello di pool e gruppo di volumi. I dischi con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Un disco abilitato alla sicurezza crittografa i dati durante la scrittura e decrta i dati durante la lettura utilizzando una chiave di crittografia univoca.
    - Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
- Per creare un volume con provisioning di risorse, tutti i dischi devono essere dischi NVMe con l'opzione Deallocated o Unwritten Logical Block Error (DULBE).

A proposito di questa attività

I volumi vengono creati da pool o gruppi di volumi idonei, visualizzati nella finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi). Per ciascun pool e gruppo di volumi idonei, vengono visualizzati il numero di dischi disponibili e la capacità libera totale.

Per alcuni carichi di lavoro specifici dell'applicazione, ciascun pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e la capacità libera rimanente in GiB. Per gli altri carichi di lavoro, la capacità proposta viene visualizzata quando si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

Fasi

1. Scegliere una di queste azioni in base alla selezione di un altro workload o di un workload specifico dell'applicazione nel passaggio precedente:
    - **Altro** — fare clic su **Aggiungi nuovo volume** in ogni pool o gruppo di volumi che si desidera utilizzare per creare uno o più volumi.

Dettagli campo

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • da 512 a 512 byte • 4K – 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi nel pool o nel gruppo di volumi sono protetti. Drive Security impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione Drive Security è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Campo	Descrizione
Provisioning delle risorse (solo EF300 e EF600)	**Yes** viene visualizzato accanto a "Resource Provisioned" (risorse fornite) solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

- **Carico di lavoro specifico dell'applicazione** — fare clic su **Avanti** per accettare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche raccomandati dal sistema per il carico di lavoro selezionato.

Dettagli campo

Campo	Descrizione
Volume Name (Nome volume)	A un volume viene assegnato un nome predefinito durante la sequenza di creazione del volume. È possibile accettare il nome predefinito o fornire un nome descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità riportata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TIB). Per i volumi spessi, la capacità minima è di 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tenere presente che la capacità di storage è necessaria anche per i servizi di copia (immagini snapshot, volumi snapshot, copie di volumi e mirror remoti); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4-GiB. Qualsiasi capacità che non sia un multiplo di 4 GiB viene allocata ma non utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4-GiB. Se esiste una capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Tipo di volume	Il tipo di volume indica il tipo di volume creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per il volume: • 512 — 512 byte • 4K — 4,096 byte

Campo	Descrizione
Dimensione segmento	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti** — il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Sicuro	**Sì** viene visualizzato accanto a "Secure-capable" solo se i dischi nel pool o nel gruppo di volumi sono protetti. La sicurezza del disco impedisce l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dallo storage array. Questa opzione è disponibile solo se la funzione di sicurezza del disco è stata attivata e se è stata impostata una chiave di sicurezza per lo storage array. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.
DA	**Sì** viene visualizzato accanto a "da" solo se i dischi del pool o del gruppo di volumi supportano Data Assurance (da). DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente allo storage array di controllare gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Campo	Descrizione
Provisioning delle risorse (solo EF300 e EF600)	**Yes** viene visualizzato accanto a "Resource Provisioned" (risorse fornite) solo se i dischi supportano questa opzione. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

2. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti**.

Fase 2d: Analisi della configurazione del volume

Nell'ultimo passaggio, viene esaminato un riepilogo dei volumi che si intende creare e vengono apportate le modifiche necessarie.

Fasi

1. Esaminare i volumi che si desidera creare. Per apportare modifiche, fare clic su **Indietro**.
2. Quando si è soddisfatti della configurazione del volume, fare clic su **fine**.

Al termine

- Nel client vSphere, creare datastore per i volumi.
- Eseguire tutte le modifiche del sistema operativo necessarie sull'host dell'applicazione in modo che le applicazioni possano utilizzare il volume.
- Eseguire il sistema basato su host `hot_add` o un'utility specifica del sistema operativo (disponibile presso un fornitore di terze parti), quindi eseguire `SMdevices` utility per correlare i nomi dei volumi con i nomi degli array di storage host.

  Il `hot_add` e a. `SMdevices` le utility sono incluse nel `SMutils` pacchetto. Il `SMutils` il pacchetto è un insieme di utility per verificare ciò che l'host vede dall'array di storage. È incluso nell'installazione del software SANtricity.

Aumentare la capacità di un volume

È possibile ridimensionare un volume per aumentarne la capacità indicata.

Prima di iniziare

Assicurarsi che:

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associati al volume.
- Il volume è ottimale e non in alcun stato di modifica.
- Nel volume non sono in uso dischi hot spare. (Si applica solo ai volumi nei gruppi di volumi).

A proposito di questa attività

Questa attività descrive come aumentare la capacità riportata (la capacità riportata agli host) di un volume utilizzando la capacità libera disponibile nel pool o nel gruppo di volumi. Assicurarsi di prendere in considerazione eventuali requisiti di capacità futuri per altri volumi in questo pool o gruppo di volumi.

L'aumento della capacità di un volume è supportato solo su alcuni sistemi operativi. Se si aumenta la capacità del volume su un sistema operativo host non supportato, la capacità espansa non è utilizzabile e non è possibile ripristinare la capacità del volume originale.

Fasi

1. Dalla pagina **Manage** (Gestisci), selezionare l'array di storage che contiene i volumi che si desidera ridimensionare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il volume per il quale si desidera aumentare la capacità, quindi selezionare **aumenta capacità**.

   Viene visualizzata la finestra di dialogo Conferma aumento capacità.

4. Selezionare **Sì** per continuare.

   Viene visualizzata la finestra di dialogo aumenta capacità riportata. Questa finestra di dialogo visualizza la capacità corrente del volume riportata e la capacità libera disponibile nel gruppo di volumi o pool associato al volume.

5. Utilizzare la casella **aumenta capacità segnalata aggiungendo…** per aggiungere capacità alla capacità corrente disponibile indicata. È possibile modificare il valore della capacità in modo che venga visualizzato in megibyte (MiB), gibibyte (GiB) o tebibyte (TIB).
6. Fare clic su **aumenta**.

   La capacità del volume viene aumentata in base alla selezione effettuata. Tenere presente che questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Al termine

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso. Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Modificare le impostazioni di un volume

È possibile modificare le impostazioni di un volume, ad esempio il nome, l'assegnazione dell'host, la dimensione del segmento, la priorità di modifica, la memorizzazione nella cache, e così via.

Prima di iniziare

Assicurarsi che il volume che si desidera modificare sia nello stato ottimale.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera modificare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il volume che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Settings (Impostazioni volume). Le impostazioni di configurazione del volume selezionato vengono visualizzate in questa finestra di dialogo.

4. Selezionare la scheda **Basic** per modificare il nome del volume e l'assegnazione dell'host.

Dettagli campo

Impostazione	Descrizione
Nome	Visualizza il nome del volume. Modificare il nome di un volume quando il nome corrente non è più significativo o applicabile.
Capacità	Visualizza la capacità riportata e allocata per il volume selezionato.
Gruppo pool/Volume	Visualizza il nome e il livello RAID del pool o del gruppo di volumi. Indica se il pool o il gruppo di volumi sono abilitati per la protezione e la protezione.
Host	Visualizza l'assegnazione del volume. Si assegna un volume a un cluster host o host in modo che sia possibile accedervi per le operazioni di i/O. Questa assegnazione consente a un host o a un cluster di host di accedere a un determinato volume o a una serie di volumi in un array di storage. • **Assegnato a** — identifica l'host o il cluster di host che ha accesso al volume selezionato. • **LUN** — Un numero di unità logica (LUN) è il numero assegnato allo spazio degli indirizzi utilizzato da un host per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host dispone di un proprio spazio di indirizzi LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi. Per le interfacce NVMe, questa colonna visualizza l'ID dello spazio dei nomi. Uno spazio dei nomi è uno storage NVM formattato per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che si riferisce a un volume nell'array di storage. L'ID dello spazio dei nomi è l'identificatore univoco del controller NVMe per lo spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.
Identificatori	Visualizza gli identificatori del volume selezionato. • WWID (World-wide identifier). Identificatore esadecimale univoco del volume. • Extended Unique Identifier (EUI). Un identificatore EUI-64 per il volume. • SSID (Subsystem Identifier). L'identificatore del sottosistema dell'array di storage di un volume.

5. Selezionare la scheda **Avanzate** per modificare le impostazioni di configurazione aggiuntive per un volume in un pool o in un gruppo di volumi.

Dettagli campo

Impostazione	Descrizione
Informazioni su applicazioni e carichi di lavoro	Durante la creazione dei volumi, è possibile creare carichi di lavoro specifici dell'applicazione o altri carichi di lavoro. Se applicabile, il nome del carico di lavoro, il tipo di applicazione e il tipo di volume vengono visualizzati per il volume selezionato. Se lo si desidera, è possibile modificare il nome del carico di lavoro.
Impostazioni della qualità del servizio	**Disable data assurance (Disattiva data assurance) in modo permanente** — questa impostazione viene visualizzata solo se il volume è abilitato per Data Assurance (da). DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. Utilizzare questa opzione per disattivare in modo permanente il da sul volume selezionato. Se disattivato, il da non può essere riattivato su questo volume. **Enable pre-Read Redundancy check** — questa impostazione viene visualizzata solo se il volume è un volume spesso. I controlli di ridondanza di pre-lettura determinano se i dati su un volume sono coerenti ogni volta che viene eseguita una lettura. Un volume con questa funzione attivata restituisce errori di lettura se i dati risultano incoerenti dal firmware del controller.
Proprietà del controller	Definisce il controller designato come controller principale o proprietario del volume. La proprietà del controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per l'i/o totale.

Impostazione	Descrizione
Dimensionamento dei segmenti	Mostra l'impostazione per il dimensionamento dei segmenti, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare le dimensioni del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — il sistema determina le transizioni consentite per le dimensioni dei segmenti. Le dimensioni dei segmenti che sono transizioni inappropriate dalla dimensione corrente dei segmenti non sono disponibili nell'elenco a discesa. Le transizioni consentite solitamente sono il doppio o la metà delle dimensioni correnti del segmento. Ad esempio, se la dimensione attuale del segmento di volume è 32 KiB, è consentita una nuova dimensione del segmento di volume di 16 KiB o 64 KiB. **Volumi SSD abilitati per la cache** — è possibile specificare una dimensione di segmento 4 KiB per i volumi SSD abilitati per la cache. Assicurarsi di selezionare le dimensioni dei segmenti 4 KiB solo per i volumi con funzionalità SSD cache che gestiscono operazioni i/o a piccoli blocchi (ad esempio, blocchi i/o di dimensioni pari o inferiori a 16 KiB). Le performance potrebbero risentire se si seleziona 4 KiB come dimensione del segmento per i volumi abilitati per la cache SSD che gestiscono grandi operazioni sequenziali a blocchi. **Tempo necessario per modificare le dimensioni dei segmenti.** il tempo necessario per modificare le dimensioni dei segmenti di un volume dipende dalle seguenti variabili: • Il carico di i/o dall'host • La priorità di modifica del volume • Il numero di dischi nel gruppo di volumi • Il numero di canali del disco • La potenza di elaborazione dei controller degli array di storage Quando si modificano le dimensioni dei segmenti di un volume, le prestazioni i/o vengono compromesse, ma i dati rimangono disponibili.
Priorità di modifica	Mostra l'impostazione della priorità di modifica, che viene visualizzata solo per i volumi in un gruppo di volumi. La priorità di modifica definisce il tempo di elaborazione allocato per le operazioni di modifica del volume in relazione alle prestazioni del sistema. È possibile aumentare la priorità di modifica del volume, anche se ciò potrebbe influire sulle prestazioni del sistema. Spostare le barre di scorrimento per selezionare un livello di priorità. **Modifica dei tassi di priorità** — il tasso di priorità più basso offre benefici alle prestazioni del sistema, ma l'operazione di modifica richiede più tempo. Il tasso di priorità più elevato è utile per l'operazione di modifica, ma le prestazioni del sistema potrebbero essere compromesse.
Caching	Mostra l'impostazione del caching, che è possibile modificare per influire sulle prestazioni i/o complessive di un volume.

Impostazione	Descrizione
Cache SSD	(Questa funzione non è disponibile sui sistemi storage EF600 o EF300). Mostra l'impostazione della cache SSD, che è possibile attivare sui volumi compatibili per migliorare le prestazioni di sola lettura. I volumi sono compatibili se condividono le stesse funzionalità di sicurezza del disco e di data assurance. La funzione SSD cache utilizza uno o più dischi a stato solido (SSD) per implementare una cache di lettura. Le performance applicative sono migliorate grazie ai tempi di lettura più rapidi per gli SSD. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. È sufficiente selezionare il volume che si desidera memorizzare nella cache, quindi il caching è automatico e dinamico.

6. Fare clic su **Save** (Salva).

Risultato

Le impostazioni del volume vengono modificate in base alle selezioni effettuate.

Aggiungere volumi al carico di lavoro

È possibile aggiungere volumi non assegnati a un carico di lavoro esistente o nuovo.

A proposito di questa attività

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera aggiungere.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

4. Selezionare **Aggiungi al carico di lavoro**.

   Viene visualizzata la finestra di dialogo Select workload (Seleziona carico di lavoro).

5. Eseguire una delle seguenti operazioni:
   - **Aggiungi volumi a un carico di lavoro esistente** — selezionare questa opzione per aggiungere volumi a un carico di lavoro esistente. Utilizzare l'elenco a discesa per selezionare un carico di lavoro. Il tipo di applicazione associato al carico di lavoro viene assegnato ai volumi aggiunti a questo carico di lavoro.
   - **Aggiungi volumi a un nuovo carico di lavoro** — selezionare questa opzione per definire un nuovo carico di lavoro per un tipo di applicazione e aggiungere volumi al nuovo carico di lavoro.
6. Selezionare **Avanti** per continuare con la sequenza di aggiunta al carico di lavoro.

   Viene visualizzata la finestra di dialogo Select Volumes (Seleziona volumi).

7. Selezionare i volumi che si desidera aggiungere al carico di lavoro.
8. Esaminare i volumi che si desidera aggiungere al carico di lavoro selezionato.
9. Quando si è soddisfatti della configurazione del carico di lavoro, fare clic su **fine**.

Modificare le impostazioni del carico di lavoro

È possibile modificare il nome di un workload e visualizzarne il tipo di applicazione associato.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage che contiene il carico di lavoro che si desidera modificare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare la scheda **applicazioni e carichi di lavoro**.

   Viene visualizzata la vista applicazioni e carichi di lavoro.

4. Selezionare il carico di lavoro che si desidera modificare, quindi selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Applications & workload Settings (Impostazioni applicazioni e carichi di lavoro).

5. (Facoltativo) modificare il nome del carico di lavoro fornito dall'utente.
6. Fare clic su **Save** (Salva).

Inizializzare i volumi

Un volume viene inizializzato automaticamente quando viene creato per la prima volta. Tuttavia, il Recovery Guru potrebbe consigliare di inizializzare manualmente un volume per eseguire il ripristino in seguito a determinate condizioni di errore.

Utilizzare questa opzione solo sotto la guida del supporto tecnico. È possibile selezionare uno o più volumi da inizializzare.

Prima di iniziare

- Tutte le operazioni di i/o sono state interrotte.
- Tutti i dispositivi o i file system sui volumi che si desidera inizializzare devono essere smontati.
- Il volume si trova in uno stato ottimale e non sono in corso operazioni di modifica sul volume.*attenzione: *Non è possibile annullare l'operazione dopo l'avvio. Tutti i dati del volume vengono cancellati. Non provare a eseguire questa operazione a meno che il Recovery Guru non lo suggerisca. Prima di iniziare questa procedura, contattare il supporto tecnico.

A proposito di questa attività

Quando si inizializza un volume, il volume mantiene le impostazioni relative a WWN, assegnazioni host, capacità allocata e capacità riservata. Inoltre, mantiene le stesse impostazioni di sicurezza e di Data Assurance (da).

Non è possibile inizializzare i seguenti tipi di volumi:

- Volume di base di un volume di snapshot
- Volume primario in una relazione mirror
- Volume secondario in relazione mirror
- Volume di origine in una copia del volume
- Volume di destinazione in una copia del volume
- Volume che ha già un'inizializzazione in corso

Questa procedura si applica solo ai volumi standard creati da pool o gruppi di volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi che si desidera inizializzare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Initialize Volumes** (Altro[Inizializza volumi]).

   Viene visualizzata la finestra di dialogo Inizializza volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Selezionare uno o più volumi da inizializzare e confermare che si desidera eseguire l'operazione.

Risultati

Il sistema esegue le seguenti operazioni:

- Cancella tutti i dati dai volumi inizializzati.
- Cancella gli indici dei blocchi, il che fa sì che i blocchi non scritti vengano letti come se fossero riempiti a zero (il volume sembra essere completamente vuoto).

Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Ridistribuire i volumi

Ridistribuisci i volumi per spostarli di nuovo nei proprietari di controller preferiti. In genere, i driver multipath spostano i volumi dal proprietario del controller preferito quando si verifica un problema lungo il percorso dei dati tra l'host e l'array di storage.

Prima di iniziare

- I volumi che si desidera ridistribuire non sono in uso o si verificano errori di i/O.
- Un driver multipath viene installato su tutti gli host che utilizzano i volumi che si desidera ridistribuire, altrimenti si verificheranno errori di i/O. Se si desidera ridistribuire i volumi senza un driver multipath sugli host, tutte le attività di i/o sui volumi durante l'operazione di ridistribuzione devono essere interrotte per evitare errori dell'applicazione.

A proposito di questa attività

La maggior parte dei driver multipath host tenta di accedere a ciascun volume su un percorso verso il proprietario del controller preferito. Tuttavia, se questo percorso preferito non è disponibile, il driver multipath sull'host esegue il failover su un percorso alternativo. Questo failover potrebbe causare la modifica della proprietà del volume nel controller alternativo. Dopo aver risolto la condizione che ha causato il failover, alcuni host potrebbero spostare automaticamente la proprietà del volume nel proprietario del controller preferito, ma in alcuni casi potrebbe essere necessario ridistribuire manualmente i volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi da ridistribuire.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare il **More › redistribuisci volumi**.

   Viene visualizzata la finestra di dialogo redistribuisci volumi. In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage il cui proprietario preferito del controller non corrisponde al proprietario corrente.

4. Selezionare uno o più volumi da ridistribuire e confermare che si desidera eseguire l'operazione.

Risultato

Il sistema sposta i volumi selezionati nei controller preferiti oppure viene visualizzata una finestra di dialogo ridistribuisci volumi non necessari.

Modificare la proprietà del controller di un volume

È possibile modificare la proprietà del controller preferito di un volume, in modo che l'i/o per le applicazioni host venga indirizzato attraverso il nuovo percorso.

Prima di iniziare

Se non si utilizza un driver multipath, tutte le applicazioni host che attualmente utilizzano il volume devono essere chiuse. Questa azione impedisce gli errori dell'applicazione quando il percorso di i/o cambia.

A proposito di questa attività

È possibile modificare la proprietà del controller per uno o più volumi in un pool o un gruppo di volumi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage che contiene i volumi per i quali si desidera modificare la proprietà del controller.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change ownership** (Altro[Modifica proprietà]).

   Viene visualizzata la finestra di dialogo Change Volume Ownership (Modifica proprietà volume). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Utilizzare l'elenco a discesa **Preferred Owner** (Proprietario preferito) per modificare il controller preferito per ciascun volume che si desidera modificare e confermare che si desidera eseguire l'operazione.

Risultati

- Il sistema modifica la proprietà del controller del volume. L'i/o al volume viene ora indirizzato attraverso questo percorso i/O.
- Il volume potrebbe non utilizzare il nuovo percorso i/o fino a quando il driver multipath non viene riconfigurato per riconoscere il nuovo percorso.

Questa operazione richiede in genere meno di cinque minuti.

Modificare le impostazioni della cache per un volume

È possibile modificare le impostazioni della cache di lettura e di scrittura per influire sulle

prestazioni i/o generali di un volume.

A proposito di questa attività

Quando si modificano le impostazioni della cache di un volume, tenere presenti le seguenti linee guida:

- Dopo aver aperto la finestra di dialogo Change cache Settings (Modifica impostazioni cache), potrebbe essere visualizzata un'icona accanto alle proprietà della cache selezionate. Questa icona indica che il controller ha temporaneamente sospeso le operazioni di caching. Questa azione potrebbe verificarsi quando una nuova batteria è in carica, quando un controller è stato rimosso o se il controller ha rilevato una mancata corrispondenza nelle dimensioni della cache. Una volta deselezionata la condizione, le proprietà della cache selezionate nella finestra di dialogo diventano attive. Se le proprietà della cache selezionate non diventano attive, contattare il supporto tecnico.
- È possibile modificare le impostazioni della cache per un singolo volume o per più volumi su un array di storage. È possibile modificare le impostazioni della cache per tutti i volumi contemporaneamente.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage contenente i volumi per i quali si desidera modificare le impostazioni della cache.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change cache settings** (Altro[Modifica impostazioni cache]).

   Viene visualizzata la finestra di dialogo Change cache Settings (Modifica impostazioni cache). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Selezionare la scheda **Basic** per modificare le impostazioni per il caching in lettura e il caching in scrittura.

   Dettagli campo

Impostazione della cache	Descrizione
Read Caching (cache lettura)	La cache di lettura è un buffer che memorizza i dati letti dai dischi. I dati di un'operazione di lettura potrebbero essere già presenti nella cache di un'operazione precedente, eliminando così la necessità di accedere ai dischi. I dati rimangono nella cache di lettura fino a quando non vengono scaricati.
Cache di scrittura	La cache di scrittura è un buffer che memorizza i dati dell'host che non sono ancora stati scritti sui dischi. I dati rimangono nella cache di scrittura fino a quando non vengono scritti sui dischi. Il caching in scrittura può aumentare le performance di i/O. La cache viene automaticamente scaricata dopo la disattivazione del caching in scrittura per un volume.

5. Selezionare la scheda **Advanced** (Avanzate) per modificare le impostazioni avanzate per i volumi spessi. Le impostazioni avanzate della cache sono disponibili solo per i volumi thick.

Dettagli campo

Impostazione	Descrizione
Precaricamento della cache di lettura dinamica	Dynamic cache Read Prefetch consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache durante la lettura dei blocchi di dati da un disco alla cache. Questo caching aumenta la possibilità che le future richieste di dati possano essere compilate dalla cache. Il prefetch dinamico della lettura della cache è importante per le applicazioni multimediali che utilizzano l'i/o sequenziale La velocità e la quantità di dati precaricati nella cache vengono regolate automaticamente in base alla velocità e alle dimensioni della richiesta dell'host. L'accesso casuale non fa sì che i dati vengano precaricati nella cache. Questa funzione non si applica quando il caching in lettura è disattivato.
Cache di scrittura senza batterie	L'impostazione Write Caching without batteries (cache di scrittura senza batterie) consente di continuare il caching in scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta del caching in scrittura senza batterie non è generalmente consigliata, in quanto i dati potrebbero andare persi in caso di interruzione dell'alimentazione. In genere, il caching in scrittura viene disattivato temporaneamente dal controller fino a quando le batterie non vengono caricate o non viene sostituita una batteria guasta. ATTENZIONE: **Possibile perdita di dati** — se si seleziona questa opzione e non si dispone di un alimentatore universale per la protezione, si potrebbero perdere i dati. Inoltre, è possibile perdere i dati se non si dispone di batterie del controller e si attiva l'opzione Write caching without batteries (cache di scrittura senza batterie).
Cache di scrittura con mirroring	Il caching in scrittura con mirroring si verifica quando i dati scritti nella memoria cache di un controller vengono scritti anche nella memoria cache dell'altro controller. Pertanto, se un controller si guasta, l'altro può completare tutte le operazioni di scrittura in sospeso. Il mirroring della cache di scrittura è disponibile solo se il caching di scrittura è attivato e sono presenti due controller. Il caching in scrittura con mirroring è l'impostazione predefinita alla creazione del volume.

6. Fare clic su **Save** (Salva) per modificare le impostazioni della cache.

Modificare le impostazioni di scansione dei supporti per un volume

Una scansione dei supporti è un'operazione in background che esegue la scansione di tutti i dati e delle informazioni di ridondanza nel volume. Utilizzare questa opzione per attivare o disattivare le impostazioni di scansione dei supporti per uno o più volumi o per modificare la durata della scansione.

Prima di iniziare

Comprendere quanto segue:

- Le scansioni dei supporti vengono eseguite continuamente a una velocità costante in base alla capacità da sottoporre a scansione e alla durata della scansione. Le scansioni in background possono essere temporaneamente sospese da un'attività in background con priorità più alta (ad esempio ricostruzione), ma vengono rieseguite alla stessa velocità costante.

- La scansione di un volume viene eseguita solo quando l'opzione di scansione dei supporti è attivata per l'array di storage e per quel volume. Se è attivata anche la verifica della ridondanza per quel volume, le informazioni di ridondanza nel volume verranno controllate per verificarne la coerenza con i dati, a condizione che il volume disponga di ridondanza. La scansione dei supporti con controllo della ridondanza è attivata per impostazione predefinita per ciascun volume al momento della creazione.
- Se durante la scansione si verifica un errore irreversibile del supporto, i dati verranno riparati utilizzando le informazioni di ridondanza, se disponibili.

  Ad esempio, le informazioni di ridondanza sono disponibili in volumi RAID 5 ottimali o in volumi RAID 6 ottimali o con un solo disco guasto. Se l'errore irreversibile non può essere riparato utilizzando le informazioni di ridondanza, il blocco di dati viene aggiunto al registro del settore illeggibile. Nel registro eventi vengono riportati errori del supporto correggibili e non correggibili.

- Se il controllo di ridondanza rileva un'incoerenza tra i dati e le informazioni di ridondanza, viene riportato nel registro eventi.

A proposito di questa attività

Le scansioni dei supporti rilevano e riparano gli errori dei supporti sui blocchi di dischi che vengono raramente letti dalle applicazioni. Ciò può impedire la perdita di dati in caso di guasto di un disco, poiché i dati dei dischi guasti vengono ricostruiti utilizzando le informazioni di ridondanza e i dati di altri dischi nel gruppo di volumi o nel pool.

È possibile eseguire le seguenti operazioni:

- Attivare o disattivare la scansione dei supporti in background per l'intero array di storage
- Modificare la durata della scansione per l'intero array di storage
- Attivare o disattivare la scansione dei supporti per uno o più volumi
- Attivare o disattivare il controllo di ridondanza per uno o più volumi

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage contenente i volumi per i quali si desidera modificare le impostazioni di scansione dei supporti.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Selezionare un volume qualsiasi, quindi **More › Change media scan settings** (Altro[Modifica impostazioni di scansione dei supporti]).

   Viene visualizzata la finestra di dialogo Change Drive Media Scan Settings (Modifica impostazioni scansione supporti unità). In questa finestra di dialogo vengono visualizzati tutti i volumi dell'array di storage.

4. Per attivare la scansione dei supporti, selezionare la casella di controllo **scansione supporti durante…**. La disattivazione della casella di controllo scansione supporti consente di sospendere tutte le impostazioni di scansione dei supporti.
5. Specificare il numero di giorni in cui si desidera eseguire la scansione del supporto.
6. Selezionare la casella di controllo **Media Scan** per ciascun volume su cui si desidera eseguire una scansione dei supporti. Il sistema attiva l'opzione Redundancy Check (controllo ridondanza) per ciascun volume su cui si sceglie di eseguire una scansione dei supporti. Se esistono singoli volumi per i quali non si desidera eseguire un controllo di ridondanza, deselezionare la casella di controllo **controllo di ridondanza**.
7. Fare clic su **Save** (Salva).

Risultato

Il sistema applica le modifiche alle scansioni dei supporti in background in base alla selezione effettuata.

Elimina volume

È possibile eliminare uno o più volumi per aumentare la capacità libera di un pool o di un gruppo di volumi.

Prima di iniziare

Sui volumi che si intende eliminare, assicurarsi che:

- Viene eseguito il backup di tutti i dati.
- All Input/Output (i/o) viene interrotto.
- Tutti i dispositivi e i file system vengono smontati.

A proposito di questa attività

In genere, i volumi vengono eliminati se sono stati creati con parametri o capacità errati o se non soddisfano più le esigenze di configurazione dello storage. L'eliminazione di un volume aumenta la capacità libera nel pool o nel gruppo di volumi.

> L'eliminazione di un volume causa la perdita di tutti i dati presenti su tali volumi.

Tenere presente che **non è possibile** eliminare un volume che presenta una delle seguenti condizioni:

- Il volume è in fase di inizializzazione.
- Il volume è in fase di ricostruzione.
- Il volume fa parte di un gruppo di volumi che contiene un disco sottoposto a un'operazione copyback.
- Il volume sta subendo un'operazione di modifica, ad esempio una modifica delle dimensioni dei segmenti, a meno che il volume non sia ora nello stato Failed (guasto).
- Il volume contiene qualsiasi tipo di prenotazione persistente.
- Il volume è un volume di origine o un volume di destinazione in un volume di copia con stato Pending (in sospeso), in Progress (in corso) o Failed (non riuscito).

> Quando un volume supera una determinata dimensione (attualmente 128 TB), l'operazione di eliminazione viene eseguita in background e lo spazio liberato potrebbe non essere immediatamente disponibile.

Fasi

1. Dalla pagina **Manage** (Gestione), selezionare l'array di storage che contiene i volumi che si desidera eliminare.
2. Selezionare **Provisioning › Manage Volumes** (Gestione volumi).
3. Fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Volumes.

4. Selezionare uno o più volumi da eliminare, quindi confermare che si desidera eseguire l'operazione.
5. Fare clic su **Delete** (Elimina).

Configurare gli host

Panoramica sulla creazione dell'host

Per gestire lo storage con Storage Plugin per vCenter, è necessario individuare o definire ciascun host della rete. Un host è un server che invia i/o a un volume su un array di storage.

Creazione automatica o manuale degli host

La creazione di un host è una delle operazioni necessarie per consentire all'array di storage di sapere quali host sono collegati e di consentire l'accesso i/o ai volumi. Un host può essere creato automaticamente o manualmente.

- **Automatico** — la creazione automatica dell'host per gli host basati su SCSI (non NVMe-of) viene avviata dall'HCA (host Context Agent). HCA è un'utility che è possibile installare su ciascun host collegato allo storage array. Ogni host su cui è installato l'HCA invia le informazioni di configurazione ai controller degli array di storage attraverso il percorso i/O. In base alle informazioni sull'host, i controller creano automaticamente l'host e le porte host associate e impostano il tipo di host. Se necessario, è possibile apportare ulteriori modifiche alla configurazione dell'host. Dopo che l'HCA ha eseguito il rilevamento automatico, l'host viene configurato automaticamente con i seguenti attributi:
  - Il nome host derivato dal nome di sistema dell'host.
  - Le porte di identificazione host associate all'host.
  - Il tipo di sistema operativo host dell'host.

> Gli host vengono creati come host standalone; l'HCA non crea o aggiunge automaticamente ai cluster di host.

- **Manuale** — durante la creazione manuale dell'host, è possibile associare gli identificatori delle porte host selezionandoli da un elenco o inserendoli manualmente. Dopo aver creato un host, è possibile assegnarvi dei volumi o aggiungerlo a un cluster host se si intende condividere l'accesso ai volumi.

Modalità di assegnazione dei volumi

Per consentire a un host di inviare i/o a un volume, è necessario assegnarvi il volume. È possibile selezionare un host o un cluster di host quando si crea un volume oppure assegnarlo in un secondo momento a un host o a un cluster di host. Un cluster host è un gruppo di host. È possibile creare un cluster host per semplificare l'assegnazione degli stessi volumi a più host.

L'assegnazione di volumi agli host è flessibile e consente di soddisfare le esigenze di storage specifiche.

- **Host standalone, non parte di un cluster di host** — è possibile assegnare un volume a un singolo host. È possibile accedere al volume solo da un host.
- **Cluster di host** — è possibile assegnare un volume a un cluster di host. Tutti gli host del cluster host possono accedere al volume.
- **Host all'interno di un cluster di host** — è possibile assegnare un volume a un singolo host che fa parte di un cluster di host. Anche se l'host fa parte di un cluster di host, è possibile accedere al volume solo dal singolo host e non da altri host del cluster di host.

Quando vengono creati i volumi, i LUN (Logical Unit Number) vengono assegnati automaticamente. Il LUN funge da indirizzo tra l'host e il controller durante le operazioni di i/O. Una volta creato il volume, è possibile

modificare i LUN.

Creare l’accesso all’host

Per gestire lo storage con Storage Plugin per vCenter, è necessario individuare o definire ciascun host della rete.

A proposito di questa attività

Creando un host, si definiscono i parametri host per fornire la connessione allo storage array e l’accesso i/o ai volumi.

È possibile consentire all’HCA (host Context Agent) di rilevare automaticamente gli host, quindi verificare che le informazioni siano corrette selezionando **Visualizza/Modifica impostazioni** dalla pagina Configura host. Tuttavia, l’HCA non è disponibile su tutti i sistemi operativi supportati ed è necessario creare l’host manualmente.

Quando si crea un host, tenere presenti le seguenti linee guida:

- È necessario definire le porte di identificazione host associate all’host.
- Assicurarsi di fornire lo stesso nome del nome di sistema assegnato all’host.
- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Fare clic sul **Create › host** (Crea[host]).

   Viene visualizzata la finestra di dialogo Create host (Crea host).

4. Selezionare le impostazioni per l’host in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	Digitare un nome per il nuovo host.
Tipo di sistema operativo host	Selezionare il sistema operativo in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia host	(Facoltativo) se si dispone di più tipi di interfaccia host supportati sull'array di storage, selezionare il tipo di interfaccia host che si desidera utilizzare.
Porte host	Effettuare una delle seguenti operazioni: • **Selezionare l'interfaccia i/o** — in genere, le porte host devono essere state registrate ed essere disponibili dall'elenco a discesa. È possibile selezionare gli identificatori della porta host dall'elenco. • **Aggiunta manuale** — se un identificatore di porta host non viene visualizzato nell'elenco, significa che la porta host non ha effettuato l'accesso. È possibile utilizzare un'utility HBA o l'utility iSCSI Initiator per individuare gli identificatori delle porte host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host o copiarli/incollarli dall'utility (uno alla volta) nel campo host ports (Porte host). È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori associati all'host. Ciascun identificatore viene visualizzato nel campo host ports (Porte host). Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto.
Impostare CHAP Initiator secret	(Facoltativo) se si seleziona o si immette manualmente una porta host con un IQN iSCSI e si desidera richiedere a un host che tenta di accedere allo storage array per l'autenticazione mediante Challenge Handshake Authentication Protocol (CHAP), selezionare la casella di controllo "Set CHAP Initiator secret" (Imposta CHAP initiator secret). Per ogni porta host iSCSI selezionata o inserita manualmente, procedere come segue: • Immettere lo stesso segreto CHAP impostato su ciascun iniziatore host iSCSI per l'autenticazione CHAP. Se si utilizza l'autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di validarsi nell'array di storage e a un array di storage di validarsi nell'host), è necessario impostare anche il segreto CHAP per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lasciare vuoto il campo se non si richiede l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato è CHAP.

5. Fare clic su **Create** (Crea).
6. Per aggiornare le informazioni sull'host, selezionare l'host dalla tabella e fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

Risultato

Una volta creato correttamente l'host, il sistema crea un nome predefinito per ciascuna porta host configurata per l'host (etichetta utente). L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per l'host IPT è `IPT_1`.

Al termine

È necessario assegnare un volume a un host in modo che possa essere utilizzato per le operazioni di i/O. Passare a. "Assegnare volumi agli host".

Creare un cluster host

Quando due o più host richiedono l'accesso i/o agli stessi volumi, è possibile creare un cluster host.

A proposito di questa attività

Tenere presenti queste linee guida quando si crea un cluster host:

- Questa operazione non viene avviata a meno che non siano disponibili due o più host per la creazione del cluster.
- Gli host nei cluster di host possono avere sistemi operativi diversi (eterogenei).
- Gli host NVMe nei cluster di host non possono essere misti con host non NVMe.
- Per creare un volume abilitato per Data Assurance (da), la connessione host che si intende utilizzare deve supportare da.

  Se una delle connessioni host sui controller dello storage array non supporta il da, gli host associati non possono accedere ai dati sui volumi abilitati da.

- Questa operazione non riesce se il nome scelto è già in uso.
- La lunghezza del nome non può superare i 30 caratteri.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare **Create › host cluster** (Crea[cluster host]).

   Viene visualizzata la finestra di dialogo Create host Cluster (Crea cluster host).

4. Selezionare le impostazioni appropriate per il cluster host.

Impostazione	Descrizione
Nome	Digitare il nome del nuovo cluster host.
Selezionare gli host per condividere l'accesso al volume	Selezionare due o più host dall'elenco a discesa. Vengono visualizzati nell'elenco solo gli host che non fanno già parte di un cluster di host.

5. Fare clic su **Create** (Crea).

Se gli host selezionati sono collegati a tipi di interfaccia che hanno diverse funzionalità di Data Assurance (da), viene visualizzata una finestra di dialogo con il messaggio che da non sarà disponibile sul cluster host. Questa non disponibilità impedisce l'aggiunta di volumi abilitati da al cluster host. Selezionare **Sì** per continuare o **No** per annullare.

DA aumenta l'integrità dei dati nell'intero sistema storage. DA consente all'array di storage di verificare la presenza di errori che potrebbero verificarsi quando i dati vengono spostati tra gli host e i dischi. L'utilizzo di da per il nuovo volume garantisce il rilevamento di eventuali errori.

Risultato

Il nuovo cluster di host viene visualizzato nella tabella con gli host assegnati nelle righe sottostanti.

Al termine

È necessario assegnare un volume a un cluster host in modo che possa essere utilizzato per le operazioni di i/O. Passare a. "Assegnare volumi agli host".

Assegnare volumi agli host

È necessario assegnare un volume a un host o a un cluster di host in modo che possa essere utilizzato per le operazioni di i/O.

Prima di iniziare

Tenere presenti queste linee guida quando si assegnano volumi agli host:

- È possibile assegnare un volume a un solo host o cluster di host alla volta.
- I volumi assegnati vengono condivisi tra i controller dell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un cluster host per accedere a un volume. È necessario utilizzare un LUN univoco.
- Per i nuovi gruppi di volumi, se si attende la creazione e l'inizializzazione di tutti i volumi prima di assegnarli a un host, il tempo di inizializzazione del volume viene ridotto. Tenere presente che, una volta mappato un volume associato al gruppo di volumi, tutti i volumi torneranno all'inizializzazione più lenta.

A proposito di questa attività

L'assegnazione di un volume consente a un host o a un cluster di host di accedere a tale volume in un array di storage.

Durante questa attività vengono visualizzati tutti i volumi non assegnati, ma le funzioni per gli host con o senza Data Assurance (da) si applicano come segue:

- Per un host da-capable, è possibile selezionare i volumi che sono da-enabled o non da-enabled.
- Per un host che non supporta da, se si seleziona un volume abilitato da, viene visualizzato un avviso che indica che il sistema deve disattivare automaticamente da sul volume prima di assegnarlo all'host.

  L'assegnazione di un volume non riesce nelle seguenti condizioni:

- Vengono assegnati tutti i volumi.
- Il volume è già assegnato a un altro host o cluster di host. La possibilità di assegnare un volume non è disponibile nelle seguenti condizioni:
- Non esistono host o cluster di host validi.
- Non sono stati definiti identificatori di porta host per l'host.

- Sono state definite tutte le assegnazioni dei volumi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host a cui si desidera assegnare i volumi, quindi fare clic su **Assign Volumes** (Assegna volumi).

   Viene visualizzata una finestra di dialogo che elenca tutti i volumi che è possibile assegnare. È possibile ordinare qualsiasi colonna o digitare qualcosa nella casella Filter (filtro) per semplificare la ricerca di volumi specifici.

4. Selezionare la casella di controllo accanto a ciascun volume che si desidera assegnare oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
5. Fare clic su **Assegna** per completare l'operazione.

Risultati

Dopo aver assegnato correttamente uno o più volumi a un host o a un cluster di host, il sistema esegue le seguenti operazioni:

- Il volume assegnato riceve il successivo numero LUN disponibile. L'host utilizza il numero LUN per accedere al volume.
- Il nome del volume fornito dall'utente viene visualizzato negli elenchi dei volumi associati all'host. Se applicabile, il volume di accesso configurato in fabbrica viene visualizzato anche negli elenchi dei volumi associati all'host.

Annullare l'assegnazione dei volumi

Se non è più necessario l'accesso i/o a un volume, è possibile annullare l'assegnazione dall'host o dal cluster host.

A proposito di questa attività

Tenere presenti queste linee guida quando si annulla l'assegnazione di un volume:

- Se si rimuove l'ultimo volume assegnato da un cluster host e il cluster host dispone anche di host con volumi assegnati specifici, assicurarsi di rimuovere o spostare tali assegnazioni prima di rimuovere l'ultima assegnazione per il cluster host.
- Se un cluster host, un host o una porta host viene assegnata a un volume registrato nel sistema operativo, è necessario annullare la registrazione prima di poter rimuovere questi nodi.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host che si desidera modificare, quindi fare clic su **Annulla assegnazione volumi**.

Viene visualizzata una finestra di dialogo che mostra tutti i volumi attualmente assegnati.

4. Selezionare la casella di controllo accanto a ciascun volume che si desidera annullare l'assegnazione oppure selezionare la casella di controllo nell'intestazione della tabella per selezionare tutti i volumi.
5. Fare clic su **Annulla assegnazione**.

Risultati

- I volumi non assegnati sono disponibili per una nuova assegnazione.
- Fino a quando le modifiche non vengono configurate sull'host, il volume viene ancora riconosciuto dal sistema operativo host.

Modificare le impostazioni di un host

È possibile modificare il nome, il tipo di sistema operativo host e i cluster host associati per un host o un cluster host.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti dell'host.

4. Per modificare le proprietà dell'host, assicurarsi che la scheda **Proprietà** sia selezionata, quindi modificare le impostazioni in base alle esigenze.

   Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome dell'host fornito dall'utente. Specificare un nome per l'host.
Cluster host associato	È possibile scegliere una delle seguenti opzioni: • **None** — l'host rimane un host standalone. Se l'host è stato associato a un cluster host, il sistema rimuove l'host dal cluster. • **<Host Cluster>** — il sistema associa l'host al cluster selezionato.
Tipo di sistema operativo host	È possibile modificare il tipo di sistema operativo in esecuzione sull'host definito.

5. Per modificare le impostazioni delle porte, fare clic sulla scheda **host Ports** (Porte host), quindi modificare le impostazioni in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Porta host	È possibile scegliere una delle seguenti opzioni: • **Add** — utilizzare Add per associare un nuovo identificatore di porta host all'host. La lunghezza del nome dell'identificatore della porta host è determinata dalla tecnologia dell'interfaccia host. I nomi degli identificatori delle porte host Fibre Channel e Infiniband devono contenere 16 caratteri. I nomi degli identificatori delle porte host iSCSI hanno un massimo di 223 caratteri. La porta deve essere univoca. Un numero di porta già configurato non è consentito. • **Delete** — utilizzare Delete per rimuovere (disassociare) un identificatore di porta host. L'opzione Delete (Elimina) non rimuove fisicamente la porta host. Questa opzione rimuove l'associazione tra la porta host e l'host. A meno che non si rimuovano host bus adapter o iSCSI Initiator, la porta host viene ancora riconosciuta dal controller. Se si elimina un identificatore di porta host, questo non viene più associato a questo host. Inoltre, l'host perde l'accesso a uno qualsiasi dei volumi assegnati tramite questo identificatore di porta host.
Etichetta	Per modificare il nome dell'etichetta della porta, fare clic sull'icona **Modifica** (matita). Il nome dell'etichetta della porta deve essere univoco. Un nome di etichetta già configurato non è consentito.
Segreto CHAP	Viene visualizzato solo per gli host iSCSI. È possibile impostare o modificare il segreto CHAP per gli iniziatori (host iSCSI). Il sistema utilizza il metodo CHAP (Challenge Handshake Authentication Protocol), che convalida l'identità di destinazioni e iniziatori durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa chiamata CHAP secret (segreto CHAP).

6. Fare clic su **Save** (Salva).

Eliminare l'host o il cluster host

È possibile rimuovere un host o un cluster di host in modo che i volumi non siano più associati a tale host.

A proposito di questa attività

Tenere presenti queste linee guida quando si elimina un host o un cluster host:

- Tutte le assegnazioni di volume specifiche vengono eliminate e i volumi associati sono disponibili per una nuova assegnazione.
- Se l'host fa parte di un cluster host che dispone di assegnazioni specifiche, il cluster host non viene influenzato. Tuttavia, se l'host fa parte di un cluster di host che non ha altre assegnazioni, il cluster di host e qualsiasi altro host o identificativo di porta host associato ereditano eventuali assegnazioni predefinite.

- Tutti gli identificatori di porta host associati all'host diventano indefiniti.

Fasi

1. Dalla pagina Manage (Gestione), selezionare lo storage array con la connessione host.
2. Selezionare **Provisioning › Configure hosts** (Configura host).

   Viene visualizzata la pagina Configure hosts (Configura host).

3. Selezionare l'host o il cluster host che si desidera eliminare, quindi fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo di conferma.

4. Confermare che si desidera eseguire l'operazione, quindi fare clic su **Delete** (Elimina).

Risultati

Se si elimina un host, il sistema esegue le seguenti operazioni:

- Elimina l'host e, se applicabile, lo rimuove dal cluster host.
- Rimuove l'accesso a tutti i volumi assegnati.
- Riporta i volumi associati a uno stato non assegnato.
- Restituisce gli identificatori di porta host associati all'host a uno stato non associato. Se si elimina un cluster host, il sistema esegue le seguenti operazioni:
  - Elimina il cluster host e gli host associati (se presenti).
  - Rimuove l'accesso a tutti i volumi assegnati.
  - Riporta i volumi associati a uno stato non assegnato.
  - Restituisce gli identificatori di porta host associati agli host a uno stato non associato.

Configurare pool e gruppi di volumi

Panoramica dei pool e dei gruppi di volumi

Per eseguire il provisioning dello storage nel plug-in di storage per vCenter, creare un pool o un gruppo di volumi che conterrà i dischi rigidi (HDD) o SSD (Solid state Disk) che si desidera utilizzare nell'array di storage.

Provisioning

L'hardware fisico viene fornito in componenti logici in modo che i dati possano essere organizzati e recuperati facilmente. Sono supportati due tipi di raggruppamenti:

- Piscine
- Gruppi di volumi

I pool e i gruppi di volumi sono le unità di storage di livello superiore in un array di storage: Suddividono la capacità dei dischi in divisioni gestibili. All'interno di queste divisioni logiche si trovano i singoli volumi o LUN in cui sono memorizzati i dati.

Quando viene implementato un sistema storage, il primo passo consiste nel presentare la capacità disponibile dei dischi ai vari host:

- Creazione di pool o gruppi di volumi con capacità sufficiente
- Aggiunta del numero di dischi necessari per soddisfare i requisiti di performance al pool o al gruppo di volumi
- Selezione del livello di protezione RAID desiderato (se si utilizzano gruppi di volumi) per soddisfare specifici requisiti di business

È possibile avere pool o gruppi di volumi sullo stesso sistema di storage, ma un'unità non può far parte di più di un pool o gruppo di volumi. I volumi presentati agli host per i/o vengono quindi creati utilizzando lo spazio nel pool o nel gruppo di volumi.

Piscine

I pool sono progettati per aggregare i dischi rigidi fisici in un ampio spazio di storage e fornire una protezione RAID avanzata per l'IT. Un pool crea molti set RAID virtuali dal numero totale di dischi assegnati al pool e distribuisce i dati in modo uniforme tra tutti i dischi partecipanti. In caso di perdita o aggiunta di un disco, il sistema ribilancia dinamicamente i dati su tutti i dischi attivi.

I pool funzionano come un altro livello RAID, virtualizzando l'architettura RAID sottostante per ottimizzare le performance e la flessibilità durante l'esecuzione di attività come la ricostruzione, l'espansione del disco e la gestione della perdita del disco. Il sistema imposta automaticamente il livello RAID a 6 in una configurazione 8+2 (otto dischi dati più due dischi di parità).

Corrispondenza dei dischi

È possibile scegliere tra HDD o SSD da utilizzare nei pool; tuttavia, come per i gruppi di volumi, tutti i dischi nel pool devono utilizzare la stessa tecnologia. I controller selezionano automaticamente i dischi da includere, quindi è necessario assicurarsi di disporre di un numero sufficiente di dischi per la tecnologia scelta.

Gestione dei dischi guasti

I pool hanno una capacità minima di 11 dischi; tuttavia, la capacità di un disco è riservata alla capacità di riserva in caso di guasto di un disco. Questa capacità di riserva è chiamata "capacità di conservazione".

Quando vengono creati i pool, viene preservata una certa quantità di capacità per l'utilizzo in caso di emergenza. Questa capacità è espressa in termini di un certo numero di dischi, ma l'implementazione effettiva è distribuita nell'intero pool di dischi. La quantità predefinita di capacità conservata si basa sul numero di dischi nel pool.

Una volta creato il pool, è possibile modificare il valore della capacità di conservazione su una capacità maggiore o minore oppure impostarlo su una capacità di conservazione non pari a 0 unità. La capacità massima che è possibile conservare (espressa come numero di dischi) è 10, ma la capacità disponibile potrebbe essere inferiore, in base al numero totale di dischi nel pool.

Gruppi di volumi

I gruppi di volumi definiscono il modo in cui la capacità viene assegnata ai volumi nel sistema di storage. I dischi sono organizzati in gruppi RAID e i volumi risiedono tra i dischi di un gruppo RAID. Pertanto, le impostazioni di configurazione dei gruppi di volumi identificano i dischi che fanno parte del gruppo e il livello RAID utilizzato.

Quando si crea un gruppo di volumi, i controller selezionano automaticamente le unità da includere nel gruppo. È necessario scegliere manualmente il livello RAID per il gruppo. La capacità del gruppo di volumi corrisponde al numero totale di dischi selezionati, moltiplicato per la capacità.

Corrispondenza dei dischi

Per le dimensioni e le prestazioni, è necessario associare le unità del gruppo di volumi. Se nel gruppo di volumi sono presenti dischi più piccoli e più grandi, tutti i dischi vengono riconosciuti come la capacità più piccola. Se nel gruppo di volumi sono presenti dischi più lenti e veloci, tutti i dischi vengono riconosciuti alla velocità più bassa. Questi fattori influiscono sulle performance e sulla capacità complessiva del sistema storage.

Non è possibile combinare diverse tecnologie di dischi (dischi HDD e SSD). RAID 3, 5 e 6 sono limitati a un massimo di 30 dischi. RAID 1 e RAID 10 utilizzano il mirroring, pertanto questi gruppi di volumi devono avere un numero pari di dischi.

Gestione dei dischi guasti

I gruppi di volumi utilizzano i dischi hot spare come standby nel caso in cui un disco si guasti in volumi RAID 1/10, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. Un'unità hot spare non contiene dati e aggiunge un altro livello di ridondanza all'array di storage.

Se un disco si guasta nell'array di storage, il disco hot spare viene sostituito automaticamente per il disco guasto senza richiedere uno swap fisico. Se il disco hot spare è disponibile quando si verifica un guasto, il controller utilizza i dati di ridondanza per ricostruire i dati dal disco guasto al disco hot spare.

Decidere se utilizzare pool o gruppi di volumi

Scegli un pool

- Se hai bisogno di una ricostruzione più rapida dei dischi e di un'amministrazione dello storage semplificata e/o di un carico di lavoro altamente casuale.
- Se si desidera distribuire i dati per ciascun volume in modo casuale su un set di dischi che compongono il pool.non è possibile impostare o modificare il livello RAID dei pool o dei volumi nei pool. I pool utilizzano il livello RAID 6.

Scegliere un gruppo di volumi

- Se hai bisogno della massima larghezza di banda del sistema, della possibilità di ottimizzare le impostazioni dello storage e di un carico di lavoro altamente sequenziale.
- Se si desidera distribuire i dati tra i dischi in base a un livello RAID. È possibile specificare il livello RAID quando si crea il gruppo di volumi.
- Se si desidera scrivere i dati per ciascun volume in sequenza nel set di dischi che compongono il gruppo di volumi.

> Poiché i pool possono coesistere con i gruppi di volumi, un array di storage può contenere sia pool che gruppi di volumi.

Creazione automatica e manuale del pool

A seconda della configurazione dello storage, è possibile consentire al sistema di creare pool automaticamente o manualmente. Un pool è un insieme di dischi raggruppati in modo logico.

Prima di creare e gestire i pool, consultare le sezioni seguenti per sapere come vengono creati automaticamente i pool e quando potrebbe essere necessario crearli manualmente.

Creazione automatica

Quando il sistema rileva una capacità non assegnata nell'array di storage, avvia la creazione automatica del pool quando il sistema rileva una capacità non assegnata in un array di storage. Viene richiesto automaticamente di creare uno o più pool o di aggiungere la capacità non assegnata a un pool esistente o a entrambi.

La creazione automatica del pool si verifica quando si verifica una di queste condizioni:

- I pool non esistono nell'array di storage e sono presenti dischi simili a sufficienza per creare un nuovo pool.
- Vengono aggiunte nuove unità a un array di storage che dispone di almeno un pool.ogni unità in un pool deve essere dello stesso tipo di unità (HDD o SSD) e avere capacità simile. Il sistema richiede di completare le seguenti attività:
- Creare un singolo pool se il numero di dischi di questi tipi è sufficiente.
- Creare più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
- Aggiungere le unità al pool esistente se un pool è già definito nell'array di storage e aggiungere nuove unità dello stesso tipo di disco al pool.
- Aggiungere i dischi dello stesso tipo al pool esistente e utilizzare gli altri tipi di dischi per creare pool diversi se i nuovi dischi sono di tipi diversi.

Creazione manuale

Se la creazione automatica non riesce a determinare la configurazione migliore, potrebbe essere necessario creare un pool manualmente. Questa situazione può verificarsi per uno dei seguenti motivi:

- I nuovi dischi potrebbero essere aggiunti a più di un pool.
- Uno o più dei nuovi candidati al pool possono utilizzare la protezione contro la perdita di shelf o la protezione contro la perdita di cassetto.
- Uno o più dei candidati attuali del pool non possono mantenere la protezione contro la perdita di shelf o lo stato di protezione contro la perdita di cassetto.è anche possibile creare un pool manualmente se si dispone di più applicazioni sull'array di storage e non si desidera che siano in concorrenza con le stesse risorse di disco. In questo caso, è possibile creare manualmente un pool più piccolo per una o più applicazioni. È possibile assegnare solo uno o due volumi invece di assegnare il carico di lavoro a un pool di grandi dimensioni con molti volumi attraverso i quali distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di un'applicazione specifica può consentire alle operazioni degli array di storage di funzionare più rapidamente, con meno conflitti.

Crea pool automaticamente

È possibile creare pool automaticamente quando il sistema rileva almeno 11 dischi non assegnati o rileva un disco non assegnato idoneo per un pool esistente. Un pool è un insieme di dischi raggruppati in modo logico.

Prima di iniziare

È possibile avviare la finestra di dialogo Configurazione automatica pool quando si verifica una delle seguenti condizioni:

- È stato rilevato almeno un disco non assegnato che può essere aggiunto a un pool esistente con tipi di disco simili.
- Sono stati rilevati undici (11) o più dischi non assegnati che possono essere utilizzati per creare un nuovo

pool (se non possono essere aggiunti a un pool esistente a causa di tipi di dischi diversi).

A proposito di questa attività

È possibile utilizzare la creazione automatica del pool per configurare facilmente tutte le unità non assegnate nell'array di storage in un unico pool e per aggiungere unità nei pool esistenti.

Tenere presente quanto segue:

- Quando si aggiungono dischi a un array di storage, il sistema rileva automaticamente i dischi e richiede di creare un singolo pool o più pool in base al tipo di disco e alla configurazione corrente.
- Se i pool sono stati precedentemente definiti, il sistema richiede automaticamente di aggiungere le unità compatibili a un pool esistente. Quando vengono aggiunte nuove unità a un pool esistente, il sistema ridistribuisce automaticamente i dati nella nuova capacità, che ora include le nuove unità aggiunte.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Per la creazione del pool, è necessario utilizzare tutti i dischi dell'array di storage.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare **More › Avvia configurazione automatica del pool**.

   La tabella dei risultati elenca i nuovi pool, i pool esistenti con le unità aggiunte o entrambi. Per impostazione predefinita, un nuovo pool viene denominato con un numero sequenziale.

   Si noti che il sistema esegue le seguenti operazioni:

   - Crea un singolo pool se il numero di dischi con lo stesso tipo di disco (HDD o SSD) è sufficiente e la capacità è simile.
   - Crea più pool se la capacità non assegnata è costituita da diversi tipi di dischi.
   - Aggiunge le unità a un pool esistente se un pool è già definito nell'array di storage e si aggiungono nuove unità dello stesso tipo di disco al pool.
   - Aggiunge le unità dello stesso tipo di unità al pool esistente e utilizza gli altri tipi di unità per creare pool diversi se le nuove unità sono di tipi diversi di unità.
4. Per modificare il nome di un nuovo pool, fare clic sull'icona **Modifica** (la matita).
5. Per visualizzare ulteriori caratteristiche del pool, posizionare il cursore o toccare l'icona Dettagli (la pagina).

   Vengono visualizzate informazioni relative al tipo di disco, alla funzionalità di sicurezza, alla funzione di data assurance (da), alla protezione contro la perdita di shelf e alla protezione contro la perdita di cassetto.

   Per gli array di storage EF600 e EF300, vengono visualizzate anche le impostazioni relative al provisioning delle risorse e alle dimensioni dei blocchi di volume.

6. Fare clic su **Accept** (Accetta).

Creare il pool manualmente

È possibile creare un pool manualmente se l'installazione non soddisfa i requisiti per la configurazione automatica del pool. Un pool è un insieme di dischi raggruppati in modo

logico.

Prima di iniziare

- È necessario disporre di un minimo di 11 dischi con lo stesso tipo di disco (HDD o SSD).
- La protezione contro la perdita di shelf richiede che i dischi che compongono il pool si trovino in almeno sei diversi shelf di dischi e che non vi siano più di due dischi in un singolo shelf di dischi.
- La protezione contro la perdita di cassetto richiede che le unità che compongono il pool siano collocate in almeno cinque cassetti diversi e che il pool includa un numero uguale di shelf di dischi da ciascun cassetto.
- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Per la creazione del pool, è necessario utilizzare tutti i dischi dell'array di storage.

A proposito di questa attività

Durante la creazione del pool, determinerai le sue caratteristiche, come il tipo di disco, la funzionalità di sicurezza, la funzionalità di data assurance (da), la protezione contro la perdita di shelf e la protezione contro la perdita di cassetto.

Per gli array di storage EF600 e EF300, le impostazioni includono anche il provisioning delle risorse e le dimensioni dei blocchi di volume.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › Pool** (Crea[Pool])

   Viene visualizzata la finestra di dialogo Create Pool (Crea pool).

4. Digitare un nome per il pool.
5. (Facoltativo) se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   La tabella dei risultati elenca tutti i pool possibili che è possibile creare.

6. Selezionare il pool candidato che si desidera utilizzare in base alle seguenti caratteristiche, quindi fare clic su **Create** (Crea).

Dettagli campo

Caratteristica	Utilizzare
Capacità libera	Mostra la capacità libera del pool Candidate in GiB. Selezionare un pool candidato con la capacità adatta alle esigenze di storage dell'applicazione. Anche la capacità di conservazione (spare) viene distribuita in tutto il pool e non fa parte della capacità libera.
Totale dischi	Mostra il numero di dischi disponibili nel pool Candidate. Il sistema riserva automaticamente il maggior numero possibile di dischi per la capacità di conservazione (per ogni sei dischi in un pool, il sistema riserva un disco per la capacità di conservazione). Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti.
Dimensioni blocco unità (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che i dischi del pool possono scrivere. I valori possono includere: • 512 — dimensione del settore di 512 byte. • 4K — dimensione del settore di 4,096 byte.
Sicuro	Indica se il pool candidato è costituito interamente da dischi con funzionalità di protezione, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). • È possibile proteggere il pool con Drive Security, ma tutte le unità devono essere sicure per poter utilizzare questa funzione. • Se si desidera creare un pool solo FDE, cercare **Yes - FDE** nella colonna Secure-capable. Se si desidera creare un pool solo FIPS, cercare **Sì - FIPS** o **Sì - FIPS (misto)**. "Misto" indica una combinazione di dischi di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il pool funzionerà al livello di sicurezza inferiore (140-2). • È possibile creare un pool composto da dischi che possono essere o meno sicuri o che sono una combinazione di livelli di sicurezza. Se i dischi del pool includono dischi che non sono sicuri, non è possibile rendere il pool sicuro.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se il pool è protetto ed è stata creata una chiave di sicurezza, è possibile attivare la protezione selezionando la casella di controllo. L'unico modo per rimuovere Drive Security dopo averlo attivato è eliminare il pool e cancellare i dischi.

Caratteristica	Utilizzare
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo candidato del pool. DA controlla e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino ai dischi. Se si desidera utilizzare da, selezionare un pool che supporti da. Questa opzione è disponibile solo se la funzione da è stata attivata. Un pool può contenere dischi che supportano da o non da, ma tutti i dischi devono essere in grado di utilizzare questa funzione.
Funzionalità di provisioning delle risorse (solo EF300 e EF600)	Mostra se il provisioning delle risorse è disponibile per questo candidato del pool. Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.
Protezione contro la perdita di shelf	Mostra se è disponibile la protezione contro la perdita di shelf. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool se si verifica una perdita totale di comunicazione con un singolo shelf di dischi.
Protezione in caso di perdita del cassetto	Mostra se è disponibile la protezione contro le perdite dei cassetti, fornita solo se si utilizza uno shelf di dischi che contiene cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi in un pool se si verifica una perdita totale di comunicazione con un singolo cassetto in uno shelf di dischi.
Dimensioni dei blocchi di volume supportate (solo EF300 e EF600)	Mostra le dimensioni del blocco che è possibile creare per i volumi nel pool: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Creare un gruppo di volumi

È possibile creare un gruppo di volumi per uno o più volumi accessibili all'host. Un gruppo di volumi è un container per volumi con caratteristiche condivise, come il livello RAID e la capacità.

Prima di iniziare

Consultare le seguenti linee guida:

- È necessario almeno un disco non assegnato.
- Esistono dei limiti per quanto riguarda la capacità di un disco in un singolo gruppo di volumi. Questi limiti variano in base al tipo di host.
- Per attivare la protezione contro la perdita di scaffali/cassetti, è necessario creare un gruppo di volumi che utilizzi dischi posizionati in almeno tre shelf o cassetti, a meno che non si utilizzi RAID 1, dove due

shelf/cassetti sono il minimo.

- Quando si configura uno storage array EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di dischi nei primi 12 slot e a un numero uguale di dischi negli ultimi 12 slot. Questa configurazione aiuta i controller a utilizzare entrambi i bus PCIe lato disco in modo più efficace. Il sistema attualmente consente la selezione del disco nella funzione Advanced (Avanzate) quando si crea un gruppo di volumi.

Esaminare in che modo la scelta del livello RAID influisce sulla capacità risultante del gruppo di volumi.

- Se si seleziona RAID 1, è necessario aggiungere due dischi alla volta per assicurarsi che sia selezionata una coppia mirrorata. Il mirroring e lo striping (noto come RAID 10 o RAID 1+0) si ottengono selezionando quattro o più dischi.
- Se si seleziona RAID 5, è necessario aggiungere almeno tre dischi per creare il gruppo di volumi.
- Se si seleziona RAID 6, è necessario aggiungere almeno cinque dischi per creare il gruppo di volumi.

A proposito di questa attività

Durante la creazione del gruppo di volumi, è possibile determinare le caratteristiche del gruppo, ad esempio il numero di dischi, la funzionalità di sicurezza, la funzionalità di data assurance (da), la protezione contro la perdita di shelf e la protezione contro la perdita di cassetto.

Per gli array di storage EF600 e EF300, le impostazioni includono anche il provisioning delle risorse, le dimensioni dei blocchi dei dischi e le dimensioni dei blocchi dei volumi.

> Con dischi con capacità maggiore e la possibilità di distribuire volumi tra controller, la creazione di più di un volume per gruppo di volumi è un buon modo per sfruttare la capacità dello storage e proteggere i dati.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage per il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › Volume group** (Crea[gruppo di volumi]).

   Viene visualizzata la finestra di dialogo Create Volume Group (Crea gruppo di volumi).

4. Digitare un nome per il gruppo di volumi.
5. Seleziona il livello RAID che meglio soddisfa i tuoi requisiti di storage e protezione dei dati. Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il livello RAID selezionato.
6. (Facoltativo) se si dispone di più di un tipo di disco nell'array di storage, selezionare il tipo di disco che si desidera utilizzare.

   Viene visualizzata la tabella dei candidati del gruppo di volumi che mostra solo i candidati che supportano il tipo di disco e il livello RAID selezionati.

7. (Facoltativo) è possibile selezionare il metodo automatico o manuale per definire le unità da utilizzare nel gruppo di volumi. Il metodo automatico è la selezione predefinita.

   > Non utilizzare il metodo manuale a meno che non si sia esperti in grado di comprendere la ridondanza dei dischi e le configurazioni ottimali dei dischi.

Per selezionare i dischi manualmente, fare clic sul collegamento **Manually Select drives (Advanced)** (Seleziona manualmente i dischi (avanzati)**). Quando si fa clic su di esso, viene visualizzato *Automatically Select drives (Advanced)**.

Il metodo Manuale consente di selezionare le unità specifiche che compongono il gruppo di volumi. È possibile selezionare dischi non assegnati specifici per ottenere la capacità richiesta. Se l'array di storage contiene dischi con tipi di supporti diversi o tipi di interfaccia diversi, è possibile scegliere solo la capacità non configurata per un singolo tipo di disco per creare il nuovo gruppo di volumi.

8. In base alle caratteristiche del disco visualizzate, selezionare le unità che si desidera utilizzare nel gruppo di volumi, quindi fare clic su **Create** (Crea).

Le caratteristiche del disco visualizzate dipendono dalla selezione del metodo automatico o manuale. Per ulteriori informazioni, consultare la documentazione di Gestione di sistema di SANtricity, "Creare un gruppo di volumi".

Aggiungere capacità a un pool o a un gruppo di volumi

È possibile aggiungere dischi per espandere la capacità libera in un pool o un gruppo di volumi esistente.

Prima di iniziare

- I dischi devono essere in uno stato ottimale.
- I dischi devono avere lo stesso tipo di disco (HDD o SSD).
- Il pool o il gruppo di volumi deve essere in uno stato ottimale.
- Se il pool o il gruppo di volumi contiene tutti i dischi con funzionalità di protezione, aggiungere solo i dischi in grado di protezione per continuare a utilizzare le funzionalità di crittografia dei dischi con funzionalità di protezione.

Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard).

A proposito di questa attività

In questa attività, è possibile aggiungere capacità libera da includere nel pool o nel gruppo di volumi. È possibile utilizzare questa capacità libera per creare volumi aggiuntivi. I dati nei volumi rimangono accessibili durante questa operazione.

Per i pool, è possibile aggiungere un massimo di 60 dischi alla volta. Per i gruppi di volumi, è possibile aggiungere un massimo di due dischi alla volta. Se è necessario aggiungere più dischi del numero massimo, ripetere la procedura. (Un pool non può contenere più dischi rispetto al limite massimo per un array di storage).

> Con l'aggiunta di dischi, potrebbe essere necessario aumentare la capacità di conservazione. Si consiglia di aumentare la capacità riservata dopo un'operazione di espansione.

> Evitare di utilizzare dischi che siano in grado di aggiungere capacità a un pool o a un gruppo di volumi che non sono in grado di supportare da. Il pool o il gruppo di volumi non può sfruttare le funzionalità del disco da-capable. Prendere in considerazione l'utilizzo di dischi che non sono in grado di supportare da in questa situazione.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.

2. Selezionare **Provisioning › Configura pool e gruppi di volumi**.
3. Selezionare il pool o il gruppo di volumi a cui si desidera aggiungere le unità, quindi fare clic su **Add Capacity** (Aggiungi capacità).

   Viene visualizzata la finestra di dialogo Add Capacity (Aggiungi capacità). Vengono visualizzate solo le unità non assegnate compatibili con il pool o il gruppo di volumi.

4. In **Select drives to add Capacity…** (Seleziona dischi per aggiungere capacità), selezionare una o più unità che si desidera aggiungere al pool o al gruppo di volumi esistente.

   Il firmware del controller dispone le unità non assegnate con le opzioni migliori elencate in alto. La capacità libera totale aggiunta al pool o al gruppo di volumi viene visualizzata sotto l'elenco in **capacità totale selezionata**.

Dettagli campo

Campo	Descrizione
Shelf	Indica la posizione dello shelf del disco.
Baia	Indica la posizione dell'alloggiamento del disco
Capacità (GiB)	Indica la capacità del disco. • Se possibile, selezionare dischi con capacità uguale a quella dei dischi correnti nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità inferiore, tenere presente che la capacità utilizzabile di ogni disco attualmente presente nel pool o nel gruppo di volumi è ridotta. Pertanto, la capacità del disco è la stessa nel pool o nel gruppo di volumi. • Se è necessario aggiungere dischi non assegnati con una capacità maggiore, tenere presente che la capacità utilizzabile dei dischi non assegnati aggiunti viene ridotta in modo che corrispondano alle capacità correnti dei dischi nel pool o nel gruppo di volumi.
Sicuro	Indica se il disco è sicuro. • È possibile proteggere il pool o il gruppo di volumi con la funzione Drive Security, ma per utilizzare questa funzione è necessario che tutti i dischi siano protetti. • È possibile creare un pool o un gruppo di volumi con una combinazione di dischi sicuri e non sicuri, ma non è possibile attivare la funzione Drive Security. • Un pool o un gruppo di volumi con tutti i dischi con funzionalità di protezione non può accettare un disco con funzionalità di protezione non sicura per lo sparing o l'espansione, anche se la funzionalità di crittografia non è in uso. • Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). Un disco FIPS può essere di livello 140-2 o 140-3, con il livello 140-3 come livello di sicurezza superiore. Se si seleziona una combinazione di dischi di livello 140-2 e 140-3, il pool o il gruppo di volumi opereranno al livello di sicurezza inferiore (140-2).

Campo	Descrizione
Compatibile CON DA	Indica se il disco è compatibile con Data Assurance (da). • Si sconsiglia l'utilizzo di dischi che non sono in grado di aggiungere capacità a un pool o a un gruppo di volumi con funzionalità da. Il pool o il gruppo di volumi non dispone più delle funzionalità da e non è più possibile attivare il da sui volumi appena creati all'interno del pool o del gruppo di volumi. • Si sconsiglia l'utilizzo di dischi in grado di aggiungere capacità a un pool o a un gruppo di volumi non compatibili con da, in quanto tale pool o gruppo di volumi non può sfruttare le funzionalità del disco compatibile con da (gli attributi del disco non corrispondono). Considerare l'utilizzo di dischi non compatibili con da in questa situazione.
Compatibile con DULBE	Indica se il disco dispone dell'opzione Deallocated (disallocato) o Unwritten Logical Block Error (DULBE). DULBE è un'opzione sui dischi NVMe che consente allo storage array EF300 o EF600 di supportare volumi con provisioning di risorse.

5. Fare clic su **Aggiungi**.

   Se si aggiungono unità a un pool o a un gruppo di volumi, viene visualizzata una finestra di dialogo di conferma se si seleziona un'unità che impedisce al pool o al gruppo di volumi di avere uno o più dei seguenti attributi:

   - Protezione contro la perdita di shelf
   - Protezione in caso di perdita del cassetto
   - Funzionalità di crittografia completa del disco
   - Funzionalità Data Assurance
   - Funzionalità DULBE
6. Per continuare, fare clic su **Sì**, altrimenti fare clic su **Annulla**.

Risultato

Dopo aver aggiunto le unità non assegnate a un pool o a un gruppo di volumi, i dati di ciascun volume del pool o del gruppo di volumi vengono ridistribuiti per includere le unità aggiuntive.

Creazione della cache SSD

Per accelerare dinamicamente le performance del sistema, puoi utilizzare la funzione SSD cache per memorizzare nella cache i dati più utilizzati (dati "hot") su unità a stato solido (SSD) a latenza inferiore. La cache SSD viene utilizzata esclusivamente per le letture host.

Prima di iniziare

L'array di storage deve contenere alcune unità SSD.

La cache SSD non è disponibile sul sistema storage EF600 o EF300.

A proposito di questa attività

Quando crei una cache SSD, puoi utilizzare una o più unità. Poiché la cache di lettura si trova nell'array di storage, il caching viene condiviso tra tutte le applicazioni che utilizzano l'array di storage. Selezionare i volumi che si desidera memorizzare nella cache, quindi il caching viene automaticamente e dinamico.

Per creare la cache SSD, seguire queste linee guida.

- È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
- È supportata una sola cache SSD per array di storage.
- La capacità massima di cache SSD utilizzabile su un array di storage dipende dalla capacità della cache primaria del controller.
- La cache SSD non è supportata sulle immagini Snapshot.
- Se si importano o esportano volumi con cache SSD attivata o disattivata, i dati memorizzati nella cache non vengono importati o esportati.
- Qualsiasi volume assegnato per l'utilizzo della cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.
- Se i volumi associati sono abilitati per la sicurezza, creare una cache SSD abilitata per la sicurezza.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage per la cache.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Fare clic sul **Create › SSD cache** (Crea[cache SSD]).

   Viene visualizzata la finestra di dialogo Create SSD cache (Crea cache SSD).

4. Digitare un nome per la cache SSD.
5. Selezionare l'SSD cache Candidate che si desidera utilizzare in base alle seguenti caratteristiche.

Dettagli campo

Caratteristica	Utilizzare
Capacità	Mostra la capacità disponibile in GiB. Selezionare la capacità per le esigenze di storage dell'applicazione. La capacità massima per la cache SSD dipende dalla capacità della cache primaria del controller. Se si assegna una quantità superiore a quella massima alla cache SSD, la capacità aggiuntiva non è utilizzabile. La capacità della cache SSD è importante per la capacità complessiva allocata.
Dischi totali	Mostra il numero di dischi disponibili per questa cache SSD. Selezionare l'SSD candidate con il numero di dischi desiderato
Sicuro	Indica se SSD cache Candidate è composto interamente da dischi sicuri, che possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). Se si desidera creare una cache SSD sicura, cercare "Yes - FDE" o "Yes - FIPS" nella colonna Secure-capable.
Abilitare la sicurezza?	Fornisce l'opzione per attivare la funzione Drive Security con dischi sicuri. Se si desidera creare una cache SSD abilitata per la protezione, selezionare la casella di controllo **Enable Security** (attiva sicurezza). NOTA: Una volta attivata, la protezione non può essere disattivata. È possibile attivare la sicurezza sulla cache SSD solo quando viene creata, non in un secondo momento.
Compatibile CON DA	Indica se Data Assurance (da) è disponibile per questo SSD cache Candidate. Data Assurance (da) verifica e corregge gli errori che potrebbero verificarsi quando i dati vengono trasferiti attraverso i controller fino ai dischi. Se si desidera utilizzare il da, selezionare un SSD cache Candidate che sia compatibile con il da. Questa opzione è disponibile solo se la funzione da è stata attivata. La cache SSD può contenere sia dischi da-capable che non da-capable, ma tutti i dischi devono essere da-capable per poter utilizzare da.

6. Associare la cache SSD ai volumi per i quali si desidera implementare il caching in lettura SSD. Per attivare immediatamente la cache SSD sui volumi compatibili, selezionare la casella di controllo **Enable SSD cache on existing compatible volumes that are mapped to hosts** (attiva cache SSD sui volumi compatibili esistenti mappati agli host).

   I volumi sono compatibili se condividono le stesse funzionalità di Drive Security e da.

7. Fare clic su **Create** (Crea).

Modificare le impostazioni di configurazione di un pool

È possibile modificare le impostazioni di un pool, inclusi nome, impostazioni degli avvisi di capacità, priorità di modifica e capacità di conservazione.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni di configurazione per un pool.

Non è possibile modificare il livello RAID di un pool utilizzando l'interfaccia del plug-in. Il plug-in configura automaticamente i pool come RAID 6.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il pool che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Pool Settings (Impostazioni pool).

4. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del pool in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome del pool fornito dall'utente. Specificare un nome per un pool è obbligatorio.
Avvisi di capacità	È possibile inviare notifiche di avviso quando la capacità libera di un pool raggiunge o supera una determinata soglia. Quando i dati memorizzati nel pool superano la soglia specificata, il plug-in invia un messaggio, consentendo di aggiungere più spazio di storage o di eliminare oggetti non necessari. Gli avvisi vengono visualizzati nell'area Notifiche della dashboard e possono essere inviati dal server agli amministratori tramite messaggi e-mail e messaggi trap SNMP. È possibile definire i seguenti avvisi di capacità: • **Critical alert** — questo avviso critico informa l'utente quando la capacità libera nel pool raggiunge o supera la soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica. • **Early alert** — questo avviso anticipato informa l'utente quando la capacità libera di un pool sta raggiungendo una soglia specificata. Utilizzare i controlli di spinner per regolare la percentuale di soglia. Selezionare la casella di controllo per disattivare questa notifica.
Priorità di modifica	È possibile specificare i livelli di priorità per le operazioni di modifica in un pool in relazione alle prestazioni del sistema. Una priorità più elevata per le operazioni di modifica in un pool consente di completare più rapidamente un'operazione, ma può rallentare le prestazioni di i/o dell'host. Una priorità più bassa fa sì che le operazioni richiedano più tempo, ma le prestazioni di i/o dell'host ne risentono meno. È possibile scegliere tra cinque livelli di priorità: Minimo, basso, medio, alto e massimo. Maggiore è il livello di priorità, maggiore è l'impatto sull'i/o host e sulle prestazioni del sistema. • **Priorità di ricostruzione critica** — questa barra di scorrimento determina la priorità di un'operazione di ricostruzione dei dati quando guasti multipli dei dischi causano una condizione in cui alcuni dati non hanno ridondanza e un guasto aggiuntivo dei dischi potrebbe causare la perdita di dati. • **Priorità di ricostruzione degradata** — questa barra di scorrimento determina la priorità dell'operazione di ricostruzione dei dati quando si verifica un guasto al disco, ma i dati continuano a essere ridondanti e un guasto aggiuntivo al disco non comporta la perdita di dati. • **Priorità delle operazioni in background** — questa barra di scorrimento determina la priorità delle operazioni in background del pool che si verificano mentre il pool si trova in uno stato ottimale. Queste operazioni includono Dynamic Volume Expansion (DVE), Instant Availability Format (IAF) e la migrazione dei dati su un disco sostituito o aggiunto.

Impostazione	Descrizione
Capacità di conservazione ("capacità di ottimizzazione" per EF600 o EF300)	**Capacità di conservazione** — è possibile definire il numero di dischi per determinare la capacità riservata al pool per supportare potenziali guasti del disco. Quando si verifica un guasto al disco, la capacità di conservazione viene utilizzata per conservare i dati ricostruiti. I pool utilizzano la capacità di conservazione durante il processo di ricostruzione dei dati invece delle unità hot spare, utilizzate nei gruppi di volumi. Utilizzare i controlli di spinner per regolare il numero di dischi. In base al numero di dischi, la capacità di conservazione nel pool viene visualizzata accanto alla casella di selezione. Tenere presenti le seguenti informazioni sulla capacità di conservazione. • Poiché la capacità di conservazione viene sottratta dalla capacità libera totale di un pool, la quantità di capacità che si riserva influisce sulla quantità di capacità libera disponibile per la creazione dei volumi. Se si specifica 0 per la capacità di conservazione, tutta la capacità libera del pool viene utilizzata per la creazione del volume. • Se si riduce la capacità di conservazione, si aumenta la capacità che può essere utilizzata per i volumi del pool. **Capacità di ottimizzazione aggiuntiva (solo array EF600 e EF300)** — quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e performance e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

5. Fare clic su **Save** (Salva).

Modificare le impostazioni di configurazione di un gruppo di volumi

È possibile modificare le impostazioni di un gruppo di volumi, inclusi il nome e il livello RAID.

Prima di iniziare

Se si modifica il livello RAID per soddisfare le esigenze di performance delle applicazioni che accedono al gruppo di volumi, assicurarsi di soddisfare i seguenti prerequisiti:

- Il gruppo di volumi deve trovarsi in uno stato ottimale.

- È necessario disporre di capacità sufficiente nel gruppo di volumi per la conversione al nuovo livello RAID.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il gruppo di volumi che si desidera modificare, quindi fare clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Volume Group Settings (Impostazioni gruppo di volumi).

4. Selezionare la scheda **Impostazioni**, quindi modificare le impostazioni del gruppo di volumi in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	È possibile modificare il nome fornito dall'utente del gruppo di volumi. Specificare un nome per un gruppo di volumi.
Livello RAID	Selezionare il nuovo livello RAID dal menu a discesa. • **RAID 0 striping** — offre performance elevate ma non fornisce alcuna ridondanza dei dati. Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi. Un gruppo RAID di striping combina due o più dischi in un'unica grande unità logica. • **Mirroring RAID 1** — offre performance elevate e la migliore disponibilità dei dati ed è adatto per la memorizzazione di dati sensibili a livello aziendale o personale. Protegge i dati eseguendo automaticamente il mirroring del contenuto di un disco nel secondo disco della coppia mirrorata. Fornisce protezione in caso di guasto di un singolo disco. • **RAID 10 striping/mirroring** — fornisce una combinazione di RAID 0 (striping) e RAID 1 (mirroring) e si ottiene selezionando quattro o più dischi. RAID 10 è adatto per applicazioni di transazioni di volumi elevati, come un database, che richiedono performance elevate e tolleranza agli errori. • **RAID 5** — ottimale per ambienti multiutente (come storage di database o file system) in cui le dimensioni i/o tipiche sono ridotte e l'attività di lettura è molto elevata. • **RAID 6** — ottimale per ambienti che richiedono una protezione di ridondanza oltre RAID 5, ma che non richiedono elevate prestazioni di scrittura. RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando (CLI). Quando si modifica il livello RAID, non è possibile annullare questa operazione dopo l'inizio. Durante la modifica, i dati rimangono disponibili.
Capacità di ottimizzazione (solo array EF600)	Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che fornisce un equilibrio tra capacità disponibile e prestazioni e durata del disco. È possibile regolare questo bilanciamento spostando il cursore verso destra per migliorare le prestazioni e la durata del disco a scapito della maggiore capacità disponibile, oppure spostandolo verso sinistra per aumentare la capacità disponibile a scapito di migliori prestazioni e durata del disco. I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata. Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

5. Fare clic su **Save** (Salva).

Viene visualizzata una finestra di dialogo di conferma se la capacità viene ridotta, la ridondanza del volume viene persa o la protezione dalla perdita di shelf/cassetto viene persa a seguito della modifica del livello RAID. Selezionare **Sì** per continuare, altrimenti fare clic su **No**.

Risultato

Se si modifica il livello RAID per un gruppo di volumi, il plug-in modifica i livelli RAID di ogni volume che comprende il gruppo di volumi. Le prestazioni potrebbero essere leggermente compromesse durante l'operazione.

Modificare le impostazioni della cache SSD

È possibile modificare il nome della cache SSD e visualizzarne lo stato, la capacità massima e corrente, lo stato di Drive Security e Data Assurance e i volumi e i dischi associati.

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con la cache SSD.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare la cache SSD che si desidera modificare, quindi fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni).

   Viene visualizzata la finestra di dialogo SSD cache Settings (Impostazioni cache SSD).

4. Rivedere o modificare le impostazioni della cache SSD in base alle esigenze.

Dettagli campo

Impostazione	Descrizione
Nome	Visualizza il nome della cache SSD, che è possibile modificare. È necessario specificare un nome per la cache SSD.
Caratteristiche	Mostra lo stato della cache SSD. Gli stati possibili includono: • Ottimale • Sconosciuto • Degradato • Non riuscito (Uno stato di errore determina un evento MEL critico). • Sospeso
Capacità	Mostra la capacità corrente e la capacità massima consentita per la cache SSD. La capacità massima consentita per la cache SSD dipende dalle dimensioni della cache principale del controller: • Fino a 1 GiB • Da 1 GiB a 2 GiB • Da 2 GiB a 4 GiB • Più di 4 GiB
Sicurezza e da	Mostra lo stato di Drive Security e Data Assurance per la cache SSD. • **Secure-capable** - indica se la cache SSD è composta interamente da dischi sicuri. Un disco sicuro è un disco con crittografia automatica in grado di proteggere i propri dati da accessi non autorizzati. • **Secure-enabled** — indica se la sicurezza è attivata nella cache SSD. • **Da Capable** — indica se la cache SSD è composta interamente da dischi compatibili con da. Un disco con funzionalità da può controllare e correggere gli errori che potrebbero verificarsi quando i dati vengono comunicati tra l'host e lo storage array.
Oggetti associati	Mostra i volumi e i dischi associati alla cache SSD.

5. Fare clic su **Save** (Salva).

Visualizzare le statistiche della cache SSD

È possibile visualizzare le statistiche per la cache SSD, ad esempio letture, scritture, accessi alla cache, percentuale di allocazione della cache, e percentuale di utilizzo della cache.

Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

A proposito di questa attività

Le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate, sono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare statistiche dettagliate per la cache SSD solo quando si esportano tutte le statistiche SSD in un file .csv.

Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con la cache SSD.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare la cache SSD per la quale si desidera visualizzare le statistiche, quindi fare clic su **More › View SSD cache** statistics.

   Viene visualizzata la finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD) che visualizza le statistiche nominali per la cache SSD selezionata.

   Dettagli campo

Impostazione	Descrizione
Letture	Mostra il numero totale di letture host dai volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Scrive	Il numero totale di scritture dell'host nei volumi abilitati per la cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Riscontri nella cache	Mostra il numero di accessi alla cache.
La cache colpisce %	Mostra la percentuale di accessi alla cache. Questo numero deriva da riscontri cache / (letture + scritture). La percentuale di hit della cache deve essere superiore al 50% per un funzionamento efficace della cache SSD.
Allocazione della cache %	Mostra la percentuale di storage cache SSD allocato, espressa come percentuale dello storage cache SSD disponibile per questo controller e derivata dai byte allocati/disponibili.
% Utilizzo cache	Mostra la percentuale di storage cache SSD che contiene i dati dei volumi abilitati, espressa come percentuale di storage cache SSD allocata. Questa quantità rappresenta l'utilizzo o la densità della cache SSD. Derivato da byte allocati/byte disponibili.
Esporta tutto	Esporta tutte le statistiche della cache SSD in formato CSV. Il file esportato contiene tutte le statistiche disponibili per la cache SSD (nominale e dettagliata).

4. Fare clic su **Annulla** per chiudere la finestra di dialogo.

Controllare la ridondanza del volume

Sotto la guida del supporto tecnico o secondo le istruzioni del Recovery Guru, è possibile controllare la ridondanza su un volume in un pool o un gruppo di volumi per determinare se i dati su quel volume sono coerenti.

I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

Prima di iniziare

- Lo stato del pool o del gruppo di volumi deve essere ottimale.
- Il pool o il gruppo di volumi non deve avere alcuna operazione di modifica del volume in corso.
- È possibile controllare la ridondanza su qualsiasi livello RAID tranne su RAID 0, perché RAID 0 non ha ridondanza dei dati. (I pool sono configurati solo come RAID 6).

> Controllare la ridondanza del volume solo quando richiesto dal Recovery Guru e sotto la guida del supporto tecnico.

A proposito di questa attività

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6 e verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se il firmware del controller determina che i dati sono incoerenti.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare **operazioni non comuni › controllare la ridondanza del volume**.

   Viene visualizzata la finestra di dialogo Check Redundancy (verifica ridondanza).

4. Selezionare i volumi che si desidera controllare, quindi digitare check per confermare che si desidera eseguire questa operazione.
5. Fare clic su **Controlla**.

   Viene avviata l'operazione di controllo della ridondanza del volume. I volumi nel pool o nel gruppo di volumi vengono sottoposti a scansione in sequenza, a partire dalla parte superiore della tabella nella finestra di dialogo. Queste azioni si verificano quando viene eseguita la scansione di ciascun volume:

   - Il volume viene selezionato nella tabella dei volumi.

- Lo stato del controllo di ridondanza viene visualizzato nella colonna Status (Stato).
- Il controllo si interrompe in caso di errore di parità o supporto, quindi riporta l'errore. La seguente tabella fornisce ulteriori informazioni sullo stato del controllo di ridondanza:

Dettagli campo

Stato	Descrizione
In sospeso	Si tratta del primo volume da sottoporre a scansione e non è stato fatto clic su Start (Avvia) per avviare il controllo di ridondanza. -Oppure- l'operazione di controllo della ridondanza viene eseguita su altri volumi nel pool o nel gruppo di volumi.
Verifica in corso	Il volume è sottoposto al controllo di ridondanza.
Superato	Il volume ha superato il controllo di ridondanza. Non sono state rilevate incongruenze nelle informazioni di ridondanza.
Non riuscito	Il volume non ha superato il controllo di ridondanza. Sono state rilevate incoerenze nelle informazioni di ridondanza.
Errore supporto	Il disco rigido è difettoso e illeggibile. Seguire le istruzioni visualizzate nel Recovery Guru.
Errore di parità	La parità non è quella che dovrebbe essere per una determinata parte dei dati. Un errore di parità è potenzialmente grave e potrebbe causare una perdita permanente di dati.

6. Fare clic su **Done** (fine) dopo aver controllato l'ultimo volume del pool o del gruppo di volumi.

Eliminare pool o gruppo di volumi

È possibile eliminare un pool o un gruppo di volumi per creare una maggiore capacità non assegnata, che è possibile riconfigurare per soddisfare le esigenze di storage dell'applicazione.

Prima di iniziare

- È necessario aver eseguito il backup dei dati su tutti i volumi del pool o del gruppo di volumi.
- È necessario aver interrotto tutti gli input/output (i/o).
- È necessario smontare tutti i file system sui volumi.
- È necessario eliminare tutte le relazioni mirror nel pool o nel gruppo di volumi.
- È necessario interrompere qualsiasi operazione di copia del volume in corso per il pool o il gruppo di volumi.
- Il pool o il gruppo di volumi non deve partecipare a un'operazione di mirroring asincrono.
- I dischi nel gruppo di volumi non devono avere una prenotazione persistente.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare un pool o un gruppo di volumi dall'elenco.

È possibile selezionare un solo pool o gruppo di volumi alla volta. Scorrere l'elenco per visualizzare altri pool o gruppi di volumi.

4. Selezionare **attività non comuni › Elimina** e confermare.

Risultati

Il sistema esegue le seguenti operazioni:

- Elimina tutti i dati del pool o del gruppo di volumi.
- Elimina tutte le unità associate al pool o al gruppo di volumi.
- Annulla l'assegnazione delle unità associate, che consente di riutilizzarle in pool o gruppi di volumi nuovi o esistenti.

Consolidare la capacità libera per un gruppo di volumi

Utilizzare l'opzione consolida capacità libera per consolidare le estensioni libere esistenti su un gruppo di volumi selezionato. Eseguendo questa azione, è possibile creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi.

Prima di iniziare

- Il gruppo di volumi deve contenere almeno un'area di capacità libera.
- Tutti i volumi nel gruppo di volumi devono essere online e in uno stato ottimale.
- Le operazioni di modifica del volume non devono essere in corso, ad esempio la modifica delle dimensioni del segmento di un volume.

A proposito di questa attività

Non è possibile annullare l'operazione dopo l'inizio. I dati rimangono accessibili durante l'operazione di consolidamento.

È possibile avviare la finestra di dialogo consolida capacità libera utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, la raccomandazione di consolidare la capacità libera viene visualizzata nella home page dell'area di notifica. Fare clic sul collegamento **consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Consolida capacità libera dalla pagina Pools & Volume Groups come descritto nella seguente attività.

Ulteriori informazioni sulle aree di capacità libera

Un'area di capacità libera è la capacità libera che può derivare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità disponibile durante la creazione del volume. Quando si crea un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume viene limitata alla maggiore area di capacità libera del gruppo di volumi. Ad esempio, se un gruppo di volumi ha una capacità libera totale di 15 GiB e l'area di capacità libera più grande è di 10 GiB, il volume più grande che è possibile creare è di 10 GiB.

È possibile consolidare la capacità libera su un gruppo di volumi per migliorare le prestazioni di scrittura. La capacità libera del gruppo di volumi si frammenterà nel tempo man mano che l'host scrive, modifica ed elimina i file. Infine, la capacità disponibile non verrà collocata in un singolo blocco contiguo, ma verrà distribuita in piccoli frammenti all'interno del gruppo di volumi. Ciò causa un'ulteriore frammentazione dei file, poiché l'host deve scrivere nuovi file come frammenti per inserirli negli intervalli disponibili dei cluster liberi.

Consolidando la capacità libera su un gruppo di volumi selezionato, si noteranno migliori performance del file system ogni volta che l'host scrive nuovi file. Il processo di consolidamento consentirà inoltre di evitare la frammentazione dei nuovi file in futuro.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage con il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il gruppo di volumi con capacità libera che si desidera consolidare, quindi selezionare **Uncommon Tasks › consolida capacità libera del gruppo di volumi**.

   Viene visualizzata la finestra di dialogo consolida capacità libera.

4. Tipo `consolidate` per confermare che si desidera eseguire questa operazione.
5. Fare clic su **consolida**.

Risultato

Il sistema inizia a consolidare (deframmentare) le aree di capacità libera del gruppo di volumi in una quantità contigua per le successive attività di configurazione dello storage.

Al termine

Dalla barra laterale di navigazione, selezionare **Operations** per visualizzare l'avanzamento dell'operazione di consolidamento della capacità libera. Questa operazione può essere lunga e può influire sulle prestazioni del sistema.

Accendere le luci di individuazione

È possibile individuare le unità per identificare fisicamente tutte le unità che comprendono un pool, un gruppo di volumi o una cache SSD selezionata. Un indicatore LED si accende su ogni disco nel pool, gruppo di volumi o cache SSD selezionato.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).

3. Selezionare il pool, il gruppo di volumi o la cache SSD che si desidera individuare, quindi fare clic su **More › Turn on locator lights** (attiva indicatori di ricerca).

   Viene visualizzata una finestra di dialogo che indica che le spie dei dischi che compongono il pool, il gruppo di volumi o la cache SSD selezionati sono accese.

4. Una volta individuati correttamente i dischi, fare clic su **Spegni**.

Rimuovere la capacità

È possibile rimuovere i dischi per ridurre la capacità di un pool o di una cache SSD esistente.

Dopo aver rimosso i dischi, i dati in ciascun volume del pool o della cache SSD vengono ridistribuiti nei dischi rimanenti. I dischi rimossi non vengono assegnati e la loro capacità diventa parte della capacità libera totale dell'array di storage.

A proposito di questa attività

Quando si rimuove la capacità, attenersi alle seguenti linee guida:

- Non è possibile rimuovere l'ultimo disco in una cache SSD senza prima eliminare la cache SSD.
- Non è possibile ridurre il numero di dischi in un pool a meno di 11 dischi.
- È possibile rimuovere un massimo di 12 dischi alla volta. Se è necessario rimuovere più di 12 dischi, ripetere la procedura.
- Non è possibile rimuovere i dischi se la capacità libera nel pool o nella cache SSD non è sufficiente per contenere i dati, quando tali dati vengono ridistribuiti ai dischi rimanenti nel pool o nella cache SSD.

Di seguito sono riportati i potenziali impatti sulle performance:

- La rimozione dei dischi da un pool o da una cache SSD potrebbe ridurre le performance dei volumi.
- La capacità di conservazione non viene consumata quando si rimuove la capacità da un pool o da una cache SSD. Tuttavia, la capacità di conservazione potrebbe diminuire in base al numero di dischi rimasti nel pool o nella cache SSD.

Di seguito sono riportati gli impatti sui dischi sicuri:

- Se si rimuove l'ultimo disco che non supporta la protezione, il pool viene lasciato con tutti i dischi che supportano la protezione. In questa situazione, è possibile attivare la protezione per il pool.
- Se si rimuove l'ultimo disco non compatibile con Data Assurance (da), il pool viene lasciato con tutti i dischi compatibili con da.
- Tutti i nuovi volumi creati nel pool saranno compatibili con da. Se si desidera che i volumi esistenti siano compatibili con il da, è necessario eliminare e ricreare il volume.

Fasi

1. Dalla pagina Manage (Gestione), selezionare l'array di storage.

   Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).

2. Selezionare il pool o la cache SSD, quindi fare clic su **More › Remove Capacity**.

   Viene visualizzata la finestra di dialogo Remove Capacity (capacità di rimozione).

3. Selezionare una o più unità nell'elenco.

   Quando si selezionano o deselezionano i dischi nell'elenco, il campo capacità totale selezionata viene aggiornato. Questo campo mostra la capacità totale del pool o della cache SSD risultante dopo la rimozione dei dischi selezionati.

4. Fare clic su **Rimuovi**, quindi confermare la rimozione delle unità.

Risultato

La nuova capacità ridotta del pool o della cache SSD viene riflessa nella vista Pools e Volume Groups.

Abilitare la protezione per un pool o un gruppo di volumi

È possibile attivare Drive Security per un pool o un gruppo di volumi per impedire l'accesso non autorizzato ai dati sulle unità contenute nel pool o nel gruppo di volumi.

L'accesso in lettura e scrittura per i dischi è disponibile solo attraverso un controller configurato con una chiave di sicurezza.

Prima di iniziare

- La funzione Drive Security deve essere attivata.
- È necessario creare una chiave di sicurezza.
- Il pool o il gruppo di volumi deve trovarsi in uno stato ottimale.
- Tutti i dischi del pool o del gruppo di volumi devono essere dischi sicuri.

A proposito di questa attività

Se si desidera utilizzare Drive Security, selezionare un pool o un gruppo di volumi che supporti la protezione. Un pool o un gruppo di volumi può contenere dischi sicuri e non sicuri, ma tutti i dischi devono essere sicuri per poter utilizzare le proprie funzionalità di crittografia.

Una volta attivato il sistema di protezione, è possibile rimuoverlo solo eliminando il pool o il gruppo di volumi, quindi cancellando i dischi.

Fasi

1. Nella pagina Manage (Gestione), selezionare l'array di storage con il pool o il gruppo di volumi.
2. Selezionare **Provisioning › Configure Pools and Volume Groups** (Configura pool e gruppi di volumi).
3. Selezionare il pool o il gruppo di volumi in cui si desidera attivare la protezione, quindi fare clic su **More › Enable Security** (Altro[attiva protezione]).

   Viene visualizzata la finestra di dialogo Conferma abilitazione protezione.

4. Confermare che si desidera attivare la protezione per il pool o il gruppo di volumi selezionato, quindi fare clic su **Enable** (attiva).

Rimuovere il plug-in di storage per vCenter

È possibile rimuovere il plug-in da vCenter Server Appliance e disinstallare il webserver del plug-in dall'host dell'applicazione.

Si tratta di due passaggi distinti che è possibile eseguire in qualsiasi ordine. Tuttavia, se si sceglie di rimuovere

il webserver del plug-in dall'host dell'applicazione prima di annullare la registrazione del plug-in, lo script di registrazione viene rimosso durante tale processo e non è possibile utilizzare il metodo 1 per annullare la registrazione.

Annullare la registrazione del plug-in da un'appliance vCenter Server

Per annullare la registrazione del plug-in da un'appliance vCenter Server, selezionare uno dei seguenti metodi:

- Metodo 1: Eseguire lo script di registrazione
- Metodo 2: Utilizzare le pagine Mob di vCenter Server

Metodo 1: Eseguire lo script di registrazione

1. Aprire un prompt dalla riga di comando e accedere alla seguente directory:

   ```
   <install directory>\vcenter-register\bin
   ```

2. Eseguire `vcenter-register.bat` file:

   ```
   vcenter-register.bat ^

   -action unregisterPlugin ^

   -vcenterHostname <vCenter FQDN> ^

   -username <Administrator Username> ^
   ```

3. Verificare che lo script sia stato eseguito correttamente.

   I registri vengono salvati in `%install_dir%/working/logs/vc-registration.log`.

Metodo 2: Utilizzare le pagine Mob di vCenter Server

1. Aprire un browser Web e immettere il seguente URL:

   https://<FQDN[] Di vCenter Server>/MOB

2. Accedere con le credenziali di amministratore.
3. Cercare il nome della proprietà di `extensionManager` e fare clic sul collegamento associato alla proprietà.
4. Espandere l'elenco delle proprietà facendo clic su **More**… in fondo all'elenco.
5. Verificare che l'interno `plugin.netapp.eseries` è nell'elenco.
6. Se presente, fare clic sul metodo `UnregisterExtension`.
7. Inserire il valore `plugin.netapp.eseries` Nella finestra di dialogo e fare clic su **Invoke method**.
8. Chiudere la finestra di dialogo e aggiornare il browser Web.
9. Verificare che il `plugin.netapp.eseries` interno non presente nell'elenco.

> Questa procedura disregistra il plug-in da vCenter Server Appliance; tuttavia, non rimuove i file dei pacchetti di plug-in dal server. Per rimuovere i file dei pacchetti, utilizzare SSH per accedere a vCenter Server Appliance e accedere alla seguente directory: `etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/`. Quindi rimuovere la directory associata al plug-in.

Rimuovere il webserver del plug-in dall'host dell'applicazione

Per rimuovere il software del plug-in dall'host dell'applicazione, attenersi alla seguente procedura:

1. Dal server applicazioni, accedere a **pannello di controllo**.
2. Accedere a **applicazioni e funzionalità**, quindi selezionare **Plugin storage SANtricity per vCenter**.
3. Fare clic su **Disinstalla/Cambia**.

   Viene visualizzata una finestra di dialogo di conferma.

4. Fare clic su **Disinstalla**.

   Una volta completata la disinstallazione, viene visualizzato un messaggio di conferma.

5. Fare clic su **fine**.

FAQ

Quali impostazioni vengono importate?

La funzione Import Settings (Impostazioni di importazione) è un'operazione batch che carica le configurazioni da un array di storage a più array di storage.

Le impostazioni importate durante questa operazione dipendono dalla configurazione dell'array di storage di origine in System Manager. È possibile importare le seguenti impostazioni in più array di storage:

- **Avvisi via email** — le impostazioni includono un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Syslog alerts** — le impostazioni includono un indirizzo del server syslog e una porta UDP.
- **SNMP alerts** — le impostazioni includono un nome di comunità e un indirizzo IP per il server SNMP.
- **AutoSupport** — le impostazioni includono le funzioni separate (AutoSupport di base, AutoSupport on Demand e Diagnostica remota), la finestra di manutenzione, il metodo di erogazione, e pianificazione delle spedizioni.
- **Directory Services** — la configurazione include il nome di dominio e l'URL di un server LDAP (Lightweight Directory Access Protocol), oltre ai mapping dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.
- **Configurazione dello storage** — le configurazioni includono volumi (solo volumi thick e non repository), gruppi di volumi, pool e assegnazioni di dischi hot spare.
- **Impostazioni di sistema** — le configurazioni includono le impostazioni di scansione dei supporti per un volume, la cache SSD per i controller e il bilanciamento automatico del carico (non include il reporting della connettività host).

Perché non vengono visualizzati tutti gli array di storage?

Durante l'operazione Import Settings (Impostazioni di importazione), alcuni storage array potrebbero non essere disponibili nella finestra di dialogo di selezione della destinazione.

Gli array di storage potrebbero non essere visualizzati per i seguenti motivi:

- La versione del firmware è inferiore alla 8.50.
- Lo storage array non è in linea.
- Il sistema non è in grado di comunicare con tale array (ad esempio, l'array presenta problemi di certificato, password o rete).

Perché questi volumi non sono associati a un carico di lavoro?

I volumi non sono associati a un carico di lavoro se sono stati creati utilizzando l'interfaccia della riga di comando (CLI) o se sono stati migrati (importati/esportati) da un array di storage diverso.

In che modo il carico di lavoro selezionato influisce sulla creazione di volumi?

Durante la creazione del volume, vengono richieste informazioni sull'utilizzo di un carico di lavoro. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata in base alle esigenze. In alternativa, è possibile saltare questo passaggio nella sequenza di creazione del volume.

Un workload è un oggetto storage che supporta un'applicazione. È possibile definire uno o più carichi di lavoro o istanze per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro in modo che contenga volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche dei volumi sono ottimizzate in base al tipo di applicazione supportata dal carico di lavoro. Ad esempio, se si crea un carico di lavoro che supporta un'applicazione Microsoft SQL Server e successivamente si creano volumi per tale carico di lavoro, le caratteristiche del volume sottostante sono ottimizzate per supportare Microsoft SQL Server.

- **Specifico dell'applicazione** — quando si creano volumi utilizzando un carico di lavoro specifico dell'applicazione, il sistema consiglia una configurazione del volume ottimizzata per ridurre al minimo i conflitti tra i/o del carico di lavoro dell'applicazione e altro traffico dall'istanza dell'applicazione. Le caratteristiche del volume come il tipo di i/o, le dimensioni del segmento, la proprietà del controller e la cache di lettura e scrittura sono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazioni.
  - Microsoft SQL Server
  - Server Microsoft Exchange
  - Applicazioni di videosorveglianza
  - VMware ESXi (per volumi da utilizzare con Virtual Machine file System)

    È possibile rivedere la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliate dal sistema utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).
- **Altri (o applicazioni senza supporto specifico per la creazione di volumi)** — Altri carichi di lavoro utilizzano una configurazione del volume che è necessario specificare manualmente quando si desidera creare un carico di lavoro non associato a un'applicazione specifica o se non esiste un'ottimizzazione

integrata per l'applicazione che si intende utilizzare sull'array di storage. Specificare manualmente la configurazione del volume utilizzando la finestra di dialogo Add/Edit Volumes (Aggiungi/Modifica volumi).

Perché non vengono visualizzati tutti i volumi, gli host o i cluster di host?

I volumi Snapshot con un volume di base abilitato da non possono essere assegnati a un host che non supporta Data Assurance (da). È necessario disattivare il da sul volume di base prima di poter assegnare un volume snapshot a un host che non supporta il da.

Prendere in considerazione le seguenti linee guida per l'host a cui si sta assegnando il volume di snapshot:

- Un host non è in grado di supportare da se è collegato all'array di storage attraverso un'interfaccia i/o che non è in grado di supportare da.
- Un cluster host non è in grado di supportare da se ha almeno un membro host che non è in grado di supportare da.

> Non è possibile disattivare il da su un volume associato a snapshot (gruppi di coerenza, gruppi di snapshot, immagini snapshot e volumi di snapshot), copie di volumi, e specchi. Tutti gli oggetti snapshot e capacità riservata associati devono essere cancellati prima che il da possa essere disattivato sul volume di base.

Perché non è possibile eliminare il carico di lavoro selezionato?

Questo carico di lavoro è costituito da un gruppo di volumi creati utilizzando l'interfaccia della riga di comando (CLI) o migrati (importati/esportati) da un array di storage diverso. Di conseguenza, i volumi di questo carico di lavoro non sono associati a un carico di lavoro specifico dell'applicazione, pertanto non è possibile eliminare il carico di lavoro.

In che modo i carichi di lavoro specifici dell'applicazione mi aiutano a gestire lo storage array?

Le caratteristiche del volume del carico di lavoro specifico dell'applicazione determinano il modo in cui il carico di lavoro interagisce con i componenti dell'array di storage e aiutano a determinare le performance dell'ambiente in una determinata configurazione.

Un'applicazione è un software come SQL Server o Exchange. È possibile definire uno o più workload per supportare ciascuna applicazione. Per alcune applicazioni, il sistema consiglia automaticamente una configurazione del volume che ottimizzi lo storage. Caratteristiche come il tipo di i/o, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume.

Cosa devo fare per riconoscere la capacità espansa?

Se si aumenta la capacità di un volume, l'host potrebbe non riconoscere immediatamente l'aumento della capacità del volume.

La maggior parte dei sistemi operativi riconosce la capacità del volume espanso e si espande automaticamente dopo l'avvio dell'espansione del volume. Tuttavia, alcuni potrebbero non farlo. Se il sistema operativo non riconosce automaticamente la capacità del volume espanso, potrebbe essere necessario eseguire una nuova scansione o un riavvio del disco.

Una volta espansa la capacità del volume, è necessario aumentare manualmente le dimensioni del file system

per ottenere la corrispondenza. Il modo in cui si esegue questa operazione dipende dal file system in uso.

Per ulteriori informazioni, consultare la documentazione del sistema operativo host.

Quando si desidera utilizzare la selezione dell'host di assegnazione in un secondo momento?

Se si desidera accelerare il processo di creazione dei volumi, è possibile saltare la fase di assegnazione dell'host in modo che i volumi appena creati vengano inizializzati offline.

I volumi appena creati devono essere inizializzati. Il sistema può inizializzarli utilizzando una delle due modalità, ovvero un processo di inizializzazione in background di IAF (immediate Available Format) o un processo offline.

Quando si esegue il mapping di un volume a un host, tutti i volumi di inizializzazione del gruppo vengono forzati a passare all'inizializzazione in background. Questo processo di inizializzazione in background consente l'i/o host simultaneo, che a volte può richiedere molto tempo.

Quando nessuno dei volumi in un gruppo di volumi viene mappato, viene eseguita l'inizializzazione offline. Il processo offline è molto più veloce del processo in background.

Cosa occorre sapere sui requisiti relativi alle dimensioni dei blocchi host?

Per i sistemi EF300 e EF600, è possibile impostare un volume in modo che supporti una dimensione di blocco di 512 byte o 4 KiB (chiamata anche "dimensione del settore"). È necessario impostare il valore corretto durante la creazione del volume. Se possibile, il sistema suggerisce il valore predefinito appropriato.

Prima di impostare le dimensioni del blocco del volume, leggere le seguenti limitazioni e linee guida.

- Alcuni sistemi operativi e macchine virtuali (in particolare VMware, al momento) richiedono una dimensione di blocco di 512 byte e non supportano 4KiB, quindi assicurarsi di conoscere i requisiti dell'host prima di creare un volume. In genere, è possibile ottenere le migliori prestazioni impostando un volume in modo che presenti una dimensione di blocco di 4 KiB; tuttavia, assicurarsi che l'host supporti blocchi da 4 KiB (o "4 Kn").
- Il tipo di dischi selezionati per il pool o il gruppo di volumi determina anche le dimensioni dei blocchi di volume supportate, come indicato di seguito:
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 512 byte, è possibile creare solo volumi con blocchi da 512 byte.
  - Se si crea un gruppo di volumi utilizzando unità che scrivono su blocchi da 4 KiB, è possibile creare volumi con blocchi da 512 byte o 4 KiB.
- Se l'array dispone di una scheda di interfaccia host iSCSI, tutti i volumi sono limitati a blocchi da 512 byte (indipendentemente dalla dimensione del blocco del gruppo di volumi). Ciò è dovuto a un'implementazione hardware specifica.
- Una volta impostata, non è possibile modificare le dimensioni di un blocco. Se è necessario modificare le dimensioni di un blocco, è necessario eliminare il volume e ricrearlo.

Perché dovrei creare un cluster host?

È necessario creare un cluster host se si desidera che due o più host condividano l'accesso allo stesso set di volumi. In genere, i singoli host dispongono di un software di

clustering installato su di essi per coordinare l'accesso ai volumi.

Come si fa a sapere quale tipo di sistema operativo host è corretto?

Il campo host Operating System Type (tipo di sistema operativo host) contiene il sistema operativo dell'host. È possibile selezionare il tipo di host consigliato dall'elenco a discesa o consentire all'HCA (host Context Agent) di configurare l'host e il tipo di sistema operativo appropriato.

I tipi di host visualizzati nell'elenco a discesa dipendono dal modello di array di storage e dalla versione del firmware. Le versioni più recenti visualizzano prima le opzioni più comuni, che sono le più probabili. L'aspetto in questo elenco non implica che l'opzione sia completamente supportata.

> Per ulteriori informazioni sul supporto degli host, fare riferimento a. "Tool di matrice di interoperabilità NetApp".

Alcuni dei seguenti tipi di host potrebbero essere visualizzati nell'elenco:

Tipo di sistema operativo host	Sistema operativo e driver multipath
Linux DM-MP (kernel 3.10 o successivo)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.10 o successivo.
VMware ESXi	Supporta i sistemi operativi VMware ESXi che eseguono l'architettura NMP (Native Multipathing Plug-in) utilizzando il modulo SATP_ALUA Storage Array Type Policy integrato da VMware.
Windows (in cluster o non in cluster)	Supporta configurazioni in cluster o non in cluster di Windows che non eseguono il driver di multipathing atto.
ATTO Cluster (tutti i sistemi operativi)	Supporta tutte le configurazioni del cluster utilizzando il driver multipathing della tecnologia atto, Inc.
Linux (Veritas DMP)	Supporta i sistemi operativi Linux che utilizzano una soluzione multipathing Veritas DMP.
Linux (atto)	Supporta i sistemi operativi Linux che utilizzano un driver multipathing per la tecnologia atto, Inc.
Sistema operativo Mac	Supporta le versioni di Mac OS che utilizzano un driver multipathing per la tecnologia atto, Inc.
Windows (atto)	Supporta i sistemi operativi Windows che utilizzano un driver multipathing per la tecnologia atto, Inc.
FlexArray (ALUA)	Supporta un sistema NetApp FlexArray che utilizza ALUA per il multipathing.
SVC IBM	Supporta una configurazione IBM SAN Volume Controller.

Tipo di sistema operativo host	Sistema operativo e driver multipath
Impostazione predefinita di fabbrica	Riservato all'avvio iniziale dello storage array. Se il tipo di sistema operativo host in uso è impostato su Factory Default, modificarlo in modo che corrisponda al sistema operativo host e al driver multipath in esecuzione sull'host connesso.
Linux DM-MP (Kernal 3.9 o precedente)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath di Device Mapper con kernel 3.9 o precedente.
Cluster di finestre (obsoleto)	Se il tipo di sistema operativo host è impostato su questo valore, utilizzare l'impostazione Windows (in cluster o non in cluster).

Una volta installato l'HCA e collegato lo storage all'host, l'HCA invia la topologia host ai controller di storage attraverso il percorso i/O. In base alla topologia dell'host, i controller di storage definiscono automaticamente l'host e le porte host associate, quindi impostano il tipo di host.

> Se l'HCA non seleziona il tipo di host consigliato, è necessario impostare manualmente il tipo di host.

Come faccio ad associare le porte host a un host?

Se si crea manualmente un host, è necessario utilizzare l'utility HBA (host bus adapter) appropriata disponibile sull'host per determinare gli identificatori di porta host associati a ciascun HBA installato nell'host.

Quando si dispone di queste informazioni, selezionare gli identificatori di porta host che hanno effettuato l'accesso allo storage array dall'elenco fornito nella finestra di dialogo Create host (Crea host).

> Assicurarsi di selezionare gli identificatori di porta host appropriati per l'host che si sta creando. Se si associano identificatori di porta host errati, potrebbe verificarsi un accesso non intenzionale da un altro host a questi dati.

Se si creano automaticamente host utilizzando l'HCA (host Context Agent) installato su ciascun host, l'HCA deve associare automaticamente gli identificatori di porta host a ciascun host e configurarli in modo appropriato.

Qual è il cluster predefinito?

Il cluster predefinito è un'entità definita dal sistema che consente a qualsiasi identificatore di porta host non associato che abbia eseguito l'accesso all'array di storage di accedere ai volumi assegnati al cluster predefinito.

Un identificatore di porta host non associato è una porta host che non è logicamente associata a un particolare host ma che è fisicamente installata in un host e collegata all'array di storage.

> Se si desidera che gli host abbiano accesso specifico a determinati volumi nell'array di storage, non è necessario utilizzare il cluster predefinito. È invece necessario associare gli identificatori delle porte host ai rispettivi host. Questa attività può essere eseguita manualmente durante l'operazione Create host (Crea host) o automaticamente utilizzando l'HCA (host Context Agent) installato su ciascun host. Quindi, assegnare i volumi a un singolo host o a un cluster host.

Utilizzare il cluster predefinito solo in situazioni speciali in cui l'ambiente di storage esterno favorisce l'accesso a tutti gli host e a tutti gli identificatori di porta host connessi allo storage array a tutti i volumi (modalità all-access) senza rendere specifici gli host noti allo storage array o all'interfaccia utente.

Inizialmente, è possibile assegnare i volumi solo al cluster predefinito tramite l'interfaccia della riga di comando (CLI). Tuttavia, dopo aver assegnato almeno un volume al cluster predefinito, questa entità (chiamata cluster predefinito) viene visualizzata nell'interfaccia utente, dove è possibile gestire questa entità.

Che cos'è il controllo di ridondanza?

Un controllo di ridondanza determina se i dati su un volume in un pool o un gruppo di volumi sono coerenti. I dati di ridondanza vengono utilizzati per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto di uno dei dischi del pool o del gruppo di volumi.

È possibile eseguire questo controllo solo su un pool o su un gruppo di volumi alla volta. Un controllo della ridondanza del volume esegue le seguenti operazioni:

- Esegue la scansione dei blocchi di dati in un volume RAID 3, RAID 5 o RAID 6, quindi verifica le informazioni di ridondanza per ciascun blocco. (RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia della riga di comando).
- Confronta i blocchi di dati sui dischi RAID 1 mirrorati.
- Restituisce errori di ridondanza se i dati sono determinati come incoerenti dal firmware del controller.

> L'esecuzione immediata di un controllo di ridondanza sullo stesso pool o gruppo di volumi potrebbe causare un errore. Per evitare questo problema, attendere da uno a due minuti prima di eseguire un altro controllo di ridondanza sullo stesso pool o gruppo di volumi.

Che cos'è la capacità di conservazione?

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata in un pool per supportare potenziali guasti del disco.

Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione in base al numero di dischi nel pool.

I pool utilizzano la capacità di conservazione durante la ricostruzione, mentre i gruppi di volumi utilizzano dischi hot spare per lo stesso scopo. Il metodo della capacità di conservazione è un miglioramento rispetto ai dischi hot spare perché consente una ricostruzione più rapida. La capacità di conservazione viene distribuita su un certo numero di dischi nel pool invece che su un disco nel caso di un disco hot spare, in modo da non essere limitati dalla velocità o dalla disponibilità di un disco.

Qual è il livello RAID migliore per la mia applicazione?

Per massimizzare le performance di un gruppo di volumi, è necessario selezionare il

livello RAID appropriato.

È possibile determinare il livello RAID appropriato conoscendo le percentuali di lettura e scrittura per le applicazioni che accedono al gruppo di volumi. Utilizzare la pagina Performance (prestazioni) per ottenere queste percentuali.

Livelli RAID e performance applicative

RAID si basa su una serie di configurazioni, chiamate livelli, per determinare il modo in cui i dati di ridondanza e utente vengono scritti e recuperati dai dischi. Ogni livello RAID offre diverse funzionalità di performance. Le applicazioni con un'elevata percentuale di lettura sono in grado di funzionare correttamente utilizzando volumi RAID 5 o RAID 6, a causa delle eccezionali prestazioni di lettura delle configurazioni RAID 5 e RAID 6.

Le applicazioni con una bassa percentuale di lettura (elevata intensità di scrittura) non funzionano altrettanto sui volumi RAID 5 o RAID 6. Le prestazioni degradate sono il risultato del modo in cui un controller scrive i dati e i dati di ridondanza sui dischi di un gruppo di volumi RAID 5 o RAID 6.

Selezionare un livello RAID in base alle seguenti informazioni.

RAID 0

Descrizione:

- Non ridondante, modalità striping.
- RAID 0 esegue lo striping dei dati su tutti i dischi del gruppo di volumi.

Caratteristiche di protezione dei dati:

- RAID 0 non è consigliato per esigenze di alta disponibilità. RAID 0 è migliore per i dati non critici.
- Se un singolo disco si guasta nel gruppo di volumi, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- Per RAID livello 0 è richiesto un minimo di un disco.
- I gruppi di volumi RAID 0 possono avere più di 30 dischi.
- È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 1 o RAID 10

Descrizione:

- Modalità striping/mirror.

Come funziona:

- RAID 1 utilizza il mirroring del disco per scrivere i dati su due dischi duplicati contemporaneamente.
- RAID 10 utilizza lo striping dei dischi per eseguire lo striping dei dati su un set di coppie di dischi mirrorati.

Caratteristiche di protezione dei dati:

- RAID 1 e RAID 10 offrono performance elevate e la migliore disponibilità dei dati.

- RAID 1 e RAID 10 utilizzano il mirroring del disco per eseguire una copia esatta da un disco a un altro.
- Se uno dei dischi di una coppia di dischi si guasta, lo storage array può passare istantaneamente all'altro disco senza alcuna perdita di dati o di servizio.
- Un guasto a un singolo disco causa il degrado dei volumi associati. L'unità mirror consente di accedere ai dati.
- Un errore di coppia di dischi in un gruppo di volumi causa il malfunzionamento di tutti i volumi associati e la perdita di dati.

Requisiti del numero di unità:

- Per RAID 1 sono necessari almeno due dischi: Un disco per i dati dell'utente e un disco per i dati mirrorati.
- Se si selezionano quattro o più dischi, RAID 10 viene configurato automaticamente nel gruppo di volumi: Due dischi per i dati dell'utente e due dischi per i dati mirrorati.
- È necessario disporre di un numero pari di dischi nel gruppo di volumi. Se non si dispone di un numero pari di dischi e si dispone di altri dischi non assegnati, passare a **Pools & Volume Groups** per aggiungere ulteriori dischi al gruppo di volumi e riprovare l'operazione.
- I gruppi di volumi RAID 1 e RAID 10 possono avere più di 30 dischi. È possibile creare un gruppo di volumi che includa tutte le unità dell'array di storage.

RAID 5

Descrizione:

- Modalità i/o elevata.

Come funziona:

- I dati dell'utente e le informazioni ridondanti (parità) vengono sottoposti a striping tra i dischi.
- La capacità equivalente di un disco viene utilizzata per le informazioni ridondanti.

Caratteristiche di protezione dei dati

- Se un singolo disco si guasta in un gruppo di volumi RAID 5, tutti i volumi associati diventano degradati. Le informazioni ridondanti consentono di accedere ai dati.
- Se due o più dischi si guastano in un gruppo di volumi RAID 5, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- È necessario disporre di un minimo di tre dischi nel gruppo di volumi.
- In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

RAID 6

Descrizione:

- Modalità i/o elevata.

Come funziona:

- I dati dell'utente e le informazioni ridondanti (doppia parità) vengono sottoposti a striping tra i dischi.

- La capacità equivalente di due dischi viene utilizzata per le informazioni ridondanti.

Caratteristiche di protezione dei dati:

- Se uno o due dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati diventano degradati, ma le informazioni ridondanti consentono di continuare ad accedere ai dati.
- Se tre o più dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati si guastano e tutti i dati vengono persi.

Requisiti del numero di unità:

- È necessario disporre di un minimo di cinque dischi nel gruppo di volumi.
- In genere, il gruppo di volumi è limitato a un massimo di 30 dischi.

> Non è possibile modificare il livello RAID di un pool. L'interfaccia utente configura automaticamente i pool come RAID 6.

Livelli RAID e protezione dei dati

RAID 1, RAID 5 e RAID 6 scrivono i dati di ridondanza sul disco per la tolleranza di errore. I dati di ridondanza possono essere una copia dei dati (mirrorati) o un codice di correzione degli errori derivato dai dati. È possibile utilizzare i dati di ridondanza per ricostruire rapidamente le informazioni su un disco sostitutivo in caso di guasto.

È possibile configurare un singolo livello RAID in un singolo gruppo di volumi. Tutti i dati di ridondanza per quel gruppo di volumi vengono memorizzati all'interno del gruppo di volumi. La capacità del gruppo di volumi è la capacità aggregata dei dischi membri meno la capacità riservata ai dati di ridondanza. La quantità di capacità necessaria per la ridondanza dipende dal livello RAID utilizzato.

Perché alcuni dischi non vengono visualizzati?

Nella finestra di dialogo Add Capacity (Aggiungi capacità), non tutti i dischi sono disponibili per l'aggiunta di capacità a un pool o a un gruppo di volumi esistente.

I dischi non sono idonei per uno dei seguenti motivi:

- Un disco deve essere non assegnato e non abilitato alla sicurezza. I dischi già parte di un altro pool, di un altro gruppo di volumi o configurati come hot spare non sono idonei. Se un disco non è assegnato ma è abilitato per la protezione, è necessario cancellarlo manualmente affinché sia idoneo.
- Un disco in uno stato non ottimale non è idoneo.
- Se la capacità di un disco è troppo piccola, non è idonea.
- Il tipo di disco deve corrispondere all'interno di un pool o di un gruppo di volumi. Non è possibile combinare i seguenti elementi:
  - Dischi rigidi (HDD) con dischi a stato solido (SSD)
  - NVMe con unità SAS
  - Dischi con blocchi di volumi da 512 byte e 4 KiB
- Se un pool o un gruppo di volumi contiene tutti i dischi con funzionalità di protezione, i dischi con funzionalità di protezione non sono elencati.
- Se un pool o un gruppo di volumi contiene tutti i dischi FIPS (Federal Information Processing Standard), i

dischi non FIPS non sono elencati.

- Se un pool o un gruppo di volumi contiene tutte le unità compatibili con Data Assurance (da) e nel pool o nel gruppo di volumi è presente almeno un volume abilitato da, un'unità che non supporta da non è idonea, quindi non può essere aggiunta a tale pool o gruppo di volumi. Tuttavia, se nel pool o nel gruppo di volumi non è presente alcun volume abilitato da, è possibile aggiungere un'unità che non supporta da a a tale pool o gruppo di volumi. Se si decide di combinare questi dischi, tenere presente che non è possibile creare volumi abilitati da.

> È possibile aumentare la capacità dell'array di storage aggiungendo nuove unità o eliminando pool o gruppi di volumi.

Perché non posso aumentare la mia capacità di conservazione?

Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, potrebbe non essere possibile aumentare la capacità di conservazione.

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata a un pool per supportare potenziali guasti del disco. Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione in base al numero di dischi nel pool. Se sono stati creati volumi su tutta la capacità utilizzabile disponibile, non è possibile aumentare la capacità di conservazione senza aggiungere capacità al pool aggiungendo unità o eliminando volumi.

È possibile modificare la capacità di conservazione da Pools & Volume Groups. Selezionare il pool che si desidera modificare. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni), quindi selezionare la scheda **Settings** (Impostazioni).

> La capacità di conservazione viene specificata come un numero di dischi, anche se la capacità di conservazione effettiva viene distribuita tra i dischi del pool.

Cos'è Data Assurance?

Data Assurance (da) implementa lo standard T10 Protection Information (PI), che aumenta l'integrità dei dati verificando e correggendo gli errori che potrebbero verificarsi quando i dati vengono trasferiti lungo il percorso di i/O.

L'utilizzo tipico della funzione Data Assurance consente di controllare la parte del percorso i/o tra i controller e i dischi. Le funzionalità DA vengono presentate a livello di pool e gruppo di volumi.

Quando questa funzione è attivata, l'array di storage aggiunge i codici di controllo degli errori (noti anche come CRC (Cyclic Redundancy Checks) a ciascun blocco di dati del volume. Dopo lo spostamento di un blocco di dati, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono scritti su disco né restituiti all'host. Se si desidera utilizzare la funzione da, selezionare un pool o un gruppo di volumi che supporti da quando si crea un nuovo volume (cercare **Sì** accanto a **da** nella tabella dei candidati del gruppo di volumi e pool).

Assicurarsi di assegnare questi volumi abilitati da a un host utilizzando un'interfaccia i/o in grado di supportare da. Le interfacce i/o in grado di da includono Fibre Channel, SAS, iSCSI su TCP/IP, NVMe/FC, NVMe/IB, NVME/RoCE e iSER su InfiniBand (estensioni iSCSI per RDMA/IB). DA non è supportato da SRP su InfiniBand.

Che cos'è la sicurezza FDE/FIPS?

La protezione FDE/FIPS si riferisce a dischi sicuri che crittografano i dati durante la scrittura e decrittare i dati durante la lettura utilizzando una chiave di crittografia univoca.

Queste unità sicure impediscono l'accesso non autorizzato ai dati su un disco che viene fisicamente rimosso dall'array di storage. Le unità compatibili con la protezione possono essere dischi con crittografia completa del disco (FDE) o dischi FIPS (Federal Information Processing Standard). I dischi FIPS sono stati sottoposti a test di certificazione.

> Per i volumi che richiedono il supporto FIPS, utilizzare solo dischi FIPS. La combinazione di dischi FIPS e FDE in un gruppo di volumi o in un pool comporterà il trattamento di tutti i dischi come dischi FDE. Inoltre, un disco FDE non può essere aggiunto o utilizzato come spare in un gruppo di volumi o pool all-FIPS.

Che cos'è il supporto sicuro (Drive Security)?

Drive Security è una funzione che impedisce l'accesso non autorizzato ai dati su dischi abilitati alla sicurezza quando vengono rimossi dallo storage array.

Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).

Come si visualizzano e interpretano tutte le statistiche della cache SSD?

È possibile visualizzare statistiche nominali e statistiche dettagliate per la cache SSD.

Le statistiche nominali sono un sottoinsieme delle statistiche dettagliate. Le statistiche dettagliate possono essere visualizzate solo quando si esportano tutte le statistiche SSD in un file .csv. Durante la revisione e l'interpretazione delle statistiche, tenere presente che alcune interpretazioni derivano da una combinazione di statistiche.

Statistiche nominali

Per visualizzare le statistiche della cache SSD, accedere alla pagina **Manage** (Gestione). Selezionare **Provisioning › Configure Pools & Volume Groups** (Configura pool e gruppi di volumi). Selezionare la cache SSD per cui si desidera visualizzare le statistiche, quindi selezionare **More › View Statistics** (Visualizza statistiche). Le statistiche nominali vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD).

> Questa funzione non è disponibile sui sistemi storage EF600 o EF300.

L'elenco include le statistiche nominali, che sono un sottoinsieme delle statistiche dettagliate.

Statistiche dettagliate

Le statistiche dettagliate sono costituite dalle statistiche nominali e da statistiche aggiuntive. Queste statistiche aggiuntive vengono salvate insieme alle statistiche nominali, ma a differenza delle statistiche nominali, non vengono visualizzate nella finestra di dialogo View SSD cache Statistics (Visualizza statistiche cache SSD). È possibile visualizzare le statistiche dettagliate solo dopo aver esportato le statistiche in un file .csv.

Le statistiche dettagliate sono elencate dopo le statistiche nominali.

Che cos'è la protezione contro la perdita di shelf e la perdita di cassetto?

La protezione contro le perdite di shelf e la protezione contro le perdite di cassetto sono attributi di pool e gruppi di volumi che consentono di mantenere l'accesso ai dati in caso di guasto di un singolo shelf o cassetto.

Protezione contro la perdita di shelf

Uno shelf è l'enclosure che contiene i dischi o i dischi e il controller. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo shelf di dischi. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione dello shelf di dischi o il guasto di entrambi i moduli i/o (IOM).

> La protezione contro la perdita di shelf non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

I criteri per la protezione dalla perdita di shelf dipendono dal metodo di protezione, come descritto nella tabella seguente.

Livello	Criteri per la protezione contro la perdita di shelf	Numero minimo di shelf richiesti
Piscina	Il pool deve includere dischi di almeno cinque shelf e deve essere presente un numero uguale di dischi in ogni shelf. La protezione contro la perdita di shelf non è applicabile agli shelf ad alta capacità; se il sistema contiene shelf ad alta capacità, fare riferimento alla protezione contro la perdita di cassetto.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo cassetto.	3
RAID 3 o RAID 5	Ogni disco del gruppo di volumi si trova in uno shelf separato.	3
RAID 1	Ogni disco di una coppia RAID 1 deve essere collocato in uno shelf separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di shelf.	Non applicabile

Protezione in caso di perdita del cassetto

Un cassetto è uno dei compartimenti di uno shelf che si tira per accedere ai dischi. Solo gli scaffali ad alta capacità dispongono di cassetti. La protezione contro la perdita dei cassetti garantisce l'accessibilità ai dati sui volumi di un pool o di un gruppo di volumi se si verifica una perdita totale di comunicazione con un singolo cassetto. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione del cassetto o il guasto di un componente interno del cassetto.

> La protezione contro la perdita di cassetto non è garantita se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a un cassetto (e di conseguenza a un altro disco nel pool o nel gruppo di volumi) causa la perdita di dati.

I criteri per la protezione dalle perdite di cassetto dipendono dal metodo di protezione, come descritto nella tabella seguente:

Livello	Criteri per la protezione contro le perdite di cassetto	Numero minimo di cassetti richiesti
Piscina	I candidati al pool devono includere unità di tutti i cassetti e deve essere presente un numero uguale di unità in ciascun cassetto. Il pool deve includere dischi di almeno cinque cassetti e deve essere presente un numero uguale di dischi in ciascun cassetto. Uno shelf da 60 dischi può ottenere la protezione contro la perdita di cassetto quando il pool contiene 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 dischi. È possibile aggiungere incrementi in multipli di 5 al pool dopo la creazione iniziale.	5
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo cassetto.	3
RAID 3 o 5	Ciascuna unità del gruppo di volumi si trova in un cassetto separato	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione perdita cassetto.	Non applicabile

Come posso mantenere la protezione contro la perdita di scaffali e cassetti?

Per mantenere la protezione contro le perdite di shelf e cassetti per un pool o un gruppo di volumi, utilizzare i criteri specificati nella tabella seguente.

Livello	Criteri per la protezione contro le perdite di scaffali/cassetti	Numero minimo di shelf/cassetti richiesti
Piscina	Per gli shelf, il pool non deve contenere più di due dischi in un singolo shelf. Per i cassetti, il pool deve includere un numero uguale di unità da ciascun cassetto.	6 per i ripiani 5 per i cassetti
RAID 6	Il gruppo di volumi non contiene più di due dischi in un singolo shelf o cassetto.	3

Livello	Criteri per la protezione contro le perdite di scaffali/cassetti	Numero minimo di shelf/cassetti richiesti
RAID 3 o RAID 5	Ciascuna unità del gruppo di volumi si trova in uno shelf o in un cassetto separato.	3
RAID 1	Ogni disco di una coppia mirrorata deve essere collocato in uno shelf o in un cassetto separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di scaffali/cassetti.	Non applicabile

La protezione contro le perdite di shelf/cassetto non viene mantenuta se un disco si è già guastato nel pool o nel gruppo di volumi. In questa situazione, la perdita dell'accesso a uno shelf o a un cassetto di dischi e, di conseguenza, a un altro disco nel pool o nel gruppo di volumi causa la perdita di dati.

Che cos'è la capacità di ottimizzazione per i pool?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un pool, la capacità non allocata è costituita dalla capacità di conservazione di un pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra performance, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Pool Settings (Impostazioni pool) consente di regolare la capacità di ottimizzazione del pool. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) è disponibile solo per i sistemi storage EF600 e EF300.

Qual è la capacità di ottimizzazione per i gruppi di volumi?

I dischi SSD avranno una maggiore durata e migliori prestazioni di scrittura massime quando una parte della loro capacità non viene allocata.

Per i dischi associati a un gruppo di volumi, la capacità non allocata è costituita dalla capacità libera di un gruppo di volumi (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile come capacità di ottimizzazione. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, come tale, non è disponibile per la creazione di volumi.

Quando viene creato un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra prestazioni, durata del disco e capacità disponibile. Il dispositivo di scorrimento Additional Optimization Capacity (capacità di ottimizzazione aggiuntiva) nella finestra di dialogo Volume Group Settings

(Impostazioni gruppo di volumi) consente di regolare la capacità di ottimizzazione di un gruppo di volumi. La regolazione del dispositivo di scorrimento garantisce migliori prestazioni e durata del disco a scapito della capacità disponibile o di capacità aggiuntiva disponibile a scapito delle prestazioni e della durata del disco.

> Additional Optimization Capacity Slider è disponibile solo per i sistemi storage EF600 e EF300.

Quali sono le funzionalità di provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Cosa occorre sapere sulla funzionalità dei volumi con provisioning delle risorse?

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

> La funzionalità di provisioning delle risorse non è al momento disponibile. In alcune viste, i componenti potrebbero essere segnalati come capaci di provisioning delle risorse, ma la capacità di creare volumi con provisioning delle risorse è stata disattivata fino a quando non sarà possibile riattivarli in un aggiornamento futuro.

Volumi con provisioning delle risorse

Un volume con provisioning di risorse è un volume denso in un gruppo di volumi o pool SSD, in cui la capacità del disco viene allocata (assegnata al volume) quando viene creato il volume, ma i blocchi disco vengono disallocati (non mappati). Per confronto, in un volume thick tradizionale, tutti i blocchi di dischi vengono mappati o allocati durante un'operazione di inizializzazione del volume in background per inizializzare i campi di informazioni di protezione Data Assurance e rendere i dati e la parità RAID coerenti in ogni stripe RAID. Con un volume con provisioning di risorse, non è prevista alcuna inizializzazione in background con time-bound. Al contrario, ogni stripe RAID viene inizializzata alla prima scrittura su un blocco di volume nello stripe.

I volumi con provisioning delle risorse sono supportati solo su gruppi di volumi e pool SSD, in cui tutti i dischi del gruppo o del pool supportano la funzionalità di ripristino degli errori NVMe Deallocated o Unwritten Logical Block Error Enable (DULBE). Quando viene creato un volume con provisioning di risorse, tutti i blocchi di

dischi assegnati al volume vengono deallocati (non mappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management. La deallocazione dei blocchi può migliorare la durata dell'utilizzo degli SSD e aumentare le massime prestazioni di scrittura. Il miglioramento varia in base al modello e alla capacità di ciascun disco.

Attivazione e disattivazione della funzione

Il provisioning delle risorse è attivato per impostazione predefinita nei sistemi in cui i dischi supportano DULBE. È possibile disattivare l'impostazione predefinita da Pools & Volume Groups. La disattivazione del provisioning delle risorse è un'azione permanente per i volumi esistenti e non può essere annullata (ad esempio, non è possibile riattivare il provisioning delle risorse per questi gruppi di volumi e pool).

Tuttavia, se si desidera riattivare il provisioning delle risorse per i nuovi volumi creati, è possibile farlo dal **Impostazioni › sistema**. Tenere presente che quando si riattiva il provisioning delle risorse, vengono influenzati solo i gruppi di volumi e i pool appena creati. Tutti i gruppi di volumi e i pool esistenti rimarranno invariati. Se lo si desidera, è anche possibile disattivare nuovamente il provisioning delle risorse dal **Impostazioni › sistema**.

Qual è la differenza tra la chiave di sicurezza interna e la gestione esterna delle chiavi di sicurezza?

Quando si implementa la funzione Drive Security, è possibile utilizzare una chiave di sicurezza interna o una chiave di sicurezza esterna per bloccare i dati quando un disco abilitato alla protezione viene rimosso dall'array di storage.

Una chiave di sicurezza è una stringa di caratteri che viene condivisa tra i dischi abilitati alla protezione e i controller di un array di storage. Le chiavi interne vengono conservate nella memoria persistente del controller. Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol).

Cosa occorre sapere prima di creare una chiave di sicurezza?

Una chiave di sicurezza viene condivisa da controller e dischi abilitati alla sicurezza all'interno di un array di storage. Se un disco abilitato alla protezione viene rimosso dall'array di storage, la chiave di sicurezza protegge i dati da accessi non autorizzati.

È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi:

- Gestione interna delle chiavi nella memoria persistente del controller.
- Gestione esterna delle chiavi su un server di gestione delle chiavi esterno.

Gestione interna delle chiavi

Le chiavi interne vengono mantenute e "nascoste" in una posizione non accessibile sulla memoria persistente del controller. Prima di creare una chiave di sicurezza interna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security.

È quindi possibile creare una chiave di sicurezza interna, che implica la definizione di un identificatore e di una passphrase. L'identificatore è una stringa associata alla chiave di sicurezza e memorizzata sul controller e su

tutti i dischi associati alla chiave. La password viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Al termine, la chiave di sicurezza viene memorizzata nel controller in una posizione non accessibile. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Gestione esterna delle chiavi

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un protocollo KMIP (Key Management Interoperability Protocol). Prima di creare una chiave di sicurezza esterna, eseguire le seguenti operazioni:

1. Installare unità sicure nell'array di storage. Questi dischi possono essere dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard).
2. Assicurarsi che la funzione Drive Security sia attivata. Se necessario, contattare il fornitore dello storage per istruzioni sull'attivazione della funzione Drive Security
3. Ottenere un file di certificato client firmato. Un certificato client convalida i controller dello storage array, in modo che il server di gestione delle chiavi possa considerare attendibili le richieste KMIP.
   a. Innanzitutto, completare e scaricare una richiesta di firma del certificato (CSR) del client. Accedere al **Impostazioni › certificati › Gestione chiavi › CSR completa**.
   b. Successivamente, viene richiesto un certificato client firmato da una CA attendibile dal server di gestione delle chiavi. È inoltre possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.
   c. Una volta ottenuto un file di certificato client, copiarlo sull'host in cui si accede a System Manager.
4. Recuperare un file di certificato dal server di gestione delle chiavi, quindi copiarlo sull'host in cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, in modo che lo storage array possa fidarsi del proprio indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

È quindi possibile creare una chiave esterna che preveda la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, vengono caricati anche i file dei certificati. Al termine, il sistema si connette al server di gestione delle chiavi con le credenziali immesse. È quindi possibile creare pool o gruppi di volumi abilitati per la protezione oppure attivare la protezione su gruppi di volumi e pool esistenti.

Perché è necessario definire una passphrase?

La password viene utilizzata per crittografare e decrittare il file della chiave di sicurezza memorizzato nel client di gestione locale. Senza la passphrase, la chiave di sicurezza non può essere decifrata e utilizzata per sbloccare i dati da un disco abilitato alla sicurezza se viene reinstallata in un altro array di storage.

Soluzioni legacy

Cloud Connector

Panoramica di SANtricity® Cloud Connector

Il connettore cloud di SANtricity è un'applicazione Linux basata su host che consente di eseguire backup e recovery completi basati su blocchi e file di volumi e-Series su

account S3 (ad esempio, Amazon Simple Storage Service e NetApp StorageGRID) e appliance NetApp AltaVault.

Disponibile per l'installazione su piattaforme Linux RedHat e SUSE, il connettore cloud SANtricity è una soluzione in pacchetto (file .bin). Dopo aver installato SANtricity Cloud Connector, è possibile configurare l'applicazione per eseguire processi di backup e ripristino dei volumi e-Series su un'appliance AltaVault o sugli account Amazon S3 o StorageGRID esistenti. Tutti i processi eseguiti tramite SANtricity Cloud Connector utilizzano API basate SU REST.

Lo strumento SANtricity Cloud Connector non è più disponibile per il download.

Considerazioni

Quando si utilizzano queste procedure, tenere presente che:

- I processi di configurazione e backup/ripristino descritti in queste procedure si applicano alla versione dell'interfaccia utente grafica di SANtricity Cloud Connector.
- I flussi di lavoro API REST per l'applicazione SANtricity Cloud Connector non sono descritti in queste procedure. Per gli sviluppatori esperti, gli endpoint sono disponibili per ogni operazione di SANtricity Cloud Connector nella documentazione API. È possibile accedere alla documentazione API accedendo a. `http://<hostname.domain>:<port>/docs` tramite un browser.

Tipi di backup

Il connettore cloud di SANtricity offre due tipi di backup: Backup basati su immagine e su file.

- **Backup basato su immagine**

  Un backup basato su immagine legge i blocchi di dati raw da un volume di snapshot ed esegue il backup su un file noto come immagine. Viene eseguito il backup di tutti i blocchi di dati del volume Snapshot, inclusi i blocchi vuoti, i blocchi occupati dai file cancellati, i blocchi associati alla partizione e i metadati del file system. I backup delle immagini hanno il vantaggio di memorizzare tutte le informazioni con il volume snapshot indipendentemente dallo schema di partizione o dai file system su di esso.

  L'immagine non viene memorizzata nella destinazione di backup come singolo file, ma viene suddivisa in una serie di blocchi di dati, che hanno una dimensione di 64 MB. I blocchi di dati consentono a SANtricity Cloud Connector di utilizzare più connessioni alla destinazione di backup, migliorando in tal modo le prestazioni del processo di backup.

  Per i backup su StorageGRID e Amazon Web Services (S3), ogni blocco di dati utilizza una chiave di crittografia separata per crittografare il blocco. La chiave è un hash SHA256 composto dalla combinazione di una passphrase fornita dall'utente e dell'hash SHA256 dei dati dell'utente. Per i backup su AltaVault, SANtricity Cloud Connector non crittografa i blocchi di dati mentre AltaVault esegue questa operazione.

- **Backup basato su file**

  Un backup basato su file legge i file contenuti in una partizione del file system e li esegue il backup in una serie di blocchi di dati di 64 MB. Un backup basato su file non esegue il backup di file cancellati o di partizioni e metadati del file system. Come per i backup basati su immagini, i blocchi di dati consentono a SANtricity Cloud Connector di utilizzare più connessioni alla destinazione di backup, migliorando in tal modo le performance del processo di backup.

  Per i backup su StorageGRID e Amazon Web Services, ogni blocco di dati utilizza una chiave di crittografia separata per crittografare il blocco. La chiave è un hash SHA256 costituito dalla combinazione di password

fornite dall'utente e hash SHA256 dei dati dell'utente. Per i backup su AltaVault, i blocchi di dati non vengono crittografati da SANtricity Cloud Connector perché AltaVault esegue questa operazione.

Requisiti di sistema per Cloud Connector

Il sistema deve soddisfare i requisiti di compatibilità per SANtricity Cloud Connector.

Requisiti hardware dell'host

L'hardware deve soddisfare i seguenti requisiti minimi:

- Almeno 5 GB di memoria; 4 GB per la dimensione massima configurata dell'heap
- L'installazione del software richiede almeno 5 GB di spazio libero su disco

È necessario installare il proxy dei servizi Web di SANtricity per utilizzare il connettore cloud di SANtricity. È possibile installare Web Services Proxy in locale oppure eseguire l'applicazione in remoto su un server diverso. Per informazioni sull'installazione del proxy dei servizi Web di SANtricity, consultare "Argomenti relativi ai proxy dei servizi Web".

Browser supportati

Con l'applicazione SANtricity Cloud Connector sono supportati i seguenti browser (sono indicate le versioni minime):

- Firefox v31
- Google Chrome v47
- Microsoft Internet Explorer v11
- Microsoft Edge, EdgeHTML 12
- Safari v9

> La documentazione API per l'applicazione Cloud Connector di SANtricity non viene caricata quando si utilizza l'impostazione visualizzazione compatibilità nel browser Microsoft Internet Explorer v11. Per garantire che la documentazione API venga visualizzata correttamente nel browser Microsoft Internet Explorer v11, si consiglia di disattivare l'impostazione visualizzazione compatibilità.

Array di storage e firmware del controller compatibili

Prima di utilizzare l'applicazione SANtricity Cloud Connector, verificare la compatibilità degli array di storage e del firmware.

Per un elenco completo e aggiornato di tutti gli array di storage compatibili e del firmware per il connettore cloud SANtricity, consultare la "Tool di matrice di interoperabilità NetApp".

Sistemi operativi compatibili

L'applicazione SANtricity Cloud Connector 4.0 è compatibile e supportata sui seguenti sistemi operativi:

Sistema operativo	Versione	Architettura
Red Hat Enterprise Linux (RHEL)	7.x	64 bit

Sistema operativo	Versione	Architettura
SUSE Linux Enterprise Server (SLES)	12.x	64 bit

File system supportati

È necessario utilizzare i file system supportati per eseguire backup e ripristini tramite l'applicazione SANtricity Cloud Connector.

I seguenti file system sono supportati per le operazioni di backup e ripristino nell'applicazione SANtricity Cloud Connector:

- ext2
- ext3
- ext4

Installare SANtricity Cloud Connector

Il pacchetto di soluzioni di connettori cloud SANtricity (file .bin) è disponibile solo per le piattaforme Linux RedHat e SUSE.

È possibile installare l'applicazione SANtricity Cloud Connector in modalità grafica o console su un sistema operativo Linux compatibile. Durante il processo di installazione, è necessario specificare i numeri delle porte non SSL e SSL per SANtricity Cloud Connector. Una volta installato, SANtricity Cloud Connector viene eseguito come processo daemon.

Lo strumento SANtricity Cloud Connector non è più disponibile per il download.

Prima di iniziare

Leggere le seguenti note:

- Se il proxy dei servizi Web di SANtricity è già installato sullo stesso server di SANtricity, si verificheranno conflitti tra numeri di porta non SSL e numeri di porta SSL. In questo caso, scegliere i numeri appropriati per la porta non SSL e la porta SSL durante l'installazione di SANtricity Cloud Connector.
- Se vengono apportate modifiche hardware all'host, reinstallare l'applicazione SANtricity Cloud Connector per garantire la coerenza della crittografia.
- I backup creati fino alla versione 3.1 dell'applicazione SANtricity Cloud Connector non sono compatibili con la versione 4.0 dell'applicazione SANtricity Cloud Connector. Se si intende mantenere questi backup, è necessario continuare a utilizzare la versione precedente di SANtricity Cloud Connector. Per garantire la corretta installazione di release 3.1 e 4.0 separate di SANtricity Cloud Connector, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

Installazione di Device Mapper multipath (DM-MP)

Tutti gli host che eseguono il connettore cloud di SANtricity devono anche eseguire il multipath (DM-MP) di Linux Device Mapper e avere installato il pacchetto multipath-tools.

Il processo di rilevamento di SANtricity Cloud Connector si basa sul pacchetto di strumenti multipath per il rilevamento e il riconoscimento dei volumi e dei file da eseguire per il backup o il ripristino. Per ulteriori informazioni su come impostare e configurare la funzione di mappatura dei dispositivi, consultare la *Guida ai*

driver multipath di SANtricity Storage Manager per la release di SANtricity in uso nella sezione "E-Series e risorse di documentazione SANtricity".

Installare Cloud Connector

È possibile installare SANtricity Cloud Connector sui sistemi operativi Linux in modalità grafica o console.

Modalità grafica

È possibile utilizzare la modalità grafica per installare SANtricity Cloud Connector su un sistema operativo Linux.

Prima di iniziare

Indicare una posizione host per l'installazione di SANtricity Cloud Connector.

Fasi

1. Scaricare il file di installazione di SANtricity Cloud Connector nella posizione host desiderata.
2. Aprire una finestra terminale.
3. Accedere al file di directory contenente il file di installazione di SANtricity Cloud Connector.
4. Avviare il processo di installazione di SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin -i gui
   ```

   In questo comando, `xxxx` indica il numero di versione dell'applicazione.

   Viene visualizzata la finestra Installer.

5. Esaminare la dichiarazione Introduzione, quindi fare clic su **Avanti**.

   Il Contratto di licenza per NetApp, Inc Il software viene visualizzato nella finestra del programma di installazione.

6. Accettare i termini del Contratto di licenza, quindi fare clic su **Avanti**.

   Vengono visualizzati i backup creati con le release precedenti di SANtricity Cloud Connector.

7. Per riconoscere i backup creati con le release precedenti di SANtricity, fare clic su **Avanti**.

   > Per installare la versione 4.0 di SANtricity Cloud Connector mantenendo una versione precedente, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

   La pagina Choose Install (Scegli installazione) viene visualizzata all'interno della finestra Installer (programma di installazione). Il campo dove si desidera installare visualizza la seguente cartella di installazione predefinita: `opt/netapp/santricity_cloud_connector4/`

8. Scegliere una delle seguenti opzioni:
   - Per accettare la posizione predefinita, fare clic su **Avanti**.
   - Per modificare la posizione predefinita, immettere una nuova posizione per la cartella. Viene visualizzata la pagina Enter the non SSL Jetty Port Number (immettere il numero di porta Jetty non

SSL). Alla porta non SSL viene assegnato il valore predefinito 8080.

9. Scegliere una delle seguenti opzioni:
   - Per accettare il numero di porta SSL predefinito, fare clic su **Avanti**.
   - Per modificare il numero di porta SSL predefinito, immettere il nuovo valore del numero di porta desiderato.
10. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta non SSL predefinito, fare clic su **Avanti**.
    - Per modificare il numero di porta non SSL predefinito, immettere il nuovo valore del numero di porta desiderato. Viene visualizzata la pagina Pre-Installation Summary (Riepilogo preinstallazione).
11. Esaminare il Riepilogo pre-installazione visualizzato, quindi fare clic su **Installa**.

    Viene avviata l'installazione di SANtricity Cloud Connector e viene visualizzata una richiesta di installazione di Webserver Daemon.

12. Fare clic su **OK** per confermare la richiesta di installazione di Webserver Daemon.

    Viene visualizzato il messaggio Installation complete (Installazione completata).

13. Fare clic su **Done** (fine) per uscire dal programma di installazione di SANtricity Cloud Connecter.

Modalità console

È possibile utilizzare la modalità console per installare SANtricity Cloud Connector su un sistema operativo Linux.

Prima di iniziare

Indicare una posizione host per l'installazione di SANtricity Cloud Connector.

Fasi

1. Scaricare il file di installazione di SANtricity Cloud Connector nella posizione dell'host i/o desiderata.
2. Aprire una finestra terminale.
3. Accedere al file di directory contenente il file di installazione di SANtricity Cloud Connector.
4. Avviare il processo di installazione di SANtricity Cloud Connector:

   ```
   ./cloudconnector-xxxx.bin -i console
   ```

   In questo comando, `xxxx` indica il numero di versione dell'applicazione.

   Il processo di installazione di SANtricity Cloud Connector viene inizializzato.

5. Premere **Invio** per procedere con il processo di installazione.

   Il Contratto di licenza con l'utente finale per NetApp, Inc Il software viene visualizzato nella finestra del programma di installazione.

   > Per annullare il processo di installazione in qualsiasi momento, digitare `quit` nella finestra del programma di installazione.

6. Premere **Invio** per passare a ciascuna parte del Contratto di licenza con l'utente finale.

   La dichiarazione di accettazione del Contratto di licenza viene visualizzata sotto la finestra del programma di installazione.

7. Per accettare i termini del Contratto di licenza con l'utente finale e procedere con l'installazione di SANtricity Cloud Connector, immettere `Y` E premere **Invio** nella finestra del programma di installazione.

   Vengono visualizzati i backup creati con le release precedenti di SANtricity Cloud Connector.

   > Se non si accettano i termini del Contratto per l'utente finale, digitare `N` E premere **Invio** per terminare il processo di installazione di SANtricity Cloud Connector.

8. Per riconoscere i backup creati con le release precedenti di SANtricity, premere **Invio**.

   > Per installare la versione 4.0 di SANtricity Cloud Connector mantenendo una versione precedente, è necessario assegnare numeri di porta univoci per ciascuna versione dell'applicazione.

   Viene visualizzato il messaggio Scegli cartella di installazione con la seguente cartella di installazione predefinita per SANtricity Cloud Connector:`/opt/netapp/santricity_cloud_connector4/`.

9. Scegliere una delle seguenti opzioni:
   - Per accettare la posizione di installazione predefinita, premere **Invio**.
   - Per modificare la posizione di installazione predefinita, immettere la nuova posizione della cartella. Viene visualizzato il messaggio inserire il numero di porta Jetty non SSL. Alla porta non SSL viene assegnato il valore predefinito 8080.
10. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta SSL predefinito, premere **Avanti**.
    - Per modificare il numero di porta SSL predefinito, immettere il nuovo valore del numero di porta desiderato.
11. Scegliere una delle seguenti opzioni:
    - Per accettare il numero di porta non SSL predefinito, premere **Invio**.
    - Per modificare il numero di porta non SSL predefinito, inserire il nuovo valore del numero di porta. Viene visualizzato il riepilogo pre-installazione di SANtricity Cloud Connector.
12. Esaminare il Riepilogo pre-installazione visualizzato e premere **Invio**.
13. Premere **Invio** per confermare la richiesta di configurazione di Webserver Daemon.

    Viene visualizzato il messaggio Installation complete (Installazione completata).

14. Premere **Invio** per uscire dal programma di installazione di SANtricity.

Aggiungere il certificato del server e il certificato CA in un archivio chiavi

Per utilizzare una connessione https sicura dal browser all'host di SANtricity Cloud Connector, è possibile accettare il certificato autofirmato dall'host di SANtricity Cloud Connector o aggiungere un certificato e una catena di attendibilità riconosciuti sia dal browser che dall'applicazione SANtricity Cloud Connector.

Prima di iniziare

L'applicazione SANtricity Cloud Connector deve essere installata su un host.

Fasi

1. Arrestare il servizio utilizzando `systemctl` comando.
2. Dalla posizione di installazione predefinita, accedere alla directory di lavoro.

   > Il percorso di installazione predefinito per SANtricity Cloud Connector è `/opt/netapp/santricity_cloud_connector4`.

3. Utilizzando il `keytool` Creare il certificato del server e la richiesta di firma del certificato (CSR).

   ESEMPIO

   ```
   keytool -genkey -dname "CN=host.example.com, OU=Engineering, O=Company,
   L=<CITY>, S=<STATE>, C=<COUNTRY>" -alias cloudconnect -keyalg "RSA"
   -sigalg SHA256withRSA -keysize 2048 -validity 365 -keystore
   keystore_cloudconnect.jks -storepass changeit
   keytool -certreq -alias cloudconnect -keystore keystore_cloudconnect.jks
   -storepass changeit -file cloudconnect.csr
   ```

4. Inviare la CSR generata all'autorità di certificazione (CA) desiderata.

   L'autorità di certificazione firma la richiesta di certificato e restituisce un certificato firmato. Inoltre, si riceve un certificato dalla CA stessa. Questo certificato CA deve essere importato nel keystore.

5. Importare il certificato e la catena del certificato CA nell'archivio chiavi dell'applicazione: `/<install Path>/working/keystore`

   ESEMPIO

   ```
   keytool -import -alias ca-root -file root-ca.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -alias ca-issuing-1 -file issuing-ca-1.cer -keystore
   keystore_cloudconnect.jks -storepass <password> -noprompt
   keytool -import -trustcacerts -alias cloudconnect -file certnew.cer
   -keystore keystore_cloudconnect.jks -storepass <password>
   ```

6. Riavviare il servizio.

Aggiungere il certificato StorageGRID in un keystore

Se si configura StorageGRID come tipo di destinazione per l'applicazione Cloud Connector di SANtricity, è necessario prima aggiungere un certificato StorageGRID nell'archivio chiavi di SANtricity Cloud Connector.

Prima di iniziare

- Si dispone di un certificato StorageGRID firmato.
- L'applicazione SANtricity Cloud Connector è installata su un host.

Fasi

1. Arrestare il servizio utilizzando `systemctl` comando.
2. Dalla posizione di installazione predefinita, accedere alla directory di lavoro.

   > Il percorso di installazione predefinito per SANtricity Cloud Connector è `/opt/netapp/santricity_cloud_connector4`.

3. Importare il certificato StorageGRID nell'archivio chiavi dell'applicazione: `/<install Path>/working/keystore`

   ESEMPIO

   ```
   opt/netapp/santricity_cloud_connector4/jre/bin/keytool -import
   -trustcacerts -storepass changeit -noprompt -alias StorageGrid_SSL -file
   /home/ictlabsg01.cer -keystore
   /opt/netapp/santricity_cloud_connector/jre/lib/security/cacerts
   ```

4. Riavviare il servizio.

Configurare SANtricity Cloud Connector per la prima volta

Una volta completata l'installazione, è possibile configurare l'applicazione SANtricity Cloud Connector tramite la configurazione guidata. La configurazione guidata viene visualizzata dopo l'accesso iniziale a SANtricity Cloud Connector.

Accedere a SANtricity Cloud Connector per la prima volta

Quando si inizializza SANtricity Cloud Connector per la prima volta, è necessario immettere una password predefinita per accedere all'applicazione.

Prima di iniziare

Assicurarsi di avere accesso a un browser connesso a Internet.

Fasi

1. Aprire un browser supportato.
2. Connettersi al server SANtricity Connector configurato (ad es. `http://localhost:8080/`).

   Viene visualizzata la pagina di accesso iniziale per l'applicazione SANtricity Cloud Connector.

3. Nel campo Password amministratore, immettere la password predefinita di `password`.
4. Fare clic su **Log in** (Accedi).

   Viene visualizzata la Configurazione guidata di SANtricity Cloud Connector.

Utilizzando la Configurazione guidata

La configurazione guidata viene visualizzata dopo aver eseguito correttamente l'accesso iniziale a SANtricity Cloud Connector.

La configurazione guidata consente di impostare la password dell'amministratore, le credenziali di gestione dell'accesso proxy dei servizi Web, il tipo di destinazione di backup desiderato e la password di crittografia per SANtricity Cloud Connector.

Fase 1: Impostare la password dell'amministratore

È possibile personalizzare la password utilizzata per gli accessi successivi a SANtricity Cloud Connector attraverso la pagina Imposta password amministratore.

La creazione di una password tramite la pagina Imposta password amministratore sostituisce effettivamente la password predefinita utilizzata durante l'accesso iniziale per l'applicazione SANtricity Cloud Connector.

Fasi

1. Nella pagina Set Administrator Password (Imposta password amministratore), inserire la password di accesso desiderata per SANtricity Cloud Connector nel campo **Enter the new Administrator password** (immettere la nuova password amministratore).
2. Nel campo **immettere nuovamente la nuova password amministratore**, immettere nuovamente la password dal primo campo.
3. Fare clic su **Avanti**.

   La password impostata per SANtricity Cloud Connector viene accettata e la pagina Imposta password viene visualizzata nella Configurazione guidata.

   > La password dell'amministratore definita dall'utente non viene impostata fino al completamento della configurazione guidata.

Fase 2: Impostare la password

Nella pagina Enter the Encryption Pass phrase (immettere la password di crittografia), è possibile specificare una password alfanumerica compresa tra 8 e 32 caratteri.

Una password specificata dall'utente è richiesta come parte della chiave di crittografia dei dati utilizzata dall'applicazione Cloud Connector di SANtricity.

Fasi

1. Nel campo **definisci una password**, immettere la password desiderata.
2. Nel campo **Re-Enter your pass phrase** (immettere nuovamente la password), immettere nuovamente la password nel primo campo.
3. Fare clic su **Avanti**.

   La password immessa per l'applicazione SANtricity Cloud Connector viene accettata e viene visualizzata la pagina Seleziona tipo di destinazione per la configurazione guidata.

Fase 3: Selezionare il tipo di destinazione

Le funzionalità di backup e ripristino sono disponibili per i tipi di destinazione Amazon S3, AltaVault e StorageGRID tramite SANtricity Cloud Connector. È possibile specificare il tipo di destinazione dello storage desiderato per l'applicazione SANtricity Cloud Connector nella pagina selezionare il tipo di destinazione.

Prima di iniziare

Assicurarsi di disporre di uno dei seguenti elementi: Punto di montaggio AltaVault, account Amazon AWS o

account StorageGRID.

Fasi

1. Nel menu a discesa, selezionare una delle seguenti opzioni:
    - Amazon AWS
    - AltaVault
    - StorageGRID

    Nella Configurazione guidata viene visualizzata la pagina Target Type (tipo di destinazione) per l'opzione selezionata.

2. Fare riferimento alle istruzioni di configurazione appropriate per AltaVault, Amazon AWS o StorageGRID.

Configurare l'appliance AltaVault

Dopo aver selezionato l'opzione AltaVault appliance nella pagina selezionare il tipo di destinazione, vengono visualizzate le opzioni di configurazione per il tipo di destinazione AltaVault.

Prima di iniziare

- Si dispone del percorso di montaggio NFS per un'appliance AltaVault.
- Hai specificato l'appliance AltaVault come tipo di destinazione.

Fasi

1. Nel campo **percorso di montaggio NFS**, inserire il punto di montaggio per il tipo di destinazione AltaVault.

    I valori nel campo **NFS Mount Path** devono seguire il formato del percorso Linux.

2. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

    Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

3. Fare clic su **Test connessione** per verificare la connessione per le impostazioni AltaVault specificate.
4. Fare clic su **Avanti**.

    Il tipo di destinazione specificato per il connettore cloud di SANtricity viene accettato e la pagina Proxy dei servizi web viene visualizzata nella Configurazione guidata.

5. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Configurare l'account Amazon AWS

Dopo aver selezionato l'opzione Amazon AWS nella pagina Select the Target Type (Seleziona tipo di destinazione), vengono visualizzate le opzioni di configurazione per il tipo di destinazione Amazon AWS.

Prima di iniziare

- Hai un account Amazon AWS stabilito.

- Hai specificato Amazon AWS come tipo di destinazione.

Fasi

1. Nel campo **Access Key ID** (ID chiave di accesso), immettere l'ID di accesso per la destinazione Amazon AWS.
2. Nel campo **Secret Access Key** (chiave di accesso segreta), immettere la chiave di accesso segreta per la destinazione.
3. Nel campo **Nome bucket**, immettere il nome del bucket per la destinazione.
4. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

   Si consiglia di attivare questa impostazione per garantire che i dati della destinazione di backup possano essere ripristinati in caso di perdita del database.

   Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

5. Fare clic su **Test Connection** (verifica connessione) per verificare le credenziali Amazon AWS immesse.
6. Fare clic su **Avanti**.

   Il tipo di destinazione specificato per il connettore cloud SANtricity viene accettato e la pagina Proxy dei servizi Web viene visualizzata nella Configurazione guidata.

7. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Configurare l'account StorageGRID

Dopo aver selezionato l'opzione StorageGRID nella pagina selezionare il tipo di destinazione, vengono visualizzate le opzioni di configurazione per il tipo di destinazione StorageGRID.

Prima di iniziare

- Hai un account StorageGRID stabilito.
- Hai un certificato StorageGRID firmato nel keystore di SANtricity Cloud Connector.
- È stato specificato StorageGRID come tipo di destinazione.

Fasi

1. Nel campo **URL**, immettere l'URL del servizio cloud Amazon S3
2. Nel campo **Access Key ID** (ID chiave di accesso), inserire l'ID di accesso per la destinazione S3.
3. Nel campo **Secret Access Key** (chiave di accesso segreta), inserire la chiave di accesso segreta per la destinazione S3.
4. Nel campo **Nome bucket**, immettere il nome del bucket per la destinazione S3.
5. Per utilizzare l'accesso in stile tracciato, selezionare la casella di controllo **Usa accesso in stile tracciato**.

   Se deselezionata, viene utilizzato l'accesso in stile host virtuale.

6. Selezionare la casella di controllo **Salva un backup del database di configurazione su questa destinazione** per creare un backup del database di configurazione sul tipo di destinazione selezionato.

> Si consiglia di attivare questa impostazione per garantire che i dati della destinazione di backup possano essere ripristinati in caso di perdita del database.

> Se durante il test della connessione viene rilevata una configurazione del database esistente sul tipo di destinazione specificato, è possibile sostituire le informazioni di configurazione del database esistente sull'host di SANtricity Cloud Connector con le nuove informazioni di backup inserite nella configurazione guidata.

7. Fare clic su **Test Connection** (verifica connessione) per verificare le credenziali S3 immesse.

> Alcuni account compatibili con S3 potrebbero richiedere connessioni HTTP protette. Per informazioni sull'inserimento di un certificato StorageGRID nell'archivio chiavi, vedere "Aggiungere il certificato StorageGRID in un keystore".

8. Fare clic su **Avanti**.

   Il tipo di destinazione specificato per il connettore cloud SANtricity viene accettato e la pagina Proxy servizi web viene visualizzata nella Configurazione guidata.

9. Passare alla "fase 4: Connessione al proxy dei servizi Web".

Fase 4: Connessione al proxy dei servizi Web

Le informazioni di accesso e di connessione per il proxy dei servizi Web utilizzato insieme a SANtricity Cloud Connector vengono inserite nella pagina Immetti credenziali e URL proxy dei servizi Web.

Prima di iniziare

Assicurarsi di disporre di una connessione stabilita con il proxy dei servizi Web di SANtricity.

Fasi

1. Nel campo **URL**, immettere l'URL del proxy dei servizi Web utilizzato per SANtricity Cloud Connector.
2. Nel campo **Nome utente**, immettere il nome utente per la connessione proxy dei servizi Web.
3. Nel campo **Password**, immettere la password per la connessione proxy dei servizi Web.
4. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali proxy dei servizi Web immesse.
5. Dopo aver verificato le credenziali di Web Services Proxy immesse tramite la connessione di prova.
6. Fare clic su **Avanti**

   Le credenziali del proxy dei servizi Web per il connettore cloud di SANtricity vengono accettate e la pagina Seleziona array di storage viene visualizzata nella Configurazione guidata.

Fase 5: Selezionare gli array di storage

In base alle credenziali del proxy dei servizi Web di SANtricity immesse tramite la Configurazione guidata, viene visualizzato un elenco degli array di storage disponibili nella pagina Seleziona array di storage. In questa pagina è possibile selezionare gli array di storage utilizzati da SANtricity Cloud Connector per i processi di backup e ripristino.

Prima di iniziare

Assicurarsi che gli array di storage siano configurati per l'applicazione proxy dei servizi Web di SANtricity.

> Gli array di storage non raggiungibili osservati dall'applicazione SANtricity Cloud Connector causeranno eccezioni API nel file di log. Questo è il comportamento previsto dell'applicazione SANtricity Cloud Connector ogni volta che un elenco di volumi viene estratto da un array irraggiungibile. Per evitare queste eccezioni API nel file di log, è possibile risolvere il problema principale direttamente con l'array di storage o rimuovere l'array di storage interessato dall'applicazione proxy dei servizi Web di SANtricity.

Fasi

1. Selezionare ciascuna casella di controllo accanto all'array di storage che si desidera assegnare all'applicazione SANtricity Cloud Connector per le operazioni di backup e ripristino.
2. Fare clic su **Avanti**.

   Gli array di storage selezionati vengono accettati e viene visualizzata la pagina Select hosts (Seleziona host) nella Configurazione guidata.

> È necessario configurare una password valida per qualsiasi array di storage selezionato nella pagina Select Storage Array (Seleziona array di storage). È possibile configurare le password degli array di storage attraverso la documentazione dell'API proxy dei servizi Web di SANtricity.

Fase 6: Selezionare gli host

In base agli array di storage ospitati dal proxy dei servizi Web selezionati tramite la Configurazione guidata, è possibile selezionare un host disponibile per mappare i volumi di backup e ripristinare i volumi candidati all'applicazione SANtricity Cloud Connector attraverso la pagina Seleziona host.

Prima di iniziare

Assicurarsi di disporre di un host tramite il proxy dei servizi Web di SANtricity.

Fasi

1. Nel menu a discesa dello storage array elencato, selezionare l'host desiderato.
2. Ripetere il passaggio 1 per tutti gli array di storage aggiuntivi elencati nella pagina Select host (Seleziona host).
3. Fare clic su **Avanti**.

   L'host selezionato per SANtricity Cloud Connector viene accettato e la pagina di revisione viene visualizzata nella Configurazione guidata.

Fase 7: Esaminare la configurazione iniziale

L'ultima pagina della configurazione guidata di SANtricity Cloud Connector fornisce un riepilogo dei risultati immessi per la revisione.

Esaminare i risultati dei dati di configurazione validati.

- Se tutti i dati di configurazione sono stati validati e stabiliti correttamente, fare clic su **fine** per completare il processo di configurazione.

- Se non è possibile validare una sezione dei dati di configurazione, fare clic su **Back** (Indietro) per accedere alla pagina appropriata della configurazione guidata e rivedere i dati inviati.

Accedere a SANtricity Cloud Connector

È possibile accedere all'interfaccia utente grafica per l'applicazione SANtricity Cloud Connector attraverso il server configurato in un browser supportato. Assicurati di disporre di un account SANtricity Cloud Connector stabilito.

Fasi

1. In un browser supportato, connettersi al server SANtricity Cloud Connector configurato (ad esempio, `http://localhost:8080/`).

   Viene visualizzata la pagina di accesso dell'applicazione SANtricity Cloud Connector.

2. Inserire la password di amministratore configurata.
3. Fare clic su **Login**.

   Viene visualizzata la landing page dell'applicazione SANtricity Cloud Connector.

Backup

Puoi accedere all'opzione Backup nel pannello di navigazione a sinistra dell'applicazione SANtricity Cloud Connector. L'opzione Backup visualizza la pagina Backup, che consente di creare nuovi processi di backup basati su immagine o file.

Utilizzare la pagina **backup** dell'applicazione SANtricity Cloud Connector per creare ed elaborare i backup dei volumi e-Series. È possibile creare backup basati su immagini o file ed eseguire tali operazioni immediatamente o in un secondo momento. Inoltre, è possibile scegliere di eseguire backup completi o incrementali in base all'ultimo backup completo eseguito. È possibile eseguire un massimo di sei backup incrementali in base all'ultimo backup completo eseguito tramite l'applicazione SANtricity Cloud Connector.

> Tutti i timestamp per i processi di backup e ripristino elencati nell'applicazione SANtricity Cloud Connector utilizzano l'ora locale.

Creare un nuovo backup basato su immagine

È possibile creare nuovi backup basati su immagini tramite la funzione Crea nella pagina dei backup dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurarsi di disporre di array di storage dal proxy dei servizi Web registrato al connettore cloud di SANtricity.

Fasi

1. Nella pagina Backup, fare clic su **Crea**.

   Viene visualizzata la finestra Create Backup (Crea backup).

2. Selezionare **Crea un backup basato su immagine**.
3. Fare clic su **Avanti**.

Nella finestra Create Backup (Crea backup) viene visualizzato un elenco dei volumi e-Series disponibili.

4. Selezionare il volume e-Series desiderato e fare clic su **Avanti**.

   Viene visualizzata la pagina **assegnare un nome al backup e fornire una descrizione** della finestra di conferma della creazione del backup.

5. Per modificare il nome del backup generato automaticamente, immettere il nome desiderato nel campo **Nome processo**.
6. Se necessario, aggiungere una descrizione per il backup nel campo **Descrizione lavoro**.

   Inserire una descrizione del lavoro che consenta di identificare facilmente il contenuto del backup.

7. Fare clic su **Avanti**.

   Un riepilogo del backup basato su immagine selezionato viene visualizzato nella pagina **Review backup information** della finestra Create Backup (Crea backup).

8. Esaminare il backup selezionato e fare clic su **fine**.

   Viene visualizzata la pagina di conferma della finestra Create Backup (Crea backup).

9. Selezionare una delle seguenti opzioni:
   - **Sì** — Avvia un backup completo per il backup selezionato.
   - **NO** — non viene eseguito Un backup completo per il backup basato sull'immagine selezionato.

   Un backup completo per il backup basato sull'immagine selezionato può essere eseguito in un secondo momento attraverso la funzione Esegui nella pagina Backup.

10. Fare clic su **OK**.

    Il backup per il volume e-Series selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Backup.

Creare una nuova cartella/backup basato su file

È possibile creare nuovi backup basati su file/cartelle tramite la funzione Crea nella pagina dei backup dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurarsi di disporre di array di storage dal proxy dei servizi Web registrato al connettore cloud di SANtricity.

Un backup basato su file esegue il backup incondizionato di tutti i file sul file system specificato. Tuttavia, è possibile eseguire un ripristino selettivo di file e cartelle.

Fasi

1. Nella pagina Backup, fare clic su **Crea**.

   Viene visualizzata la finestra Create Backup (Crea backup).

2. Selezionare **Crea un backup basato su file/cartella**.

3. Fare clic su **Avanti**.

   Nella finestra Create Backup (Crea backup) viene visualizzato un elenco di volumi contenenti file system disponibili per il backup.

4. Selezionare il volume desiderato e fare clic su **Avanti**.

   Nella finestra Create Backup (Crea backup) viene visualizzato un elenco dei filesystem disponibili sul volume selezionato.

   > Se il file system non viene visualizzato, verificare che il tipo di file sia supportato dall'applicazione SANtricity Cloud Connector. Per ulteriori informazioni, fare riferimento a. "File system supportati".

5. Selezionare il file system desiderato contenente la cartella o i file di cui eseguire il backup e fare clic su **Avanti**.

   Viene visualizzata la pagina **assegnare un nome al backup e fornire una descrizione** della finestra di conferma della creazione del backup.

6. Per modificare il nome del backup generato automaticamente, immettere il nome desiderato nel campo **Nome processo**.
7. Se necessario, aggiungere una descrizione per il backup nel campo **Descrizione lavoro**.

   > Inserire una descrizione del lavoro che consenta di identificare facilmente il contenuto del backup.

8. Fare clic su **Avanti**.

   Un riepilogo del backup basato su file o cartella selezionato viene visualizzato nella pagina **Review backup information** della finestra Create Backup (Crea backup).

9. Esaminare la cartella o il backup basato su file selezionato e fare clic su **fine**.

   Viene visualizzata la pagina di conferma della finestra Create Backup (Crea backup).

10. Selezionare una delle seguenti opzioni:
    - **Sì** — Avvia un backup completo per il backup selezionato.
    - **NO** — non viene eseguito Un backup completo per il backup selezionato.

    > Un backup completo per il backup basato su file selezionato può essere eseguito anche in un secondo momento attraverso la funzione Esegui nella pagina dei backup.

11. Fare clic su **Chiudi**.

    Il backup per il volume e-Series selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Backup.

Eseguire backup completi e incrementali

È possibile eseguire backup completi e incrementali tramite la funzione Esegui nella pagina dei backup. I backup incrementali sono disponibili solo per i backup basati su file.

Prima di iniziare

Assicurarsi di aver creato un processo di backup tramite SANtricity Cloud Connector.

Fasi

1. Nella scheda Backup, selezionare il processo di backup desiderato e fare clic su **Esegui**.

   > Il backup completo viene eseguito automaticamente ogni volta che viene selezionato un processo di backup basato su immagine o un processo di backup senza un backup iniziale eseguito in precedenza.

   Viene visualizzata la finestra Esegui backup.

2. Selezionare una delle seguenti opzioni:
   - **Completo** — esegue il backup di tutti i dati per il backup basato su file selezionato.
   - **Incrementale** — esegue il backup delle modifiche apportate solo dall'ultimo backup eseguito.

     > È possibile eseguire un numero massimo di sei backup incrementali in base all'ultimo backup completo eseguito tramite l'applicazione SANtricity Cloud Connector.

3. Fare clic su **Esegui**.

   Viene avviata la richiesta di backup.

Eliminare un processo di backup

La funzione Delete (Elimina) elimina i dati di backup nella posizione di destinazione specificata per il backup selezionato insieme al set di backup.

Prima di iniziare

Assicurarsi che sia presente un backup con lo stato completato, non riuscito o annullato.

Fasi

1. Nella pagina Backup, selezionare il backup desiderato e fare clic su **Delete** (Elimina).

   > Se si seleziona un backup di base completo per l'eliminazione, vengono eliminati anche tutti i backup incrementali associati.

   Viene visualizzata la finestra Confirm Delete (Conferma eliminazione).

2. Nel campo **Type delete**, digitare `DELETE` per confermare l'azione di eliminazione.
3. Fare clic su **Delete** (Elimina).

   Il backup selezionato viene eliminato.

Ripristini

È possibile accedere all'opzione Ripristina nel pannello di navigazione a sinistra dell'applicazione SANtricity Cloud Connector. L'opzione Restore (Ripristina) visualizza la pagina Restore (Ripristina), che consente di creare nuovi processi di ripristino basati su

immagine o file.

Il connettore cloud di SANtricity utilizza il concetto di job per eseguire il ripristino effettivo di un volume e-Series. Prima di eseguire un ripristino, è necessario identificare il volume e-Series da utilizzare per l'operazione. Dopo aver aggiunto un volume e-Series per il ripristino all'host di SANtricity Cloud Connector, è possibile utilizzare `Restore` Dell'applicazione SANtricity Cloud Connector per creare ed elaborare i ripristini.

> Tutti i timestamp per i processi di backup e ripristino elencati nell'applicazione SANtricity Cloud Connector utilizzano l'ora locale.

Creare un nuovo ripristino basato su immagine

È possibile creare nuovi ripristini basati su immagine tramite la funzione Crea nella pagina di ripristino dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurati di avere a disposizione un backup basato su immagine tramite SANtricity Cloud Connector.

Fasi

1. Nella pagina di ripristino dell'applicazione SANtricity Cloud Connector, fare clic su **Crea**.

   Viene visualizzata la finestra Restore (Ripristino).

2. Selezionare il backup desiderato.
3. Fare clic su **Avanti**.

   La pagina Select Backup Point (Seleziona punto di backup) viene visualizzata nella finestra Restore (Ripristino).

4. Selezionare il backup completo desiderato.
5. Fare clic su **Avanti**.

   La pagina Select Restore Target (Seleziona destinazione ripristino) viene visualizzata nella finestra Restore (Ripristino).

6. Selezionare il volume di ripristino e fare clic su **Avanti**.

   La pagina Review (Revisione) viene visualizzata nella finestra Restore (Ripristino).

7. Esaminare l'operazione di ripristino selezionata e fare clic su **fine**.

   Il ripristino per il volume host di destinazione selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Creare un nuovo ripristino basato su file

È possibile creare nuovi ripristini basati su file tramite la funzione Crea nella pagina Ripristino dell'applicazione SANtricity Cloud Connector.

Prima di iniziare

Assicurati di avere a disposizione un backup basato su file tramite SANtricity Cloud Connector.

Fasi

1. Nella pagina di ripristino dell'applicazione SANtricity Cloud Connector, fare clic su **Crea**.

   Viene visualizzata la finestra Restore (Ripristino).

2. Nella finestra Restore (Ripristino), selezionare il backup basato su file desiderato.
3. Fare clic su **Avanti**.

   La pagina Select Backup Point (Seleziona punto di backup) viene visualizzata nella finestra Create Restore Job (Crea processo di ripristino).

4. Nella pagina Select Backup Point (Seleziona punto di backup), selezionare il backup completo desiderato.
5. Fare clic su **Avanti**.

   Nella finestra Restore (Ripristino) viene visualizzato un elenco dei file system o delle cartelle/file disponibili.

6. Selezionare le cartelle o i file da ripristinare e fare clic su **Avanti**.

   La pagina Select Restore Target (Seleziona destinazione ripristino) viene visualizzata nella finestra Restore (Ripristino).

7. Selezionare il volume di ripristino e fare clic su **Avanti**.

   La pagina Review (Revisione) viene visualizzata nella finestra Restore (Ripristino).

8. Esaminare l'operazione di ripristino selezionata e fare clic su **fine**.

   Il ripristino per il volume host di destinazione selezionato viene avviato e lo stato dell'attività viene visualizzato nella sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Eliminare un ripristino

È possibile utilizzare la funzione Delete (Elimina) per eliminare un elemento di ripristino selezionato dalla sezione Result list (elenco risultati) della pagina Restore (Ripristino).

Prima di iniziare

Assicurarsi che sia presente un processo di ripristino con lo stato completato, non riuscito o annullato.

Fasi

1. Nella pagina Restore (Ripristino), fare clic su **Delete** (Elimina).

   Viene visualizzata la finestra Confirm Delete (Conferma eliminazione).

2. Nel campo **Type delete**, digitare `delete` per confermare l'azione di eliminazione.
3. Fare clic su **Delete** (Elimina).

   > Non è possibile eliminare un ripristino sospeso.

   Il ripristino selezionato viene eliminato.

Modificare le impostazioni di SANtricity Cloud Connector

L'opzione Settings (Impostazioni) consente di modificare le configurazioni correnti

dell'applicazione per l'account S3, gli array e gli host di storage gestiti e le credenziali del proxy dei servizi Web. Puoi anche modificare la password per l'applicazione SANtricity Cloud Connector tramite l'opzione Impostazioni.

Modificare le impostazioni dell'account S3

È possibile modificare le impostazioni S3 esistenti per l'applicazione SANtricity Cloud Connector nella finestra S3 account Settings (Impostazioni account S3).

Prima di iniziare

Quando si modificano le impostazioni dell'URL o dell'etichetta del bucket S3, tenere presente che l'accesso a qualsiasi backup esistente configurato tramite SANtricity Cloud Connector verrà compromesso.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni > Configurazione**.

   Viene visualizzata la pagina Impostazioni - Configurazione.

2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni) per S3 account Settings (Impostazioni account S3).

   Viene visualizzata la pagina S3 account Settings (Impostazioni account S3).

3. Nel file URL, immettere l'URL per il servizio cloud S3.
4. Nel campo **Access Key ID** (ID chiave di accesso), inserire l'ID di accesso per la destinazione S3.
5. Nel campo **Secret Access Key** (chiave di accesso segreta), inserire la chiave di accesso per la destinazione S3.
6. Nel campo **S3 Bucket Name** (Nome bucket S3), immettere il nome del bucket per la destinazione S3.
7. Se necessario, selezionare la casella di controllo **Usa accesso stile percorso**.
8. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali S3 immesse.
9. Fare clic su **Save** (Salva) per applicare le modifiche.

   Vengono applicate le impostazioni modificate dell'account S3.

Gestire gli array di storage

È possibile aggiungere o rimuovere gli array di storage dal proxy dei servizi Web registrato sull'host di SANtricity Cloud Connector nella pagina Gestione array di storage.

La pagina Gestisci array di storage visualizza un elenco di array di storage dal proxy dei servizi Web disponibile per la registrazione con l'host di SANtricity Cloud Connector.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni > Storage Array**.

   Viene visualizzata la schermata Settings - Storage Arrays (Impostazioni - array di storage).

2. Per aggiungere array di storage a SANtricity Cloud Connector, fare clic su **Aggiungi**.
   a. Nella finestra Add Storage Arrays (Aggiungi array di storage), selezionare ciascuna casella di controllo

accanto agli array di storage desiderati dall'elenco dei risultati.

b. Fare clic su **Aggiungi**.

L'array di storage selezionato viene aggiunto al connettore cloud SANtricity e visualizzato nella sezione Result list (elenco risultati) della schermata Settings - Storage Arrays (Impostazioni - array di storage).

3. Per modificare l'host per un array di storage aggiunto, fare clic su **Edit** (Modifica) per la voce nella sezione Result list (elenco risultati) della schermata Settings - Storage Arrays (Impostazioni - array di storage).
   a. Nel menu a discesa Associated host (host associato), selezionare l'host desiderato per lo storage array.
   b. Fare clic su **Save** (Salva).

   L'host selezionato viene assegnato all'array di storage.

4. Per rimuovere un array di storage esistente dall'host di SANtricity Cloud Connector, selezionare gli array di storage desiderati dall'elenco dei risultati in basso e fare clic su **Rimuovi**.
   a. Nel campo Confirm Remove Storage Array (Conferma rimozione array di storage), digitare `REMOVE`.
   b. Fare clic su **Rimuovi**.

   L'array di storage selezionato viene rimosso dall'host del connettore cloud SANtricity.

Modificare le impostazioni del proxy dei servizi Web

È possibile modificare le impostazioni proxy dei servizi Web esistenti per l'applicazione SANtricity connettore nella finestra Impostazioni proxy dei servizi Web.

Prima di iniziare

Il proxy dei servizi Web utilizzato con il connettore cloud SANtricity deve avere aggiunto gli array appropriati e la password corrispondente impostata.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni › Configurazione**.

   Viene visualizzata la schermata Impostazioni - Configurazione.

2. Fare clic su **View/Edit Settings** (Visualizza/Modifica impostazioni) per Web Services Proxy.

   Viene visualizzata la schermata delle impostazioni del proxy dei servizi Web.

3. Nel campo URL, immettere l'URL del proxy dei servizi Web utilizzato per SANtricity Cloud Connector.
4. Nel campo User Name (Nome utente), immettere il nome utente per la connessione proxy dei servizi Web.
5. Nel campo Password, immettere la password per la connessione proxy dei servizi Web.
6. Fare clic su **Test Connection** (verifica connessione) per verificare la connessione per le credenziali proxy dei servizi Web immesse.
7. Fare clic su **Save** (Salva) per applicare le modifiche.

Modificare la password di SANtricity Cloud Connector

È possibile modificare la password per l'applicazione SANtricity Cloud Connector nella schermata Modifica password.

Fasi

1. Nella barra degli strumenti a sinistra, fare clic su **Impostazioni › Configurazione**.

   Viene visualizzata la schermata Impostazioni - Configurazione.

2. Fare clic su **Modifica password** per SANtricity Cloud Connector.

   Viene visualizzata la schermata Change Password (Modifica password).

3. Nel campo Current password (Password corrente), immettere la password corrente per l'applicazione SANtricity Cloud Connector.
4. Nel campo Nuova password, immettere la nuova password per l'applicazione SANtricity Cloud Connector.
5. Nel campo Confirm new password (Conferma nuova password), immettere nuovamente la nuova password.
6. Fare clic su **Change** (Modifica) per applicare la nuova password.

   La password modificata viene applicata all'applicazione SANtricity Cloud Connector.

Disinstallare SANtricity Cloud Connector

È possibile disinstallare SANtricity Cloud Connector tramite il programma di disinstallazione grafico o la modalità console.

Disinstallare utilizzando la modalità grafica

È possibile utilizzare la modalità grafica per disinstallare SANtricity Cloud Connector su un sistema operativo Linux.

Fasi

1. Dalla finestra di un terminale, accedere alla directory contenente il file di disinstallazione di SANtricity Cloud Connector.

   Il file di disinstallazione per SANtricity Cloud Connector è disponibile nella seguente directory predefinita:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Dalla directory contenente il file di disinstallazione di SANtricity Cloud Connector, eseguire il seguente comando:

   ```
   ./uninstall_cloud_connector4 -i gui
   ```

   Il processo di disinstallazione di SANtricity Cloud Connector viene inizializzato.

3. Nella finestra di disinstallazione, fare clic su **Disinstalla** per procedere con la disinstallazione di SANtricity Cloud Connector.

   Il processo di disinstallazione viene completato e l'applicazione SANtricity Cloud Connector viene disinstallata nel sistema operativo Linux.

Disinstallare utilizzando la modalità console

È possibile utilizzare la modalità console per disinstallare SANtricity Cloud Connector su un sistema operativo Linux.

Fasi

1. Dalla finestra di un terminale, accedere alla directory contenente il file di disinstallazione di SANtricity Cloud Connector.

   Il file di disinstallazione per SANtricity Cloud Connector è disponibile nella seguente directory predefinita:

   ```
   /opt/netapp/santricity_cloud_connector4/uninstall_cloud_connector4
   ```

2. Dalla directory contenente il file di disinstallazione di SANtricity Cloud Connector, eseguire il seguente comando:

   ```
   ./uninstall_cloud_connector4 -i console
   ```

   Il processo di disinstallazione di SANtricity Cloud Connector viene inizializzato.

3. Nella finestra di disinstallazione, premere **Invio** per procedere con la disinstallazione di SANtricity Cloud Connector.

   Il processo di disinstallazione viene completato e l'applicazione SANtricity Cloud Connector viene disinstallata nel sistema operativo Linux.

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)"

Report tecnici

Sfoglia i report tecnici della piattaforma

TR della piattaforma

"TR-4725: Panoramica delle funzionalità degli array E2800"	**"+TR-4724: Panoramica delle funzionalità degli array E5700"**	**"+TR-4877: Panoramica delle funzionalità degli array EF300"**
Descrive le funzionalità hardware e software dell'array ibrido E2800 e le più recenti funzionalità del sistema operativo SANtricity.	Descrive le informazioni sul prodotto E5700, incluse le nuove funzionalità hardware e software introdotte con la versione più recente di SANtricity.	Descrive le funzionalità hardware e software dell'array all-flash EF300 e le nuove funzionalità del sistema operativo SANtricity.
"TR-4800: Panoramica delle funzionalità degli array EF600"		
Descrive le caratteristiche hardware e software dell'array all-flash EF600 e le nuove funzionalità del sistema operativo SANtricity.		

Sfoglia i report tecnici sulla sicurezza

TR di sicurezza

"TR-4474: Guida alle funzionalità di sicurezza del disco SANtricity"	**"TR-4712: Funzioni di sicurezza per la gestione SANtricity"**	**"TR-4813: Gestione dei certificati per i sistemi e-Series"**
Descrive la funzionalità di crittografia completa dei dischi per i sistemi e-Series, incluso il supporto per le unità convalidate FIPS 140-2 e il supporto per la gestione delle chiavi sia interne che esterne.	Descrive le funzioni di sicurezza di SANtricity per NetApp e-Series E2800, E5700, EF280, EF570, EF300, E sistemi storage EF600.	Descrive come gestire i certificati di sicurezza con i controller e le applicazioni e-Series più recenti.
"TR-4855: Guida al rafforzamento della sicurezza per SANtricity"	**"TR-4853: Gestione degli accessi per sistemi e-Series"**	
Descrive come implementare SANtricity per soddisfare gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.	Descrive come configurare la gestione degli accessi, inclusi RBAC (role-based access control), LDAP (Lightweight Directory Access Protocol) e SAML (Security Assertion Markup Language).	

Sfoglia i report tecnici in primo piano

TR di funzionalità

"TR-4893: Volumi di storage remoto SANtricity"	**"TR-4839: Mirroring sincrono e asincrono di SANtricity"**	**"TR-4747: Panoramica delle funzionalità Snapshot di SANtricity e guida all'implementazione"**
Descrive l'architettura della soluzione e come utilizzare il sistema di storage e-Series per importare i dati da un dispositivo di storage remoto esistente.	Descrive la funzione di mirroring sincrono e asincrono di SANtricity.	Descrive la funzione Snapshot di SANtricity, incluse le istruzioni di navigazione della GUI mediante Gestione di sistema di SANtricity.
"TR-4652: Pool di dischi dinamici SANtricity"	**"TR-4737: Bilanciamento automatico del carico SANtricity"**	**"TR-4736: API dei servizi web SANtricity"**
Descrive come gli amministratori dello storage possono raggruppare set di dischi simili in una topologia di pool in cui tutte le unità del pool partecipano al flusso di lavoro di i/O.	Viene fornita una panoramica del comportamento della funzionalità ALB, dei parametri di configurazione principali e dei miglioramenti all'interoperabilità degli host.	Viene fornita una panoramica dei servizi Web di SANtricity, un'API utilizzata per la configurazione e la gestione dei sistemi storage e-Series.

Sfoglia i report tecnici delle soluzioni

Splunk

"TR-4623: E5700 con Splunk Enterprise"	**"TR-4903: EF300 con Splunk Enterprise"**	**"TR-4930: EF600 con Splunk Enterprise"**
Descrive l'architettura integrata del sistema E5700 e la progettazione di Splunk. Questo documento riassume anche i risultati dei test delle performance ottenuti da uno strumento di simulazione degli eventi del log di Splunk.	Descrive l'architettura integrata dell'array all-flash EF300 e il design Splunk. Questo documento riassume anche i risultati dei test delle performance ottenuti da uno strumento di simulazione degli eventi del log di Splunk.	Descrive l'architettura integrata dell'array all-flash EF600 e il design Splunk. Questo documento riassume anche i risultati dei test delle performance ottenuti da uno strumento di simulazione degli eventi del log di Splunk.

Database aziendali

"TR-4764: Guida alle Best practice per Microsoft SQL Server con NetApp EF-Series"	**"TR-4794: Database Oracle su NetApp EF-Series"**	
Aiuta gli amministratori dello storage e i database a implementare con successo Microsoft SQL Server sullo storage NetApp EF-Series.	Aiuta gli amministratori dello storage e gli amministratori del database a implementare con successo Oracle sullo storage NetApp EF-Series.	

Backup e ripristino

"TR-4320: Best Practice con CommVault Data Platform V11"	**"TR-4471: Best Practices with Veeam Backup and Replication"**	**"TR-4704: Implementazione di Veritas NetBackup con NetApp e-Series Storage"**
Descrive l'architettura di riferimento e le Best practice per l'utilizzo dello storage NetApp e-Series in un ambiente CommVault Data Platform V11.	Descrive l'architettura di riferimento e le Best practice per l'utilizzo dello storage NetApp e-Series in un ambiente Veeeam Backup & Replication 9.5.	Descrive l'implementazione di Veritas NetBackup su storage NetApp e-Series.

VSS

"TR-4825: Guida alle Best practice di NetApp e-Series per la videosorveglianza"	**"TR-4818: Virtualizzazione dei sistemi di gestione video con lo storage NetApp e-Series"**	**"TR-4848: Soluzione di registrazione video Bosch con array di storage su disco NetApp e-Series E2800"**
Descrive le Best practice per l'implementazione degli array e-Series negli ambienti di videosorveglianza.	Descrive come progettare e implementare sistemi di gestione video con lo storage NetApp e-Series.	Descrive l'architettura della soluzione di videosorveglianza e include dettagli sui componenti e sulle Best practice per lo storage.
"TR-4838: E2800 ed E5700 con Milestone XProtect VMS Certification Report"	**"TR-4771-DESIGN: Software di gestione video NetApp e-Series e Genetec"**	
Descrive i risultati dei test di certificazione eseguiti sugli array di storage ibridi NetApp E2800 e E5700.	Descrive i risultati della certificazione del software di gestione video (VMS) Genetec Security Center sugli array di storage ibridi NetApp E2800 e E5700.	

HPC

"TR-4884: Sistemi HPC entry-level con NetApp e-Series e IBM Spectrum Scale"	**"TR-4859: Implementazione di IBM Spectrum Scale con lo storage NetApp e-Series"**	**"TR-4856: Alta disponibilità di BeeGFS con e-Series con Red Hat Enterprise Linux Server"**
Descrive l'architettura di riferimento per i sistemi HPC entry-level basati sui sistemi storage NetApp e-Series e IBM Spectrum Scale.	Descrive il processo di implementazione di una soluzione di file system completamente parallela basata sullo stack software Spectrum Scale di IBM.	Descrive le configurazioni richieste per l'implementazione dell'alta disponibilità in un'architettura BeeGFS supportata dal sistema NetApp e-Series e utilizzando RedHat Enterprise Linux per i servizi di storage, metadati e gestione BeeGFS.
"TR-4862: Alta disponibilità di BeeGFS con e-Series con SUSE Linux Enterprise Server"		

Descrive le configurazioni richieste per l'implementazione dell'alta disponibilità in un'architettura BeeGFS supportata dal sistema NetApp e-Series e utilizzando SUSE Linux Enterprise Server per i servizi di storage, metadati e gestione BeeGFS.		

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"