Documentazione software SANtricity 11.9

SANtricity software

NetApp
March 18, 2026

This PDF was generated from https://docs.netapp.com/it-it/e-series-santricity-119/index.html on March 18, 2026. Always check docs.netapp.com for the latest.

Sommario

Documentazione software SANtricity 11.9 . . . 1
Note di rilascio . . . 2
Novità in SANtricity OS 11.90 . . . 2
Nuove funzionalità in Version 11.90R5 . . . 2
Nuove funzionalità in Version 11.90R4 . . . 2
Nuove funzionalità in Version 11.90R3 . . . 2
Nuove funzionalità in Version 11.90R2 . . . 2
Nuove funzionalità in Version 11.90R1 . . . 2
Nuove funzionalità in Version 11.90 . . . 2
Note di rilascio . . . 3
Inizia . . . 4
Scopri il software SANtricity . . . 4
SANtricity System Manager . . . 4
SANtricity Unified Manager . . . 5
Supporto per browser e sistemi operativi del software SANtricity . . . 7
Browser . . . 7
Sistemi operativi . . . 7
Configurazione di SANtricity System Manager . . . 8
Accedi a SANtricity System Manager . . . 8
Scopri la procedura guidata di configurazione di SANtricity System Manager . . . 9
Domande frequenti sulla configurazione del sistema storage per SANtricity System Manager . . . 10
Configurazione di SANtricity Unified Manager . . . 12
Installare SANtricity Unified Manager . . . 12
Accedi a SANtricity Unified Manager . . . 12
Gestione di un singolo array con SANtricity System Manager 11.9 . . . 14
Interfaccia principale . . . 14
Scopri l’interfaccia di SANtricity System Manager . . . 14
Visualizza i dati sulle prestazioni . . . 15
Visualizza la gerarchia dello storage in SANtricity System Manager . . . 24
Gestisci le impostazioni dell’interfaccia . . . 26
Gestisci notifiche . . . 29
Domande frequenti sull’interfaccia di gestione di SANtricity System Manager . . . 33
Pool e gruppi di volume . . . 37
Scopri pool e gruppi di volume in SANtricity System Manager . . . 37
Concetti . . . 38
Configura lo storage . . . 46
Gestisci storage . . . 58
Modifica le impostazioni del pool e del gruppo . . . 64
Gestisci Cache SSD . . . 73
Gestisci la capacità riservata . . . 80
Domande frequenti su pool e gruppi di volume per SANtricity System Manager . . . 89
Volumi e carichi di lavoro . . . 102
Scopri volumi e carichi di lavoro in SANtricity System Manager . . . 102

- Concetti 103
- Configura lo storage 121
- Gestisci i volumi 132
- Gestisci le impostazioni 137
- Utilizzare i servizi di copia 146
- Domande frequenti su volumi e carichi di lavoro per SANtricity System Manager 152

Host e cluster di host 157
- Scopri host e cluster di host nel software SANtricity 157
- Concetti 157
- Configura l'accesso host 161
- Gestisci host e cluster 166
- Gestisci le impostazioni 169
- Domande frequenti sui sistemi host e cluster host per SANtricity System Manager 172

Istantanee 175
- Scopri gli snapshot in SANtricity System Manager 175
- Concetti 176
- Crea Snapshot e oggetti Snapshot 187
- Gestisci le pianificazioni Snapshot 200
- Gestisci le immagini Snapshot 202
- Gestisci i gruppi di coerenza Snapshot 208
- Gestisci i volumi Snapshot 211
- Domande frequenti sulle Snapshot per SANtricity System Manager 216

Mirroring 219
- Panoramica 219
- Concetti asincroni 221
- Concetti di sincronizzazione 232
- Gestisci i gruppi di coerenza mirror asincroni 240
- Gestisci coppie mirrorate asincrone 246
- Gestisci le coppie mirrorate sincronizzate 250
- Disattiva mirroring 254
- Domande frequenti sul mirroring asincrono per SANtricity System Manager 255
- Domande frequenti sul mirroring sincrono per SANtricity System Manager 260

Archiviazione remota 264
- Scopri la funzionalità Remote Storage in SANtricity System Manager 264
- Concetti 265
- Gestire l'archiviazione remota 269
- Domande frequenti sullo storage remoto per SANtricity System Manager 273

Componenti hardware 275
- Visualizza e gestisci i componenti hardware in SANtricity System Manager 275
- Informazioni correlate 276
- Concetti 276
- Gestisci i componenti dello shelf 286
- Gestire i controller 291
- Gestisci le porte iSCSI 303
- Gestisci le porte NVMe 313

Gestisci le unità . . . 318
Gestire i ricambi a caldo . . . 330
Domande frequenti sullo shelf di storage per SANtricity System Manager . . . 334
Domande frequenti sullo storage controller per SANtricity System Manager . . . 336
Domande frequenti sul protocollo iSCSI per SANtricity System Manager . . . 339
Domande frequenti sul protocollo NVMe per SANtricity System Manager . . . 342
Domande frequenti sui dischi di storage per SANtricity System Manager . . . 344
Avvisi . . . 345
Scopri gli avvisi in SANtricity System Manager . . . 345
Concetti . . . 346
Gestisci gli avvisi email . . . 348
Gestisci gli avvisi SNMP . . . 351
Gestire gli avvisi syslog . . . 358
Domande frequenti sugli avvisi del sistema di storage per SANtricity System Manager . . . 360
Impostazioni array . . . 361
Scopri la panoramica delle impostazioni in SANtricity System Manager . . . 361
Concetti . . . 362
Configura le impostazioni dell'array . . . 365
Configura le funzionalità aggiuntive . . . 371
Scarica l'interfaccia a riga di comando (CLI) SANtricity . . . 374
Domande frequenti sulle impostazioni degli array di storage per SANtricity System Manager . . . 375
Sicurezza del disco . . . 377
Scopri la sicurezza delle unità disco in SANtricity System Manager . . . 377
Concetti . . . 378
Configura le chiavi di sicurezza . . . 382
Gestisci le chiavi di sicurezza . . . 387
Domande frequenti sulla sicurezza delle unità di archiviazione per SANtricity System Manager . . . 394
Gestione degli accessi . . . 397
Scopri la gestione degli accessi in SANtricity System Manager . . . 397
Concetti . . . 398
Utilizzare i ruoli utente locali . . . 405
Utilizzare i servizi di directory . . . 407
Usa SAML . . . 417
Usa i token di accesso . . . 424
Gestisci syslog . . . 426
Domande frequenti sulla gestione degli accessi utente per SANtricity System Manager . . . 432
Certificati . . . 436
Scopri i certificati in SANtricity System Manager . . . 436
Concetti . . . 436
Usa i certificati . . . 439
Domande frequenti sui certificati firmati da CA e autofirmati per SANtricity System Manager . . . 448
Supporto . . . 449
Ottieni supporto in SANtricity System Manager . . . 449
Visualizza informazioni e diagnostica . . . 449
Raccogli dati diagnostici . . . 454

Intraprendere azioni di recupero . . . 458
Gestisci AutoSupport . . . 460
Visualizza eventi . . . 466
Gestisci gli aggiornamenti . . . 470
AutoSupport FAQ per SANtricity System Manager . . . 482
Gestione di array multipli con SANtricity Unified Manager 7 . . . 489
Interfaccia principale . . . 489
Scopri SANtricity Unified Manager . . . 489
Browser supportati per SANtricity Unified Manager . . . 490
Scopri la protezione della password di amministratore in SANtricity Unified Manager . . . 490
Modifica la password di admin in SANtricity Unified Manager . . . 491
Gestire i timeout di sessione in SANtricity Unified Manager . . . 492
Array di archiviazione . . . 492
Scopri la scoperta in SANtricity Unified Manager . . . 492
Concetti . . . 493
Scopri gli array . . . 494
Gestisci array . . . 498
Importazione delle impostazioni . . . 499
Scopri come importare le impostazioni dell'array di storage in SANtricity Unified Manager . . . 499
Concetti . . . 500
Utilizzare le importazioni batch . . . 502
Domande frequenti sulle impostazioni di importazione per SANtricity Unified Manager . . . 507
Gruppi di array . . . 507
Scopri la panoramica dei gruppi in SANtricity Unified Manager . . . 507
Configurare un gruppo di array di storage in SANtricity Unified Manager . . . 508
Rimuovi gli array di storage da un gruppo in SANtricity Unified Manager . . . 509
Eliminare un gruppo di array di storage in SANtricity Unified Manager . . . 509
Rinominare un gruppo di array di storage in SANtricity Unified Manager . . . 509
Aggiornamenti . . . 510
Scopri il Centro aggiornamenti in SANtricity Unified Manager . . . 510
Aggiorna software e firmware . . . 512
Mirroring . . . 517
Scopri il mirroring in SANtricity Unified Manager . . . 517
Concetti . . . 517
Configura il mirroring . . . 523
Domande frequenti sul mirroring dello storage per SANtricity Unified Manager . . . 529
Certificati . . . 533
Panoramica dei certificati . . . 533
Concetti . . . 533
Utilizzare certificati firmati da CA per il sistema di gestione . . . 536
Reimposta i certificati di gestione . . . 538
Utilizzare certificati array . . . 539
Gestisci i certificati . . . 541
Gestione degli accessi . . . 542
Scopri la gestione degli accessi con SANtricity Unified Manager . . . 542

Concetti . . . 543
Utilizzare i ruoli utente locali . . . 548
Utilizzare i servizi di directory . . . 550
Usa SAML . . . 560
Domande frequenti sulla gestione degli accessi utente per SANtricity Unified Manager . . . 567
Versioni precedenti . . . 570
Documentazione hardware per le versioni precedenti . . . 570
Documentazione software per le versioni precedenti . . . 570
SANtricity Release 11.8 . . . 570
SANtricity Release 11.7 . . . 570
SANtricity Release 11.6 . . . 570
SANtricity Release 11.5 . . . 570
SANtricity Release 11.4 . . . 570
Note legali . . . 571
Copyright . . . 571
Marchi . . . 571
Brevetti . . . 571
Informativa sulla privacy . . . 571
Open source . . . 571

Documentazione software SANtricity 11.9

Note di rilascio

Novità in SANtricity OS 11.90

La tabella seguente descrive le nuove funzionalità in SANtricity System Manager 11.9.

Nuove funzionalità in Version 11.90R5

Questa versione contiene solo correzioni di errori e nessuna nuova funzionalità. Per ulteriori informazioni sulle modifiche in questa versione, consultare il README di E-Series SANtricity OS 11.90R5.

Nuove funzionalità in Version 11.90R4

Questa versione contiene solo piccole modifiche e nessuna nuova funzionalità. Per ulteriori informazioni sulle modifiche in questa versione, consultare il README di E-Series SANtricity OS 11.90R4.

Nuove funzionalità in Version 11.90R3

Nuova funzionalità	Descrizione
Supporto di SANtricity OS per IOM12C e DCM3	Il supporto per gli shelf IOM12C e DCM3 SAS-3 è ora disponibile per il firmware del controller 11.90R3 o superiore. Gli shelf IOM12C e DCM3 sono sostituti degli shelf IOM12B e DCM2.

Nuove funzionalità in Version 11.90R2

Questa versione contiene solo modifiche minori e nessuna nuova funzionalità. Per ulteriori informazioni sulle modifiche in questa versione, fare riferimento a "Note di rilascio E-Series 11.90".

Nuove funzionalità in Version 11.90R1

Nuova funzionalità	Descrizione
Nuovi modelli di sistema storage – EF300C e EF600C	Questa release introduce i sistemi storage all-flash NVMe EF300C e EF600C. EF300C e EF600C sono versioni flash a elevata capacità dei sistemi storage EF300 e EF600 già esistenti. Unità SSD NVMe a elevata capacità da 30TB o 60TB sono supportate con EF300C e EF600C. EF300C/EF600C sono compatibili solo per l'utilizzo in Dynamic Disk Pool senza supporto RAID legacy.
Supporto per interfacce SAS 12Gb su EF4000	Il controller E4000 ora supporta schede di interfaccia verso gli host SAS da 12 Gb.

Nuove funzionalità in Version 11.90

Nuova funzionalità	Descrizione
Nuovo modello di sistema storage – E4000	Questa versione introduce il sistema storage E4000 a basso costo. L'E4000 supporta 12 e 60 unità e una singola scheda di interfaccia verso gli host (HIC) per controller. Per la versione iniziale, le schede di interfaccia verso gli host supportate includono iSCSI e Fibre Channel. I sistemi storage E4000 e altri sistemi storage E-Series possono essere visualizzati e gestiti in Unified Manager.
Capacità aumentata per i Dynamic Disk Pools	La capacità dei Dynamic Disk Pools (DDP) è stata aumentata a 12 PB quando la capacità di ciascuna delle singole unità disco all'interno del pool è superiore a 23 TB. Se la capacità della singola unità disco è inferiore a 23 TB, la capacità dei DDP è di 6 PB.
Impostazioni predefinite della scansione dei supporti aumentate	La frequenza di scansione dei supporti predefinita è stata aumentata a 120 giorni.
La chiave privata è ora accettata per External Key Management	Il file di richiesta di firma del certificato (CSR) generato esternamente tramite coppie di chiavi private e pubbliche può ora essere importato tramite System Manager.
La funzione di blocco dell'accesso è ora disponibile per Web Services	Configurabile esclusivamente tramite REST API, è ora disponibile una nuova impostazione di blocco dell'accesso per i servizi Web incorporati e proxy.

Note di rilascio

Le note di rilascio sono disponibili al di fuori di questo sito. Ti verrà richiesto di accedere utilizzando le tue credenziali del sito di supporto NetApp.

- "Note di rilascio 11.90"
- "Note di rilascio 11.80"
- "Note di rilascio 11.70"
- "Note di rilascio 11.60"
- "Note di rilascio 11.50"

Inizia

Scopri il software SANtricity

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

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

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

Gli array di storage EF600/EF600C e EF300/EF300C non supportano il mirroring sincrono o i volumi thin.

SANtricity System Manager

System Manager è software di gestione basato su web, integrato in ciascun controller. Per accedere all'interfaccia utente, punta un browser all'indirizzo IP del controller. Un setup wizard ti aiuta a iniziare con la configurazione del sistema.

System Manager offre una varietà di funzionalità di gestione, tra cui:

Prestazioni
Visualizza fino a 30 giorni di dati sulle prestazioni, inclusi latenza I/O, IOPS, utilizzo della CPU e throughput.
Storage
Effettua il provisioning dello storage utilizzando pool o gruppi di volumi e crea workload applicativi.
Protezione dei dati
Eseguire backup e ripristino di emergenza utilizzando snapshot, volume copy e remote mirroring.

Hardware
Verifica lo stato dei componenti ed esegui alcune funzioni relative a tali componenti, come l'assegnazione di hot spare drive.
Avvisi
Notifica agli amministratori gli eventi importanti che si verificano sull'array di storage. Gli avvisi possono essere inviati tramite email, trap SNMP e syslog.
Gestione degli accessi
Configura l'autenticazione degli utenti che richiede agli utenti di accedere al sistema con credenziali assegnate.
Impostazioni di sistema
Configura altre funzionalità relative alle prestazioni del sistema, come SSD cache e il bilanciamento automatico del carico.
Supporto
Visualizza i dati diagnostici, gestisci gli aggiornamenti e configura AutoSupport, che monitora lo stato di salute di un array di storage e invia notifiche automatiche al supporto tecnico.

SANtricity Unified Manager

Unified Manager è un software basato su web utilizzato per gestire l'intero dominio. Da una vista centrale, puoi vedere lo stato di tutti i più recenti array E-Series ed EF-Series, come E4000, E2800, EF280, EF300, E5700, EF570, EF600, EF300C ed EF600C. Puoi anche eseguire operazioni batch sugli array di storage selezionati.

Unified Manager viene installato su un server di gestione insieme al Web Services Proxy. Per accedere a Unified Manager, apri un browser e inserisci l'URL che punta al server in cui è installato il Web Services Proxy.

Unified Manager offre una varietà di funzionalità di gestione, tra cui:

Scopri gli array di storage
Individua e aggiungi gli array di storage che desideri gestire nella rete della tua organizzazione. Puoi quindi visualizzare lo stato di tutti gli array di storage da un'unica pagina.
Lancio
Aprire un'istanza di System Manager per eseguire singole operazioni di gestione su uno specifico storage array.
Importa impostazioni
Eseguire un'importazione batch da un array di archiviazione a più array, incluse le impostazioni per gli avvisi, AutoSupport e i servizi di directory.
Specchiamento
Configura coppie di mirroring asincrono o sincrono tra due array di storage.
Gestisci gruppi
Organizza gli array di storage in gruppi per una gestione più semplice.
Centro di aggiornamento

Aggiorna il software SANtricity OS su più array di storage.
Certificati
Crea richieste di firma dei certificati (CSR), importa certificati e gestisci i certificati esistenti per più array di archiviazione.
Gestione degli accessi
Configura l'autenticazione degli utenti che richiede agli utenti di accedere a Unified Manager con le credenziali assegnate.

Supporto per browser e sistemi operativi del software SANtricity

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

Browser

Sono supportati i seguenti browser e versioni.

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

Per Unified Manager, il proxy dei servizi Web deve essere installato e disponibile per il browser. Per ulteriori informazioni, vedere "Panoramica del proxy di SANtricity Web Services"

Sistemi operativi

Sono supportati i seguenti sistemi operativi e versioni.

Sistema operativo	Versione/architettura minima
Red Hat Enterprise Linux (RHEL)	7.x, 8.x / 64-bit

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

Configurazione di SANtricity System Manager

Accedi a SANtricity System Manager

Per accedere all'interfaccia utente di SANtricity System Manager, è sufficiente puntare un browser all'indirizzo IP del controller. Un setup wizard ti aiuta a iniziare con la configurazione del sistema.

Prima di iniziare

- Installa e configura l'hardware, come descritto in una delle guide di configurazione rapida:
  - "Configurazione express di Linux"
  - "Configurazione express VMware"
  - "Configurazione express di Windows"
- Configurare una stazione di management che soddisfi i seguenti requisiti:
  - Connesso a una rete che è 1 Gbps o più veloce.
  - Collegato alla stessa sottorete delle porte di gestione del sistema storage.
  - Utilizzata come stazione separata, anziché come host (I/O collegati) per la gestione dei dati.
  - Configurazione per out-of-band management, in cui una stazione di gestione dello storage invia comandi al sistema storage tramite le connessioni Ethernet al controller.
  - Configura con un browser supportato. Vedi "Browser e sistemi operativi supportati".

Passaggi

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

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

   La prima volta che System Manager viene aperto su un array che non è stato configurato, viene visualizzato il prompt "Imposta password amministratore".

2. Inserisci la password di System Manager per il ruolo admin nei campi Imposta password amministratore e Conferma password, quindi fai clic su **Imposta password**.

   La setup wizard si avvia al primo accesso.

3. Utilizzare il setup wizard per eseguire le seguenti operazioni:

- **Verifica hardware (controller e unità)** — Verifica il numero di controller e unità nell'array di storage. Assegna un nome all'array.
- **Verifica host e sistemi operativi** — Verifica i tipi di host e di sistema operativo a cui lo storage array può accedere.
- **Accetta pool** — Accetta la configurazione del pool consigliata per il metodo di installazione rapida. Un pool è un gruppo logico di unità.
- **Configura gli avvisi** — Consenti a System Manager di ricevere notifiche automatiche quando si verifica un problema con l'array di storage.
- **Abilita AutoSupport** — Monitora automaticamente lo stato di salute del tuo array di storage e invia segnalazioni al supporto tecnico.

Per ulteriori informazioni sul setup wizard, vedere "Panoramica del setup wizard".

Scopri la procedura guidata di configurazione di SANtricity System Manager

Utilizza la procedura guidata di configurazione per configurare il tuo array di storage, inclusi hardware, host, applicazioni, carichi di lavoro, pool, avvisi e AutoSupport.

Configurazione iniziale

Quando si apre System Manager per la prima volta, viene avviata la procedura guidata di configurazione. La procedura guidata richiede di eseguire attività di configurazione di base, come assegnare un nome all'array di storage, configurare gli host, selezionare le applicazioni e creare pool di storage.

Prima di continuare con la configurazione iniziale, vai al Centro aggiornamenti (**Support › Upgrade Center**) e assicurati che il software SANtricity OS sia aggiornato. Se necessario, esegui l'aggiornamento alla versione più recente e aggiorna il browser per continuare la configurazione. Per ulteriori informazioni, vedi "Panoramica di Upgrade Center".

Se si annulla la procedura guidata, non è possibile riavviarla manualmente. La procedura guidata si riavvia automaticamente quando si apre System Manager o si aggiorna il browser e *almeno una* delle seguenti condizioni è soddisfatta:

- Non vengono rilevati pool e gruppi di volume.
- Non viene rilevato alcun workload.
- Nessuna notifica è configurata.

Terminologia

La procedura guidata di configurazione utilizza i seguenti termini.

Termine	Descrizione
Applicazione	Un'applicazione è un programma software, come Microsoft SQL Server o Microsoft Exchange.
Avviso	Gli avvisi notificano agli amministratori gli eventi importanti che si verificano sugli array di storage. Gli avvisi possono essere inviati tramite email, trap SNMP o syslog.

Termine	Descrizione
AutoSupport	La funzionalità AutoSupport monitora lo stato di salute di un array di storage e invia automaticamente segnalazioni al supporto tecnico.
Hardware	L'hardware del sistema storage include array di storage, controller e unità disco.
Host	Un host è un server che invia I/O a un volume su un array di storage.
Oggetto	Un oggetto è qualsiasi componente di storage logico o fisico. Gli oggetti logici includono gruppi di volumi, pool e volumi. Gli oggetti fisici includono l'array di storage, i controller dell'array, gli host e le unità.
Pool	Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage. Un volume viene creato a partire dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Sebbene un volume possa essere costituito da più unità, un volume appare come un singolo componente logico per l'host.
Gruppo di volumi	Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)
Carico di lavoro	Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.

Domande frequenti sulla configurazione del sistema storage per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa succede se non vedo tutti i miei componenti hardware?

Se nella finestra di dialogo Verifica hardware non vengono visualizzati tutti i componenti hardware, potrebbe significare che uno shelf di dischi non è collegato correttamente oppure che nello storage array è installato uno shelf incompatibile.

Verifica che tutti gli alloggiamenti per unità disco siano collegati correttamente. Se non sei sicuro di quali alloggiamenti per unità disco siano compatibili, contatta il supporto tecnico.

E se non visualizzo tutti i miei host?

Se non visualizzi gli host connessi, il rilevamento automatico non è riuscito, gli host non sono connessi correttamente o non è attualmente connesso alcun host.

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

- È possibile creare manualmente gli host e associare gli identificatori di porta host appropriati accedendo al **Storage › Hosts**. Gli host creati manualmente vengono visualizzati anche nella procedura guidata di **Initial Setup**.
- Il target e l'host devono essere configurati per il tipo di porta host (ad esempio, iSCSI o NVMe over RoCE) e una sessione con il sistema storage deve essere stabilita prima che il rilevamento automatico possa funzionare.

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

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

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

Che cos'è un workload?

Per alcune applicazioni nella tua rete, come Microsoft SQL Server o Microsoft Exchange, puoi definire un carico di lavoro che ottimizza lo storage per quell'applicazione.

Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.

Durante la creazione dei volumi, il sistema richiede di rispondere a domande sull'utilizzo di un carico di lavoro. Ad esempio, se si stanno creando volumi per Microsoft Exchange, viene chiesto di quante mailbox si ha bisogno, quali sono i requisiti medi di capacità delle mailbox e quante copie del database si desidera. Il sistema utilizza queste informazioni per creare una configurazione ottimale del volume, che può essere modificata secondo necessità.

Come configuro il metodo di consegna per AutoSupport?

Per accedere alle attività di configurazione per i metodi di consegna di AutoSupport, vai al **Supporto › Support Center**, quindi fai clic sulla scheda **AutoSupport**.

Sono supportati i seguenti protocolli: HTTPS e SMTP.

Come faccio a sapere se devo accettare la configurazione del pool consigliata?

Se si accetta la configurazione del pool consigliata dipende da alcuni fattori.

Determina il tipo di storage che è migliore per le tue esigenze rispondendo alle seguenti domande:

- Preferisci più pool di capacità ridotta, piuttosto che i pool più grandi possibili?
- Preferisci i gruppi di volumi RAID ai pool?
- Preferisci effettuare il provisioning manuale delle tue unità, invece di ricevere una configurazione consigliata?

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

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

Se non visualizzi gli host connessi, il rilevamento automatico non è riuscito, gli host non sono connessi correttamente o non è attualmente connesso alcun host.

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

- È possibile creare manualmente gli host e associare gli identificatori di porta host appropriati accedendo al **Storage › Hosts**. Gli host creati manualmente vengono visualizzati anche nella procedura guidata di **Initial Setup**.
- Il target e l'host devono essere configurati per il tipo di porta host (ad esempio, iSCSI o NVMe over RoCE) e una sessione con il sistema storage deve essere stabilita prima che il rilevamento automatico possa funzionare.

Configurazione di SANtricity Unified Manager

Installare SANtricity Unified Manager

SANtricity Unified Manager è incluso con il Web Services Proxy, che è un server API RESTful installato separatamente su un sistema host per gestire i sistemi storage NetApp E-Series.

Per installare Web Services Proxy e Unified Manager, consultare le seguenti istruzioni nel centro documentazione di E-Series e SANtricity:

1. "Esaminare i requisiti di installazione e aggiornamento"
2. "Scarica e installa il file Web Services Proxy"

Accedi a SANtricity Unified Manager

Dopo aver installato il Web Services Proxy, puoi accedere a SANtricity Unified Manager per gestire più sistemi storage tramite un'interfaccia basata su web.

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

Passaggi

1. Apri un browser e inserisci il seguente URL:

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

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

   Si apre la pagina di accesso di Unified Manager.

2. Al primo accesso, inserisci `admin` per il nome utente, quindi imposta e conferma una password per l'utente admin.

   La password può contenere fino a 30 caratteri.

Per ulteriori informazioni su utenti e password, vedere "Come funziona la gestione degli accessi".

Gestione di un singolo array con SANtricity System Manager 11.9

Interfaccia principale

Scopri l'interfaccia di SANtricity System Manager

SANtricity System Manager è un'interfaccia basata su web che consente di gestire un sistema storage in una singola vista.

Pagina iniziale

La pagina iniziale fornisce una vista dalla dashboard per la gestione quotidiana del tuo array di storage. Quando accedi a System Manager, la pagina iniziale è la prima schermata visualizzata.

La vista dalla dashboard comprende quattro aree di riepilogo che contengono informazioni chiave sullo stato e la salute del tuo array di storage. Puoi trovare ulteriori informazioni nell'area di riepilogo.

Area	Descrizione
Notifiche	L'area Notifiche visualizza le notifiche relative ai problemi che indicano lo stato dell'array di storage e dei suoi componenti. Inoltre, questo portlet visualizza avvisi automatici che possono aiutarti a risolvere i problemi prima che influiscano su altre aree del tuo ambiente di storage.
Prestazioni	L'area Prestazioni consente di confrontare l'utilizzo delle risorse nel tempo. È possibile visualizzare le metriche delle prestazioni di un array di storage per il tempo di risposta (IOPS), le velocità di trasferimento (MiB/s) e la quantità di capacità di elaborazione utilizzata (CPU).
Capacità	L'area Capacità visualizza un grafico della capacità allocata, della capacità storage libera e della capacità storage non assegnata nel tuo storage array.
Gerarchia di archiviazione	L'area Gerarchia di archiviazione fornisce una visualizzazione organizzata dei vari componenti hardware e oggetti di storage gestiti dal tuo array di storage. Fai clic sulla freccia a discesa per eseguire una determinata azione su quel componente hardware o oggetto di storage.

Impostazioni dell'interfaccia

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

Impostazione	Descrizione
Preferenze di visualizzazione	Modifica i valori di capacità e l'intervallo di tempo dal menu a discesa Preferenze nell'angolo in alto a destra dell'interfaccia.

Impostazione	Descrizione
Timeout di sessione	Configura i timeout in modo che le sessioni inattive degli utenti vengano disconnesse dopo un tempo specificato.
Aiuto	Accedi alla documentazione di Help e ad altre risorse dal menu a tendina nell'angolo in alto a destra dell'interfaccia.

Accessi utente e password

L'utente attualmente connesso al sistema viene visualizzato in alto a destra dell'interfaccia.

Per ulteriori informazioni su utenti e password, consultare:

- "Imposta la protezione con password di amministratore"
- "Modifica password"

Visualizza i dati sulle prestazioni

Scopri la panoramica delle prestazioni in SANtricity System Manager

La pagina Prestazioni offre semplici modi per monitorare le prestazioni del tuo storage array.

Cosa posso imparare dai dati sulle prestazioni?

I grafici e le tabelle delle prestazioni mostrano i dati sulle prestazioni quasi in real-time, il che ti aiuta a determinare se un array di storage sta riscontrando problemi. Puoi anche salvare i dati sulle prestazioni per costruire una vista storica di un array di storage e identificare quando è iniziato un problema o cosa lo ha causato.

Per saperne di più:

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

Come posso visualizzare i dati sulle prestazioni?

I dati sulle prestazioni sono disponibili nella Home page e nella Storage page.

Per saperne di più:

- "Visualizza i dati sulle prestazioni in formato grafico"
- "Visualizza e salva i dati tabellari sulle prestazioni"
- "Interpretare i dati sulle prestazioni"

Scopri i grafici delle prestazioni e le linee guida in SANtricity System Manager

La pagina Prestazioni fornisce grafici e tabelle di dati che consentono di valutare le prestazioni dello storage array in diverse aree chiave.

Le funzioni di performance consentono di svolgere questi compiti:

- Visualizza i dati sulle prestazioni in near real-time per aiutarti a determinare se un array di storage sta riscontrando problemi.
- Esporta i dati sulle prestazioni per costruire una vista storica di un array di storage e identificare quando è iniziato un problema o cosa ha causato un problema.
- Seleziona gli oggetti, le metriche sulle prestazioni e l'intervallo di tempo che desideri visualizzare.
- Confronta metriche.

È possibile visualizzare i dati sulle prestazioni in tre formati:

- **Rappresentazione grafica in real-time** — Visualizza i dati sulle prestazioni su un grafico in quasi real-time.
- **Tabellare quasi real-time** — Elenca i dati sulle prestazioni in una tabella in quasi real-time.
- **File CSV esportato** — Consente di salvare i dati sulle prestazioni in formato tabellare in un file di valori separati da virgole per ulteriori visualizzazioni e analisi.

Caratteristiche dei formati dei dati sulle prestazioni

Tipologia di monitoraggio delle prestazioni	Intervallo di campionamento	Durata visualizzata	Numero massimo di oggetti visualizzati	Possibilità di salvare i dati
Grafica in tempo reale, live Grafico in tempo reale, storico	10 sec (live) 5 min (storico) I punti dati visualizzati dipendono dall'intervallo di tempo selezionato	L'intervallo di tempo predefinito è 1 ora. Scelte: • 5 minuti • 1 ora • 8 ore • 1 giorno • 7 giorni • 30 giorni	5	No
Visualizzazione tabellare (vista tabella) quasi in real-time	10 sec -1 ora	Valore più recente	Illimitato	Sì
File di valori separati da virgole (CSV)	Dipende dall'intervallo di tempo selezionato	Dipende dall'intervallo di tempo selezionato	Illimitato	Sì

Linee guida per la visualizzazione dei dati sulle prestazioni

- La raccolta di dati sulle prestazioni è sempre attiva. Non è possibile disattivarla.
- Ogni volta che trascorre l'intervallo di campionamento, l'array di storage viene interrogato e i dati vengono

aggiornati.

- Per i dati grafici, l'intervallo di 5 minuti supporta aggiornamenti ogni 10 secondi, mediati su 5 minuti. Tutti gli altri intervalli di tempo vengono aggiornati ogni 5 minuti, mediati sull'intervallo di tempo selezionato.
- I dati sulle prestazioni nelle visualizzazioni grafiche vengono aggiornati in tempo reale. I dati sulle prestazioni nella visualizzazione tabellare vengono aggiornati quasi in tempo reale.
- Se un oggetto monitorato cambia durante il periodo di raccolta di dati, potrebbe non disporre di un set completo di punti dati relativi all'intervallo di tempo selezionato. Ad esempio, i set di volumi possono cambiare quando i volumi vengono creati, eliminati, assegnati o non assegnati; oppure le unità disco possono essere aggiunte, rimosse o guastarsi.

Scopri la terminologia relativa alle prestazioni nel software SANtricity

Scopri come i termini relativi alle prestazioni si applicano al tuo storage array.

Termine	Descrizione
Applicazione	Un'applicazione è un programma software, come SQL o Exchange.
CPU	CPU è l'acronimo di "unità centrale di elaborazione". CPU indica la percentuale di capacità di elaborazione dell'array di storage utilizzata.
Host	Un host è un server che invia I/O a un volume su un array di storage.
IOPS	IOPS è l'acronimo di operazioni di input/output al secondo.
Latenza	La latenza è l'intervallo di tempo tra una richiesta, come un comando di lettura o scrittura, e la risposta dell'host o dell'array di storage.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi che un host utilizza 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 indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi differenti.
MiB	MiB è l'abbreviazione di mebibyte (mega binary byte). Un MiB equivale a 220, ovvero 1.048.576 byte. Confronta con MB, che indica un valore in base 10. Un MB equivale a 1.024 byte.
Oggetto	Un oggetto è qualsiasi componente di storage logico o fisico. Gli oggetti logici includono gruppi di volumi, pool e volumi. Gli oggetti fisici includono lo storage array, i controller di array, gli host e le unità.
Pool	Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)

Termine	Descrizione
Leggi	Read è l'abbreviazione di "operazione di lettura", che si verifica quando l'host richiede dati dall'array di storage.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage. Un volume viene creato a partire dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Sebbene un volume possa essere costituito da più unità, un volume appare come un singolo componente logico per l'host.
Nome volume	Il nome di un volume è una stringa di caratteri assegnata al volume al momento della sua creazione. È possibile accettare il nome predefinito oppure specificare un nome più descrittivo che indichi il tipo di dati memorizzato nel volume.
Gruppo di volumi	Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)
Carico di lavoro	Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.
Scrivi	Write è l'abbreviazione di "write operation", quando i dati vengono inviati dall'host all'array per lo storage.

Visualizza i dati sulle prestazioni in formato grafico in SANtricity System Manager

È possibile visualizzare i dati sulle prestazioni in formato grafico per oggetti logici, oggetti fisici, applicazioni e carichi di lavoro.

Informazioni su questa attività

I grafici delle prestazioni mostrano dati storici così come dati in tempo reale attualmente in fase di acquisizione. Una linea verticale sul grafico, etichettata Live updating, distingue i dati storici dai dati in tempo reale.

Visualizzazione home page

La pagina iniziale contiene un grafico che mostra le prestazioni a livello di array di storage. È possibile selezionare solo alcune metriche da questa visualizzazione oppure fare clic su **Visualizza dettagli prestazioni** per selezionare tutte le metriche disponibili.

Vista dettagliata

I grafici disponibili nella visualizzazione dettagliata delle prestazioni sono organizzati sotto tre schede:

- **Vista logica** — Visualizza i dati sulle prestazioni degli oggetti logici raggruppati per gruppi di volumi e pool. Gli oggetti logici includono gruppi di volumi, pool e volumi.
- **Vista fisica** — Visualizza i dati sulle prestazioni del controller, dei canali host, dei canali drive e dei drive.
- **Vista Applications & Workloads** — Visualizza un elenco di oggetti logici (volumi) raggruppati in base ai tipi di applicazione e ai carichi di lavoro che hai definito.

Passaggi

1. Seleziona **Home**.
2. Per selezionare una visualizzazione a livello di array, fai clic sul pulsante IOPS, MiB/s o CPU.
3. Per visualizzare maggiori dettagli, fai clic su **View Performance Details**.
4. Seleziona la scheda **Logical View**, la scheda **Physical View** o la scheda **Applications & Workloads View**.

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

Visualizza schede	Dati sulle prestazioni visualizzati per ciascun tipo di oggetto
Vista logica	• **Array di archiviazione**: IOPS, MiB/s • **Pools**: Latenza, IOPS, MiB/s • **Gruppi di volumi**: Latenza, IOPS, MiB/s • **Volumi**: Latenza, IOPS, MiB/s
Vista fisica	• **Controller**: IOPS, MiB/s, CPU, Headroom • **Canali host**: Latenza, IOPS, MiB/s, Headroom • **Drive channels**: Latenza, IOPS, MiB/s • **Drives**: Latenza, IOPS, MiB/s
Vista Applicazioni & Workloads	• **Array di archiviazione**: IOPS, MiB/s • **Applicazioni**: Latenza, IOPS, MiB/s • **Carichi di lavoro**: Latenza, IOPS, MiB/s • **Volumi**: Latenza, IOPS, MiB/s

5. Utilizza le opzioni per visualizzare gli oggetti e le informazioni di cui hai bisogno.

Opzioni

Opzioni per la visualizzazione degli oggetti	Descrizione
Espandi un cassetto per visualizzare l'elenco degli oggetti.	I *navigation drawers* contengono oggetti di archiviazione, come pool, gruppi di volumi e unità. Fai clic sul cassetto per visualizzare l'elenco degli oggetti nel cassetto.
Seleziona oggetti da visualizzare.	Seleziona la check box a sinistra di ciascun oggetto per scegliere i dati sulle prestazioni che desideri visualizzare.
Utilizza Filter per trovare nomi di oggetti o parti di nomi.	Nella casella Filtro, inserire il nome o una parte del nome degli oggetti per elencare solo quegli oggetti nel drawer.
Fai clic su **Aggiorna grafici** dopo aver selezionato gli oggetti.	Dopo aver selezionato gli oggetti dai cassetti, seleziona **Aggiorna grafici** per visualizzare i dati grafici per gli elementi che hai selezionato.
Nascondi o mostra grafico	Seleziona il titolo del grafico per nascondere o mostrare il grafico.

6. Se necessario, utilizzare le opzioni aggiuntive per visualizzare i dati sulle prestazioni.

Opzioni aggiuntive

Opzione	Descrizione
Intervallo di tempo	Seleziona la durata di visualizzazione desiderata (5 minuti, 1 ora, 8 ore, 1 giorno, 7 giorni o 30 giorni). L'impostazione predefinita è 1 ora. Il caricamento dei dati sulle prestazioni relativi a un periodo di 30 giorni può richiedere diversi minuti. Non abbandonare la pagina web, non aggiornarla e non chiudere il browser mentre i dati vengono caricati.
Dettagli del punto dati	Passa il cursore sul grafico per visualizzare le metriche di un determinato punto dati.
barra di scorrimento	Utilizza la barra di scorrimento sotto il grafico per visualizzare un intervallo di tempo precedente o successivo.
Barra zoom	Sotto il grafico, trascina le maniglie della barra di zoom per ridurre lo zoom su un intervallo di tempo. Più ampia è la barra di zoom, meno granulari saranno i dettagli del grafico. Per reimpostare il grafico, selezionare una delle opzioni dell'intervallo di tempo.
Trascina e rilascia	Sul grafico, trascina il cursore da un punto nel tempo a un altro per ingrandire un intervallo di tempo. Per reimpostare il grafico, selezionare una delle opzioni dell'intervallo di tempo.

Visualizza e salva i dati tabellari sulle prestazioni in SANtricity System Manager

È possibile visualizzare e salvare i dati dei grafici delle prestazioni in formato tabellare. Questo consente di filtrare i dati che si desidera visualizzare.

Passaggi

1. Da qualsiasi grafico dei dati sulle prestazioni, fai clic su **Launch table view**.

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

2. Utilizza il menu a tendina per la selezione degli oggetti e il filtro secondo necessità.
3. Fai clic sul pulsante **Mostra/Nascondi colonne** per selezionare le colonne che vuoi includere nella tabella.

   Puoi fare clic su ciascuna check box per selezionare o deselezionare un elemento.

4. Seleziona **Export** in fondo alla schermata per salvare la visualizzazione tabellare in un file di valori separati da virgole (CSV).

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

5. Fai clic su **Esporta** per procedere con il download o fai clic su **Annulla**.

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

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

Interpretare i dati sulle prestazioni in SANtricity System Manager

I dati sulle prestazioni possono guidarti nell'ottimizzazione delle prestazioni del tuo storage array.

Quando si interpretano i dati sulle prestazioni, tenere presente che diversi fattori influenzano le prestazioni dell'array di storage. La tabella seguente descrive le principali aree da considerare.

Dati sulle prestazioni	Implicazioni per la messa a punto delle prestazioni
Latenza (millisecondi, o ms)	Monitora l'attività di I/O di un oggetto specifico. Identificare potenzialmente gli oggetti che costituiscono colli di bottiglia: • Se un gruppo di volumi è condiviso tra più volumi, i singoli volumi potrebbero necessitare dei propri gruppi di volumi per migliorare le prestazioni sequenziali delle unità e diminuire la latenza. • Con i pool, si introducono latenze maggiori e potrebbero verificarsi carichi di lavoro non uniformi tra le unità, rendendo i valori di latenza meno significativi e, in generale, più elevati. • Il tipo e la velocità dell'unità influenzano la latenza. Con I/O casuale, le unità con velocità di rotazione più elevata impiegano meno tempo a spostarsi da e verso diverse posizioni sul disco. • Un numero insufficiente di unità comporta un maggior numero di comandi in coda e un periodo di tempo maggiore per l'elaborazione del comando da parte dell'unità, aumentando la latenza generale del sistema. • Le operazioni di I/O di maggiori dimensioni presentano una latenza maggiore a causa del tempo aggiuntivo necessario per il trasferimento dei dati. • Una latenza più elevata potrebbe indicare che il modello di I/O è di natura casuale. Le unità con I/O casuale avranno una latenza maggiore rispetto a quelle con flussi sequenziali. • Una disparità di latenza tra le unità o i volumi di uno stesso gruppo di volumi potrebbe indicare un'unità lenta.

Dati sulle prestazioni	Implicazioni per la messa a punto delle prestazioni
IOPS	I fattori che influenzano le operazioni di input/output al secondo (IOPS o IOs/sec) includono questi elementi: • Modalità di accesso (casuale o sequenziale) • Dimensione I/O • livello RAID • Dimensione del blocco cache • Se la cache di lettura è abilitata • Se la cache di scrittura è abilitata • Precaricamento dinamico della cache di lettura • Dimensione del segmento • Il numero di unità nei gruppi di volumi o nell'array di storage Maggiore è il cache hit rate, maggiori saranno i tassi di I/O. Si riscontrano tassi di I/O in scrittura più elevati con la cache di scrittura abilitata rispetto a quando è disabilitata. Nel decidere se abilitare la cache di scrittura per un singolo volume, osserva le IOPS attuali e le IOPS massime. Dovresti vedere tassi più elevati per i pattern di I/O sequenziali rispetto ai pattern di I/O casuali. Indipendentemente dal tuo pattern di I/O, abilita la cache di scrittura per massimizzare il tasso di I/O e ridurre il tempo di risposta dell'applicazione. È possibile visualizzare i miglioramenti delle prestazioni derivanti dalla modifica della dimensione del segmento nelle statistiche IOPS di un volume. Esegui delle prove per determinare la dimensione ottimale del segmento oppure utilizza la dimensione del file system o la dimensione del blocco del database.
MiB/s	Le velocità di trasferimento o di throughput sono determinate dalle dimensioni dell'I/O dell'applicazione e dalla frequenza di I/O. In genere, le richieste di I/O di piccole dimensioni comportano una velocità di trasferimento inferiore ma offrono una frequenza di I/O più elevata e tempi di risposta più brevi. Con richieste di I/O di dimensioni maggiori, sono possibili velocità di throughput più elevate. Comprendere i tipici modelli di I/O della tua applicazione può aiutarti a determinare le velocità massime di trasferimento I/O per uno specifico storage array.

Dati sulle prestazioni	Implicazioni per la messa a punto delle prestazioni
CPU	Questo valore è una percentuale della capacità di elaborazione che viene utilizzata. Potreste notare una discrepanza nell'utilizzo della CPU da parte di oggetti dello stesso tipo. Ad esempio, l'utilizzo della CPU di un controller è elevato o aumenta nel tempo, mentre quello dell'altro controller è inferiore o più stabile. In questo caso, potreste voler trasferire la proprietà di uno o più volumi al controller con la percentuale di CPU inferiore. Potrebbe essere opportuno monitorare la CPU sull'array di storage. Se la CPU continua ad aumentare nel tempo mentre le prestazioni delle applicazioni diminuiscono, potrebbe essere necessario aggiungere array di storage. Aggiungendo array di storage all'azienda, è possibile continuare a soddisfare le esigenze delle applicazioni con un livello di prestazioni accettabile.
Headroom	Il margine di sicurezza (headroom) si riferisce alla capacità prestazionale residua dei controller, dei canali host dei controller e dei canali drive dei controller. Questo valore è espresso come percentuale e rappresenta il divario tra le massime prestazioni possibili che questi oggetti sono in grado di fornire e i livelli di prestazioni attuali. • Per i controller, il margine di sicurezza è una percentuale del massimo numero di IOPS possibili. • Per i canali, il margine di sicurezza (headroom) è una percentuale del throughput massimo, o MiB/s. Il throughput in lettura, il throughput in scrittura e il throughput bidirezionale sono inclusi nel calcolo.

Visualizza la gerarchia dello storage in SANtricity System Manager

La Storage Hierarchy nell'interfaccia principale fornisce una visualizzazione organizzata dei vari componenti hardware e degli oggetti di storage gestiti dal tuo storage array.

Per visualizzare la gerarchia di archiviazione, vai alla pagina iniziale e fai clic sulla freccia a discesa su un componente array di storage o su un oggetto di storage. Un array di storage è costituito da una raccolta di componenti sia fisici che logici.

Componenti fisici

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

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

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

Componenti logici

Le unità disco nell'array di storage forniscono la capacità di storage fisico per i dati. Utilizzare System Manager per configurare la capacità fisica in componenti logici, come pool, gruppi di volumi e volumi. Questi componenti sono gli strumenti che si utilizzano per configurare, archiviare, gestire e preservare i dati sull'array di storage. I componenti logici di un array di storage sono descritti in questa tabella.

Componente	Descrizione
Pool	Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)
Gruppo di volumi	Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage.

Componente	Descrizione
Numero di unità logica (LUN)	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi che un host utilizza 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 indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi differenti.

Gestisci le impostazioni dell'interfaccia

Gestisci la protezione tramite password in SANtricity System Manager

È necessario configurare l'array di archiviazione con password per proteggerlo da accessi non autorizzati.

Imposta e modifica le password

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

Per motivi di sicurezza, puoi tentare di inserire una password solo cinque volte prima che l'array di storage entri in uno stato di "blocco". In questo stato, l'array di storage rifiuterà i successivi tentativi di inserimento della password. Devi attendere 10 minuti affinché l'array di storage si reimposti in uno stato "normale" prima di provare nuovamente a inserire una password.

Oltre alla password di amministratore, l'array di storage include profili utente predefiniti con uno o più ruoli associati. Per ulteriori informazioni, vedere "Autorizzazioni per i ruoli mappati". I profili utente e le mappature non possono essere modificati. Solo le password possono essere modificate. Se si desidera modificare la password di amministratore o le password di altri utenti, vedere "Modifica password".

Reinserisci le password dopo il timeout della sessione

Il sistema richiede la password una sola volta durante una singola sessione di gestione. Tuttavia, una sessione scade dopo 30 minuti di inattività, momento in cui è necessario inserire nuovamente la password. Se un altro utente che gestisce lo stesso storage array da un altro client di gestione modifica la password mentre la tua sessione è in corso, ti verrà richiesta la password la prossima volta che tenterai un'operazione di configurazione o di visualizzazione.

È possibile regolare il timeout della sessione oppure disabilitare completamente i timeout della sessione. Vedi "Gestisci i timeout di sessione".

Rimuovere le unità o la protezione tramite password

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

- **Se si rimuovono unità protette da password** — La password è memorizzata in un'area riservata di ciascuna unità nell'array di storage. Se si rimuovono tutte le unità da un array di storage, la password non funzionerà più. Per correggere questa condizione, reinstallare una delle unità originali nell'array di storage.
- **Se si desidera rimuovere la protezione tramite password** — Se non si desidera più che i comandi siano

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

> L'esecuzione di comandi di configurazione su un array di storage può causare gravi danni, inclusa la perdita di dati. Per questo motivo, dovresti sempre impostare una password di amministratore per il tuo array di storage. Usa una password di amministratore lunga, con almeno 15 caratteri alfanumerici, per aumentare la sicurezza.

Imposta le unità predefinite per i valori di capacità in SANtricity System Manager

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

Le preferenze vengono memorizzate nella memoria locale del browser, così tutti gli utenti possono avere le proprie impostazioni.

Passaggi

1. Seleziona **Preferenze › Imposta preferenze**.
2. Fai clic sul pulsante di opzione per **Gibibytes** o **Tebibytes** e conferma di voler eseguire l'operazione.

   Consultare la tabella seguente per abbreviazioni e valori.

Abbreviazione	Valore
GiB	1.024^3 byte
TiB	$1,024^4$ byte

Imposta l'intervallo di tempo predefinito per i grafici delle prestazioni in SANtricity System Manager

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

Informazioni su questa attività

I grafici delle prestazioni visualizzati nella pagina Home e nella pagina Prestazioni mostrano inizialmente un intervallo di tempo di 1 ora. Le preferenze vengono memorizzate nella memoria locale del browser, così tutti gli utenti possono avere le proprie impostazioni.

Passaggi

1. Seleziona **Preferenze › Imposta preferenze**.
2. Nell'elenco a discesa, seleziona **5 minuti**, **1 ora**, **8 ore**, **1 giorno** o **7 giorni** e conferma che vuoi eseguire l'operazione.

Configura il banner di accesso in SANtricity System Manager

È possibile creare un banner di accesso che viene mostrato agli utenti prima che stabiliscano una sessione in SANtricity System Manager. Il banner può includere un avviso e un messaggio di consenso.

Informazioni su questa attività

Quando crei un banner, appare prima della schermata di accesso in una finestra di dialogo.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Nella sezione Generale, seleziona **Configure Login Banner**.

   Si apre la finestra di dialogo Configure Login Banner.

3. Inserisci il testo che desideri venga visualizzato nel banner di login.

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

4. Fare clic su **Save**.

Risultati

La prossima volta che gli utenti accederanno a System Manager, il testo si aprirà in una finestra di dialogo. Gli utenti devono fare clic su **OK** per continuare alla schermata di accesso.

Gestisci i timeout di sessione in SANtricity System Manager

È possibile configurare i timeout in SANtricity System Manager, in modo che le sessioni inattive degli utenti vengano disconnesse dopo un periodo di tempo specificato.

Informazioni su questa attività

Per impostazione predefinita, il timeout della sessione per System Manager è di 30 minuti. Puoi regolare tale tempo oppure puoi disabilitare completamente i timeout di sessione.

Se la gestione degli accessi è configurata utilizzando le funzionalità Security Assertion Markup Language (SAML) integrate nell'array, potrebbe verificarsi un timeout di sessione quando la sessione SSO dell'utente raggiunge il limite massimo. Ciò potrebbe accadere prima del timeout di sessione di System Manager.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Nella sezione Generale, seleziona **Abilita/Disabilita timeout sessione**.

   Si apre la finestra di dialogo Enable/Disable Session Timeout.

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

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

   Per disabilitare i timeout di sessione, deselezionare la casella di controllo **Imposta la durata di tempo…**.

4. Fare clic su **Save**.

Gestisci notifiche

Scopri le notifiche relative ai problemi di SANtricity System Manager

SANtricity System Manager utilizza icone e diversi altri metodi per notificare che esistono problemi con l'array di storage.

Icone

System Manager utilizza queste icone per indicare lo stato dell'array di storage e dei suoi componenti.

Icona	Descrizione
	Ottimale
	Non ottimale o non riuscito
	Necessita di attenzione o correzione
	Attenzione

System Manager visualizza queste icone in varie posizioni.

- Nell'area Notifiche della Home page vengono visualizzati l'icona di errore e un messaggio.
- L'icona della pagina iniziale nell'area di navigazione visualizza l'icona di errore.
- Nella pagina Componenti, la grafica relativa a unità e controller visualizza l'icona di errore.

Avvisi e LED

Inoltre, System Manager ti notifica i problemi anche in altri modi.

- System Manager invia notifiche SNMP o messaggi di errore email.
- I LED Service Action Required sull'hardware si accendono.

Quando ricevi una notifica di un problema, utilizza il Recovery Guru per aiutarti a risolvere il problema. Se necessario, utilizza la documentazione hardware insieme ai passaggi di ripristino per sostituire i componenti guasti.

Visualizza e intervieni sulle operazioni in corso in SANtricity System Manager

Per visualizzare e intervenire sulle operazioni di lunga durata, utilizzare la pagina Operations in Progress.

Informazioni su questa attività

Per ogni operazione elencata nella pagina Operazioni in corso, vengono visualizzate la percentuale di completamento e il tempo stimato rimanente per completare l'operazione. In alcuni casi, puoi interrompere un'operazione o assegnarle una priorità maggiore o minore. Puoi anche rimuovere un'operazione Volume Copy completata dall'elenco.

Passaggi

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

   Viene visualizzata la pagina Operazioni in corso.

2. Se lo si desidera, utilizzare i collegamenti nella colonna Azioni per interrompere un'operazione o modificarne la priorità.

   Leggere tutti i testi di avviso forniti nelle finestre di dialogo, in particolare quando si interrompe un'operazione.

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

3. Una volta completata un'operazione di copia del volume, puoi selezionare **Clear** per rimuoverla dall'elenco.

   Nella parte superiore della Home page, vengono visualizzati un messaggio informativo e un'icona a forma di chiave inglese gialla quando un'operazione è completata. Questo messaggio include un collegamento che consente di cancellare l'operazione dalla pagina Operations in Progress.

Le operazioni visualizzate nella pagina Operazioni in corso includono le seguenti:

Operazione	Possibile stato dell'operazione	Azioni che puoi intraprendere
Copia del volume	Completato	Chiaro
Copia del volume	In corso	• Modifica priorità • Arresta
Copia del volume	In attesa	Chiaro
Copia del volume	Fallito	• Chiaro • Ricopia
Copia del volume	Arrestato	• Chiaro • Ricopia
Creazione volume (solo volumi thick pool superiori a 64TiB)	In corso	*none*
Eliminazione del volume (solo volumi thick pool di dimensioni superiori a 64TiB)	In corso	*none*
Sincronizzazione iniziale del gruppo di mirror asincroni	In corso	Sospendi
Sincronizzazione iniziale del gruppo di mirror asincroni	Sospeso	Riprendi

Operazione	Possibile stato dell'operazione	Azioni che puoi intraprendere
Specchiamento sincrono	In corso	Sospendi
Specchiamento sincrono	Sospeso	Riprendi
Ripristino dell'immagine Snapshot	In corso	Annulla
Ripristino dell'immagine Snapshot	In attesa	Annulla
Ripristino dell'immagine Snapshot	In pausa	• Annulla • Riprendi
Evacuazione del disco	In corso	Annulla (dipende dal tipo di evacuazione dell'unità)
Aggiungi capacità al pool o al gruppo di volumi	In corso	*none*
Modificare un livello RAID per un volume	In corso	*none*
Ridurre la capacità di un pool	In corso	*none*
Reclamazione dei volumi thin	In corso	*none*
Verifica il tempo rimanente su un'operazione in formato di disponibilità istantanea (IAF) per i volumi del pool	In corso	*none*
Verificare la ridondanza dei dati di un gruppo di volumi	In corso	*none*
Deframmenta un gruppo di volumi	In corso	*none*
Inizializza un volume	In corso	*none*
Aumenta la capacità per un volume	In corso	*none*
Modificare la dimensione del segmento per un volume	In corso	*none*
Copia dell'unità	In corso	*none*
Ricostruzione dei dati	In corso	*none*

Operazione	Possibile stato dell'operazione	Azioni che puoi intraprendere
Copyback	In corso	*none*
Cancellazione drive	In corso	*none*
Importazione da storage remoto	In corso	• Modifica priorità • Arresta
Importazione da storage remoto	Arrestato	• Riprendi • Disconnetti
Importazione da storage remoto	Fallito	• Riprendi • Disconnetti
Importazione da storage remoto	Completato	Disconnetti

Recupera dai problemi utilizzando il SANtricity System Manager Recovery Guru

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

Passaggi

1. Seleziona **Home**.
2. Fai clic sul collegamento etichettato **Ripristina da *n* problemi** al centro in alto della finestra.

   Viene visualizzata la finestra di dialogo Recovery Guru.

3. Seleziona il primo problema visualizzato nell'elenco riepilogativo, quindi segui le istruzioni della procedura di ripristino per correggere il problema. Se necessario, utilizza le istruzioni di sostituzione per sostituire i componenti guasti. Ripeti questo passaggio per ogni problema elencato.

   All'interno di un array di storage possono presentarsi diversi problemi correlati. In questo caso, l'ordine in cui vengono risolti i problemi può influire sul risultato. Selezionare e correggere i problemi nell'ordine in cui sono elencati nella lista di riepilogo.

   I guasti multipli relativi a un contenitore di alimentazione vengono raggruppati e elencati come un unico problema nell'elenco riepilogativo. I guasti multipli relativi a un contenitore di ventola vengono anch'essi elencati come un unico problema.

4. Per verificare che la procedura di ripristino sia andata a buon fine, fai clic su **Recheck**.

   Se hai selezionato un problema per un gruppo di mirroring asincrono o per un membro di un gruppo di mirroring asincrono, fai prima clic su **Clear** per eliminare l'errore dal controller, quindi fai clic su **Recheck** per rimuovere l'evento da Recovery Guru.

   Se tutti i problemi sono stati risolti, l'icona dell'array di storage passa infine da Needs Attention a Optimal. Per alcuni problemi, viene visualizzata un'icona Fixing mentre è in corso un'operazione, come la ricostruzione.

5. **Facoltativo:** Per salvare le informazioni di Recovery Guru in un file, fai clic sull'icona **Save**.

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

6. Per stampare le informazioni di Recovery Guru, fai clic sull'icona **Print**.

Domande frequenti sull'interfaccia di gestione di SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Quali sono i browser supportati?

SANtricity System Manager supporta queste versioni del browser.

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

Quali sono le scorciatoie da tastiera?

È possibile navigare in SANtricity System Manager utilizzando solo la tastiera.

Navigazione generale

Azione	Scorciatoia da tastiera
Passa all'elemento successivo.	Scheda
Passa all'elemento precedente.	Maiusc + Tab
Seleziona un elemento.	Inserisci
Elenco a discesa—Passa all'elemento successivo o precedente.	freccia in basso o freccia in alto
Casella di controllo—Seleziona un elemento.	Barra spaziatrice
Pulsanti radio: consente di passare da un elemento all'altro.	freccia in basso o freccia in alto
Testo espandibile: espandi o comprimi l'elemento.	Inserisci

Navigazione tabella

Azione	Scorciatoia da tastiera
Seleziona una riga.	Premi Tab per selezionare una riga, quindi premi Invio
Scorri verso l'alto o verso il basso.	Freccia giù/freccia su o Pagina giù/Pagina su
Modifica l'ordinamento di una colonna.	Premi Tab per selezionare un'intestazione di colonna, quindi premi Invio

Navigazione nel calendario

Azione	Scorciatoia da tastiera
Passa al mese precedente.	Pagina su
Passa al mese successivo.	Pagina giù
Passa all'anno precedente.	Ctrl + Pagina Su
Passa all'anno successivo.	Ctrl + Pagina giù
Apri il selettore della data se chiuso.	Ctrl + Home
Passa al mese corrente.	Ctrl / Cmd + Home
Passa al giorno precedente.	Control / Command + Sinistra
Passa al giorno successivo.	Control / Command + Destra
Passa alla settimana precedente.	Control / Command + Su
Passa alla settimana successiva.	Controllo / Comando + Giù
Seleziona la data focalizzata.	Inserisci
Chiudi il selettore della data e cancella la data.	Control / Command + Fine
Chiudi il selettore di date senza selezione.	Escape

In che modo le statistiche delle prestazioni dei singoli volumi si rapportano al totale?

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

La capacità riservata viene utilizzata internamente dal sistema storage per supportare volumi thin, snapshot e

mirroring asincrono e non è visibile agli host I/O. Di conseguenza, le statistiche del pool, del controller e dell'array di storage potrebbero non corrispondere alla somma dei volumi visibili.

Tuttavia, per le statistiche di applicazione e carico di lavoro, vengono aggregati solo i volumi visibili.

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

Quando viene visualizzato uno zero per un punto dati nei grafici e nelle tabelle, significa che non vi è alcuna attività di I/O per l'oggetto in quel momento. Questa situazione può verificarsi perché l'host non sta avviando I/O su quell'oggetto, oppure potrebbe trattarsi di un problema dell'oggetto stesso.

I dati storici relativi all'oggetto sono ancora disponibili per la visualizzazione. I grafici e la tabella mostreranno dati diversi da zero non appena inizierà l'attività di I/O per l'oggetto.

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

Tipo di oggetto a livello di array	Motivo per cui i dati vengono visualizzati come zero
Volume	• Il volume non aveva un host assegnato.
Gruppo di volumi	• Il gruppo di volumi è in fase di importazione. • Il gruppo di volumi non contiene un volume assegnato a un host, ***e*** il gruppo di volumi non contiene alcuna capacità riservata.
Unità	• L'unità è guasta. • L'unità è stata rimossa. • L'unità si trova in uno stato sconosciuto.
Controller	• Il controller è offline. • Il controller è guasto. • Il controller è stato rimosso. • Il controller è in uno stato sconosciuto.
matrice di archiviazione	• L'array di storage non contiene volumi.

Cosa mostra il grafico della latenza?

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

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

- Tempo di lettura.
- Tempo di scrittura.

- Dimensione media I/O.

Cosa mostra il grafico IOPS?

Il grafico IOPS visualizza statistiche relative alle operazioni di input/output al secondo. Nella pagina Home, questo grafico visualizza statistiche per lo storage array. Nelle schede Logical View, Physical View e Applications & Workloads View del riquadro Performance, questo grafico visualizza statistiche per lo storage array, i volumi, i gruppi di volumi, i pool, le applicazioni e i carichi di lavoro.

IOPS è l'abbreviazione di *operazioni di input/output (I/O) al secondo*. Passa il cursore su un punto del grafico per visualizzare i seguenti valori per quel punto nel tempo:

- Numero di operazioni di lettura.
- Numero di operazioni di scrittura.
- Totale delle operazioni di lettura e scrittura combinate.

Cosa mostra il grafico MiB/s?

Il grafico MiB/s visualizza le statistiche sulla velocità di trasferimento in mebibyte al secondo. Nella pagina Home, questo grafico visualizza le statistiche per il sistema storage. Nelle schede Vista logica, Vista fisica e Vista Applicazioni & Carichi di lavoro del riquadro Prestazioni, questo grafico visualizza le statistiche per il sistema storage, i volumi, i gruppi di volumi, i pool, le applicazioni e i carichi di lavoro.

MiB/s è l'abbreviazione di , ovvero 1.048.576 byte al secondo. Passa il cursore su un punto del grafico per visualizzare i seguenti valori relativi a quel preciso istante:

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

Cosa mostra il grafico della CPU?

Il grafico della CPU visualizza le statistiche sulla capacità di elaborazione per ciascun controller (controller A e controller B). CPU è l'abbreviazione di *central processing unit*. Nella pagina Home, questo grafico visualizza le statistiche per l'array di storage. Nella scheda Vista fisica del riquadro Prestazioni, questo grafico visualizza le statistiche per l'array di storage e le unità.

Il grafico della CPU mostra la percentuale di capacità di elaborazione della CPU utilizzata rispetto alle operazioni sull'array. Anche in assenza di I/O esterni, la percentuale di utilizzo della CPU può essere diversa da zero perché il sistema operativo per lo storage potrebbe eseguire operazioni in background e attività di monitoraggio. Passando il cursore su un punto del grafico, è possibile visualizzare la percentuale di capacità di elaborazione utilizzata in quel momento.

Cosa mostra il grafico Headroom?

Il grafico Headroom si riferisce alla capacità prestazionale residua dei controller dell'array di storage. Questo grafico è visibile nella pagina Home e nella scheda Physical View del riquadro Performance.

Il grafico Headroom mostra la capacità prestazionale residua degli oggetti fisici nel sistema storage. Passa il cursore su un punto del grafico per visualizzare le percentuali di capacità IOPS e MiB/s rimanenti per il controller A e per il controller B.

Dove posso trovare ulteriori informazioni sulle preferenze di visualizzazione?

Per trovare informazioni sulle opzioni di visualizzazione disponibili:

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

Pool e gruppi di volume

Scopri pool e gruppi di volume in SANtricity System Manager

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

Che cosa sono i pool e i gruppi di volume?

Un pool è un insieme di unità raggruppate logicamente. Un volume group è un container per volumi con caratteristiche condivise. È possibile utilizzare un pool o un volume group per creare volumi accessibili a un host.

Per saperne di più:

- "Come funzionano i pool e i gruppi di volume"
- "Terminologia della capacità"
- "Decidere se utilizzare un pool o un gruppo di volume"

Come si creano i pool?

È possibile consentire a System Manager di creare automaticamente i pool quando rileva capacità non assegnata in un array di storage. In alternativa, quando la creazione automatica non può determinare la configurazione migliore, è possibile creare i pool manualmente dal **Storage › Pools & Volume Groups**.

Per saperne di più:

- "Creazione automatica o manuale del pool"
- "Crea pool automaticamente"
- "Crea pool manualmente"
- "Aggiungi capacità a un pool o a un volume group"

Come si creano i gruppi di volumi?

È possibile creare gruppi di volumi dal **Storage › Pools & Volume Groups**.

Per saperne di più:

- "Crea un gruppo di volumi"
- "Aggiungi capacità a un pool o a un volume group"

Informazioni correlate

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

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

Concetti

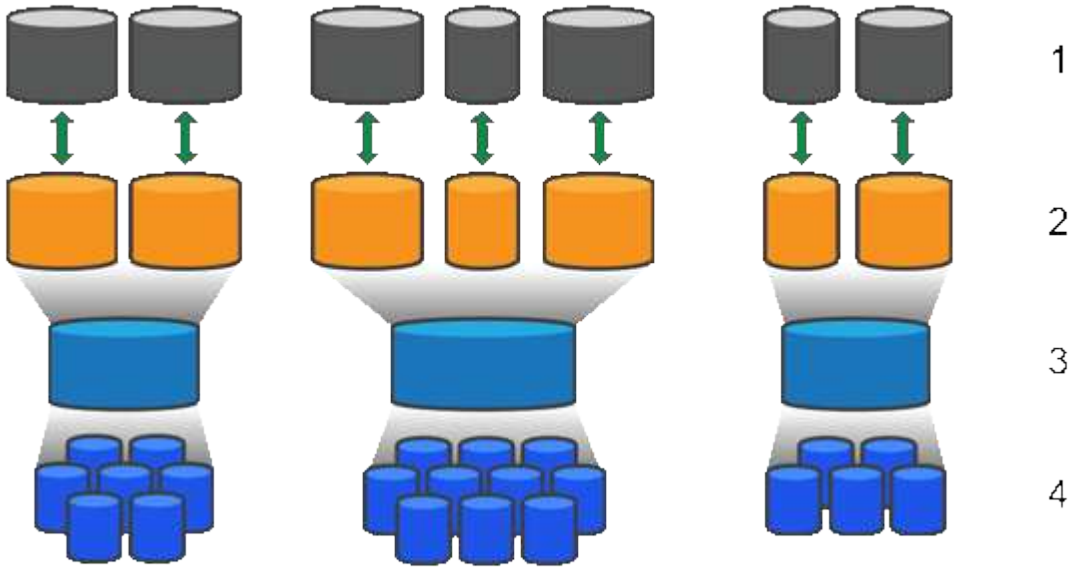
Come funzionano pool e gruppi di volume nel software SANtricity

Per predisporre lo storage, crei un pool o un gruppo di volumi che conterrà le Hard Disk Drives (HDD) o le Solid State Disk (SSD) che vuoi utilizzare nel tuo storage array.

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

- Pool
- Gruppi di volumi RAID

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



[1] LUN host; [2] Volumi; [3] Gruppi di volumi o pool; [4] HDD o SSD drives

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

- Creazione di pool o gruppi di volume con capacità sufficiente
- Aggiunta del numero di dischi necessari per soddisfare i requisiti di prestazioni al pool o al gruppo di volumi
- Selezionare il livello di protezione RAID desiderato (se si utilizzano gruppi di volumi) per soddisfare specifiche esigenze aziendali

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

Pool

I pool sono progettati per aggregare dischi rigidi fisici in un ampio spazio di storage e per fornire una protezione RAID avanzata. Un pool crea numerosi set RAID virtuali a partire dal numero totale di unità assegnate al pool e distribuisce i dati in modo uniforme tra tutte le unità partecipanti. Se un'unità viene persa o aggiunta, System Manager ribilancia dinamicamente i dati tra tutte le unità attive.

I pool fungono da un altro livello RAID, virtualizzando l'architettura RAID sottostante per ottimizzare prestazioni e flessibilità durante attività quali la ricostruzione, l'espansione delle unità e la gestione della perdita di unità. System Manager imposta automaticamente il livello RAID a 6 in una configurazione 8+2 (otto dischi dati più due dischi di parità).

Abbinamento drive

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

Gestione dei dischi guasti

I pool hanno una capacità minima di 11 unità; tuttavia, una capacità equivalente a quella di un'unità è riservata come capacità di riserva in caso di guasto di un'unità. Questa capacità di riserva è chiamata "preservation capacity."

Quando si creano dei pool, una certa quantità di capacità viene riservata per uso di emergenza. Questa capacità viene espressa in termini di numero di drive in System Manager, ma l'implementazione effettiva è distribuita sull'intero pool di drive. La quantità predefinita di capacità che viene riservata si basa sul numero di drive nel pool.

Dopo la creazione del pool, è possibile modificare il valore della capacità di conservazione, aumentandola o diminuendola, oppure impostarla su nessuna capacità di conservazione (equivalente a 0 drive). La quantità massima di capacità che può essere conservata (espressa come numero di drive) è 10, ma la capacità disponibile potrebbe essere inferiore, in base al numero totale di drive presenti nel pool.

Gruppi di volume

I gruppi di volumi definiscono come la capacità viene allocata nel sistema storage ai volumi. Le unità disco sono organizzate in gruppi RAID e i volumi risiedono sulle unità all'interno di un gruppo RAID. Pertanto, le impostazioni di configurazione dei gruppi di volumi identificano quali unità fanno parte del gruppo e quale livello RAID viene 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 è il totale del numero di unità selezionate, moltiplicato per la loro capacità.

Abbinamento drive

È necessario che le unità nel gruppo di volumi corrispondano per dimensioni e prestazioni. Se nel gruppo di volumi sono presenti unità più piccole e più grandi, tutte le unità vengono riconosciute come della capacità più piccola. Se nel gruppo di volumi sono presenti unità più lente e più veloci, tutte le unità vengono riconosciute alla velocità più lenta. Questi fattori influiscono sulle prestazioni e sulla capacità complessiva del sistema

storage.

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

Gestione dei dischi guasti

I gruppi di volumi utilizzano hot spare come unità di riserva in caso di guasto di un disco nei volumi RAID 1/10, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. Un hot spare non contiene dati e aggiunge un ulteriore livello di ridondanza al tuo array di storage.

Se un drive si guasta nell'array di storage, il drive hot spare viene automaticamente sostituito al drive guasto senza richiedere una sostituzione fisica. Se il drive hot spare è disponibile quando un drive si guasta, il controller utilizza i dati di ridondanza per ricostruire i dati dal drive guasto al drive hot spare.

Scopri la terminologia relativa alla capacità nel software SANtricity

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

Oggetti di storage

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

Oggetto di storage	Descrizione
Host	Un host è un server che invia I/O a un volume su un array di storage.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi che un host utilizza 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 indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi differenti.
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un container per una o più coppie mirror. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror.
Coppia di volumi speculari	Una coppia speculare è composta da due volumi, un volume primario e un volume secondario.
Pool	Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)
Gruppo di coerenza Snapshot	Un gruppo di coerenza snapshot è una raccolta di volumi che vengono trattati come un'unica entità quando viene creata un'immagine snapshot. Ciascuno di questi volumi ha la propria immagine snapshot, ma tutte le immagini vengono create nello stesso momento.

Oggetto di storage	Descrizione
Gruppo Snapshot	Un gruppo di snapshot è una raccolta di immagini snapshot da un singolo volume di base.
Volume Snapshot	Un volume snapshot consente all'host di accedere ai dati nell'immagine snapshot. Il volume snapshot contiene una propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine snapshot originale.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage.
Gruppo di volumi	Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)

Capacità di storage

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

Tipo di capacità	Descrizione
Capacità assegnata	La capacità allocata è la capacità fisica allocata dalle unità in un pool o in un gruppo di volumi. Si utilizza la capacità allocata per creare volumi e per le operazioni dei servizi di copia.
Capacità libera	La capacità libera è la capacità disponibile in un pool o in un gruppo di volumi che non è stata ancora allocata alla creazione di volumi, alle operazioni dei servizi di copia e agli oggetti di storage.
Capacità del pool o del gruppo di volumi	La capacità di un pool, di un volume o di un gruppo di volumi è la capacità in un array di storage che è stata assegnata a un pool o a un gruppo di volumi. Questa capacità viene utilizzata per creare volumi e soddisfare le varie esigenze di capacità delle operazioni dei servizi di copia e degli oggetti di storage.
Capacità inutilizzabile del pool	La capacità inutilizzabile di un pool è lo spazio in un pool che non può essere utilizzato a causa di dimensioni dei dischi non corrispondenti.
Capacità di conservazione	La capacità di conservazione è la quantità di capacità (numero di unità) che viene riservata in un pool per supportare potenziali guasti delle unità.
Capacità segnalata	La capacità segnalata è la capacità che viene comunicata all'host e a cui l'host può accedere.

Tipo di capacità	Descrizione
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copia del servizio e oggetto di archiviazione. Non è direttamente leggibile dall'host.
Cache SSD	Cache SSD è un insieme di unità a stato solido (SSD) che vengono raggruppate logicamente nell'array di storage. La funzionalità Cache SSD memorizza nella cache i dati a cui si accede più frequentemente (dati "caldi") su unità SSD a bassa latenza per accelerare dinamicamente i carichi di lavoro delle applicazioni.
Capacità non assegnata	La capacità non assegnata è lo spazio in un array di storage che **non** è stato assegnato a un pool o a un volume group.
Capacità scritta	La capacità scritta è la quantità di capacità che è stata scritta dalla capacità riservata allocata per i volumi sottili.

Scopri pool e gruppi di volume nel software SANtricity

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

Motivi per scegliere un pool o un gruppo di volumi

Scegli un pool

- Se hai bisogno di ricostruzioni più rapide delle unità e di una gestione semplificata dello storage, richiedi volumi thin e/o hai un carico di lavoro altamente casuale.
- Se si desidera distribuire i dati di ciascun volume in modo casuale su un insieme di unità 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.

Scegli 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 le unità 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 sull'insieme di unità che compongono il gruppo di volumi.

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

Differenze di funzionalità tra pool e gruppi di volume

La tabella seguente fornisce un confronto delle funzionalità tra gruppi di volume e pool.

Usa	Pool	Gruppo di volumi
Carico di lavoro casuale	Meglio	Bene
Carico di lavoro sequenziale	Bene	Meglio
Tempo di ricostruzione dell'unità	Più veloce	Più lentamente
Prestazioni (modalità ottimale)	Buono: ideale per carichi di lavoro a piccoli blocchi e casuali.	Buono: ideale per carichi di lavoro sequenziali di grandi dimensioni
Prestazioni (modalità di ricostruzione dell'unità)	Migliore: Solitamente migliore rispetto a RAID 6	Degradato: calo delle prestazioni fino al 40%
Guasti multipli alle unità disco	Maggiore protezione dei dati: ricostruzioni più rapide e prioritarie	Minore protezione dei dati: ricostruzioni lente, maggiore rischio di perdita di dati
Aggiunta di dischi	Più veloce: aggiungi al pool al volo	Più lento: richiede l'operazione Dynamic Capacity Expansion
Supporto per volumi sottili	Sì	No
Supporto per Solid State Disk (SSD)	Sì	Sì
Amministrazione semplificata	Sì: nessun hot spare o impostazione RAID da configurare	No: è necessario allocare hot spare e configurare RAID
Prestazioni regolabili	No	Sì

Confronto funzionale tra pool e gruppi di volume

La funzione e lo scopo di un pool e di un gruppo di volumi sono gli stessi. Entrambi gli oggetti sono un insieme di unità raggruppate logicamente in un array di storage e vengono utilizzati per creare volumi a cui un host può accedere.

La tabella seguente ti aiuta a decidere se un pool o un volume group è più adatto alle tue esigenze di archiviazione.

Funzione	Pool	Gruppo di volumi
Supporto per diversi livelli RAID	No. Sempre RAID 6 in System Manager.	Sì. RAID 0, 1, 10, 5 e 6 disponibili.

Funzione	Pool	Gruppo di volumi
Volumi thin supportati	Sì	No
Crittografia completa del disco (FDE) supportata	Sì	Sì
Data Assurance (DA) supportata	Sì	Sì
Protezione contro la perdita di shelf supportata	Sì	Sì
Protezione contro la perdita del cassetto supportata	Sì	Sì
Velocità dei dischi miste supportate	Si consiglia che siano uguali, ma non è obbligatorio. La velocità dell'unità più lenta determina la velocità di tutte le unità.	Si consiglia che siano uguali, ma non è obbligatorio. La velocità dell'unità più lenta determina la velocità di tutte le unità.
Capacità di dischi mista supportata	Si consiglia che siano uguali, ma non è obbligatorio. L'unità più piccola determina la capacità di tutte le unità.	Si consiglia che siano uguali, ma non è obbligatorio. L'unità più piccola determina la capacità di tutte le unità.
Numero minimo di unità	11	Dipende dal livello RAID. RAID 0 richiede 1. RAID 1 o 10 richiede 2 (è necessario un numero pari). Il minimo per RAID 5 è 3. Il minimo per RAID 6 è 5.
Numero massimo di unità	Fino al limite massimo per l'array di archiviazione	RAID 1 e 10—fino al limite massimo dell'array di archiviazione RAID 5, 6—30 unità
È possibile scegliere singole unità quando si crea un volume	No	Sì
È possibile specificare la dimensione del segmento quando si crea un volume	Sì. 128K supportato.	Sì
È possibile specificare le caratteristiche di I/O durante la creazione di un volume	No	Sì. File system, database, multimedia e configurazioni personalizzate sono supportati.

Funzione	Pool	Gruppo di volumi
Protezione in caso di guasto dell'unità	Utilizza la capacità di preservazione su ogni unità del pool, rendendo la ricostruzione più veloce.	Utilizza un hot spare. La ricostruzione è limitata dagli IOPS dell'unità.
Avviso al raggiungimento del limite di capacità	Sì. È possibile impostare un avviso quando la capacità utilizzata raggiunge una percentuale della capacità massima.	No
Migrazione a un array di storage diverso supportata	No. Richiede che tu esegua prima la migrazione a un gruppo di volumi.	Sì
Dimensione dinamica del segmento (DSS)	No	Sì
È possibile modificare il livello RAID	No	Sì
Espansione del volume (aumento della capacità)	Sì	Sì
Espansione della capacità (aggiungi capacità)	Sì	Sì
Riduzione della capacità	Sì	No

Tipi di unità misti (HDD, SSD) non sono supportati né per i pool né per i gruppi di volumi.

Scopri la creazione automatica rispetto a quella manuale dei pool in SANtricity System Manager

Crei pool automaticamente o manualmente per consentire che lo storage fisico sia raggruppato e quindi allocato dinamicamente secondo necessità. Quando viene creato un pool, puoi aggiungere unità fisiche.

Creazione automatica

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

La creazione automatica del pool avviene quando una di queste condizioni è vera:

- Nell'array di storage non esistono pool e sono presenti unità simili a sufficienza per creare un nuovo pool.
- Vengono aggiunti nuovi dischi 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 una capacità simile. System Manager ti chiederà di completare le seguenti attività:

- Crea un singolo pool se sono presenti un numero sufficiente di unità di quei tipi.
- Crea più pool se la capacità non assegnata è costituita da diversi tipi di unità.
- Aggiungi le unità al pool esistente se un pool è già definito nell'array di storage e aggiungi al pool nuove unità dello stesso tipo di unità.
- Aggiungi 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.

Creazione manuale

Potrebbe essere necessario creare un pool manualmente quando la creazione automatica non riesce a determinare la configurazione ottimale. Questa situazione può verificarsi per uno dei seguenti motivi:

- Le nuove unità potrebbero potenzialmente essere aggiunte a più di un pool.
- Uno o più dei nuovi candidati per il pool possono utilizzare la shelf loss protection o la drawer loss protection.
- Uno o più degli attuali candidati del pool non possono mantenere lo stato di protezione contro la perdita dello shelf o la perdita del drawer.

Potresti anche voler creare un pool manualmente se hai più applicazioni sul tuo storage array e non vuoi che competano per le stesse risorse delle unità. In questo caso, potresti considerare di creare manualmente un pool più piccolo per una o più applicazioni. Puoi assegnare solo uno o due volumi invece di assegnare il carico di lavoro a un pool di grandi dimensioni che ha molti volumi su cui distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di una specifica applicazione può consentire alle operazioni dello storage array di essere eseguite più rapidamente e con meno contesa.

Configura lo storage

Crea automaticamente un pool in SANtricity System Manager

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

Prima di iniziare

È possibile avviare la finestra di dialogo Pool Auto-Configuration quando si verifica una delle seguenti condizioni:

- È stato rilevato almeno un disco singolo non assegnato che può essere aggiunto a un pool esistente con tipi di disco simili.
- Sono stati rilevati undici (11) o più dischi singoli 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 disco dissimili).

Informazioni su questa attività

Tenete presente quanto segue:

- Quando si aggiungono drive a un array di storage, System Manager rileva automaticamente i drive e

chiede di creare un disco singolo pool o più pool in base al tipo di drive e alla configurazione corrente.

- Se in precedenza erano stati definiti dei pool, System Manager propone automaticamente l'opzione di aggiungere i dischi compatibili a un pool esistente. Quando vengono aggiunti nuovi dischi a un pool esistente, System Manager ridistribuisce automaticamente i dati sulla nuova capacità, che ora include i nuovi dischi aggiunti.
- Quando si configura un array di storage EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di drive nei primi 12 slot e a un numero uguale di drive negli ultimi 12 slot. Questa configurazione consente ai controller di utilizzare in modo più efficace entrambi i bus PCIe lato drive.

È possibile avviare la finestra di dialogo Pool Auto-Configuration utilizzando uno dei seguenti metodi:

- Quando viene rilevata capacità non assegnata, il suggerimento Pool Auto-Configuration viene visualizzato nella pagina iniziale, nell'area Notifiche. Fare clic su **View Pool Auto-Configuration** per aprire la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Configurazione automatica del pool dalla pagina Pool e Volume Groups, come descritto nell'attività seguente.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Selezionare **Altro › Avvia configurazione automatica del pool**.

   La tabella dei risultati elenca i nuovi pool, i pool esistenti a cui sono stati aggiunti dischi o entrambi. Un nuovo pool viene denominato con un numero sequenziale per impostazione predefinita.

   System Manager esegue le seguenti attività:

   - Crea un disco singolo pool se è presente un numero sufficiente di drive con lo stesso tipo di drive (HDD o SSD) e con capacità simili.
   - Crea più pool se la capacità non assegnata è costituita da diversi tipi di drive.
   - Aggiunge i dischi a un pool esistente se un pool è già definito nell'array di storage e si aggiungono nuovi dischi dello stesso tipo di disco al pool.
   - Aggiunge i dischi dello stesso tipo di disco al pool esistente e utilizza gli altri tipi di disco per creare pool diversi se i nuovi dischi sono di tipi di disco diversi.
3. Per modificare il nome di un nuovo pool, fai clic sull'icona **Edit** (la matita).
4. Per visualizzare ulteriori caratteristiche del pool, posiziona il cursore sull'icona **Dettagli** (la pagina) o toccala.

   Vengono visualizzate informazioni sul tipo di disco, sulla funzionalità di sicurezza, sulla funzionalità di data assurance (DA), sulla shelf loss protection e sulla drawer loss protection.

   Per gli array di storage EF600 e EF300, vengono visualizzate anche le impostazioni relative al resource provisioning e alle dimensioni dei volume block.
5. Fai clic su **Accept**.

Creare un pool manualmente in SANtricity System Manager

È possibile creare un pool manualmente (da un insieme di candidati) se la funzione Pool Auto Configuration non fornisce un pool che soddisfa le proprie esigenze.

Un pool fornisce la capacità di archiviazione logica necessaria dalla quale è possibile creare volumi individuali che possono poi essere utilizzati per ospitare le tue applicazioni.

Prima di iniziare

- È necessario disporre di un minimo di 11 dischi dello stesso tipo (HDD o SSD).
- La protezione contro la perdita di shelf richiede che le unità che compongono il pool siano collocate in almeno sei diversi shelf di unità e che non vi siano più di due unità in un singolo shelf di unità.
- 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 alloggiamenti per unità provenienti da ciascun cassetto.
- Quando si configura un array di storage EF600 o EF300, assicurarsi che ciascun controller abbia accesso a un numero uguale di drive nei primi 12 slot e a un numero uguale di drive negli ultimi 12 slot. Questa configurazione consente ai controller di utilizzare entrambi i bus PCIe lato drive in modo più efficace. Attualmente System Manager consente la selezione dei drive nella funzione Avanzate durante la creazione di un gruppo di volumi. Per la creazione di un pool, si consiglia di utilizzare tutti i drive presenti nell'array di storage.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fare clic su **Create › Pool**.

   Viene visualizzata la finestra di dialogo Create Pool.

3. Inserisci un nome per il pool.
4. **Facoltativo:** Se nel tuo array di archiviazione sono presenti più tipi di drive, seleziona il tipo di drive che desideri utilizzare.

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

5. Seleziona il candidato del pool che desideri utilizzare in base alle seguenti caratteristiche, quindi fai clic su **Create**.

Caratteristica	Usa
Capacità libera	Mostra la capacità libera del pool candidato in GiB. Seleziona un pool candidato con la capacità per le esigenze di archiviazione della tua applicazione. La capacità di riserva (spare) è anch'essa distribuita in tutto il pool e non fa parte della capacità libera.
Dischi totali	Mostra il numero di dischi disponibili nel pool candidate. System Manager riserva automaticamente il maggior numero possibile di dischi per la capacità di conservazione (per ogni sei dischi in un pool, System Manager riserva un disco per la capacità di conservazione). Quando si verifica un guasto di un disco, la capacità di conservazione viene utilizzata per contenere i dati ricostruiti.

Caratteristica	Usa
Dimensione blocco disco (solo EF300 e EF600)	Indica la dimensione del blocco (dimensione del settore) che le unità del pool possono scrivere. I valori possibili includono: • 512 — settore da 512 byte. • 4K — dimensione settore 4.096 byte.
Secure-Capable	Indica se questo pool candidato è composto interamente da drive con funzionalità di sicurezza, che possono essere drive Full Disk Encryption (FDE) o drive Federal Information Processing Standard (FIPS). • È possibile proteggere il pool con Drive Security, ma tutte le unità devono essere secure-capable per utilizzare questa funzione. • Se si desidera creare un pool solo FDE, cercare **Sì - 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 unità di livello 140-2 e 140-3. Se si utilizza una combinazione di questi livelli, tenere presente che il pool opererà al livello di sicurezza inferiore (140-2). • È possibile creare un pool composto da dischi che possono essere o meno secure-capable oppure da una combinazione di livelli di sicurezza. Se i dischi nel pool includono dischi che non sono secure-capable, non è possibile rendere il pool sicuro.
Abilitare la sicurezza?	Offre la possibilità di abilitare la funzionalità Drive Security con dischi compatibili con la sicurezza. Se il pool è compatibile con la sicurezza e hai creato una chiave di sicurezza, puoi abilitare la sicurezza selezionando la check box. L'unico modo per rimuovere Drive Security dopo averlo attivato è eliminare il pool e cancellare i dischi.
Compatibile con DA	Indica se Data Assurance (DA) è disponibile per questo pool candidato. DA verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati dai controller alle unità. DA è abilitato se tutte le unità sono compatibili con DA. DA può essere disabilitato dopo la creazione del volume selezionando **Storage › Volumes › View/Edit Settings › Advanced › Permanently disable data assurance**. Se DA è disabilitato su un volume, non può essere riabilitato.
Resource Provisioning Capable (solo EF300 e EF600)	Indica se Resource Provisioning è disponibile per questo pool candidate. Resource Provisioning è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background.

Caratteristica	Usa
Protezione perdita shelf	Indica se la protezione contro la perdita dello shelf è disponibile. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi in un pool in caso di perdita totale della comunicazione con una shelf di dischi singola.
Protezione contro la perdita del cassetto	Indica se è disponibile la protezione contro la perdita dei cassetti, che viene fornita solo se si utilizza un drive shelf che contiene cassetti. La protezione contro la perdita di un singolo cassetto garantisce l'accessibilità ai dati sui volumi in un pool se si verifica una perdita totale di comunicazione con un singolo cassetto in una drive shelf.
Dimensioni dei blocchi volume supportate (EF300 e EF600 only)	Mostra le dimensioni dei blocchi che possono essere creati per i volumi nel pool: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Crea un gruppo di volumi in SANtricity System Manager

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

Grazie a unità con maggiore capacità e alla possibilità di distribuire i volumi su più controller, la creazione di più di un volume per gruppo di volumi rappresenta un ottimo modo per sfruttare al meglio la capacità di archiviazione e proteggere i dati.

Prima di iniziare

Esaminare queste linee guida prima di creare un gruppo di volumi:

- È necessario almeno un disco non assegnato.
- Esistono dei limiti al numero di drive che è possibile avere in un singolo gruppo di volumi. Questi limiti variano a seconda del livello RAID.
- Per abilitare la protezione dalla perdita di shelf/drawer, è necessario creare un gruppo di volumi che utilizzi dischi situati in almeno tre shelf o drawer, a meno che non si utilizzi RAID 1, dove il minimo è di due shelf/drawer.
- Se si dispone di un array di storage EF600 o EF300 e si intende creare un gruppo di volumi manualmente, assicurarsi che ciascun controller abbia accesso a un numero uguale di drive nei primi 12 slot e a un numero uguale di drive negli ultimi 12 slot. Questa configurazione consente ai controller di utilizzare entrambi i bus PCIe lato drive in modo più efficace. Attualmente System Manager consente la selezione dei drive nella funzione Avanzate durante la creazione di un gruppo di volumi.
- Verifica 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 unità alla volta per assicurarsi che venga

selezionata una coppia con mirroring. Il mirroring e lo striping (noti come RAID 10 o RAID 1+0) si ottengono quando si selezionano quattro o più unità.

- Se si seleziona RAID 5, è necessario aggiungere almeno tre drive per creare il gruppo di volumi.
- Se si seleziona RAID 6, è necessario aggiungere un minimo di cinque dischi per creare il gruppo di volumi.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fare clic su **Create › Volume group**.

   Viene visualizzata la finestra di dialogo Create Volume Group.

3. Inserisci un nome per il gruppo di volumi.
4. Seleziona il livello RAID che meglio soddisfa i tuoi requisiti per l'archiviazione e la protezione dei dati.

   La tabella dei gruppi di volumi candidati viene visualizzata e mostra solo i candidati che supportano il livello RAID selezionato.

5. **Facoltativo:** Se nel tuo array di archiviazione sono presenti più tipi di drive, seleziona il tipo di drive che desideri utilizzare.

   La tabella dei gruppi di volumi candidati viene visualizzata e mostra solo i candidati che supportano il tipo di unità selezionata e il livello RAID.

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

   Per selezionare manualmente le unità, fare clic sul collegamento **Manually select drives (advanced)**. Quando si fa clic, cambia in **Automatically select drives (advanced)**.

   Il metodo manuale consente di selezionare le unità specifiche che compongono il gruppo di volumi. È possibile selezionare unità specifiche non assegnate per ottenere la capacità richiesta. Se l'array di memorizzazione contiene unità con tipi di supporti diversi o tipi di interfaccia diversi, è possibile scegliere solo la capacità non configurata per un singolo tipo di disco per creare il nuovo gruppo di volumi.

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

7. In base alle caratteristiche delle unità visualizzate, seleziona le unità che vuoi utilizzare nel gruppo di volumi, quindi fai clic su **Crea**.

   Le caratteristiche del disco visualizzate dipendono dal fatto che sia stato selezionato il metodo automatico o quello manuale.

Caratteristiche dell'unità con metodo automatico

Caratteristica	Usa
Capacità libera	Mostra la capacità disponibile in GiB. Seleziona un candidato gruppo di volumi con la capacità per le esigenze di archiviazione della tua applicazione.
Dischi totali	Mostra il numero di drive disponibili per questo gruppo di volumi. Seleziona un candidato gruppo di volumi con il numero di drive che desideri.
Dimensione blocco disco (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che le unità del gruppo possono scrivere. I valori possono includere: • 512 — settore da 512 byte. • 4K — dimensione settore 4.096 byte.
Secure-Capable	Indica se questo candidato gruppo di volumi è composto interamente da unità con capacità di protezione, che possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). • È possibile proteggere il gruppo di volumi con Drive Security, ma tutte le unità devono essere secure-capable per poter utilizzare questa funzione. • Se si desidera creare un gruppo di volumi solo FDE, cercare **Yes - FDE** nella colonna Secure-Capable. Se si desidera creare un gruppo di volumi solo FIPS, cercare **Yes - FIPS** o **Yes - FIPS (Mixed)**. "Mixed" indica una miscela di unità di livello 140-2 e 140-3. Se si utilizza una miscela di questi livelli, si tenga presente che il gruppo di volumi funzionerà con il livello di sicurezza inferiore (140-2). • È possibile creare un gruppo di volumi composto da unità che possono essere o meno secure-capable o che sono un mix di livelli di sicurezza. Se le unità del gruppo di volumi includono unità che non sono secure-capable, non è possibile rendere sicuro il gruppo di volumi.
Abilitare la sicurezza?	Fornisce l'opzione per abilitare la funzione Drive Security con le unità secure-capable. Se il gruppo di volumi è secure-capable e si è impostata una chiave di sicurezza, è possibile abilitare Drive Security selezionando la check box. L'unico modo per rimuovere Drive Security dopo che è stato attivato è eliminare il gruppo di volumi ed eliminare le unità.

Caratteristica	Usa
Compatibile con DA	Indica se Data Assurance (DA) è disponibile per questo gruppo. Data Assurance (DA) controlla e corregge gli errori che possono verificarsi durante il trasferimento dei dati attraverso i controller fino ai drive. Se si desidera utilizzare DA, selezionare un gruppo di volumi che supporta DA. (Per le unità compatibili con DA, DA viene attivata automaticamente sui volumi creati nel pool.) Un gruppo di volumi può contenere unità che sono DA-capable o non DA-capable, ma tutte le unità devono essere DA-capable per poter utilizzare questa funzione.
Resource Provisioning Capable (solo EF300 e EF600)	Mostra se Resource Provisioning è disponibile per questo gruppo. Resource Provisioning è una funzione disponibile negli array di archiviazione EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.
Protezione perdita shelf	Mostra se è disponibile la shelf loss protection. La shelf loss protection garantisce l'accessibilità ai dati sui volumi di un gruppo di volumi in caso di perdita totale della comunicazione con uno shelf.
Protezione contro la perdita del cassetto	Mostra se è disponibile la protezione contro la perdita di cassetto, che viene fornita solo se si utilizza un drive shelf che contiene cassetti. La protezione contro la perdita di cassetto garantisce l'accessibilità ai dati sui volumi di un volume group se si verifica una perdita totale di comunicazione con un singolo cassetto in un drive shelf.
Dimensioni dei blocchi volume supportate (EF300 e EF600 only)	Mostra le dimensioni dei blocchi che possono essere create per i volumi del gruppo: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.

Caratteristiche dell'unità con metodo manuale

Caratteristica	Usa
Tipo di media	Indica il tipo di supporto. Sono supportati i seguenti tipi di supporto: • Disco rigido • Disco allo stato solido (SSD) Tutte le unità di un gruppo di volumi devono essere dello stesso tipo di supporto (tutte SSD o tutte unità rigide). I gruppi di volumi non possono contenere un mix di tipi di supporto o di tipi di interfaccia.
Dimensione blocco disco (solo EF300 e EF600)	Mostra la dimensione del blocco (dimensione del settore) che le unità del gruppo possono scrivere. I valori possono includere: • 512 — settore da 512 byte. • 4K — dimensione settore 4.096 byte.
Capacità dell'unità	Indica la capacità dell'unità. • Ogni volta che è possibile, selezionare unità con una capacità pari a quella delle unità correnti del gruppo di volumi. • Se si devono aggiungere unità non assegnate con una capacità inferiore, tenere presente che la capacità utilizzabile di ogni unità attualmente presente nel gruppo di volumi viene ridotta. Pertanto, la capacità di ciascuna unità è la stessa in tutto il gruppo di volumi. • Se si devono aggiungere unità non assegnate con una capacità maggiore, tenere presente che la capacità utilizzabile delle unità non assegnate che si aggiungono viene ridotta in modo da corrispondere alle capacità attuali delle unità nel gruppo di volumi.
Vassoio	Indica la posizione del vassoio dell'unità.
slot	Indica la posizione dello slot dell'unità.
Velocità (rpm)	Indica la velocità del drive.
Dimensione del settore logico	Indica la dimensione e il formato del settore.

Caratteristica	Usa
Secure-Capable	Indica se questo candidato gruppo di volumi è composto interamente da unità con capacità di protezione, che possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). • È possibile proteggere il gruppo di volumi con Drive Security, ma tutte le unità devono essere secure-capable per poter utilizzare questa funzione. • Se si desidera creare un gruppo di volumi solo FDE, cercare **Yes - FDE** nella colonna Secure-Capable. Se si desidera creare un gruppo di volumi solo FIPS, cercare **Yes - FIPS** o **Yes - FIPS (Mixed)**. "Mixed" indica una miscela di unità di livello 140-2 e 140-3. Se si utilizza una miscela di questi livelli, si tenga presente che il gruppo di volumi funzionerà con il livello di sicurezza inferiore (140-2). • È possibile creare un gruppo di volumi composto da unità che possono essere o meno secure-capable o che sono un mix di livelli di sicurezza. Se le unità del gruppo di volumi includono unità che non sono secure-capable, non è possibile rendere sicuro il gruppo di volumi.
Compatibile con DA	Indica se la Data Assurance (DA) è disponibile per questo gruppo. La Data Assurance (DA) controlla e corregge gli errori che possono verificarsi durante la comunicazione dei dati attraverso i controller fino ai dischi. Se si desidera utilizzare DA, selezionare un gruppo di volumi che supporta DA. (Per le unità compatibili con DA, DA viene attivata automaticamente sui volumi creati nel pool.) Un gruppo di volumi può contenere unità che sono DA-capable o non DA-capable, ma tutte le unità devono essere DA-capable per poter utilizzare questa funzione.
Dimensioni dei blocchi volume supportate (EF300 e EF600 only)	Mostra le dimensioni dei blocchi che possono essere create per i volumi del gruppo: • 512n — 512 byte nativi. • 512e — 512 byte emulati. • 4K — 4,096 byte.
Resource Provisioning Capable (solo EF300 e EF600)	Mostra se Resource Provisioning è disponibile per questo gruppo. Resource Provisioning è una funzione disponibile negli array di archiviazione EF300 e EF600, che consente di utilizzare immediatamente i volumi senza alcun processo di inizializzazione in background.

Aggiungere capacità a un pool o a un gruppo di volumi in SANtricity System Manager

È possibile aggiungere unità per espandere la capacità libera in un pool o volume group esistente.

L’espansione comporta l’inclusione di ulteriore capacità libera nel pool o nel gruppo di volumi. È possibile utilizzare questa capacità libera per creare volumi aggiuntivi. I dati nei volumi rimangono accessibili durante questa operazione.

Prima di iniziare

- Le unità devono essere in stato Ottimale.
- Le unità devono avere lo stesso tipo di drive (HDD o SSD).
- Il pool o il gruppo di volumi deve essere in stato Ottimale.
- Il numero massimo di volumi consentiti in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello del sistema storage:
  - 2,048 volumi (serie EF600 e E5700)
  - 1,024 volumi (EF300)
  - 512 volumi (serie E4000 e E2800)
- Se il pool o il gruppo di volumi contiene tutte unità secure-capable, aggiungi solo unità secure-capable per continuare a utilizzare le capacità di crittografia delle unità secure-capable.

  Le unità con funzionalità di sicurezza possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS).

Informazioni su questa attività

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

Con l’aggiunta di unità, potrebbe essere necessario aumentare la capacità di preservazione. Si consiglia di valutare l’opportunità di incrementare la capacità riservata dopo un’operazione di espansione.

Evitate di utilizzare unità compatibili con Data Assurance (DA) per aggiungere capacità a un pool o a un gruppo di volumi non compatibile con DA. Il pool o il gruppo di volumi non può sfruttare le funzionalità dell’unità compatibile con DA. Considerate l’utilizzo di unità non compatibili con DA in questa situazione.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il pool o il gruppo di volumi a cui desideri aggiungere unità, quindi fai clic su **Add Capacity**.

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

3. In **Seleziona le unità a cui aggiungere capacità…**, seleziona una o più unità che desideri aggiungere al pool o al gruppo di volumi esistente.

   Il firmware del controller organizza le unità non assegnate, visualizzando in cima all’elenco le opzioni migliori. La capacità libera totale aggiunta al pool o al gruppo di volumi viene visualizzata sotto l’elenco in **Capacità totale selezionata**.

Dettagli del campo

Campo	Descrizione
Shelf	Indica la posizione dell'unità sullo scaffale.
Baia	Indica la posizione della baia del drive.
Capacità (GiB)	Indica la capacità dell'unità. • Quando possibile, selezionare unità che abbiano una capacità pari a quella delle unità attualmente presenti nel pool o nel gruppo di volumi. • Se è necessario aggiungere unità non assegnate con una capacità inferiore, tenere presente che la capacità utilizzabile di ciascuna unità attualmente presente nel pool o nel gruppo di volumi viene ridotta. Pertanto, la capacità dell'unità è la stessa in tutto il pool o gruppo di volumi. • Se è necessario aggiungere unità non assegnate con una capacità maggiore, tenere presente che la capacità utilizzabile delle unità non assegnate che si aggiungono viene ridotta in modo da corrispondere alle capacità attuali delle unità presenti nel pool o nel gruppo di volumi.
Secure-Capable	Indica se l'unità è compatibile con la sicurezza. • Per proteggere il pool o il gruppo di volumi con la funzionalità Sicurezza unità, tutte le unità devono essere compatibili con la sicurezza. • È possibile creare un pool o un gruppo di volumi con un mix di unità con funzionalità di sicurezza e unità senza funzionalità di sicurezza, ma la funzionalità Drive Security non può essere abilitata. • Un pool o un gruppo di volumi composto interamente da unità con funzionalità di sicurezza non può accettare un'unità senza funzionalità di sicurezza per la sostituzione o l'espansione, anche se la funzionalità di crittografia non è in uso. • Le unità segnalate come secure-capable possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). • Un'unità FIPS può essere di livello 140-2 o 140-3, con il livello 140-3 come livello di sicurezza più elevato. Se si seleziona una combinazione di unità di livello 140-2 e 140-3, il pool o il gruppo di volumi opererà al livello di sicurezza inferiore (140-2).

Campo	Descrizione
Compatibile con DA	Indica se l'unità è compatibile con Data Assurance (DA). • Si sconsiglia di utilizzare unità non compatibili con Data Assurance (DA) per aggiungere capacità a un pool o a un gruppo di volumi compatibile con DA. Il pool o il gruppo di volumi non avrà più funzionalità DA e non sarà più possibile abilitare DA sui volumi appena creati all'interno del pool o del gruppo di volumi. • Si sconsiglia di utilizzare unità compatibili con Data Assurance (DA) per aggiungere capacità a un pool o a un gruppo di volumi non compatibile con DA, poiché tale pool o gruppo di volumi non può sfruttare le funzionalità dell'unità compatibile con DA (gli attributi dell'unità non corrispondono). Considerare l'utilizzo di unità non compatibili con DA in questa situazione.
DULBE compatibile	Indica se l'unità dispone dell'opzione per Deallocated or Unwritten Logical Block Error (DULBE). DULBE è un'opzione presente sulle unità NVMe che consente all'array di storage EF300 o EF600 di supportare volumi con provisioning delle risorse.

4. Fai clic su **Add**.

   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 fa sì che il pool o il gruppo di volumi non abbia più uno o più dei seguenti attributi:

   ◦ Protezione contro la perdita dello shelf *
   ◦ Protezione contro la perdita del cassetto *
   ◦ Funzionalità di crittografia completa del disco
   ◦ Capacità Data Assurance
   ◦ Capacità DULBE

   * Attualmente, la finestra di dialogo di conferma non viene visualizzata quando si aggiungono unità a un pool con shelf loss protection o drawer loss protection.

1. Per continuare, fai clic su **Yes**; altrimenti, fai clic su **Cancel**.

Risultati

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

Gestisci storage

Verifica la ridondanza del volume in SANtricity System Manager

Con la guida del supporto tecnico o come indicato dal Recovery Guru, puoi verificare la ridondanza su un volume in un pool o 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'unità sostitutiva se una delle unità nel pool o nel gruppo di volumi si guasta.

Prima di iniziare

- Lo stato del pool o del gruppo di volumi deve essere Optimal.
- Il pool o il gruppo di volumi non deve avere operazioni di modifica del volume in corso.
- È possibile verificare la ridondanza su qualsiasi livello RAID, ad eccezione del RAID 0, perché il RAID 0 non offre alcuna ridondanza.

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

Informazioni su questa attività

È possibile eseguire questo controllo solo su un pool o gruppo di volumi alla volta. Un controllo di ridondanza dei volumi esegue le seguenti azioni:

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

> 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.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Selezionare **Attività non comuni › Verifica ridondanza volume**.

   Viene visualizzata la finestra di dialogo Check Redundancy.

3. Seleziona i volumi che desideri controllare, quindi digita `check` per confermare che vuoi eseguire questa operazione.
4. Fai clic su **Check**.

   L'operazione di verifica della ridondanza dei volumi ha inizio. I volumi nel pool o nel gruppo di volumi vengono analizzati in sequenza, partendo dall'alto della tabella nella finestra di dialogo. Queste azioni si verificano durante la scansione di ciascun volume:

   - Il volume è selezionato nella tabella dei volumi.
   - Lo stato della verifica della ridondanza è indicato nella colonna **Stato**.
   - Il controllo si interrompe su qualsiasi errore relativo al supporto di memorizzazione o alla parità riscontrato e quindi segnala l'errore.

Maggiori informazioni sullo stato della verifica della ridondanza

Stato	Descrizione
In attesa	Questo è il primo volume da scansionare e non hai fatto clic su Avvia per iniziare il controllo di ridondanza. o L'operazione di verifica della ridondanza viene eseguita su altri volumi nel pool o nel gruppo di volumi.
Verifica	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.
Fallito	Il volume non ha superato il controllo di ridondanza. Sono state rilevate incongruenze nelle informazioni di ridondanza.
Errore multimediale	L'unità disco è difettosa e illeggibile. Segui le istruzioni visualizzate in Recovery Guru.
Errore di parità	La parità non è quella prevista per una determinata porzione di dati. Un errore di parità è potenzialmente grave e potrebbe causare una perdita permanente di dati.

5. Fare clic su **Fine** dopo che l'ultimo volume nel pool o gruppo di volumi è stato controllato.

Eliminare un pool o un gruppo di volumi in SANtricity System Manager

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

Prima di iniziare

- È necessario aver eseguito il backup dei dati su tutti i volumi nel pool o nel gruppo di volumi.
- È necessario aver interrotto tutte le operazioni di input/output (I/O).
- È necessario smontare tutti i file system sui volumi.
- È necessario aver eliminato tutte le relazioni mirror nel pool o nel gruppo di volumi.
- È necessario aver interrotto qualsiasi operazione di copia di 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.
- Le unità del gruppo di volumi non devono avere una prenotazione permanente.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona un pool o un gruppo di volumi dall'elenco.

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

3. Seleziona **Uncommon Tasks › Delete** e conferma.

Risultati

System Manager esegue le seguenti azioni:

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

Consolidare la capacità libera per un gruppo di volumi in SANtricity System Manager

Utilizza l'opzione Consolidate Free Capacity per consolidare gli extent liberi esistenti su un gruppo di volumi selezionato. Eseguendo questa azione, puoi 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 del gruppo di volumi devono essere online e in stato Optimal.
- Non devono essere in corso operazioni di modifica del volume, come cambiare la dimensione del segmento di un volume.

Informazioni su questa attività

Non è possibile annullare l'operazione una volta avviata. I dati rimangono accessibili durante l'operazione di consolidamento.

È possibile avviare la finestra di dialogo Consolidate Free Capacity utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, il suggerimento "Consolida capacità libera" viene visualizzato nella pagina iniziale, nell'area Notifiche. Fai clic sul collegamento **Consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile avviare la finestra di dialogo Consolidate Free Capacity dalla pagina Pools & Volume Groups, come descritto nell'attività seguente.

Ulteriori informazioni sulle aree a capacità libera

Un'area di capacità libera è la capacità libera che può risultare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità libera disponibile durante la creazione di un volume. Quando crei un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume è limitata all'area di capacità libera più grande in quel 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 puoi creare è di 10 GiB.

Si consolida 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 file. Alla fine, la capacità disponibile non sarà situata in un singolo blocco contiguo, ma sarà dispersa in piccoli frammenti all'interno del gruppo di volumi. Questo causa un'ulteriore frammentazione dei file, poiché l'host deve scrivere i nuovi file come frammenti per adattarli agli intervalli disponibili di cluster liberi.

Consolidando la capacità libera su un gruppo di volumi selezionato, si noterà un miglioramento delle prestazioni del file system ogni volta che l'host scrive nuovi file. Il processo di consolidamento contribuirà anche a prevenire che i nuovi file vengano frammentati in futuro.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il gruppo di volumi con capacità libera che desideri consolidare, quindi seleziona **Attività non comuni › Consolida la capacità libera del gruppo di volumi**.

   Viene visualizzata la finestra di dialogo Consolidate Free Capacity.

3. Digita `consolidate` per confermare che vuoi eseguire questa operazione.
4. Fai clic su **Consolidate**.

   System Manager avvia il consolidamento (deframmentazione) delle aree di capacità libera del gruppo di volumi in un'unica quantità contigua per le successive attività di configurazione dello storage.

Dopo aver finito

Selezionare **Home › Visualizza operazioni in corso** per visualizzare l'avanzamento dell'operazione Consolidate Free Capacity. Questa operazione può essere lunga e potrebbe influire sulle prestazioni del sistema.

Esportazione/Importazione di gruppi di volumi nella SANtricity CLI

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

La funzione di esportazione/importazione non è supportata nell'interfaccia utente di SANtricity System Manager. È necessario utilizzare la Command Line Interface (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Attiva le spie di localizzazione in un pool, un gruppo di volumi o Cache SSD in SANtricity System Manager

È possibile individuare le unità per identificare fisicamente tutte le unità che compongono un pool, un gruppo di volumi o una Cache SSD. Un indicatore LED si accende su

ciascuna unità nel pool, nel gruppo di volumi o nella Cache SSD.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il pool, il gruppo di volumi o la Cache SSD che desideri individuare, quindi fai clic su **More › Turn on locator lights**.

   Viene visualizzata una finestra di dialogo che indica che le spie delle unità che compongono il pool selezionato, il gruppo di volumi o la Cache SSD sono accese.

3. Dopo aver individuato correttamente le unità, fai clic su **Turn Off**.

Rimuovere la capacità da un pool o dalla Cache SSD in SANtricity System Manager

È possibile rimuovere le unità per ridurre la capacità di un pool esistente o della Cache SSD.

Dopo aver rimosso le unità, i dati presenti in ciascun volume del pool o Cache SSD vengono ridistribuiti alle unità rimanenti. Le unità rimosse diventano non assegnate e la loro capacità diventa parte della capacità libera totale dell'array di storage.

Informazioni su questa attività

Segui queste linee guida quando rimuovi capacità:

- Non è possibile rimuovere l'ultima unità 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 unità alla volta. Se è necessario rimuovere più di 12 unità, ripetere la procedura.
- Non è possibile rimuovere le unità se non c'è spazio libero sufficiente nel pool o nella Cache SSD per contenere i dati, quando questi dati vengono ridistribuiti alle unità rimanenti nel pool o nella Cache SSD.

Leggi i potenziali impatti sulle prestazioni

- La rimozione delle unità da un pool o Cache SSD potrebbe comportare una riduzione delle prestazioni del volume.
- La capacità di conservazione non viene consumata quando si rimuove capacità da un pool o SSD Cache. Tuttavia, la capacità di conservazione potrebbe diminuire in base al numero di unità rimanenti nel pool o SSD Cache.

Leggi gli impatti sulle unità compatibili con la sicurezza

- Se si rimuove l'ultima unità che non è secure-capable, il pool rimane con tutte unità secure-capable. In questa situazione, viene offerta la possibilità di abilitare la sicurezza per il pool.
- Se si rimuove l'ultima unità che non è compatibile con Data Assurance (DA), il pool rimane composto solo da unità compatibili con DA.

Tutti i nuovi volumi creati sul pool saranno compatibili con DA. Se si desidera che i volumi esistenti siano compatibili con DA, è necessario eliminarli e quindi ricrearli.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il pool o la Cache SSD, quindi fai clic su **More › Rimuovi capacità**.

   Viene visualizzata la finestra di dialogo Remove Capacity.

3. Seleziona una o più unità nell'elenco.

   Quando si selezionano o deselezionano unità nell'elenco, il campo **Capacità totale selezionata** si aggiorna. Questo campo mostra la capacità totale del pool o della Cache SSD che risulta dopo la rimozione delle unità selezionate.

4. Fai clic su **Remove** e poi conferma di voler rimuovere le unità.

   La nuova capacità ridotta del pool o della Cache SSD si riflette nella vista Pool e gruppi di volumi.

Modifica le impostazioni del pool e del gruppo

Modificare le impostazioni di configurazione di un pool in SANtricity System Manager

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

Informazioni su questa attività

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

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il pool che desideri modificare, quindi fai clic su **View/Edit Settings**.

   Viene visualizzata la finestra di dialogo Pool Setting.

3. Seleziona la scheda **Settings** e quindi modifica le impostazioni del pool secondo necessità.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome del pool fornito dall'utente. Specificare un nome per il pool è obbligatorio.
Avvisi di capacità	È possibile inviare notifiche di avviso quando la capacità libera in un pool raggiunge o supera una soglia specificata. Quando i dati archiviati nel pool superano la soglia specificata, System Manager invia un messaggio, consentendo di aggiungere altro 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 email e messaggi SNMP trap. È possibile definire i seguenti avvisi di capacità: • **Avviso critico** — Questo avviso critico ti notifica quando la capacità libera nel pool raggiunge o supera la soglia specificata. Utilizza i controlli a rotella per regolare la percentuale della soglia. Seleziona la check box per disattivare questa notifica. • **Avviso preventivo** — Questo avviso preventivo ti notifica quando la capacità libera in un pool sta per raggiungere una soglia specificata. Utilizza i controlli a rotella per regolare la percentuale della soglia. Seleziona la check box per disattivare questa notifica.

Impostazione	Descrizione
Priorità di modifica	È possibile specificare i livelli di priorità per le operazioni di modifica in un pool in relazione alle prestazioni del sistema. Una priorità più elevata per le operazioni di modifica in un pool consente di completare un'operazione più rapidamente, ma può rallentare le prestazioni di I/O dell'host. Una priorità inferiore comporta tempi di esecuzione più lunghi, ma le prestazioni di I/O dell'host ne risentono in misura minore. È possibile scegliere tra cinque livelli di priorità: minimo, basso, medio, alto e massimo. Maggiore è il livello di priorità, maggiore è l'impatto su I/O dell'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 più guasti delle unità determinano una condizione in cui alcuni dati non hanno ridondanza e un ulteriore guasto dell'unità potrebbe comportare 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 dell'unità, ma i dati hanno ancora ridondanza e un ulteriore guasto dell'unità 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 quando il pool è in uno stato ottimale. Queste operazioni includono Dynamic Volume Expansion (DVE), Instant Availability Format (IAF) e la migrazione dei dati verso un drive sostituito o aggiunto.

Impostazione	Descrizione
Capacità di conservazione ("Capacità di ottimizzazione" per EF600 o EF300)	**Capacità di conservazione** — È possibile definire il numero di drive per determinare la capacità riservata nel pool per supportare potenziali guasti dei drive. Quando si verifica un guasto di un drive, la capacità di conservazione viene utilizzata per memorizzare i dati ricostruiti. I pool utilizzano la capacità di conservazione durante il processo di ricostruzione dei dati al posto dei drive hot spare, che vengono utilizzati nei gruppi di volumi. Utilizza i comandi a rotella per regolare il numero di drive. In base al numero di drive, la capacità di preservazione nel pool viene visualizzata accanto al riquadro della rotella. Tenete presente 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 riservata influisce sulla quantità di capacità libera disponibile per la creazione di volumi. Se si specifica 0 per la capacità di conservazione, tutta la capacità libera del pool viene utilizzata per la creazione di volumi. • 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 per array EF600 e EF300) — Quando viene creato un pool, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra capacità disponibile rispetto a prestazioni e durata delle unità. Puoi regolare questo equilibrio spostando il cursore verso destra per ottenere prestazioni e durata delle unità migliori a scapito di una maggiore capacità disponibile, oppure spostandolo verso sinistra per ottenere una maggiore capacità disponibile a scapito di prestazioni e durata delle unità migliori. Le unità SSD avranno una durata maggiore e migliori prestazioni massime di scrittura se una parte della loro capacità non è allocata. Per le unità associate a un pool, la capacità non allocata è composta dalla capacità di conservazione del pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile riservata come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, di conseguenza, non è disponibile per la creazione di volumi.

4. Fare clic su **Save**.

Modificare le impostazioni di configurazione per un gruppo di volumi in SANtricity System Manager

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 prestazionali delle applicazioni che accedono al gruppo

di volumi, assicurarsi di soddisfare i seguenti prerequisiti:

- Il gruppo di volumi deve trovarsi nello stato Optimal.
- È necessario disporre di capacità sufficiente nel gruppo di volumi per convertire al nuovo livello RAID.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il gruppo di volumi che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni Volume Group.

3. Seleziona la scheda **Impostazioni** e quindi modifica le impostazioni del gruppo di volume come appropriato.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome assegnato dall'utente al gruppo di volumi. Specificare un nome per il gruppo di volumi è obbligatorio.
livello RAID	Seleziona il nuovo livello RAID dal menu a discesa. • **RAID 0 striping** — Offre prestazioni elevate, ma non fornisce alcuna ridondanza dei dati. Se un disco singolo si guasta nel gruppo di volumi, tutti i volumi associati smettono di funzionare e tutti i dati vengono persi. Un gruppo RAID striping combina due o più dischi in un'unica grande unità logica. • **RAID 1 mirroring** — Offre prestazioni elevate e la migliore disponibilità dei dati, ed è adatto per l'archiviazione di dati sensibili a livello aziendale o personale. Protegge i tuoi dati replicando automaticamente il contenuto di un disco sul secondo disco della coppia in mirroring. Fornisce protezione in caso di guasto di un disco singolo. • **RAID 10 striping/mirroring** — Offre una combinazione di RAID 0 (striping) e RAID 1 (mirroring) e si ottiene selezionando quattro o più drive. RAID 10 è adatto per applicazioni con elevato volume di transazioni, come un database, che richiedono prestazioni elevate e tolleranza ai guasti. • **RAID 5** — Ottimale per ambienti multiutente (come database o file system storage) in cui la dimensione tipica dell'I/O è ridotta e vi è un'elevata percentuale di attività di lettura. • **RAID 6** — Ottimale per ambienti che richiedono una protezione di ridondanza superiore a RAID 5, ma non necessitano di elevate prestazioni di scrittura. RAID 3 può essere assegnato solo ai gruppi di volumi utilizzando l'interfaccia a riga di comando (CLI). Quando si modifica il livello RAID, non è possibile annullare questa operazione dopo che è iniziata. Durante la modifica, i dati rimangono disponibili.

Impostazione	Descrizione
Capacità di ottimizzazione (solo array EF600)	Quando si crea un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra capacità disponibile, prestazioni e durata delle unità. È possibile regolare questo equilibrio spostando il cursore verso destra per ottenere prestazioni e durata delle unità migliori a scapito di una maggiore capacità disponibile, oppure spostandolo verso sinistra per ottenere una maggiore capacità disponibile a scapito di prestazioni e durata delle unità migliori. Le unità SSD avranno una durata maggiore e prestazioni di scrittura massime superiori se una parte della loro capacità non è allocata. Per le unità associate a un gruppo di volumi, la capacità non allocata è composta dalla capacità libera del gruppo (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile riservata come capacità di ottimizzazione aggiuntiva. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, pertanto, non è disponibile per la creazione di volumi.

4. Fare clic su **Save**.

   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**.

Risultati

Se si modifica il livello RAID per un gruppo di volumi, System Manager modifica i livelli RAID di tutti i volumi che compongono il gruppo di volumi. Le prestazioni potrebbero essere leggermente influenzate durante l'operazione.

Abilitare o disabilitare il provisioning delle risorse su gruppi di volumi e pool esistenti in SANtricity System Manager

Per qualsiasi unità compatibile con DULBE, puoi abilitare o disabilitare il provisioning delle risorse sui volumi esistenti in un pool o in un gruppo di volumi.

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background. Tutti i blocchi di unità assegnati al volume sono deallocati (unmapped), il che può migliorare la durata degli SSD e aumentare le prestazioni massime di scrittura.

Per impostazione predefinita, il provisioning delle risorse è abilitato sui sistemi in cui le unità supportano DULBE. Non è necessario abilitare il provisioning delle risorse a meno che non sia stato precedentemente disabilitato.

Prima di iniziare

- È necessario disporre di un array di storage EF300 o EF600.

  DULBE non è supportato sugli array di storage EF300C o EF600C al momento.

- È necessario disporre di gruppi o pool di volumi SSD, in cui tutte le unità supportano la funzionalità di ripristino degli errori NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE). Altrimenti, l'opzione di provisioning delle risorse non è disponibile.

Informazioni su questa attività

Quando si abilita il provisioning delle risorse per gruppi di volumi e pool esistenti, tutti i volumi nel gruppo di volumi o pool selezionato vengono modificati per consentire la deallocazione dei blocchi. Questo processo potrebbe comportare un'operazione in background per garantire un'allocazione coerente alla granularità di unmap. Questa operazione non esegue l'unmap di alcuno spazio. Una volta completata l'operazione in background, il sistema operativo deve eseguire l'unmap di tutti i blocchi non utilizzati per creare spazio libero.

Quando si disabilita il provisioning delle risorse per gruppi o pool di volumi esistenti, un'operazione in background riscrive tutti i blocchi logici in ogni volume. I dati esistenti rimangono intatti. Le operazioni di scrittura mappano o assegnano risorse ai blocchi sulle unità associate al gruppo o pool di volumi.

Per i nuovi gruppi e pool di volumi, puoi abilitare o disabilitare il provisioning delle risorse dal **Settings › Sistema › Impostazioni aggiuntive › Abilita/Disabilita volumi con provisioning delle risorse**.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona un pool o un gruppo di volumi dall'elenco.

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

3. Seleziona **Attività non comuni** e quindi **Abilita il provisioning delle risorse** oppure **Disabilita il provisioning delle risorse**.
4. Nella finestra di dialogo, conferma l'operazione.

Se hai riattivato DULBE — Dopo il completamento dell'operazione in background, potrebbe essere necessario riavviare l'host affinché rilevi le modifiche alla configurazione DULBE e quindi rimontare tutti i filesystem.

Abilitare o disabilitare il provisioning delle risorse per nuovi gruppi di volumi o pool in SANtricity System Manager

Se in precedenza avevi disabilitato la funzionalità predefinita per il provisioning delle risorse, puoi riattivarla per tutti i nuovi gruppi o pool di volumi SSD che crei. Puoi anche disabilitare nuovamente l'impostazione.

Il provisioning delle risorse è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background. Tutti i blocchi di unità assegnati al volume sono deallocati (unmapped), il che può migliorare la durata degli SSD e aumentare le prestazioni massime di scrittura.

Per impostazione predefinita, il provisioning delle risorse è abilitato sui sistemi in cui le unità supportano DULBE.

Prima di iniziare

- È necessario disporre di un array di storage EF300 o EF600.
- È necessario disporre di gruppi o pool di volumi SSD, in cui tutte le unità supportano la capacità di ripristino degli errori NVMe Deallocated or Unwritten Logical Block Error Enable (DULBE).

> DULBE non è supportato sugli array di storage EF300C o EF600C al momento.

Informazioni su questa attività

Quando si riattiva il provisioning delle risorse per nuovi gruppi di volumi o pool, vengono interessati solo i gruppi di volumi e i pool appena creati. I gruppi di volumi e i pool esistenti con il provisioning delle risorse abilitato rimarranno invariati.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive** e poi fai clic su **Abilita/Disabilita volumi con provisioning delle risorse**.

   La descrizione dell'impostazione indica se il provisioning delle risorse è attualmente abilitato o disabilitato.
3. Nella finestra di dialogo, conferma l'operazione.

Risultati

L'attivazione o la disattivazione del provisioning delle risorse ha effetto solo sui nuovi pool SSD o gruppi di volumi che crei. I pool o gruppi di volumi esistenti rimangono invariati.

Abilitare la sicurezza per un pool o un gruppo di volumi in SANtricity System Manager

È possibile abilitare Drive Security per un pool o un gruppo di volumi per impedire l'accesso non autorizzato ai dati presenti sulle unità contenute nel pool o nel gruppo di volumi. L'accesso in lettura e scrittura alle unità è consentito solo tramite un controller configurato con una chiave di sicurezza.

Prima di iniziare

- La funzionalità Drive Security deve essere abilitata.
- È necessario creare una chiave di sicurezza.
- Il pool o il gruppo di volumi deve trovarsi in uno stato ottimale.
- Tutti i dischi nel pool o nel gruppo di volumi devono essere dischi secure-capable.

Informazioni su questa attività

Se si desidera utilizzare Drive Security, selezionare un pool o un gruppo di volumi che sia secure-capable. Un pool o un gruppo di volumi può contenere sia drive secure-capable che drive non secure-capable, ma tutti i drive devono essere secure-capable per poter utilizzare le loro capacità di crittografia.

Dopo aver abilitato la sicurezza, puoi rimuoverla solo eliminando il pool o il gruppo di volumi e quindi cancellando i dischi.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona il pool o il gruppo di volumi su cui desideri abilitare la sicurezza, quindi fai clic su **More › Enable**

security.

Viene visualizzata la finestra di dialogo Confirm Enable Security.

3. Conferma che vuoi abilitare la sicurezza per il pool o il gruppo di volumi selezionato, quindi fai clic su **Abilita**.

Gestisci Cache SSD

Come funziona la Cache SSD nel software SANtricity

La funzionalità Cache SSD è una soluzione basata sul controller che memorizza nella cache i dati a cui si accede più frequentemente (dati "caldi") su unità a stato solido (SSD) a bassa latenza per accelerare dinamicamente le prestazioni del sistema. Cache SSD viene utilizzata esclusivamente per le letture dell'host.

Cache SSD rispetto alla cache primaria

Cache SSD è una cache secondaria da utilizzare insieme alla cache primaria nella memoria ad accesso casuale dinamica (DRAM) del controller.

Cache SSD funziona in modo diverso rispetto alla cache primaria:

- Per la cache primaria, ogni operazione di I/O deve far transitare i dati attraverso la cache per poter eseguire l'operazione.

  Nella cache primaria, i dati vengono memorizzati nella DRAM dopo una lettura da parte dell'host.

- Cache SSD viene utilizzata solo se è vantaggioso posizionare i dati nella cache per migliorare le prestazioni complessive del sistema.

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

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

Come viene utilizzata la Cache SSD

La memorizzazione intelligente nella cache posiziona i dati su un'unità a bassa latenza, così le risposte alle future richieste di tali dati possono avvenire molto più rapidamente. Se un programma richiede dati presenti nella cache (chiamato un "cache hit"), allora l'unità a bassa latenza può gestire quella transazione. Altrimenti, si verifica un "cache miss" e i dati devono essere recuperati dall'unità originale, più lenta. Man mano che si verificano più cache hit, le prestazioni complessive migliorano.

Quando un programma host accede alle unità dell'array di storage, i dati vengono memorizzati nella Cache SSD. Quando lo stesso programma host accede nuovamente agli stessi dati, questi vengono letti dalla Cache SSD invece che dai dischi rigidi. I dati a cui si accede più frequentemente vengono memorizzati nella Cache SSD. I dischi rigidi vengono consultati solo quando i dati non possono essere letti dalla Cache SSD.

Cache SSD viene utilizzata solo quando è vantaggioso posizionare i dati nella cache per migliorare le prestazioni complessive del sistema.

Quando la CPU deve elaborare i dati di lettura, segue i passaggi seguenti:

1. Verifica cache DRAM.
2. Se non viene trovato nella cache DRAM, controlla quindi la Cache SSD.
3. Se non trovato nella Cache SSD, recupera dal disco rigido. Se i dati sono ritenuti degni di essere memorizzati nella Cache SSD, copiali nella Cache SSD.

Prestazioni migliorate

Copiare i dati più utilizzati (hot spot) nella Cache SSD consente un funzionamento più efficiente del disco rigido, una latenza ridotta e velocità di lettura e scrittura accelerate. L'utilizzo di SSD ad alte prestazioni per memorizzare nella cache i dati dai volumi HDD migliora le prestazioni I/O e i tempi di risposta.

Vengono utilizzati semplici meccanismi di I/O del volume per spostare i dati da e verso la Cache SSD. Dopo che i dati sono stati memorizzati nella Cache SSD e sugli SSD, le successive letture di tali dati vengono eseguite sulla Cache SSD, eliminando così la necessità di accedere al volume HDD.

Cache SSD e la funzione Drive Security

Per utilizzare Cache SSD su un volume che utilizza anche Drive Security (is secure-enabled), le funzionalità di Drive Security del volume e della Cache SSD devono corrispondere. Se non corrispondono, il volume non sarà secure-enabled.

Implementare Cache SSD

Per implementare Cache SSD, procedi come segue:

1. Crea la Cache SSD.
2. Associa la Cache SSD ai volumi per cui vuoi implementare la cache di lettura SSD.

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

Scopri le limitazioni della Cache SSD nel software SANtricity

Scopri le limitazioni relative all'utilizzo della Cache SSD sul tuo array di storage.

Restrizioni

- Qualsiasi volume assegnato all'utilizzo della Cache SSD di un controller non è idoneo per un trasferimento automatico del bilanciamento del carico.
- Attualmente, è supportata una sola Cache SSD per array di storage.
- La capacità massima di Cache SSD utilizzabile su un array di storage è di 10 TB.
- Cache SSD non è supportata sulle immagini snapshot.
- Se si importano o esportano volumi con Cache SSD abilitata o disabilitata, i dati memorizzati nella cache non vengono importati o esportati.
- Non è possibile rimuovere l'ultima unità in una Cache SSD senza prima eliminare la Cache SSD.

Restrizioni con Drive Security

- È possibile abilitare la sicurezza sulla Cache SSD solo quando si crea la Cache SSD. Non è possibile abilitare la sicurezza in un secondo momento come si può fare su un volume.
- Se si combinano unità compatibili con la sicurezza con unità non compatibili con la sicurezza nella Cache SSD, non è possibile abilitare Drive Security per queste unità.
- I volumi secure-enabled devono avere una Cache SSD secure-enabled.

Creare una Cache SSD in SANtricity System Manager

Per accelerare dinamicamente le prestazioni del sistema, è possibile utilizzare la funzionalità Cache SSD per memorizzare nella cache i dati a cui si accede più frequentemente (dati "caldi") su unità a stato solido (SSD) a bassa latenza. Cache SSD viene utilizzata esclusivamente per le letture dell'host.

Prima di iniziare

Il tuo array di archiviazione deve contenere alcune SSD.

Informazioni su questa attività

Quando si crea una nuova Cache SSD, è possibile utilizzare un disco singolo o più unità. Poiché la cache di lettura si trova nell'array di storage, la cache è condivisa tra tutte le applicazioni che utilizzano l'array di storage. Si selezionano i volumi che si desidera memorizzare nella cache e la memorizzazione nella cache sarà automatica e dinamica.

Segui queste linee guida quando crei una nuova Cache SSD.

- È possibile abilitare la sicurezza sulla Cache SSD solo al momento della sua creazione, non in un secondo momento.
- È supportata una sola Cache SSD per array di storage.
- Se solo un volume ha la Cache SSD abilitata, l'intera Cache SSD verrà assegnata al controller proprietario di quel volume.
- La capacità massima utilizzabile della Cache SSD su un array di storage dipende dalla capacità della cache primaria del controller.
- Cache SSD non è supportata sulle immagini snapshot.
- Se si importano o esportano volumi con Cache SSD abilitata o disabilitata, i dati memorizzati nella cache non vengono importati o esportati.
- Qualsiasi volume assegnato all'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 protezione, crea una Cache SSD abilitata per la protezione.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic su **Create › SSD Cache**.

   Viene visualizzata la finestra di dialogo Crea Cache SSD.

3. Inserisci un nome per la Cache SSD.
4. Seleziona la Cache SSD candidata da utilizzare in base alle seguenti caratteristiche.

Caratteristica	Usa
Capacità	Mostra la capacità disponibile in GiB. Seleziona la capacità per le esigenze di archiviazione della tua applicazione. La capacità massima per Cache SSD dipende dalla capacità della cache primaria del controller. Se si assegna alla Cache SSD più della quantità massima, la capacità in eccesso risulterà inutilizzabile. La capacità della Cache SSD contribuisce alla capacità totale allocata.
Unità totali	Mostra il numero di dischi disponibili per questa Cache SSD. Seleziona il candidato SSD con il numero di dischi desiderato.
Compatibile con la sicurezza	Indica se il candidato Cache SSD è composto interamente da unità con funzionalità di sicurezza, che possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Se desideri creare una Cache SSD abilitata alla sicurezza, cerca **Yes - FDE** o **Yes - FIPS** nella colonna Secure-capable.
Abilitare la sicurezza?	Offre la possibilità di abilitare la funzione Drive Security con le unità compatibili con la sicurezza. Se si desidera creare una Cache SSD con sicurezza abilitata, selezionare la check box Abilita sicurezza. Una volta attivata, la sicurezza non può essere disattivata. È possibile attivare la sicurezza sulla Cache SSD solo al momento della sua creazione, non in un secondo momento.
Compatibile DA	Indica se Data Assurance (DA) è disponibile per questo candidato Cache SSD. Data Assurance (DA) verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati dai controller alle unità. Se desideri utilizzare DA, seleziona un candidato Cache SSD che supporti DA. Questa opzione è disponibile solo quando la funzionalità DA è stata abilitata. Cache SSD può contenere sia unità DA-capable che non DA-capable, ma tutte le unità devono essere DA-capable per poter utilizzare DA.

5. Associa la Cache SSD ai volumi per i quali desideri implementare la cache di lettura SSD. Per abilitare la Cache SSD sui volumi compatibili esistenti che sono mappati agli host immediatamente, seleziona la check box **Abilita Cache SSD sui volumi compatibili esistenti che sono mappati agli host**.

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

6. Fai clic su **Create**.

Modifica le impostazioni della Cache SSD in SANtricity System Manager

È possibile modificare il nome della Cache SSD e visualizzarne lo stato, la capacità massima e attuale, lo stato di Drive Security e Data Assurance, nonché i volumi e le unità

associati.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la Cache SSD che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni Cache SSD.

3. Rivedi o modifica le impostazioni della Cache SSD, se necessario.

Dettagli del campo

Impostazione	Descrizione
Nome	Visualizza il nome della Cache SSD, che è possibile modificare. È necessario specificare un nome per la Cache SSD.
Caratteristiche	Mostra lo stato della Cache SSD. Gli stati possibili includono: • Ottimale • Sconosciuto • Degradato • Errore (Uno stato di errore genera un evento MEL critico.) • Sospeso
Capacità	Mostra la capacità attuale e la capacità massima consentita per la Cache SSD. La capacità massima consentita per la Cache SSD dipende dalla dimensione della cache primaria 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 sicurezza dell'unità e di protezione dei dati per la Cache SSD. • **Secure-capable** — Indica se la Cache SSD è composta interamente da unità secure-capable. Un'unità secure-capable è un'unità autocrittografante in grado di proteggere i dati da accessi non autorizzati. • **Secure-enabled** — Indica se la sicurezza è abilitata sulla Cache SSD. • **Compatibile con DA** — Indica se la Cache SSD è composta interamente da unità compatibili con DA. Un'unità compatibile con DA può verificare e correggere gli errori che potrebbero verificarsi durante la comunicazione dei dati tra l'host e l'array di storage.
Oggetti associati	Mostra i volumi e le unità associati alla Cache SSD.

4. Fare clic su **Save**.

Visualizza le statistiche della Cache SSD in SANtricity System Manager

È possibile visualizzare le statistiche per la Cache SSD, come letture, scritture, cache hit,

percentuale di allocazione della cache e percentuale di utilizzo della cache.

Le statistiche nominali, che costituiscono un sottoinsieme delle statistiche dettagliate, vengono visualizzate nella finestra di dialogo Visualizza statistiche Cache SSD. È possibile visualizzare statistiche dettagliate per la Cache SSD solo quando si esportano tutte le statistiche SSD in un `.csv` file.

Durante la revisione e l'interpretazione delle statistiche, tieni presente che alcune interpretazioni sono derivate dall'osservazione di una combinazione di statistiche.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la Cache SSD per la quale desideri visualizzare le statistiche, quindi fai clic su **Altro › Visualizza statistiche Cache SSD**.

   Viene visualizzata la finestra di dialogo Visualizza statistiche Cache SSD e vengono visualizzate le statistiche nominali per la Cache SSD selezionata.

   Dettagli del campo

Impostazioni	Descrizione
Letture	Mostra il numero totale di letture dell'host dai volumi con Cache SSD abilitata. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Scritture	Il numero totale di scritture dell'host sui volumi con Cache SSD abilitata. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Cache hit	Mostra il numero di cache hit.
Cache hit %	Mostra la percentuale di cache hit. Questo numero è derivato da cache hit / (letture + scritture). La percentuale di cache hit dovrebbe essere superiore al 50 percento per un funzionamento efficace della Cache SSD.
Allocazione cache %	Mostra la percentuale di spazio di archiviazione della Cache SSD allocato, espressa come percentuale dello spazio di archiviazione della Cache SSD disponibile per questo controller ed è calcolata come rapporto tra byte allocati e byte disponibili.
Utilizzo cache %	Mostra la percentuale di spazio di archiviazione della Cache SSD che contiene dati provenienti da volumi abilitati, espressa come percentuale dello spazio di archiviazione della Cache SSD allocato. Questo valore 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 (sia nominali che dettagliate).

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

Gestisci la capacità riservata

Come funziona la capacità riservata nel software SANtricity

La capacità riservata viene creata automaticamente quando vengono fornite operazioni di servizio di copia, come Snapshot o operazioni di mirroring asincrono, per i tuoi volumi.

Lo scopo della capacità riservata è memorizzare le modifiche ai dati su questi volumi, qualora si verifichi un problema. Come i volumi, la capacità riservata viene creata da pool o gruppi di volumi.

Copia gli oggetti del servizio che utilizzano la capacità riservata

La capacità riservata è lo storage sottostante utilizzato da questi oggetti del servizio di copia:

- Gruppi di Snapshot
- Lettura/scrittura di volumi Snapshot
- Volumi dei membri del gruppo di coerenza
- Volumi a coppia speculare

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

Volumi thin e capacità riservata

Per un volume thin, se è stata raggiunta la capacità massima dichiarata di 256 TiB, non è possibile aumentarne la capacità. Assicurati che la capacità riservata del volume thin sia impostata su una dimensione superiore alla capacità massima dichiarata. (Un volume thin è sempre thinly-provisioned, il che significa che la capacità viene allocata man mano che i dati vengono scritti sul volume.)

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

- Se la capacità riservata di un volume thin non funziona, il volume thin stesso non passerà automaticamente allo stato Failed. Tuttavia, poiché tutte le operazioni di I/O su un volume thin richiedono l'accesso al volume di capacità riservata, le operazioni di I/O restituiranno sempre una Check Condition all'host richiedente. Se il problema di fondo relativo al volume di capacità riservata può essere risolto, il volume di capacità riservata tornerà allo stato Optimal e il volume thin tornerà a funzionare correttamente.
- Se si utilizza un volume thin esistente per completare una coppia mirror asincrona, tale volume thin viene reinizializzato con un nuovo volume di capacità riservata. Solo i blocchi di cui è stato effettuato il provisioning sul lato primario vengono trasferiti durante il processo di sincronizzazione iniziale.

Avvisi di capacità

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

Quando la capacità riservata di un volume oggetto copy service si sta avvicinando al limite di riempimento, viene emesso un avviso all'utente. Per impostazione predefinita, questo avviso viene emesso quando il

volume di capacità riservata è pieno al 75%; tuttavia, puoi regolare questa soglia di avviso verso l'alto o verso il basso secondo necessità. Se ricevi questo avviso, puoi aumentare la capacità del volume di capacità riservata in quel momento. Ogni copy service object può essere configurato in modo indipendente a questo riguardo.

Volumi di capacità riservata orfani

Un volume di capacità riservata orfano è un volume che non memorizza più dati per le operazioni del servizio di copia perché il suo oggetto del servizio di copia associato è stato eliminato. Quando l'oggetto del servizio di copia è stato eliminato, anche il suo volume di capacità riservata avrebbe dovuto essere eliminato. Tuttavia, il volume di capacità riservata non è stato eliminato.

Poiché i volumi di capacità riservata orfani non vengono acceduti da alcun host, sono candidati al recupero. Elimina manualmente il volume di capacità riservata orfano in modo da poter utilizzare la sua capacità per altre operazioni.

System Manager ti avvisa della presenza di volumi di capacità riservata orfani con un messaggio "Recupera capacità inutilizzata" nell'area Notifiche della pagina iniziale. Puoi fare clic su **Recupera capacità inutilizzata** per visualizzare la finestra di dialogo Recupera capacità inutilizzata, dove puoi eliminare il volume di capacità riservata orfano.

Caratteristiche della capacità di riserva

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

Aumentare la capacità riservata in SANtricity System Manager

È possibile aumentare la capacità riservata, ovvero la capacità fisicamente allocata utilizzata per qualsiasi operazione di copy service su un oggetto di archiviazione.

Per le operazioni di snapshot, in genere è il 40 percento del volume di base; per le operazioni di mirroring asincrono, in genere è il 20 percento del volume di base. In genere, si aumenta la capacità riservata quando si riceve un avviso che la capacità riservata dell'oggetto di archiviazione sta per esaurirsi.

Prima di iniziare

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

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

Informazioni su questa attività

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

- Gruppo Snapshot
- Volume Snapshot
- Volume membro del gruppo di coerenza
- Volume della coppia mirrorata

Utilizza una percentuale elevata se ritieni che il volume primario subirà molte modifiche o se la durata di una particolare operazione di copy service sarà molto lunga.

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la scheda **Reserved Capacity**.
3. Seleziona l'oggetto storage per cui desideri aumentare la capacità riservata, quindi fai clic su **Aumenta capacità**.

   Viene visualizzata la finestra di dialogo Increase Reserved Capacity.

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

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

5. Fai clic su **Increase**.

Risultati

System Manager esegue le seguenti azioni:

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

Ridurre la capacità riservata in SANtricity System Manager

L'opzione Riduci capacità consente di diminuire la capacità riservata per i seguenti oggetti di archiviazione: gruppo di snapshot, volume di snapshot e volume membro del gruppo di coerenza. È possibile ridurre la capacità riservata solo delle quantità utilizzate per aumentarla.

Prima di iniziare

- L'oggetto di archiviazione deve contenere più di un volume di capacità riservata.
- L'oggetto di archiviazione non deve essere un volume di coppia mirror.
- Se l'oggetto di archiviazione è un volume snapshot, deve essere un volume snapshot disabilitato.
- Se l'oggetto di archiviazione è un gruppo di snapshot, allora non deve contenere alcuna immagine snapshot associata.

Informazioni su questa attività

Esaminare le seguenti linee guida:

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona l'oggetto di archiviazione per cui desideri diminuire la capacità riservata, quindi fai clic su **Diminuisci capacità**.

   Viene visualizzata la finestra di dialogo Decrease Reserved Capacity.

4. Seleziona la quantità di capacità di cui desideri diminuire la capacità riservata, quindi fai clic su **Riduci**.

Risultati

System Manager esegue le seguenti azioni:

- Aggiorna la capacità per l'oggetto di archiviazione.
- Visualizza la nuova capacità riservata aggiornata per l'oggetto di archiviazione.
- Quando si riduce la capacità di un volume snapshot, System Manager passa automaticamente il volume snapshot allo stato Disabilitato. Disabilitato significa che il volume snapshot non è attualmente associato a una snapshot image e, pertanto, non può essere assegnato a un host per I/O.

Modificare le impostazioni di capacità riservata per un gruppo di Snapshot in SANtricity System Manager

È possibile modificare le impostazioni di un gruppo di snapshot per cambiarne il nome, le impostazioni di eliminazione automatica, il numero massimo di immagini snapshot consentite, la percentuale alla quale SANtricity System Manager invia una notifica di avviso sulla capacità riservata, o la policy da utilizzare quando la capacità riservata raggiunge la percentuale massima definita.

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona il gruppo di Snapshot che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Snapshot Group Settings.

4. Modifica le impostazioni del gruppo di Snapshot in base alle esigenze.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del gruppo di Snapshot	Nome
Nome del gruppo di snapshot. È obbligatorio specificare un nome per il gruppo di snapshot.	Eliminazione automatica
Un'impostazione che mantiene il numero totale di immagini Snapshot nel gruppo pari o inferiore a un massimo definito dall'utente. Quando questa opzione è abilitata, System Manager elimina automaticamente l'immagine Snapshot più vecchia del gruppo ogni volta che ne viene creata una nuova, per rispettare il numero massimo di immagini Snapshot consentite per il gruppo.	Limite delle immagini Snapshot
Un valore configurabile che specifica il numero massimo di immagini di Snapshot consentite per un gruppo di Snapshot.	calendario di Snapshot
Se sì, viene impostato un calendario per la creazione automatica di Snapshot.	**Impostazioni di capacità riservata**

Impostazione	Descrizione
Avvisami quando…	Utilizzare il selettore a rotella per regolare la percentuale al punto in cui System Manager invia una notifica di avviso quando la capacità riservata per un gruppo di Snapshot sta per esaurirsi. Quando la capacità riservata per il gruppo di snapshot supera la soglia specificata, System Manager invia un avviso, consentendoti di aumentare la capacità riservata o di eliminare oggetti non necessari.
Politica per la piena capacità riservata	È possibile scegliere una delle seguenti policy: • **Elimina l'immagine snapshot più vecchia** — System Manager elimina automaticamente l'immagine snapshot più vecchia nel gruppo di snapshot, liberando la capacità riservata dell'immagine snapshot per il riutilizzo all'interno del gruppo. • **Rifiuta le scritture sul volume base** — Quando la capacità riservata raggiunge la percentuale massima definita, System Manager rifiuta qualsiasi richiesta di scrittura I/O sul volume base che ha attivato l'accesso alla capacità riservata.
Oggetti associati	Volume base
Il nome del volume di base utilizzato per il gruppo. Un volume di base è la fonte da cui viene creata un'immagine Snapshot. Può essere un volume thick o thin e viene in genere assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un pool di dischi.	Immagini Snapshot

5. Fai clic su **Salva** per applicare le modifiche alle impostazioni del gruppo di Snapshot.

Modificare le impostazioni di capacità riservata per un volume Snapshot in SANtricity System Manager

È possibile modificare le impostazioni di un volume Snapshot per regolare la percentuale al raggiungimento della quale il sistema invia una notifica di avviso quando la capacità riservata per un volume Snapshot sta per esaurirsi.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona il volume Snapshot che desideri modificare, quindi fai clic su **View/Edit Settings**.

Viene visualizzata la finestra di dialogo Snapshot Volume Reserved Capacity Settings.

4. Modificare le impostazioni di capacità riservata per il volume Snapshot come appropriato.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare il selettore a rotella per regolare il punto percentuale in cui il sistema invia una notifica di avviso quando la capacità riservata per un volume membro sta per essere piena. Quando la capacità riservata per il volume Snapshot supera la soglia specificata, il sistema invia un avviso, permettendoti di aumentare la capacità riservata o di eliminare oggetti non necessari.

5. Fai clic su **Save** per applicare le modifiche alle impostazioni della capacità riservata del volume Snapshot.

Modificare le impostazioni della capacità riservata per un volume membro di un gruppo di coerenza in SANtricity System Manager

È possibile modificare le impostazioni per un volume membro di un gruppo di coerenza per regolare la percentuale al raggiungimento della quale SANtricity System Manager invia una notifica di avviso quando la capacità riservata per un volume membro sta per esaurirsi e per modificare la policy da utilizzare quando la capacità riservata raggiunge la percentuale massima definita.

Informazioni su questa attività

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona il volume del membro del gruppo di coerenza che desideri modificare, quindi fai clic su **Visualizza/Modifica Settings**.

   Viene visualizzata la finestra di dialogo Impostazioni capacità riservata Member Volume.

4. Modificare le impostazioni della capacità riservata per il volume membro come appropriato.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare il selettore a rotella per regolare il punto percentuale al quale System Manager invia una notifica di avviso quando la capacità riservata per un volume membro sta per esaurirsi. Quando la capacità riservata per il volume membro supera la soglia specificata, System Manager invia un avviso, consentendoti di aumentare la capacità riservata o di eliminare oggetti non necessari. La modifica dell'impostazione di Alert per un volume membro comporterà la modifica per *tutti* i volumi membri appartenenti allo stesso consistency group.
Politica per la piena capacità riservata	È possibile scegliere una delle seguenti policy: • **Elimina l'immagine snapshot più vecchia** — System Manager elimina automaticamente l'immagine snapshot più vecchia nel gruppo di coerenza, liberando la capacità riservata al membro per il riutilizzo all'interno del gruppo. • **Rifiuta le scritture sul volume base** — Quando la capacità riservata raggiunge la percentuale massima definita, System Manager rifiuta qualsiasi richiesta di scrittura I/O sul volume base che ha attivato l'accesso alla capacità riservata.

5. Fai clic su **Salva** per applicare le modifiche.

Risultati

System Manager modifica le impostazioni della capacità riservata per il volume membro, così come le impostazioni della capacità riservata per tutti i volumi membri nel gruppo di coerenza.

Modificare le impostazioni di capacità riservata per un volume di coppia mirror in SANtricity System Manager

È possibile modificare le impostazioni di un volume con mirroring per regolare la percentuale di soglia oltre la quale SANtricity System Manager invia una notifica di avviso quando la capacità riservata per un volume con mirroring sta per esaurirsi.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la scheda **Reserved Capacity**.
3. Seleziona il volume della coppia mirrored che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni capacità riservata Mirrored Pair Volume.

4. Modificare le impostazioni di capacità riservata per il volume della coppia mirrorata, se necessario.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare il selettore a rotella per regolare il punto percentuale al quale System Manager invia una notifica di avviso quando la capacità riservata per una coppia mirror sta per esaurirsi. Quando la capacità riservata per la coppia mirror supera la soglia specificata, System Manager invia un avviso, consentendoti di aumentare la capacità riservata. La modifica dell'impostazione di avviso per una coppia mirrorata modifica l'impostazione di avviso per tutte le coppie mirrorate che appartengono allo stesso mirror consistency group.

5. Fai clic su **Salva** per applicare le modifiche.

Annulla un'immagine Snapshot in sospeso in SANtricity System Manager

È possibile annullare un'immagine snapshot in sospeso prima che venga completata. Le snapshot si verificano in modo asincrono e lo stato della snapshot è in sospeso fino al completamento della snapshot. L'immagine snapshot si completa non appena l'operazione di sincronizzazione è completata.

Informazioni su questa attività

Un'immagine Snapshot si trova nello stato Pending a causa delle seguenti condizioni simultanee:

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona il gruppo di snapshot per cui desideri annullare un'immagine snapshot in sospeso, quindi fai clic su **Uncommon Tasks › Cancel pending snapshot image**.
4. Fai clic su **Sì** per confermare che desideri annullare l'immagine snapshot in sospeso.

Eliminare un gruppo di Snapshot in SANtricity System Manager

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

Informazioni su questa attività

Quando un gruppo di snapshot viene eliminato, tutte le immagini snapshot nel gruppo vengono eliminate.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Fai clic sulla scheda **Reserved Capacity**.
3. Seleziona il gruppo di snapshot che desideri eliminare, quindi fai clic su **Uncommon Tasks › Delete snapshot group**.

   Viene visualizzata la finestra di dialogo Conferma eliminazione gruppo Snapshot.

4. Digita `delete` per confermare.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutte le immagini Snapshot associate al gruppo di Snapshot.
- Disabilita tutti i volumi Snapshot associati alle immagini del gruppo Snapshot.
- Elimina la capacità riservata che esiste per il gruppo di snapshot.

Domande frequenti su pool e gruppi di volume per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è un gruppo di volume?

Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)

Che cos'è un pool?

Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)

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

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

Che cos'è la capacità riservata?

La capacità riservata è la capacità fisicamente allocata che memorizza i dati per oggetti del servizio di copia come le immagini snapshot, i volumi dei membri del gruppo di coerenza e i volumi delle coppie mirror.

Il volume di capacità riservata associato a un'operazione del servizio di copia risiede in un pool o in un gruppo di volumi. Si crea la capacità riservata da un pool o da un gruppo di volumi.

Che cos'è la sicurezza FDE/FIPS?

La sicurezza FDE/FIPS si riferisce alle unità compatibili con la crittografia che crittografano i dati durante la scrittura e decrittografano i dati durante la lettura utilizzando una chiave di crittografia univoca. Queste unità compatibili con la crittografia impediscono l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage.

Le unità con funzionalità di sicurezza possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Le unità FIPS sono state sottoposte a test di certificazione.

> Per i volumi che richiedono il supporto FIPS, utilizzare solo unità FIPS. La combinazione di unità FIPS e FDE in un gruppo o pool di volumi comporterà che tutte le unità vengano trattate come unità FDE. Inoltre, un'unità FDE non può essere aggiunta o utilizzata come hot spare in un gruppo o pool di volumi composto esclusivamente da unità FIPS.

Che cos'è un controllo di ridondanza?

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

È possibile eseguire questo controllo solo su un pool o gruppo di volumi alla volta. Un controllo di ridondanza dei volumi esegue le seguenti azioni:

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

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

Quali sono le differenze tra pool e gruppi di volume?

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

- I dati in un pool vengono memorizzati in modo casuale su tutti i dischi del pool, a differenza dei dati in un gruppo di volumi, che vengono memorizzati sullo stesso set di dischi.
- Un pool presenta un minore peggioramento delle performance in caso di guasto di un disco e richiede meno tempo per essere ricostruito.
- Un pool ha una capacità di preservazione integrata; pertanto non richiede hot spare drive dedicati.
- Un pool consente di raggruppare un gran numero di dischi.
- Un pool non necessita di un livello RAID specificato.

Perché dovrei voler configurare manualmente un pool?

I seguenti esempi descrivono perché si potrebbe voler configurare manualmente un pool.

- Se sul tuo array di storage sono presenti più applicazioni e non desideri che competano per le stesse

risorse del disco, potresti considerare di creare manualmente un pool più piccolo per una o più delle applicazioni.

È possibile assegnare solo uno o due volumi anziché assegnare il carico di lavoro a un pool di grandi dimensioni con molti volumi su cui distribuire i dati. La creazione manuale di un pool separato dedicato al carico di lavoro di una specifica applicazione può consentire alle operazioni dell'array di storage di essere eseguite più rapidamente, con meno contesa.

Per creare manualmente un pool: selezionare **Archiviazione**, quindi **Pool & gruppi di volumi**. Dalla scheda All Capacity, fare clic su **Create › Pool**.

- Se sono presenti più pool dello stesso tipo di drive, viene visualizzato un messaggio che indica che System Manager non può consigliare automaticamente i drive per un pool. Tuttavia, puoi aggiungere manualmente i drive a un pool esistente.

  Per aggiungere manualmente dischi a un pool esistente: dalla pagina Pools & Volume Groups, selezionare il pool e quindi fare clic su **Add Capacity**.

Perché gli avvisi di capacità sono importanti?

Gli avvisi di capacità indicano quando aggiungere unità a un pool. Un pool necessita di una capacità libera sufficiente per eseguire correttamente le operazioni sull'array di storage. È possibile evitare interruzioni a queste operazioni configurando SANtricity System Manager in modo che invii avvisi quando la capacità libera di un pool raggiunge o supera una percentuale specificata.

Imposti questa percentuale quando crei un pool utilizzando l'opzione **Configurazione automatica del pool** o l'opzione **Crea pool**. Se scegli l'opzione automatica, le impostazioni predefinite determinano automaticamente quando ricevi le notifiche di avviso. Se scegli di creare manualmente il pool, puoi determinare le impostazioni di notifica degli avvisi; oppure, se preferisci, puoi accettare le impostazioni predefinite. Puoi modificare queste impostazioni successivamente in **Impostazioni › Avvisi**.

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

Perché non posso aumentare la mia capacità di conservazione?

Se hai creato volumi su tutta la capacità utilizzabile disponibile, potresti non essere in grado di aumentare la capacità di preservazione.

La capacità di conservazione è la quantità di capacità (numero di dischi) riservata in un pool per supportare potenziali guasti dei dischi. Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione a seconda del numero di dischi nel pool. Se hai creato volumi su tutta la capacità utilizzabile disponibile, non puoi aumentare la capacità di conservazione senza aggiungere capacità al pool, aggiungendo dischi o eliminando volumi.

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

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

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

SANtricity System Manager imposta dei limiti su quante unità è possibile rimuovere da un pool.

- Non è possibile ridurre il numero di dischi in un pool a meno di 11 dischi.
- Non è possibile rimuovere i dischi se non c'è capacità libera sufficiente nel pool per contenere i dati dei dischi rimossi quando tali dati vengono ridistribuiti ai dischi rimanenti nel pool.
- È possibile rimuovere un massimo di 60 dischi alla volta. Se si selezionano più di 60 dischi, l'opzione Rimuovi dischi viene disabilitata. Se è necessario rimuovere più di 60 dischi, ripetere l'operazione Rimuovi dischi.

Quali tipi di media sono supportati per un drive?

Sono supportati i seguenti tipi di media: Hard Disk Drive (HDD) e Solid State Disk (SSD).

Perché alcuni dischi non vengono visualizzati?

Nella finestra di dialogo Aggiungi capacità, non tutte le unità sono disponibili per aggiungere capacità a un pool o a un gruppo di volumi esistente.

I dischi non sono idonei per nessuno dei seguenti motivi:

- Un'unità deve essere non assegnata e non abilitata per la protezione. Le unità già appartenenti a un altro pool, a un altro gruppo di volumi o configurate come hot spare non sono idonee. Se un'unità non è assegnata ma è abilitata per la protezione, è necessario cancellarla manualmente affinché diventi idonea.
- Un disco che si trova in uno stato non ottimale non è idoneo.
- Se la capacità di un drive è troppo piccola, non è idonea.
- Il tipo di supporto dell'unità deve corrispondere all'interno del pool o del gruppo di volumi. Non è possibile combinare i seguenti:
  - Dischi rigidi (HDDs) con Solid State Disks (SSDs)
  - NVMe con unità SAS
  - Unità con dimensioni dei blocchi di volume di 512 byte e 4KiB
- Se un pool o un gruppo di volumi contiene tutte unità secure-capable, le unità non secure-capable non vengono elencate.
- Se un pool o un gruppo di volumi contiene tutte unità Federal Information Processing Standards (FIPS), le unità non-FIPS non vengono elencate.
- Se un pool o un gruppo di volumi contiene tutte unità compatibili con Data Assurance (DA) e c'è almeno un volume abilitato per DA nel pool o nel gruppo di volumi, un'unità non compatibile con DA non è idonea, quindi non può essere aggiunta a quel pool o gruppo di volumi. Tuttavia, se nel pool o nel gruppo di volumi non è presente alcun volume abilitato per DA, un'unità non compatibile con DA può essere aggiunta a quel pool o gruppo di volumi. Se si decide di combinare queste unità, tenere presente che non sarà possibile creare alcun volume abilitato per DA.

> La capacità del tuo array di storage può essere aumentata aggiungendo nuovi dischi o eliminando pool o gruppi di volumi.

Come posso mantenere la protezione dalla perdita di shelf/cassetto?

Per mantenere la protezione contro la perdita di shelf/cassetto per un pool o un gruppo di volumi, utilizzare i

criteri specificati nella tabella seguente.

Livello	Criteri per la protezione contro la perdita di shelf/cassetti	Numero minimo di shelf/cassetti richiesti
Pool	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 dischi da ciascun cassetto.	6 per scaffali 5 per cassetti
RAID 6	Il gruppo di volumi contiene al massimo due dischi in un singolo shelf o drawer.	3
RAID 3 o RAID 5	Ciascun disco del gruppo di volumi è alloggiato in uno shelf o cassetto separato.	3
RAID 1	Ciascun disco in una coppia mirror deve essere collocato in uno shelf o cassetto separato.	2
RAID 0	Impossibile ottenere la protezione contro la perdita di ripiano/cassetto.	Non applicabile

La protezione contro la perdita 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 di accesso a uno shelf o a un cassetto, e di conseguenza a un altro disco nel pool o nel gruppo di volumi, causa la perdita di dati.

Qual è il posizionamento ottimale dei dischi per pool e gruppi di volumi?

Quando si creano pool e gruppi di volumi, assicurarsi di bilanciare la selezione dei dischi tra gli slot dei dischi superiori e inferiori.

Per i controller EF600 e EF300, gli slot per unità da 0 a 11 sono collegati a un bridge PCI, mentre gli slot da 12 a 23 sono collegati a un bridge PCI diverso. Per prestazioni ottimali, è consigliabile bilanciare la selezione delle unità includendo un numero approssimativamente uguale di unità dagli slot superiori e inferiori. Questa disposizione garantisce che i volumi non raggiungano un limite di larghezza di banda prima del necessario.

Quale livello RAID è il più adatto alla 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 delle applicazioni che accedono al gruppo di volumi. Utilizzare la pagina Performance per ottenere queste percentuali.

Livelli RAID e prestazioni delle applicazioni

RAID si basa su una serie di configurazioni, chiamate livelli, per determinare come i dati utente e di ridondanza vengono scritti e recuperati dalle unità. Ogni livello RAID offre caratteristiche di performance diverse. Le applicazioni con un'elevata percentuale di lettura otterranno buone performance utilizzando volumi RAID 5 o volumi RAID 6 grazie all'eccellente performance di lettura delle configurazioni RAID 5 e RAID 6.

Le applicazioni con una bassa percentuale di lettura (ad alta intensità di scrittura) non offrono prestazioni ottimali su volumi RAID 5 o volumi RAID 6. Il peggioramento delle performance è il risultato del modo in cui un controller scrive i dati e i dati di ridondanza sui dischi in un gruppo di volumi RAID 5 o un gruppo di volumi RAID 6.

Seleziona un livello RAID in base alle seguenti informazioni.

RAID 0

- **Descrizione**
  - Modalità non ridondante, striping.
- **Come funziona**
  - RAID 0 distribuisce i dati su tutti i dischi del gruppo di volumi.
- **Funzionalità di protezione dei dati**
  - RAID 0 non è consigliato per esigenze di elevata disponibilità. RAID 0 è più indicato per dati non critici.
  - Se un disco singolo del gruppo di volumi si guasta, tutti i volumi associati smettono di funzionare e tutti i dati vengono persi.
- **Requisiti relativi al numero di drive**
  - È necessario almeno un disco per il livello RAID 0.
  - I gruppi di volumi RAID 0 possono avere più di 30 drive.
  - È possibile creare un gruppo di volumi che includa tutti i dischi nell'array di storage.

RAID 1 o RAID 10

- **Descrizione**
  - Modalità striping/mirror.
- **Come funziona**
  - RAID 1 utilizza il mirroring del disco per scrivere dati su due dischi duplicati contemporaneamente.
  - RAID 10 utilizza lo striping delle unità per distribuire i dati su un insieme di coppie di dischi mirrorati.
- **Funzionalità di protezione dei dati**
  - RAID 1 e RAID 10 offrono prestazioni elevate e la migliore disponibilità dei dati.
  - RAID 1 e RAID 10 utilizzano il mirroring dei dischi per creare una copia esatta da un disco a un altro disco.
  - Se una delle unità in una coppia di unità si guasta, l'array di storage può passare istantaneamente all'altra unità senza alcuna perdita di dati o servizio.
  - Il guasto di un disco singolo causa il degrado dei volumi associati. Il disco mirror consente l'accesso ai dati.
  - Il guasto di una coppia di dischi in un gruppo di volumi provoca il malfunzionamento di tutti i volumi associati e potrebbe verificarsi una perdita di dati.

- **Requisiti relativi al numero di drive**
  - Per il RAID 1 sono necessari almeno due dischi: uno per i dati utente e uno per i dati mirrorati.
  - Se selezioni quattro o più dischi, RAID 10 viene configurato automaticamente sul gruppo di volumi: due dischi per i dati utente e due dischi per i dati mirrorati.
  - Il gruppo di volumi deve contenere un numero pari di unità. Se il numero di unità non è pari e alcune unità rimangono non assegnate, vai su **Pools & Volume Groups** per aggiungere altre unità al gruppo di volumi e riprovare l'operazione.
  - I gruppi di volumi RAID 1 e RAID 10 possono avere più di 30 dischi. Un gruppo di volumi può essere creato includendo tutti i dischi nell'array di storage.

RAID 5

- **Descrizione**
  - Modalità I/O elevato.
- **Come funziona**
  - I dati utente e le informazioni ridondanti (parità) sono distribuiti tra i dischi.
  - La capacità equivalente di un drive viene utilizzata per le informazioni ridondanti.
- **Funzionalità di protezione dei dati**
  - Se un disco singolo si guasta in un gruppo di volumi RAID 5, tutti i volumi associati risultano degradati. Le informazioni ridondanti consentono comunque l'accesso ai dati.
  - Se due o più unità si guastano in un gruppo di volumi RAID 5, tutti i volumi associati smettono di funzionare e tutti i dati vengono persi.
- **Requisiti relativi al numero di drive**
  - È necessario disporre di almeno tre dischi nel gruppo di volumi.
  - In genere, sei limitato a un massimo di 30 dischi nel gruppo di volumi.

RAID 6

- **Descrizione**
  - Modalità I/O elevato.
- **Come funziona**
  - I dati utente e le informazioni ridondanti (doppia parità) sono distribuiti a strisce sui dischi.
  - Viene utilizzata una capacità equivalente a due dischi per le informazioni ridondanti.
- **Funzionalità di protezione dei dati**
  - Se uno o due dischi si guastano in un gruppo di volumi RAID 6, tutti i volumi associati risultano degradati, ma le informazioni ridondanti consentono comunque l'accesso ai dati.
  - Se tre o più unità si guastano in un gruppo di volumi RAID 6, tutti i volumi associati smettono di funzionare e tutti i dati vengono persi.
- **Requisiti relativi al numero di drive**
  - È necessario disporre di un minimo di cinque dischi nel gruppo di volumi.
  - In genere, sei limitato a un massimo di 30 dischi nel gruppo di volumi.

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 supporto del disco per la tolleranza ai guasti. 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 di un disco.

Si configura un singolo livello RAID su un singolo gruppo di volumi. Tutti i dati di ridondanza per tale gruppo di volumi vengono archiviati all'interno del gruppo stesso. La capacità del gruppo di volumi è pari alla capacità totale delle unità che lo compongono, meno la capacità riservata ai dati di ridondanza. La quantità di capacità necessaria per la ridondanza dipende dal livello RAID utilizzato.

Che 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 durante il trasferimento dei dati lungo il percorso di I/O.

L'utilizzo tipico della funzionalità Data Assurance prevede la verifica della porzione del percorso I/O tra i controller e le unità. Le funzionalità DA sono presentate a livello di pool e di gruppo di volumi.

Quando questa funzionalità è abilitata, l'array di storage aggiunge codici di controllo degli errori (noti anche come controlli di ridondanza ciclica o CRC) a ciascun blocco di dati nel volume. Dopo che un blocco di dati è stato spostato, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono né scritti su disco né restituiti all'host. Se si desidera utilizzare la funzionalità DA, selezionare un pool o un gruppo di volumi compatibile con DA durante la creazione di un nuovo volume (verificare la presenza di "Sì" accanto a "DA" nella tabella dei pool e dei gruppi di volumi candidati).

Assicurati di assegnare questi volumi abilitati DA a un host utilizzando un'interfaccia I/O in grado di 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 (iSCSI Extensions for RDMA/IB). DA non è supportato da SRP su InfiniBand.

Che cos'è secure-capable (Drive Security)?

Drive Security è una funzionalità che impedisce l'accesso non autorizzato ai dati sulle unità abilitate alla sicurezza quando vengono rimosse dall'array di storage. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).

Cosa devo sapere sull'aumento della capacità riservata?

In genere, dovresti aumentare la capacità quando ricevi un avviso che la capacità riservata rischia di esaurirsi. Puoi aumentare la capacità riservata solo in incrementi di 8 GiB.

- È necessario disporre di una capacità libera sufficiente nel pool o nel gruppo di volumi affinché possa essere espanso se necessario.

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

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

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

Perché non posso scegliere un altro importo da cui diminuire?

È possibile ridurre la capacità riservata solo della stessa quantità utilizzata per aumentarla. La capacità riservata per i volumi dei membri può essere rimossa solo nell'ordine inverso rispetto a quello in cui è stata aggiunta.

Non è possibile ridurre la capacità riservata per un oggetto di archiviazione se esiste una delle seguenti condizioni:

- Se l'oggetto di archiviazione è un volume mirrored pair.
- Se l'oggetto di archiviazione contiene un solo volume per la capacità riservata. L'oggetto di archiviazione deve contenere almeno due volumi per la capacità riservata.
- Se l'oggetto di archiviazione è un volume snapshot disabilitato.
- Se l'oggetto di archiviazione contiene una o più immagini snapshot associate.

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

Non è possibile ridurre la capacità riservata per un volume snapshot di sola lettura perché non ha alcuna capacità riservata associata. Solo i volumi snapshot di lettura-scrittura richiedono capacità riservata.

Perché ho bisogno di capacità riservata per ogni volume membro?

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

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

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

Come posso visualizzare e interpretare tutte le statistiche della Cache SSD?

È possibile visualizzare le statistiche nominali e le 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, tieni presente che alcune interpretazioni sono derivate dall'osservazione di una combinazione di statistiche.

Statistiche nominali

Per visualizzare le statistiche della Cache SSD, selezionare **Storage › Pools & Volume Groups**. Selezionare la Cache SSD per cui si desidera visualizzare le statistiche, quindi selezionare **More › View Statistics**. Le statistiche nominali vengono mostrate nella finestra di dialogo View SSD Cache Statistics.

Il seguente elenco comprende statistiche nominali, che costituiscono un sottoinsieme delle statistiche dettagliate.

statistica nominale	Descrizione
Letture/Scritture	Il numero totale di letture o scritture dell'host sui volumi con Cache SSD abilitata. Confronta le letture rispetto alle scritture. Le letture devono essere superiori alle scritture per un funzionamento efficace della Cache SSD. Maggiore è il rapporto tra letture e scritture, migliore è il funzionamento della cache.
Cache hit	Un conteggio del numero di cache hit.
Cache hit (%)	Derivato da cache hit / (letture + scritture). La percentuale di cache hit dovrebbe essere superiore al 50 percento per un funzionamento efficace della Cache SSD. Un valore basso potrebbe indicare diverse cose: • Il rapporto tra letture e scritture è troppo basso • Le letture non vengono ripetute • La capacità della cache è troppo piccola
Allocazione cache (%)	La quantità di spazio di archiviazione Cache SSD allocato, espressa come percentuale dello spazio di archiviazione Cache SSD disponibile per questo controller. Derivata da byte allocati / byte disponibili. La percentuale di allocazione della Cache normalmente risulta pari al 100 percento. Se questo numero è inferiore al 100 percento, significa che la cache non è stata riscaldata oppure che la capacità della Cache SSD è superiore a tutti i dati a cui si accede. In quest'ultimo caso, una capacità della Cache SSD inferiore potrebbe fornire lo stesso livello di prestazioni. Nota che questo non indica che i dati memorizzati nella cache siano stati inseriti nella Cache SSD; si tratta semplicemente di una fase preparatoria prima che i dati possano essere inseriti nella Cache SSD.

statistica nominale	Descrizione
Utilizzo della cache (%)	La quantità di storage della Cache SSD che contiene dati provenienti da volumi abilitati, espressa come percentuale dello storage della Cache SSD allocato. Questo valore rappresenta l'utilizzo o la densità della Cache SSD derivata dal rapporto tra byte di dati utente e byte allocati. La percentuale di utilizzo della Cache SSD è normalmente inferiore al 100 percento, forse anche molto inferiore. Questo numero mostra la percentuale della capacità della Cache SSD che è riempita con dati di cache. Questo numero è inferiore al 100 percento perché ogni unità di allocazione della Cache SSD, il blocco della Cache SSD, è suddivisa in unità più piccole chiamate sub-blocchi, che vengono riempite in modo relativamente indipendente. Un numero più alto è generalmente migliore, ma i miglioramenti delle prestazioni possono essere significativi anche con un numero più basso.

Statistiche dettagliate

Le statistiche dettagliate consistono nelle statistiche nominali, più statistiche aggiuntive. Queste statistiche aggiuntive vengono salvate insieme alle statistiche nominali, ma a differenza delle statistiche nominali, non vengono visualizzate nella finestra di dialogo Visualizza statistiche Cache SSD. È possibile visualizzare le statistiche dettagliate solo dopo aver esportato le statistiche in un `.csv` file.

Quando visualizzi il `.csv` file, nota che le statistiche dettagliate sono elencate dopo le statistiche nominali:

Statistiche dettagliate	Descrizione
Blocchi di lettura	Il numero di blocchi nelle letture host.
Blocchi di scrittura	Il numero di blocchi nelle scritture dell'host.
Blocchi di cache hit completi	Il numero di blocchi in cache hit. I blocchi full hit indicano il numero di blocchi che sono stati letti interamente dalla Cache SSD. La Cache SSD è vantaggiosa per le prestazioni solo per le operazioni che sono full cache hit.
Successi parziali	Il numero di letture host in cui almeno un blocco, ma non tutti i blocchi, erano presenti nella Cache SSD. Un riscontro parziale è un **miss** della Cache SSD in cui le letture sono state soddisfatte dal volume base.
Hit parziali - Blocchi	Il numero di blocchi nei Partial Hits. I Partial cache hits e i partial cache hit blocks derivano da un'operazione che ha solo una parte dei suoi dati nella Cache SSD. In questo caso, l'operazione deve recuperare i dati dal volume del disco rigido (HDD) memorizzato nella cache. La Cache SSD non offre alcun vantaggio in termini di prestazioni per questo tipo di hit. Se il numero di partial cache hit blocks è superiore ai full cache hit blocks, un diverso tipo di caratteristica I/O (file system, database o web server) potrebbe migliorare le prestazioni. È prevedibile che ci sarà un numero maggiore di Partial Hits e Misses rispetto ai Cache Hits mentre la Cache SSD si sta scaldando.

Statistiche dettagliate	Descrizione
Mancate	Il numero di letture host in cui nessuno dei blocchi era presente nella Cache SSD. Un miss della Cache SSD si verifica quando le letture sono state soddisfatte dal volume di base. È previsto che ci sarà un numero maggiore di Partial Hits e Misses rispetto ai Cache Hits mentre la Cache SSD si sta riscaldando.
Misses - Blocchi	Il numero di blocchi in Misses.
Popola azioni (letture host)	Il numero di letture host in cui i dati sono stati copiati dal volume base alla Cache SSD.
Popola azioni (letture host) - Blocchi	Il numero di blocchi in Populate Actions (Host Reads).
Popola azioni (Host Writes)	Il numero di scritture host in cui i dati sono stati copiati dal volume base alla Cache SSD. Il conteggio delle Populate Actions (scritture host) potrebbe essere zero per le impostazioni di configurazione della cache che non riempiono la cache a seguito di un'operazione di I/O di scrittura.
Popola azioni (scritture host) - Blocchi	Il numero di blocchi in Populate Actions (Host Writes).
Invalidare azioni	Il numero di volte in cui i dati sono stati invalidati o rimossi dalla Cache SSD. Un'operazione di invalidazione della cache viene eseguita per ogni richiesta di scrittura dell'host, per ogni richiesta di lettura dell'host con Forced Unit Access (FUA), per ogni richiesta di verifica e in alcune altre circostanze.
Azioni di riciclo	Il numero di volte in cui il blocco della Cache SSD è stato riutilizzato per un altro volume di base e/o un diverso intervallo di indirizzamento a blocchi logici (LBA). Per un funzionamento efficace della cache, il numero di ricicli deve essere basso rispetto al numero combinato di operazioni di lettura e scrittura. Se il numero di azioni di riciclo è vicino al numero combinato di letture e scritture, la Cache SSD è in uno stato di thrashing. È necessario aumentare la capacità della cache oppure il carico di lavoro non è favorevole all'utilizzo con Cache SSD.
Byte disponibili	Il numero di byte disponibili nella Cache SSD per l'utilizzo da parte di questo controller.
Byte allocati	Il numero di byte allocati dalla Cache SSD da questo controller. I byte allocati dalla Cache SSD potrebbero essere vuoti o potrebbero contenere dati provenienti dai volumi di base.
Byte di dati utente	Il numero di byte allocati nella Cache SSD che contengono dati provenienti dai volumi di base. I byte disponibili, i byte allocati e i byte di dati utente vengono utilizzati per calcolare la percentuale di allocazione della Cache e la percentuale di utilizzo della Cache.

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

Le unità SSD avranno una durata maggiore e prestazioni di scrittura massime migliori quando una parte della loro capacità non è allocata.

Per le unità associate a un pool, la capacità non allocata è composta dalla capacità di conservazione del pool, dalla capacità libera (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile riservata 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 si crea un pool, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra prestazioni, durata dei drive e capacità disponibile. Il cursore Capacità di ottimizzazione aggiuntiva, presente nella finestra di dialogo Impostazioni pool, consente di regolare la capacità di ottimizzazione del pool. Regolando il cursore è possibile ottenere prestazioni e durata dei drive migliori a scapito della capacità disponibile, oppure una maggiore capacità disponibile a scapito delle prestazioni e della durata dei drive.

Il cursore Capacità di ottimizzazione aggiuntiva è disponibile solo per i sistemi storage EF600 e EF300.

Che cos'è la capacità di ottimizzazione per i gruppi di volumi?

Le unità SSD avranno una durata maggiore e prestazioni di scrittura massime migliori quando una parte della loro capacità non è allocata.

Per le unità associate a un gruppo di volumi, la capacità non allocata è composta dalla capacità libera del gruppo di volumi (capacità non utilizzata dai volumi) e da una parte della capacità utilizzabile riservata come capacità di ottimizzazione. La capacità di ottimizzazione aggiuntiva garantisce un livello minimo di capacità di ottimizzazione riducendo la capacità utilizzabile e, pertanto, non è disponibile per la creazione di volumi.

Quando si crea un gruppo di volumi, viene generata una capacità di ottimizzazione consigliata che offre un equilibrio tra prestazioni, durata dell'unità e capacità disponibile. Il cursore Capacità di ottimizzazione aggiuntiva nella finestra di dialogo Impostazioni gruppo di volumi consente di regolare la capacità di ottimizzazione di un gruppo di volumi. Regolando il cursore è possibile ottenere prestazioni e durata dell'unità migliori a scapito della capacità disponibile, oppure una maggiore capacità disponibile a scapito delle prestazioni e della durata dell'unità.

Il cursore Capacità di ottimizzazione aggiuntiva è disponibile solo per i sistemi storage EF600 e EF300.

Cosa può fare il provisioning delle risorse?

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

Un volume con risorse allocate è un volume thick in un gruppo o pool di volumi SSD, in cui la capacità dell'unità viene allocata (assegnata al volume) al momento della creazione del volume, ma i blocchi dell'unità vengono deallocati (non mappati). Al contrario, in un volume thick tradizionale, tutti i blocchi dell'unità vengono mappati o allocati durante un'operazione di inizializzazione del volume in background, al fine di inizializzare i campi delle informazioni di protezione Data Assurance e di rendere coerenti i dati e la parità RAID in ogni RAID stripe. Con un volume con risorse allocate, non è prevista alcuna inizializzazione in background a tempo determinato. Invece, ogni RAID stripe viene inizializzata alla prima scrittura su un blocco del volume nella stripe.

I volumi con risorse allocate sono supportati solo su gruppi e pool di volumi SSD, dove tutte le unità 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 risorse allocate, tutti i blocchi di unità assegnati al volume vengono deallocati (smappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management o il comando SCSI Unmap. La deallocazione dei blocchi può migliorare la durata dell'SSD e aumentare le prestazioni massime di scrittura. Il miglioramento varia a seconda del modello e della capacità dell'unità.

DULBE non è supportato sugli array di storage EF300C o EF600C al momento.

Cosa devo 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 mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background.

Un volume con risorse allocate è un volume thick in un gruppo o pool di volumi SSD, in cui la capacità dell'unità viene allocata (assegnata al volume) al momento della creazione del volume, ma i blocchi dell'unità vengono deallocati (non mappati). Al contrario, in un volume thick tradizionale, tutti i blocchi dell'unità vengono mappati o allocati durante un'operazione di inizializzazione del volume in background, al fine di inizializzare i campi delle informazioni di protezione Data Assurance e di rendere coerenti i dati e la parità RAID in ogni RAID stripe. Con un volume con risorse allocate, non è prevista alcuna inizializzazione in background a tempo determinato. Invece, ogni RAID stripe viene inizializzata alla prima scrittura su un blocco del volume nella stripe.

I volumi con risorse allocate sono supportati solo su gruppi e pool di volumi SSD, dove tutte le unità 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 risorse allocate, tutti i blocchi di unità assegnati al volume vengono deallocati (smappati). Inoltre, gli host possono deallocare i blocchi logici nel volume utilizzando il comando NVMe Dataset Management o il comando SCSI Unmap. La deallocazione dei blocchi può migliorare la durata dell'SSD e aumentare le prestazioni massime di scrittura. Il miglioramento varia a seconda del modello e della capacità dell'unità.

Il provisioning delle risorse è abilitato per impostazione predefinita sui sistemi in cui le unità supportano DULBE. È possibile disabilitare questa impostazione predefinita da **Pools & Volume Groups**.

DULBE non è supportato sugli array di storage EF300C o EF600C al momento.

Volumi e carichi di lavoro

Scopri volumi e carichi di lavoro in SANtricity System Manager

È possibile creare un volume come container in cui applicazioni, database e file system archiviano i dati. Durante la creazione di un volume, si seleziona anche un workload per personalizzare la configurazione dell'array di storage per una specifica applicazione.

Cosa sono i volumi e i carichi di lavoro?

Un *volume* è il componente logico creato con una capacità specifica a cui l'host può accedere. Sebbene un volume possa essere costituito da più unità, un volume appare come un unico componente logico all'host. Una volta definito un volume, puoi aggiungerlo a un carico di lavoro. Un *carico di lavoro* è un oggetto di storage che supporta un'applicazione, come SQL Server o Exchange, che puoi utilizzare per ottimizzare lo storage per quell'applicazione.

Per saperne di più:

- "Come funzionano i volumi"
- "Come funzionano i workload"
- "Terminologia del volume"
- "Come viene allocata la capacità per i volumi"
- "Operazioni che è possibile eseguire sui volumi"

Come si creano volumi e workload?

Innanzitutto, si crea un carico di lavoro. Andare al **Storage › Volumes** e aprire una procedura guidata che guida l'utente attraverso i passaggi. Successivamente, si crea un volume dalla capacità disponibile in un pool o in un gruppo di volumi, e poi si assegna il carico di lavoro creato.

Per saperne di più:

- "Flusso di lavoro per la creazione di volumi"
- "Crea carichi di lavoro"
- "Crea volumi"
- "Aggiungi volumi al carico di lavoro"

Informazioni correlate

Scopri di più sui concetti relativi ai volumi:

- "Integrità dei dati e sicurezza dei dati per i volumi"
- "Cache SSD e volumi"
- "Monitoraggio del volume sottile"

Concetti

Come funzionano i volumi nel software SANtricity

I volumi sono contenitori di dati che gestiscono e organizzano lo spazio di storage sul tuo storage array.

Si creano volumi a partire dalla capacità di storage disponibile sull'array di storage e si rende facile organizzare e utilizzare le risorse del sistema. Questo concetto è simile all'utilizzo di cartelle/directory su un computer per organizzare i file per un accesso facile e rapido.

I volumi rappresentano l'unico livello dati visibile agli host. In un ambiente SAN, i volumi vengono mappati a numeri di unità logica (LUN), che sono visibili agli host. Le LUN contengono i dati utente accessibili tramite uno o più protocolli di accesso host supportati dall'array di storage, tra cui FC, iSCSI e SAS.

Tipi di volume che puoi creare da pool e gruppi di volumi

I volumi traggono la loro capacità da pool o gruppi di volumi. È possibile creare i seguenti tipi di volumi dai pool o gruppi di volumi presenti nel proprio storage array.

- **Dai pool** — È possibile creare volumi da un pool come *volumi completamente configurati (thick)* o *volumi*

con thin provisioning (thin).

> L'interfaccia di System Manager non offre la possibilità di creare volumi thin. Se si desidera creare volumi thin, utilizzare la Command Line Interface (CLI).

- **Dai gruppi di volumi** — È possibile creare volumi da un gruppo di volumi solo come *fully-provisioned (thick) volumes*.

I volumi spessi e i volumi sottili sfruttano la capacità dello storage array in modi diversi:

- La capacità per un volume thick viene allocata quando il volume viene creato.
- La capacità di un volume thin viene allocata come dati quando vengono scritti sul volume.

Il thin provisioning aiuta a evitare sprechi di capacità allocata e può far risparmiare alle aziende sui costi iniziali di storage. Tuttavia, il full provisioning offre il vantaggio di una minore latenza perché tutto lo storage viene allocato contemporaneamente quando vengono creati i volumi thick.

> I sistemi di storage EF600/EF600C e EF300/EF300C non supportano thin provisioning.

Caratteristiche dei volumi

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

- **Dimensione del segmento** — Un segmento è la quantità di dati in kilobyte (KiB) che viene memorizzata su un'unità prima che l'array di storage passi all'unità successiva nella striscia (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** — Crei 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 deve avere abbastanza capacità libera per creare il volume.
- **Proprietà del controller** — Tutti gli array di storage possono avere uno o due controller. In un array con un singolo controller, il carico di lavoro di un volume è gestito da un unico controller. In un array con due controller, un volume avrà un controller preferito (A o B) che "possiede" il volume. In una configurazione a due controller, la proprietà del volume viene regolata automaticamente utilizzando la funzionalità 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 un bilanciamento automatico del carico di lavoro I/O e garantisce che il traffico I/O in entrata dagli host venga gestito e bilanciato dinamicamente tra entrambi i controller.
- **Assegnazione dei volumi** — È possibile concedere agli host l'accesso a un volume al momento della creazione del volume o in un secondo momento. Tutto l'accesso degli host è gestito tramite un numero di unità logica (LUN). Gli host rilevano i LUN che, a loro volta, vengono assegnati ai volumi. Se si assegna un volume a più host, utilizzare un 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. Tieni presente questa limitazione quando crei volumi da utilizzare per un host particolare.

- **Nome descrittivo** — Puoi assegnare al volume qualsiasi nome desideri, ma ti consigliamo di rendere il nome descrittivo.

Durante la creazione del volume, a ciascun volume vengono assegnati capacità, nome, dimensione del

segmento (solo gruppi di volumi), proprietà del controller e assegnazione volume-host. I dati del volume vengono automaticamente bilanciati tra i controller, secondo necessità.

Come funzionano i carichi di lavoro nel software SANtricity

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

Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.

Durante la creazione del volume, il sistema richiede di rispondere a domande sull'utilizzo del carico di lavoro. Ad esempio, se si stanno creando volumi per Microsoft Exchange, viene chiesto di quante caselle di posta si ha bisogno, quali sono i requisiti medi di capacità delle caselle di posta e quante copie del database si desiderano. Il sistema utilizza queste informazioni per creare una configurazione di volume ottimale per te, che può essere modificata secondo necessità. Facoltativamente, 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 per applicazioni e altri.

- **Specifico per l'applicazione**. Quando si creano volumi utilizzando un carico di lavoro specifico per un'applicazione, il sistema può consigliare una configurazione del volume ottimizzata per ridurre al minimo la contesa tra l'I/O del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. Le caratteristiche del volume, come il tipo di I/O, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura, vengono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazione.
  - Microsoft® SQL Server™
  - Microsoft® server Exchange™
  - Applicazioni di videosorveglianza
  - VMware ESXi™ (per volumi da utilizzare con Virtual Machine File System)

    È possibile esaminare la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliati dal sistema utilizzando la finestra di dialogo Add/Edit Volumes.
- **Altro** (o applicazioni senza supporto specifico per la creazione di volumi). Altri carichi di lavoro utilizzano una configurazione di volume che è necessario specificare manualmente quando si desidera creare un carico di lavoro non associato a una specifica applicazione o se il sistema non dispone di ottimizzazione integrata per l'applicazione che si intende utilizzare sull'array di storage. È necessario specificare manualmente la configurazione del volume tramite la finestra di dialogo Aggiungi/Modifica volumi.

Viste dell'applicazione e del carico di lavoro

Per visualizzare applicazioni e carichi di lavoro, avvia SANtricity System Manager. Da tale interfaccia, puoi visualizzare le informazioni associate a un carico di lavoro specifico di un'applicazione in diversi modi:

- È possibile selezionare la scheda **Applications & Workloads** nel riquadro Volumi per visualizzare i volumi dell'array di storage raggruppati per carico di lavoro e per tipo di applicazione a cui il carico di lavoro è

associato.

- È possibile selezionare la scheda **Applications & Workloads** nel riquadro Prestazioni per visualizzare le metriche delle prestazioni (latenza, IOPS e MB) per gli oggetti logici. Gli oggetti sono raggruppati per applicazione e carico di lavoro associato. Raccogliendo questi dati sulle prestazioni a intervalli regolari, è possibile stabilire parametri di riferimento e analizzare le tendenze, il che può essere utile durante l'indagine di problemi relativi alle prestazioni di I/O.

Scopri la terminologia relativa ai volumi nel software SANtricity

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

Tutti i tipi di volume

Termine	Descrizione
Capacità assegnata	Si utilizza la capacità allocata per creare volumi e per le operazioni dei servizi di copia. La capacità allocata e la capacità segnalata coincidono per i volumi thick, ma sono diverse per i volumi thin. Per un volume thick, lo spazio fisicamente allocato è uguale allo spazio che viene segnalato all'host. Per un volume thin, la capacità segnalata è la capacità che viene segnalata agli host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocata per la scrittura dei dati.
Applicazione	Un'applicazione è un software come SQL Server o Exchange. Si definiscono uno o più carichi di lavoro a supporto di ciascuna applicazione. Per alcune applicazioni, il sistema consiglia automaticamente una configurazione del volume che ottimizza lo storage. Caratteristiche come il tipo di I/O, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura sono incluse nella configurazione del volume.
Capacità	La capacità è la quantità di dati che è possibile memorizzare in un volume.
Proprietà del controller	La proprietà del controller definisce il controller che è designato come controller proprietario, o primario, del volume. Un volume può avere un controller preferito (A o B) che "possiede" il volume. La proprietà del volume viene regolata automaticamente tramite la funzionalità 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 un bilanciamento automatico del carico di lavoro I/O e garantisce che il traffico I/O in entrata dagli host venga gestito e bilanciato dinamicamente tra entrambi i controller.

Termine	Descrizione
Precaricamento dinamico della cache di lettura	Il precaricamento dinamico della cache di lettura consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i blocchi di dati da un'unità alla cache. Questo caching aumenta la probabilità che le future richieste di dati possano essere soddisfatte dalla cache. Il precaricamento dinamico della cache di lettura è importante per le applicazioni multimediali che utilizzano I/O sequenziale. La velocità e la quantità di dati precaricati nella cache si regolano automaticamente in base alla velocità e alla dimensione delle richieste di lettura dell'host. L'accesso casuale non comporta il precaricamento dei dati nella cache. Questa funzionalità non si applica quando il caching di lettura è disabilitato. Per un volume thin, il precaricamento dinamico della cache di lettura è sempre disabilitato e non può essere modificato.
Area di capacità libera	Un'area di capacità libera è la capacità libera che può risultare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità libera disponibile durante la creazione di un volume. Quando crei un volume in un gruppo di volumi che dispone di una o più aree di capacità libera, la capacità del volume è limitata all'area di capacità libera più grande in quel 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 puoi creare è di 10 GiB. Consolidando la capacità libera, puoi creare volumi aggiuntivi dalla quantità massima di capacità libera in un gruppo di volumi.
Host	Un host è un server che invia I/O a un volume su un array di storage.
Cluster host	Un cluster di host è un gruppo di host. Si crea un cluster di host per semplificare l'assegnazione degli stessi volumi a più host.
hot spare drive	Le unità hot spare sono supportate solo con i gruppi di volumi. Un'unità hot spare non contiene dati e funge da standby in caso di guasto di un'unità nei volumi RAID 1, RAID 3, RAID 5 o RAID 6 contenuti in un gruppo di volumi. L'unità hot spare aggiunge un ulteriore livello di ridondanza al tuo array di storage.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi che un host utilizza 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 indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi differenti.
Scansione dei supporti	Una scansione dei supporti di memorizzazione consente di rilevare gli errori dei supporti prima che vengano individuati durante una normale operazione di lettura o scrittura dai dischi. Una scansione dei supporti viene eseguita come operazione in background e analizza tutti i dati e le informazioni di ridondanza presenti nei volumi utente definiti.

Termine	Descrizione
Spazio dei nomi	Un namespace è una memoria NVM formattata per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che corrisponde a un volume nell'array di storage.
Pool	Un pool è un insieme di unità disco raggruppate logicamente. È possibile utilizzare un pool per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un pool o da un gruppo di volumi.)
Capacità del pool o del gruppo di volumi	La capacità di un pool, di un volume o di un gruppo di volumi è la capacità in un array di storage che è stata assegnata a un pool o a un gruppo di volumi. Questa capacità viene utilizzata per creare volumi e soddisfare le varie esigenze di capacità delle operazioni dei servizi di copia e degli oggetti di storage.
cache di lettura	La cache di lettura è un buffer che memorizza i dati letti dalle unità. I dati per un'operazione di lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando la necessità di accedere alle unità. I dati rimangono nella cache di lettura finché non vengono svuotati.
Capacità segnalata	La capacità segnalata è la capacità che viene comunicata all'host e a cui l'host può accedere. La capacità dichiarata e la capacità allocata coincidono per i volumi thick, ma sono diverse per i volumi thin. Per un volume thick, lo spazio fisicamente allocato è uguale allo spazio dichiarato all'host. Per un volume thin, la capacità dichiarata è la capacità dichiarata all'host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocata per la scrittura dei dati.
Dimensione del segmento	Un segmento è la quantità di dati in kilobyte (KiB) che viene memorizzata su un'unità prima che l'array di storage si sposti sull'unità successiva nella striscia (gruppo RAID). La dimensione del segmento è uguale o inferiore alla capacità del gruppo di volumi. La dimensione del segmento è fissa e non può essere modificata per i pool.
Striping	Lo striping è un modo di memorizzare i dati sull'array di storage. Lo striping suddivide il flusso di dati in blocchi di una certa dimensione (chiamata "dimensione del blocco") e poi scrive questi blocchi sulle unità una alla volta. Questo modo di memorizzare i dati viene utilizzato per distribuire e archiviare i dati su più unità fisiche. Lo striping è sinonimo di RAID 0 e distribuisce i dati su tutte le unità di un gruppo RAID senza parità.
Volume	Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage.
Assegnazione del volume	L'assegnazione del volume è il modo in cui le LUN host vengono assegnate a un volume.

Termine	Descrizione
Nome volume	Il nome di un volume è una stringa di caratteri assegnata al volume al momento della sua creazione. È possibile accettare il nome predefinito oppure specificare un nome più descrittivo che indichi il tipo di dati memorizzato nel volume.
Gruppo di volumi	Un gruppo di volumi è un container per volumi con caratteristiche condivise. Un gruppo di volumi ha una capacità definita e livello RAID. È possibile utilizzare un gruppo di volumi per creare uno o più volumi accessibili a un host. (È possibile creare volumi da un gruppo di volumi o da un pool.)
Carico di lavoro	Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.
cache di scrittura	La cache di scrittura è un buffer che memorizza i dati provenienti dall'host che non sono ancora stati scritti sulle unità. I dati rimangono nella cache di scrittura finché non vengono scritti sulle unità. La cache di scrittura può aumentare le prestazioni di I/O.
Caching della scrittura con mirroring	La cache di scrittura con mirroring si verifica quando i dati scritti nella cache di un controller vengono scritti anche nella 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 la cache di scrittura è abilitata e sono presenti due controller. La cache di scrittura con mirroring è l'impostazione predefinita alla creazione del volume.
Cache di scrittura senza batterie	L'impostazione cache di scrittura senza batterie consente alla cache di scrittura di continuare anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta della cache di scrittura senza batterie non è generalmente raccomandata, perché i dati potrebbero andare persi in caso di perdita di alimentazione. In genere, la cache di scrittura viene disattivata temporaneamente dal controller fino a quando le batterie non sono cariche o una batteria guasta viene sostituita.

Specifico per volumi thin

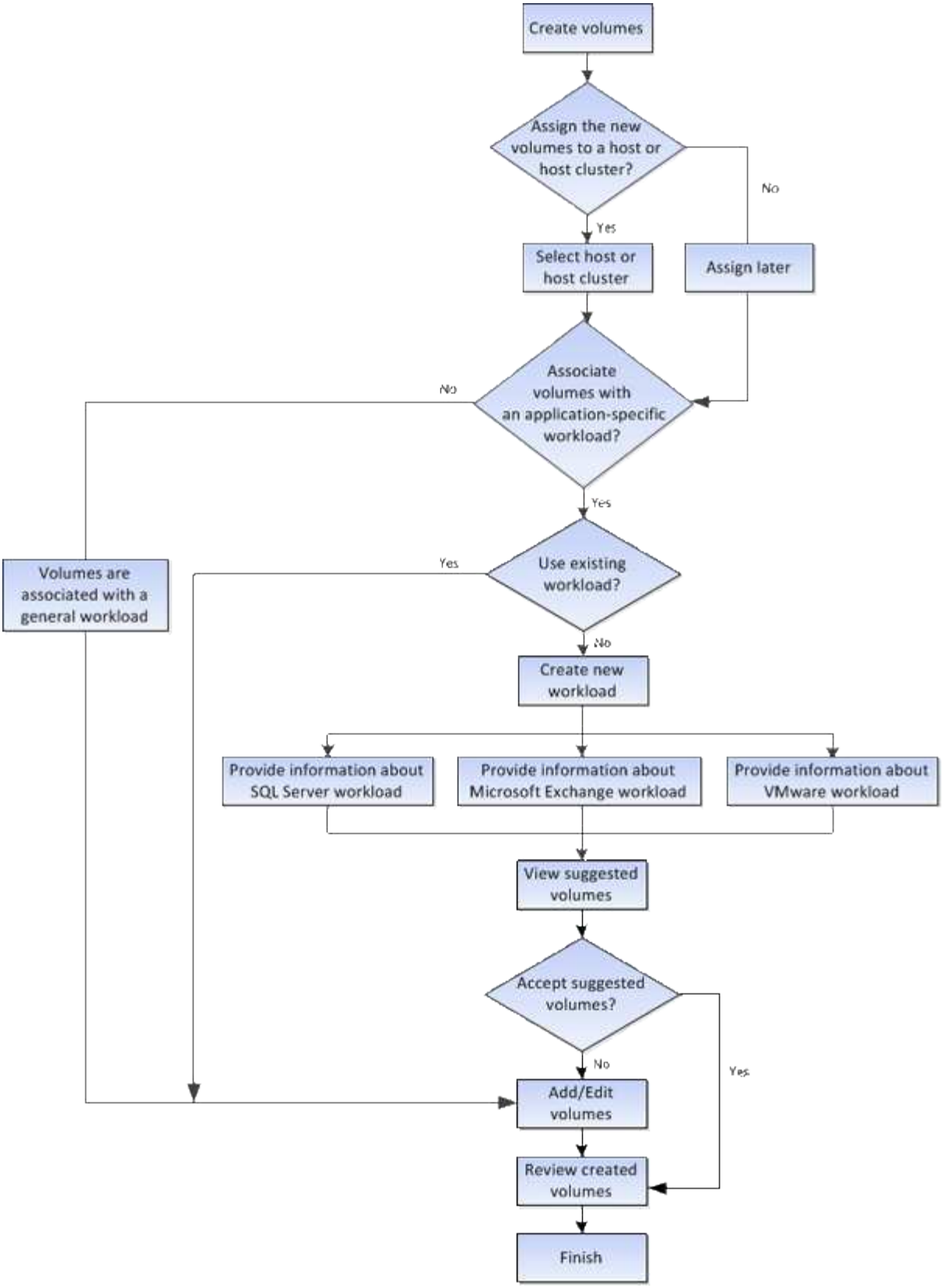
System Manager non offre un'opzione per creare volumi thin. Se si desidera creare volumi thin, utilizzare la command line interface (CLI).

I volumi con thin provisioning non sono disponibili sui sistemi storage EF600/EF600C o EF300/EF300C.

Termine	Descrizione
Limite di capacità assegnata	Il limite di capacità allocata è il limite massimo su quanto può crescere la capacità fisica allocata per un volume thin.
Capacità scritta	La capacità scritta è la quantità di capacità che è stata scritta dalla capacità riservata allocata per i volumi sottili.
Soglia di attenzione	È possibile impostare una soglia di avviso che verrà emessa quando la capacità allocata per un volume thin raggiunge la percentuale di riempimento (la soglia di avviso).

Come funziona la creazione di volumi in SANtricity System Manager

In SANtricity System Manager, puoi creare volumi seguendo questi passaggi.



Scopri l'integrità e la sicurezza dei dati per i volumi nel software SANtricity

È possibile abilitare i volumi all'utilizzo della funzionalità Data Assurance (DA) e della funzionalità Drive Security. Queste funzionalità sono presentate a livello di pool e di gruppo di volumi.

Data Assurance

Data Assurance (DA) implementa lo standard T10 Protection Information (PI), che aumenta l'integrità dei dati verificando e correggendo gli errori che potrebbero verificarsi durante il trasferimento dei dati lungo il percorso I/O. L'utilizzo tipico della funzionalità Data Assurance prevede il controllo della porzione del percorso I/O compresa tra i controller e le unità. Le funzionalità DA sono disponibili a livello di pool e di gruppo di volumi.

Quando questa funzionalità è abilitata, l'array di storage aggiunge codici di controllo degli errori (noti anche come controlli di ridondanza ciclica o CRC) a ciascun blocco di dati nel volume. Dopo che un blocco di dati è stato spostato, l'array di storage utilizza questi codici CRC per determinare se si sono verificati errori durante la trasmissione. I dati potenzialmente corrotti non vengono né scritti su disco né restituiti all'host. Se si desidera utilizzare la funzionalità DA, selezionare un pool o un gruppo di volumi compatibile con DA durante la creazione di un nuovo volume (verificare la presenza di "Sì" accanto a "DA" nella tabella dei pool e dei gruppi di volumi candidati).

Sicurezza del drive

La sicurezza delle unità è una funzionalità che impedisce l'accesso non autorizzato ai dati sulle unità protette quando vengono rimosse dall'array di storage. Queste unità possono essere unità Full Disk Encryption (FDE) o unità certificate conformi ai Federal Information Processing Standards 140-2 livello 2 (unità FIPS).

Come funziona Drive Security a livello di drive

Un'unità con funzionalità di sicurezza, FDE o FIPS, crittografa i dati durante la scrittura e li decrittografa durante la lettura. Questa crittografia e decrittografia non influisce sulle prestazioni o sul flusso di lavoro dell'utente. Ogni unità ha la propria chiave di crittografia univoca, che non può mai essere trasferita dall'unità.

Come funziona Drive Security a livello di volume

Quando si crea un pool o un gruppo di volumi da unità secure-capable, è anche possibile abilitare Drive Security per tali pool o gruppi di volumi. L'opzione Drive Security rende le unità e i gruppi di volumi e pool associati secure-enabled. Un pool o un gruppo di volumi può contenere sia unità secure-capable che non secure-capable, ma tutte le unità devono essere secure-capable per poter utilizzare le loro capacità di crittografia.

Come implementare Drive Security

Per implementare Drive Security, eseguire i seguenti passaggi.

1. Dotate il vostro storage array di unità compatibili con la sicurezza, ovvero unità FDE o unità FIPS. (Per i volumi che richiedono il supporto FIPS, utilizzate solo unità FIPS. La combinazione di unità FIPS e FDE in un gruppo o pool di volumi comporterà il trattamento di tutte le unità come unità FDE. Inoltre, un'unità FDE non può essere aggiunta o utilizzata come unità di riserva in un gruppo o pool di volumi interamente composto da unità FIPS.)
2. Crea una chiave di sicurezza, ovvero una stringa di caratteri condivisa tra il controller e le unità per l'accesso in lettura/scrittura. Puoi creare una chiave interna dalla memoria persistente del controller oppure una chiave esterna da un key management server. Per la gestione delle chiavi esterne, è necessario stabilire l'autenticazione con il key management server.
3. Abilita la sicurezza delle unità per pool e gruppi di volumi:
    - Crea un pool o un gruppo di volumi (cerca **Yes** nella colonna **Secure-capable** nella tabella Candidates).
    - Selezionate un pool o un gruppo di volumi quando create un nuovo volume (cercate **Sì** accanto a **Compatibile con Secure** nella tabella dei candidati per pool e gruppi di volumi).

Con la funzione Drive Security, si crea una chiave di sicurezza che viene condivisa tra le unità abilitate alla sicurezza e i controller in un array di storage. Ogni volta che l'alimentazione delle unità viene interrotta e riattivata, le unità abilitate alla sicurezza passano a uno stato Security Locked finché il controller non applica la chiave di sicurezza.

Scopri la Cache SSD e i volumi nel software SANtricity

È possibile aggiungere un volume alla Cache SSD per migliorare le prestazioni in sola lettura. La Cache SSD consiste in un insieme di unità a stato solido (SSD) che vengono raggruppate logicamente nell'array di storage.

Volumi

Vengono utilizzati semplici meccanismi di I/O del volume per spostare i dati da e verso la Cache SSD. Dopo che i dati sono stati memorizzati nella Cache SSD e sugli SSD, le successive letture di tali dati vengono eseguite sulla Cache SSD, eliminando così la necessità di accedere al volume HDD.

Cache SSD è una cache secondaria da utilizzare insieme alla cache primaria nella memoria ad accesso casuale dinamica (DRAM) del controller.

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

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

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

Funzione di sicurezza dell'unità

Per utilizzare Cache SSD su un volume che utilizza anche Drive Security (is secure-enabled), le funzionalità di Drive Security del volume e della Cache SSD devono corrispondere. Se non corrispondono, il volume non sarà secure-enabled.

Azioni che è possibile eseguire sui volumi in SANtricity System Manager

È possibile eseguire diverse azioni su un volume: aumentare la capacità, eliminare, copiare, inizializzare, ridistribuire, modificare la proprietà, modificare le impostazioni della cache e modificare le impostazioni di scansione dei supporti.

Aumenta la capacità

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

- Utilizza la capacità libera disponibile nel pool o nel gruppo di volume.

  Aggiungi capacità a un volume selezionando **Storage › Pools and Volume Groups › Add Capacity**.

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

volume. Utilizza questa opzione quando non è presente capacità libera nel pool o nel gruppo di volumi.

Si aggiunge capacità non assegnata al pool o al gruppo di volumi selezionando menu:Storage [Pools and Volume Groups > Add Capacity].

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

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file system in modo che corrispondano. Come farlo dipende dal file system in uso. Consultare la documentazione del sistema operativo host per dettagli.

Elimina

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

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

Copia

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

Inizializzare

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

È possibile inizializzare i volumi selezionando **Storage › Volumes › More › Initialize volumes**.

Ridistribuire

Si ridistribuiscono i volumi per riportarli ai rispettivi controller proprietari preferiti. In genere, i driver multipath spostano i volumi dal controller proprietario preferito quando si verifica un problema lungo il percorso dei dati tra l'host e l'array di storage.

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

È possibile ridistribuire i volumi selezionando **Storage › Volumes › More › Redistribute volumes**.

Modifica proprietà del volume

La modifica della proprietà di un volume modifica il controller proprietario preferito del volume. Il controller proprietario preferito di un volume è elencato nel **Storage › Volumes › View/Edit Settings › Advanced tab**.

È possibile modificare la proprietà di un volume selezionando **Storage › Volumes › More › Change ownership**.

Mirroring e proprietà del volume

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

Se un mirror consistency group contiene un volume secondario locale e la proprietà del controller viene modificata, il volume secondario viene automaticamente trasferito al suo controller proprietario originale alla prima operazione di scrittura. Non è possibile modificare la proprietà del controller di un volume secondario utilizzando l'opzione **Change ownership**.

Copia volume e proprietà del volume

Durante un'operazione di copia volume, lo stesso controller deve possedere sia il volume di origine che il volume di destinazione. Talvolta, all'avvio dell'operazione di copia volume, i due volumi non hanno lo stesso controller preferito. Pertanto, la proprietà del volume di destinazione viene automaticamente trasferita al controller preferito del volume di origine. Quando la copia volume è completata o viene interrotta, la proprietà del volume di destinazione viene ripristinata al suo controller preferito.

Se la proprietà del volume di origine viene modificata durante l'operazione di copia del volume, anche la proprietà del volume di destinazione viene modificata. In alcuni ambienti di sistema operativo, potrebbe essere necessario riconfigurare il driver host multipath prima che un percorso I/O possa essere utilizzato. (Alcuni driver multipath richiedono una modifica per riconoscere il percorso I/O. Consultare la documentazione del driver per ulteriori informazioni.)

Modifica le impostazioni della cache

La cache memory è un'area di memoria volatile temporanea (RAM) sul controller che ha un tempo di accesso più rapido rispetto al supporto del drive. Se si utilizza la cache memory, è possibile aumentare le prestazioni I/O complessive per i seguenti motivi:

- I dati richiesti all'host per una lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando così la necessità di accedere all'unità.
- I dati vengono inizialmente scritti nella cache, il che consente all'applicazione di continuare invece di attendere che i dati vengano scritti sull'unità.

Seleziona **Storage › Volumes › More › Change cache settings** per modificare le seguenti impostazioni della cache:

- **Cache di lettura e scrittura** — La cache di lettura è un buffer che memorizza i dati letti dalle unità. I dati per un'operazione di lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando la necessità di accedere alle unità. I dati rimangono nella cache di lettura finché non vengono svuotati.

  La cache di scrittura è un buffer che memorizza i dati provenienti dall'host che non sono ancora stati scritti

sulle unità. I dati rimangono nella cache di scrittura finché non vengono scritti sulle unità. La cache di scrittura può aumentare le prestazioni di I/O.

- **Cache di scrittura con mirroring** — La cache di 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 la cache di scrittura è abilitata e sono presenti due controller. La cache di scrittura con mirroring è l'impostazione predefinita alla creazione del volume.
- **Cache di scrittura senza batterie** — L'impostazione cache di scrittura senza batterie consente di continuare la cache di scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta della cache di scrittura senza batterie non è generalmente consigliata, perché i dati potrebbero andare persi se si verifica un'interruzione di corrente. In genere, la cache di scrittura viene temporaneamente disattivata dal controller fino a quando le batterie non sono cariche o una batteria guasta viene sostituita.

  Questa impostazione è disponibile solo se è stata abilitata la cache di scrittura. Questa impostazione non è disponibile per i volumi thin.

- **Precaricamento dinamico della cache di lettura** — Il precaricamento dinamico della cache di lettura consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i blocchi di dati da un'unità alla cache. Questa memorizzazione nella cache aumenta la probabilità che le future richieste di dati possano essere soddisfatte dalla cache. Il precaricamento dinamico della cache di lettura è importante per le applicazioni multimediali che utilizzano I/O sequenziali. La velocità e la quantità di dati precaricati nella cache si regolano automaticamente in base alla velocità e alla dimensione delle richieste di lettura dell'host. L'accesso casuale non causa il precaricamento dei dati nella cache. Questa funzione non si applica quando la memorizzazione nella cache di lettura è disabilitata.

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

Modifica le impostazioni della scansione dei supporti

Le scansioni dei supporti rilevano e riparano gli errori sui blocchi del disco che vengono letti raramente dalle applicazioni. Questa scansione può prevenire la perdita di dati se altre unità nel pool o nel gruppo di volumi si guastano, poiché i dati delle unità guaste vengono ricostruiti utilizzando le informazioni di ridondanza e i dati provenienti da altre unità del pool o del gruppo di volumi.

Le scansioni dei supporti vengono eseguite in modo continuo 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 a priorità più elevata (ad esempio, la ricostruzione), ma riprenderanno alla stessa velocità costante.

È possibile abilitare e impostare la durata di esecuzione della scansione dei supporti selezionando **Storage › Volumes › More › Change media scan settings**.

Un volume viene scansionato solo quando l'opzione di scansione dei supporti è abilitata per l'array di storage e per quel volume. Se il controllo di ridondanza è anche abilitato 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 di ridondanza è abilitata per impostazione predefinita per ogni volume al momento della sua 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 nei volumi RAID 5 ottimali o nei volumi RAID 6 che sono ottimali o hanno un solo disco guasto. Se l'errore irreversibile

non può essere riparato utilizzando le informazioni di ridondanza, il blocco di dati verrà aggiunto al registro dei settori illeggibili. Sia gli errori del supporto correggibili che quelli non correggibili vengono segnalati nel registro eventi.

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

Come viene allocata la capacità per i volumi in SANtricity System Manager

Le unità disco del tuo array di storage forniscono la capacità di storage fisico per i tuoi dati. Prima di poter iniziare a memorizzare i dati, devi configurare la capacità allocata in componenti logici noti come pool o gruppi di volumi. Utilizzi questi oggetti di storage per configurare, archiviare, gestire e preservare i dati sul tuo array di storage.

Utilizzo della capacità per creare ed espandere volumi

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

- Quando si crea un volume da capacità non assegnata, è possibile creare un pool o un gruppo di volumi e il volume allo stesso tempo.
- 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 in modo che corrispondano. Come farlo dipende dal file system in uso. Consultare la documentazione del sistema operativo host per dettagli.

Tipi di capacità per volumi spessi e volumi sottili

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

- Per un volume thick, la capacità dichiarata del volume è uguale alla quantità di storage fisico allocato. L'intera quantità di storage fisico deve essere presente. Lo spazio fisicamente allocato è uguale allo spazio che viene dichiarato all'host.

  In genere, si imposta la capacità dichiarata del volume thick sulla capacità massima a cui si pensa che il volume crescerà. I volumi thick offrono prestazioni elevate e prevedibili per le applicazioni principalmente perché tutta la capacità utente viene riservata e allocata al momento della creazione.

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

  La capacità dichiarata può essere superiore alla capacità allocata sull'array di storage. I volumi thin possono essere dimensionati per adattarsi alla crescita, indipendentemente dalle risorse attualmente disponibili.

> SANtricity System Manager non offre la possibilità di creare volumi thin. Se si desidera creare volumi thin, utilizzare la Command Line Interface (CLI).

Limiti di capacità per volumi spessi

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

Quando si aumenta la capacità dichiarata per un volume thick, tenere a mente le seguenti linee guida:

- È possibile specificare fino a tre cifre decimali (per 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 Dynamic Segment Size (DSS). La migrazione DSS è una funzionalità del software che consente di modificare la dimensione del segmento di un volume.

- Volumi superiori a 2 TiB sono supportati da alcuni sistemi operativi host (la capacità massima riportata è determinata dal sistema operativo host). In effetti, alcuni sistemi operativi host supportano volumi fino a 128 TiB. Consultare la documentazione del proprio sistema operativo host per ulteriori dettagli.

Limiti di capacità per volumi sottili

È possibile creare volumi thin con una capacità dichiarata elevata e una capacità allocata relativamente ridotta, il che è vantaggioso per l'utilizzo e l'efficienza dello storage. I volumi thin possono semplificare l'amministrazione dello storage perché la capacità allocata può aumentare al variare delle esigenze dell'applicazione, senza interrompere l'applicazione, consentendo un migliore utilizzo dello storage.

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

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

Tipo di capacità	Dimensione minima	Dimensione massima
Segnalato	32 MiB	256 TiB
Assegnato	4 MiB	64 TiB

Per un volume thin, se è stata raggiunta la capacità massima dichiarata di 256 TiB, non è possibile aumentarne la capacità. Assicurarsi che la capacità riservata del volume thin sia impostata su un valore superiore alla capacità massima dichiarata.

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

Per modificare il limite di capacità allocata, selezionare **Storage › Volumes › scheda Thin Volume Monitoring › Change Limit**.

Poiché System Manager non alloca l'intera capacità quando crea un volume thin, potrebbe non esserci spazio libero sufficiente nel pool. Lo spazio insufficiente può bloccare le scritture nel pool, non solo per i volumi thin, ma anche per altre operazioni che richiedono capacità dal pool (ad esempio, immagini snapshot o volumi snapshot). Tuttavia, è comunque possibile eseguire operazioni di lettura dal pool. Se si verifica questa situazione, si riceve un avviso di soglia di allerta.

Scopri il monitoraggio dei volumi sottili nel software SANtricity

È possibile monitorare i volumi thin per lo spazio e generare avvisi appropriati per prevenire condizioni di esaurimento della capacità.

Gli ambienti thin provisioning possono allocare più spazio logico di quanto abbiano nello storage fisico sottostante. Puoi selezionare la scheda **Storage › Volumes › Thin Volume Monitoring** per monitorare quanto possono crescere i tuoi volumi thin prima che raggiungano il limite massimo di capacità allocata.

È possibile utilizzare la vista Thin Monitoring per eseguire le seguenti azioni:

- Definisci il limite che restringe la capacità allocata a cui un volume sottile può espandersi automaticamente.
- Imposta la percentuale alla quale viene inviato un avviso (soglia di avvertimento superata) all'area Notifiche nella pagina iniziale quando un volume thin si avvicina al limite massimo di capacità allocata.

Per aumentare la capacità di un volume sottile, aumenta la sua capacità dichiarata.

System Manager non offre la possibilità di creare volumi con thin provisioning. Se si desidera creare volumi con thin provisioning, utilizzare la Command Line Interface (CLI).

I volumi con thin provisioning non sono disponibili sui sistemi storage EF600/EF600C o EF300/EF300C.

Scopri i volumi thick e thin nel software SANtricity

Un volume thick è sempre fully-provisioned, il che significa che tutta la capacità viene assegnata al momento della creazione del volume. Un volume thin è sempre con thin provisioning, il che significa che la capacità viene assegnata man mano che i dati vengono scritti sul volume.

System Manager non offre la possibilità di creare volumi con thin provisioning. Se si desidera creare volumi con thin provisioning, utilizzare la Command Line Interface (CLI).

Tipo di volume	Descrizione
Volumi thick	• I volumi thick vengono creati da un pool o da un gruppo di volumi. • Con i volumi spessi, una grande quantità di spazio di storage viene fornita in anticipo in previsione delle future esigenze di storage. • I volumi thick vengono creati con l'intera dimensione del volume pre-allocata sullo storage fisico al momento della creazione del volume. Questa pre-allocazione significa che la creazione di un volume da 100 GiB consuma effettivamente 100 GiB di capacità allocata sulle unità. Tuttavia, lo spazio potrebbe rimanere inutilizzato, causando un sotto-utilizzo della capacità di storage. • Quando si creano volumi thick, assicurarsi di non allocare una capacità eccessiva per un singolo volume. Un'allocazione eccessiva di capacità per un singolo volume può rapidamente esaurire tutto lo storage fisico nel sistema. • Tieni presente che la capacità di storage è necessaria anche per i servizi di copia (immagini Snapshot, volumi Snapshot, copie di volumi e mirroring asincrono), quindi non allocare tutta la capacità ai volumi thick. Uno spazio insufficiente può bloccare le scritture sul pool o sul gruppo di volumi. Ricevi un avviso di soglia di capacità libera se si verifica questa situazione.
Volumi con thin provisioning	• I volumi con thin provisioning vengono creati solo da un pool, non da un gruppo di volumi. • I volumi thin devono essere RAID 6. • I volumi con thin provisioning non sono disponibili sui sistemi storage EF600/EF600C o EF300/EF300C. • È necessario utilizzare la CLI per creare volumi con thin provisioning. • A differenza dei volumi spessi, lo spazio necessario per il volume con thin provisioning non viene allocato durante la creazione, ma viene fornito su richiesta in un secondo momento. • Un volume con thin provisioning consente di sovra-allocare le sue dimensioni. Cioè, è possibile assegnare una dimensione LUN maggiore rispetto alla dimensione del volume. È quindi possibile espandere il volume secondo necessità (aggiungendo, se necessario, unità disco) senza espandere la dimensione della LUN e quindi senza disconnettere gli utenti. • È possibile utilizzare la space reclamation dei blocchi con thin provisioning (UNMAP) per recuperare blocchi di un volume con thin provisioning sull'array di storage tramite un comando SCSI UNMAP emesso dall'host. Un array di storage che supporta il thin provisioning può riutilizzare lo spazio recuperato per soddisfare le richieste di allocazione per un altro volume con thin provisioning all'interno dello stesso array di storage, consentendo una migliore rendicontazione del consumo di spazio su disco e un utilizzo più efficiente delle risorse.

Limitazioni dei volumi con thin provisioning

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

- Non è possibile modificare la dimensione del segmento di un volume con thin provisioning.

- Non è possibile abilitare il controllo di ridondanza prelettura per un volume con thin provisioning.
- Non è possibile utilizzare un volume con thin provisioning come volume di destinazione in un'operazione Copy Volume.
- È possibile modificare il limite di capacità allocata e la soglia di avviso di un volume con thin provisioning solo sul lato primario di una coppia mirror asincrona. Qualsiasi modifica a questi parametri sul lato primario viene propagata automaticamente al lato secondario.

Configura lo storage

Crea carichi di lavoro in SANtricity System Manager

È possibile creare workload per qualsiasi tipo di applicazione.

Informazioni su questa attività

Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Selezionare **Create › Workload**.

   Viene visualizzata la finestra di dialogo Crea Application Workload.

3. Utilizza l'elenco a discesa per selezionare il tipo di applicazione per cui desideri creare il workload e quindi digita un nome per il workload.
4. Fai clic su **Create**.

Dopo aver finito

Ora sei pronto per aggiungere capacità di storage al workload che hai creato. Utilizza l'opzione **Create Volume** per creare uno o più volumi per un'applicazione e per allocare quantità specifiche di capacità a ciascun volume.

Creare volumi in SANtricity System Manager

Si creano volumi per aggiungere capacità di archiviazione a un carico di lavoro specifico di un'applicazione e per rendere i volumi creati visibili a un host o a un cluster. Inoltre, la sequenza di creazione dei volumi fornisce opzioni per allocare quantità specifiche di capacità a ogni volume che si desidera creare.

Informazioni su questa attività

La maggior parte dei tipi di applicazione ha come impostazione predefinita una configurazione di volume definita dall'utente. Alcuni tipi di applicazione hanno una configurazione intelligente applicata al momento della creazione del volume. Ad esempio, se si creano volumi per l'applicazione Microsoft Exchange, viene chiesto di quante caselle di posta si ha bisogno, quali sono i requisiti di capacità media delle caselle di posta e quante copie del database si desidera. System Manager utilizza queste informazioni per creare una configurazione di volume ottimale, che può essere modificata se necessario.

Il processo per creare un volume è una procedura a più fasi.

Passo 1: Seleziona host per un volume

Si creano volumi per aggiungere capacità di archiviazione a un carico di lavoro specifico di un'applicazione e per rendere i volumi creati visibili a un host o a un cluster. Inoltre, la sequenza di creazione dei volumi fornisce opzioni per allocare quantità specifiche di capacità a ogni volume che si desidera creare.

Prima di iniziare

- Host o cluster di host validi esistono sotto il riquadro Hosts.
- Sono stati definiti identificatori di porta host per l'host.
- Prima di creare un volume abilitato per DA, la connessione host che si intende utilizzare deve supportare DA. Se una qualsiasi delle connessioni host sui controller nel tuo storage array non supporta DA, gli host associati non possono accedere ai dati sui volumi abilitati per DA.

Informazioni su questa attività

Tenete presenti queste linee guida quando assegnate i volumi:

- Il sistema operativo di un host può avere limiti specifici sul numero di volumi a cui l'host può accedere. Tieni presente questa limitazione quando crei volumi da utilizzare per un particolare host.
- È possibile definire un'assegnazione per ciascun volume nel sistema storage.
- I volumi assegnati sono condivisi tra i controller nell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un host cluster per accedere a un volume. È necessario utilizzare un LUN univoco.
- Se si desidera velocizzare 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 andrà a buon fine se si tenta di assegnare un volume a un cluster di host che è in conflitto con un'assegnazione già stabilita per un host nei cluster di host.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona **Create › Volume**.

   Viene visualizzata la finestra di dialogo Create Volumes.

3. Dall'elenco a discesa, seleziona un host specifico o un cluster di host a cui desideri assegnare i volumi, oppure scegli di assegnare l'host o il cluster di host in un secondo momento.
4. Per continuare la sequenza di creazione del volume per l'host o host cluster selezionato, fare clic su **Avanti** e procedere a Passaggio 2: Seleziona un carico di lavoro per un volume.

   Viene visualizzata la finestra di dialogo Select Workload.

Passaggio 2: Seleziona un carico di lavoro per un volume

Seleziona un carico di lavoro per personalizzare la configurazione dell'array di storage per un'applicazione specifica, come Microsoft SQL Server, Microsoft Exchange, applicazioni di videosorveglianza o VMware. Puoi selezionare "Altra applicazione" se l'applicazione che intendi utilizzare su questo array di storage non è presente nell'elenco.

Informazioni su questa attività

Questa attività descrive come creare volumi per un workload esistente.

- Quando si creano volumi utilizzando un carico di lavoro specifico per un'applicazione, il sistema potrebbe consigliare una configurazione di volume ottimizzata per ridurre al minimo la contesa tra l'I/O del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza dell'applicazione. È possibile esaminare la configurazione di volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliati dal sistema tramite la finestra di dialogo Aggiungi/Modifica volumi.
- *Quando si creano volumi utilizzando applicazioni "Altro"* (o applicazioni senza supporto specifico per la creazione di volumi), si specifica manualmente la configurazione del volume tramite la finestra di dialogo Aggiungi/Modifica volumi.

Passaggi

1. Eseguire una delle seguenti operazioni:
   - Seleziona l'opzione **Crea volumi per un carico di lavoro esistente** per creare volumi per un carico di lavoro esistente.
   - Seleziona l'opzione **Crea un nuovo carico di lavoro** per definire un nuovo carico di lavoro per un'applicazione supportata o per "Other" applicazioni.
     - Dall'elenco a discesa, seleziona il nome dell'applicazione per cui desideri creare il nuovo workload.

       Seleziona una delle voci "Altro" se l'applicazione che intendi utilizzare su questo storage array non è elencata.

     - Inserisci un nome per il workload che desideri creare.
2. Fai clic su **Avanti**.
3. Se il tuo carico di lavoro è associato a un tipo di applicazione supportato, inserisci le informazioni richieste; altrimenti, vai a Passaggio 3: Aggiungi o modifica i volumi.

Passaggio 3: Aggiungi o modifica i volumi

System Manager potrebbe suggerire una configurazione del volume in base all'applicazione o al carico di lavoro selezionato. Questa configurazione del volume è ottimizzata in base al tipo di applicazione che il carico di lavoro supporta. Puoi accettare la configurazione del volume consigliata oppure modificarla secondo necessità. Se hai selezionato una delle applicazioni "Other", devi specificare manualmente i volumi e le caratteristiche che desideri creare.

Prima di iniziare

- I pool o i gruppi di volume devono avere sufficiente capacità libera.
- Il numero massimo di volumi consentiti in un gruppo di volumi è 256.
- Il numero massimo di volumi consentiti in un pool dipende dal modello del sistema storage:
  - 2,048 volumi (EF600, EF600C e E5700 series)
  - 1,024 volumi (EF300 e EF300C)
  - 512 volumi (serie E4000 e E2800)
- Per creare un volume con Data Assurance (DA) abilitato, la connessione host che si intende utilizzare deve supportare DA.

Selezione di un pool o di un gruppo di volumi secure-capable

Se si desidera creare un volume abilitato per DA, selezionare un pool o un gruppo di volumi compatibile con DA (verificare la presenza di **Yes** accanto a "DA" nella tabella dei pool e dei gruppi di volumi candidati).

Le funzionalità DA sono presentate a livello di pool e di gruppo di volumi in System Manager. La protezione DA verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati dai controller fino alle unità. La selezione di un pool o di un gruppo di volumi compatibile con DA per il nuovo volume garantisce che eventuali errori vengano rilevati e corretti.

Se una qualsiasi delle connessioni host sui controller nel tuo storage array non supporta DA, gli host associati non possono accedere ai dati sui volumi abilitati per DA.

- Per creare un volume abilitato alla sicurezza, è necessario creare una chiave di sicurezza per lo storage array.

Selezione di un pool o di un gruppo di volumi secure-capable

Se si desidera creare un volume con funzionalità di sicurezza, selezionare un pool o un gruppo di volumi secure capable (verificare la presenza di **Yes** accanto a "Secure-capable" nella tabella dei pool e dei gruppi di volumi candidati).

Le funzionalità di sicurezza delle unità vengono presentate a livello di pool e di gruppo di volumi in System Manager. Le unità con funzionalità di sicurezza impediscono l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage. Un'unità con funzionalità di sicurezza crittografa i dati durante la scrittura e li decrittografa durante la lettura utilizzando una chiave di crittografia univoca.

Un pool o un gruppo di volumi può contenere sia unità secure-capable che unità non secure-capable, ma tutte le unità devono essere secure-capable per poter utilizzare le loro funzionalità di crittografia.

- Per creare un volume con allocazione di risorse, tutte le unità devono essere unità NVMe con l'opzione Deallocated or Unwritten Logical Block Error (DULBE).

Informazioni su questa attività

È possibile creare volumi da pool o gruppi di volumi. La finestra di dialogo Aggiungi/Modifica volumi mostra tutti i pool e i gruppi di volumi idonei presenti nell'array di storage. Per ogni pool e gruppo di volumi idoneo, vengono visualizzati il numero di unità disponibili e la capacità libera totale.

Per alcuni carichi di lavoro specifici dell'applicazione, ogni pool o gruppo di volumi idoneo mostra la capacità proposta in base alla configurazione del volume suggerita e mostra la capacità libera rimanente in GiB. Per altri carichi di lavoro, la capacità proposta viene visualizzata man mano che si aggiungono volumi a un pool o a un gruppo di volumi e si specifica la capacità riportata.

Passaggi

1. Scegli una di queste azioni in base al fatto che tu abbia selezionato Other o un carico di lavoro specifico dell'applicazione:
   - **Altro** — Fai clic su **Aggiungi nuovo volume** in ogni pool o gruppo di volumi che vuoi usare per creare uno o più volumi.

Dettagli del campo

Campo	Descrizione
Nome volume	A un volume viene assegnato un nome predefinito da System Manager durante la sequenza di creazione del volume. È possibile accettare il nome predefinito oppure fornire uno più descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità segnalata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TiB). Per i volumi Thick, la capacità minima è 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tieni presente che la capacità di storage è necessaria anche per i servizi di copia (snapshot images, snapshot volumes, volume copies e remote mirrors); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 GiB o 8 GiB, a seconda del tipo di unità. Qualsiasi capacità che non sia un multiplo di 4 o 8 GiB viene allocata ma non è utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4 GiB o 8 GiB. Se esiste capacità inutilizzabile, l'unico modo per recuperarla è aumentare la capacità del volume.
Dimensione blocco volume (EF300 e EF600 solo)	Mostra le dimensioni dei blocchi che possono essere creati per il volume: • 512 — 512 byte • 4K — 4,096 byte

Campo	Descrizione
Dimensione del segmento	Mostra l'impostazione per la dimensione del segmento, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare la dimensione del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — System Manager determina le transizioni di dimensione del segmento che sono consentite. Le dimensioni dei segmenti che rappresentano transizioni inappropriate rispetto alla dimensione corrente del segmento non sono disponibili nell'elenco a discesa. Le transizioni consentite sono solitamente il doppio o la metà della dimensione corrente del segmento. Ad esempio, se la dimensione corrente 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 abilitata** — È possibile specificare una dimensione del segmento di 4 KiB per i volumi con Cache SSD abilitata. Assicurarsi di selezionare la dimensione del segmento di 4 KiB solo per i volumi con Cache SSD abilitata che gestiscono operazioni di I/O a blocchi di piccole dimensioni (ad esempio, dimensioni di blocchi I/O di 16 KiB o inferiori). Le prestazioni potrebbero risentirne se si seleziona 4 KiB come dimensione del segmento per i volumi con Cache SSD abilitata che gestiscono operazioni sequenziali a blocchi di grandi dimensioni. **Tempo necessario per modificare la dimensione del segmento** — Il tempo necessario per modificare la dimensione del segmento di un volume dipende da queste variabili: • Il carico I/O dall'host • La priorità di modifica del volume • Il numero di unità nel gruppo di volumi • Il numero di canali drive • La potenza di elaborazione dei controller degli array di storage Quando si modifica la dimensione del segmento di un volume, le prestazioni di I/O sono influenzate, ma i dati rimangono disponibili.
Compatibile con la sicurezza	**Sì** appare accanto a "Secure-capable" solo se le unità nel pool o nel gruppo di volumi sono secure-capable. Drive Security impedisce l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage. Questa opzione è disponibile solo quando la funzione Drive Security è stata abilitata e una chiave di sicurezza è stata configurata per l'array di storage. Un pool o un gruppo di volumi può contenere sia unità secure-capable che unità non secure-capable, ma tutte le unità devono essere secure-capable per poter utilizzare le loro funzionalità di crittografia.

Campo	Descrizione
DA	**Sì** compare accanto a "DA" solo se le unità nel pool o nel gruppo di volumi supportano Data Assurance (DA). 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 durante il trasferimento dei dati attraverso i controller fino alle unità. L'utilizzo di DA per il nuovo volume garantisce che eventuali errori vengano rilevati.
Risorsa allocata (solo EF300 e EF600)	**Sì** viene visualizzato accanto a "Resource provisioned" solo se le unità supportano questa opzione. Resource Provisioning è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background.

- **Carico di lavoro specifico dell'applicazione** — Fare clic su **Avanti** per accettare i volumi e le caratteristiche consigliati dal sistema per il carico di lavoro selezionato, oppure fare clic su **Modifica volumi** per modificare, aggiungere o eliminare i volumi e le caratteristiche consigliati dal sistema per il carico di lavoro selezionato.

Dettagli del campo

Campo	Descrizione
Nome volume	A un volume viene assegnato un nome predefinito da System Manager durante la sequenza di creazione del volume. È possibile accettare il nome predefinito oppure fornire uno più descrittivo che indichi il tipo di dati memorizzati nel volume.
Capacità segnalata	Definire la capacità del nuovo volume e le unità di capacità da utilizzare (MiB, GiB o TiB). Per i volumi Thick, la capacità minima è 1 MiB e la capacità massima è determinata dal numero e dalla capacità delle unità nel pool o nel gruppo di volumi. Tieni presente che la capacità di storage è necessaria anche per i servizi di copia (snapshot images, snapshot volumes, volume copies e remote mirrors); pertanto, non allocare tutta la capacità ai volumi standard. La capacità in un pool viene allocata in incrementi di 4 GiB o 8 GiB, a seconda del tipo di unità. Qualsiasi capacità che non sia un multiplo di 4 o 8 GiB viene allocata ma non è utilizzabile. Per assicurarsi che l'intera capacità sia utilizzabile, specificare la capacità in incrementi di 4 GiB o 8 GiB. Se esiste 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 che è stato creato per un carico di lavoro specifico dell'applicazione.
Dimensione blocco volume (EF300 e EF600 solo)	Mostra le dimensioni dei blocchi che possono essere creati per il volume: • 512 — 512 byte • 4K — 4,096 byte

Campo	Descrizione
Dimensione del segmento	Mostra l'impostazione per la dimensione del segmento, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare la dimensione del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — System Manager determina le transizioni di dimensione del segmento che sono consentite. Le dimensioni dei segmenti che rappresentano transizioni inappropriate rispetto alla dimensione corrente del segmento non sono disponibili nell'elenco a discesa. Le transizioni consentite sono solitamente il doppio o la metà della dimensione corrente del segmento. Ad esempio, se la dimensione corrente 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 abilitata** — È possibile specificare una dimensione del segmento di 4 KiB per i volumi con Cache SSD abilitata. Assicurarsi di selezionare la dimensione del segmento di 4 KiB solo per i volumi con Cache SSD abilitata che gestiscono operazioni di I/O a blocchi di piccole dimensioni (ad esempio, dimensioni di blocchi I/O di 16 KiB o inferiori). Le prestazioni potrebbero risentirne se si seleziona 4 KiB come dimensione del segmento per i volumi con Cache SSD abilitata che gestiscono operazioni sequenziali a blocchi di grandi dimensioni. **Tempo necessario per modificare la dimensione del segmento** — Il tempo necessario per modificare la dimensione del segmento di un volume dipende da queste variabili: • Il carico I/O dall'host • La priorità di modifica del volume • Il numero di unità nel gruppo di volumi • Il numero di canali drive • La potenza di elaborazione dei controller degli array di storage Quando si modifica la dimensione del segmento di un volume, le prestazioni di I/O vengono influenzate, ma i dati rimangono disponibili.

Campo	Descrizione
Compatibile con la sicurezza	**Sì** appare accanto a "Secure-capable" solo se le unità nel pool o nel gruppo di volumi sono secure-capable. La protezione dell'unità impedisce l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage. Questa opzione è disponibile solo se la funzionalità di protezione dell'unità è stata abilitata e se è stata configurata una chiave di sicurezza per l'array di storage. Un pool o un gruppo di volumi può contenere sia unità secure-capable che unità non secure-capable, ma tutte le unità devono essere secure-capable per poter utilizzare le loro funzionalità di crittografia.
DA	**Sì** compare accanto a "DA" solo se le unità nel pool o nel gruppo di volumi supportano Data Assurance (DA). 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 durante il trasferimento dei dati attraverso i controller fino alle unità. L'utilizzo di DA per il nuovo volume garantisce che eventuali errori vengano rilevati.
Risorsa allocata (solo EF300 e EF600)	**Sì** viene visualizzato accanto a "Resource Provisioned" solo se le unità supportano questa opzione. Resource Provisioning è una funzionalità disponibile negli array di storage EF300 e EF600, che consente di mettere in uso i volumi immediatamente senza alcun processo di inizializzazione in background.

2. Per continuare la sequenza di creazione del volume per l'applicazione selezionata, fare clic su **Avanti** e andare a Passaggio 4: Rivedi la configurazione del volume.

Passaggio 4: Rivedi la configurazione del volume

Esamina un riepilogo dei volumi che intendi creare e apporta le modifiche necessarie.

Passaggi

1. Rivedi i volumi che desideri creare. Fai clic su **Back** per apportare eventuali modifiche.
2. Quando sei soddisfatto della configurazione del volume, fai clic su **Finish**.

Risultati

System Manager crea i nuovi volumi nei pool e nei gruppi di volumi selezionati, quindi visualizza i nuovi volumi nella tabella Tutti i volumi.

Dopo aver finito

- Eseguire tutte le modifiche necessarie al sistema operativo sull'host dell'applicazione affinché le applicazioni possano utilizzare il volume.
- Eseguire l'utilità specifica del sistema operativo (disponibile presso un fornitore di terze parti), quindi eseguire il comando SMcli `-identifyDevices` per correlare i nomi dei volumi con i nomi degli array di storage host.

  SMcli è disponibile direttamente tramite SANtricity System Manager. Questa versione scaricabile di SMcli è disponibile sui controller E4000, EF600, EF600C, EF300, EF300C, E5700, EF570, E2800 e EF280. Per scaricare SMcli all'interno di SANtricity System Manager, selezionare **Impostazioni** > **Sistema** e **Componenti aggiuntivi** > **Interfaccia a riga di comando**.

Aggiungere volumi a un workload in SANtricity System Manager

È possibile aggiungere uno o più volumi a un carico di lavoro esistente o nuovo per i volumi che non sono attualmente associati a un carico di lavoro.

Informazioni su questa attività

I volumi non sono associati a un workload se sono stati creati tramite la command line interface (CLI) o se sono stati migrati (importati/esportati) da un diverso storage array.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona la scheda **Applications & Workloads**.

   Viene visualizzata la vista Applications & Workloads.

3. Seleziona **Add to Workload**.

   Viene visualizzata la finestra di dialogo Select Workload.

4. Eseguire una delle seguenti azioni:
   - **Aggiungi volumi a un workload esistente** — Seleziona questa opzione per aggiungere volumi a un workload esistente.

     Utilizza l'elenco a discesa per selezionare un carico di lavoro. Il tipo di applicazione associato al carico di lavoro viene assegnato ai volumi che aggiungi a questo carico di lavoro.

   - **Aggiungi volumi a un nuovo workload** — Seleziona questa opzione per definire un nuovo workload per un application type e aggiungere volumi al nuovo workload.
5. Seleziona **Avanti** per continuare con la sequenza di aggiunta al workload.

   Viene visualizzata la finestra di dialogo Seleziona volumi.

6. Seleziona i volumi che desideri aggiungere al workload.
7. Esamina i volumi che desideri aggiungere al workload selezionato.
8. Quando sei soddisfatto della configurazione del workload, fai clic su **Finish**.

Gestisci i volumi

Aumentare la capacità di un volume in SANtricity System Manager

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

Prima di iniziare

- È disponibile una capacità libera sufficiente nel pool o nel gruppo di volumi associato al volume.
- Il volume è ottimale e non si trova in alcuno stato di modifica.
- La capacità massima riportata di 256 TiB non è stata raggiunta per i volumi thin.
- Nessuna unità hot spare è in uso nel volume. (Si applica solo ai volumi nei gruppi di volumi.)

> È possibile espandere la capacità del volume fino a 128 TiB alla volta.

Informazioni su questa attività

Tieni presente eventuali requisiti di capacità futuri che potresti avere per altri volumi in questo pool o volume group. Assicurati di lasciare spazio libero sufficiente per creare snapshot, volumi snapshot o mirror remoti.

> L'aumento della capacità di un volume è supportato solo su determinati sistemi operativi. Se si aumenta la capacità del volume su un sistema operativo host non supportato, la capacità espansa è inutilizzabile e non è possibile ripristinare la capacità originale del volume.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona il volume per cui desideri aumentare la capacità, quindi seleziona **Aumenta capacità**.

   Viene visualizzata la finestra di dialogo Confirm Increase Capacity.

3. Seleziona **Yes** per continuare.

   Viene visualizzata la finestra di dialogo Increase Reported Capacity.

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

4. Utilizza la casella **Aumenta la capacità segnalata aggiungendo…** per aggiungere capacità alla capacità segnalata attualmente disponibile. Puoi modificare il valore della capacità da visualizzare in mebibyte (MiB), gibibyte (GiB) o tebibyte (TiB).
5. Fai clic su **Increase**.

Risultati

- System Manager aumenta la capacità del volume in base alla tua selezione.
- Selezionare **Home › View Operations in Progress** per visualizzare l'avanzamento dell'operazione di aumento della capacità attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e potrebbe influire sulle prestazioni del sistema.

Dopo aver finito

Dopo aver espanso la capacità del volume, è necessario aumentare manualmente le dimensioni del file

system in modo che corrispondano. Come farlo dipende dal file system in uso. Consultare la documentazione del sistema operativo host per dettagli.

Inizializzare i volumi in SANtricity System Manager

Un volume viene inizializzato automaticamente al momento della sua creazione. Tuttavia, il Recovery Guru potrebbe consigliare di inizializzare manualmente un volume per ripristinare 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 stato ottimale e non sono in corso operazioni di modifica sul volume.

> Non è possibile annullare l'operazione una volta avviata. Tutti i dati del volume vengono cancellati. Non tentare questa operazione a meno che il Recovery Guru non lo consigli. Contatta il supporto tecnico prima di iniziare questa procedura.

Informazioni su questa attività

Quando si inizializza un volume, il volume mantiene il proprio WWN, le assegnazioni host, la capacità allocata e le impostazioni di capacità riservata. Mantiene inoltre le stesse impostazioni di Data Assurance (DA) e di sicurezza.

I seguenti tipi di volumi *non* possono essere inizializzati:

- Volume base di un volume snapshot
- Volume primario in una relazione speculare
- Volume secondario in una relazione speculare
- Volume di origine in una copia volume
- Volume di destinazione in una copia del volume
- Volume che ha già un'inizializzazione in corso

Questo argomento si applica solo ai volumi standard creati da pool o gruppi di volumi.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona un volume qualsiasi, quindi seleziona **More › Initialize volumes**.

   Viene visualizzata la finestra di dialogo Inizializza volumi. Tutti i volumi sull'array di storage vengono visualizzati in questa finestra di dialogo.

3. Seleziona uno o più volumi che desideri inizializzare e conferma che vuoi eseguire l'operazione.

Risultati

System Manager esegue le seguenti azioni:

- Cancella tutti i dati dai volumi che sono stati inizializzati.

- Cancella gli indici dei blocchi, il che fa sì che i blocchi non scritti vengano letti come se fossero riempiti di zeri (il volume appare completamente vuoto).

Selezionare **Home › Visualizza operazioni in corso** per visualizzare l'avanzamento dell'operazione di inizializzazione attualmente in esecuzione per il volume selezionato. Questa operazione può essere lunga e potrebbe influire sulle prestazioni del sistema.

Ridistribuire i volumi in SANtricity System Manager

Si ridistribuiscono i volumi per riportarli ai rispettivi controller proprietari preferiti. In genere, i driver multipath spostano i volumi dal controller proprietario 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 verificheranno errori di I/O.
- Su tutti gli host che utilizzano i volumi che si desidera ridistribuire è installato un driver multipath, oppure si verificheranno errori di I/O.

  Se si desidera ridistribuire i volumi senza un driver multipath sugli host, tutte le attività di I/O sui volumi *mentre l'operazione di ridistribuzione è in corso* devono essere interrotte per evitare errori dell'applicazione.

Informazioni su questa attività

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

Passaggi

1. Selezionare **Storage › Volumes**.
2. Selezionare **More › Ridistribuisci volumi**.

   Viene visualizzata la finestra di dialogo Ridistribuisci volumi. Tutti i volumi sullo storage array il cui proprietario del controller preferito non corrisponde al proprietario corrente vengono visualizzati in questa finestra di dialogo.

3. Seleziona uno o più volumi che desideri ridistribuire e conferma di voler eseguire l'operazione.

Risultati

System Manager sposta i volumi selezionati sui rispettivi controller proprietari oppure potrebbe essere visualizzata una finestra di dialogo Redistribuisci volumi non necessari.

Modificare la proprietà del controller di un volume in SANtricity System Manager

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 arrestate. Questa operazione previene errori delle applicazioni quando cambia il percorso di I/O.

Informazioni su questa attività

È possibile modificare la proprietà del controller per uno o più volumi in un pool o gruppo di volumi.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona un volume qualsiasi, quindi seleziona **More › Change ownership**.

   Viene visualizzata la finestra di dialogo Cambia proprietà del volume. Tutti i volumi sull'array di storage vengono visualizzati in questa finestra di dialogo.

3. Utilizza l'elenco a discesa **Proprietario preferito** per modificare il controller preferito per ciascun volume che desideri modificare e conferma che vuoi eseguire l'operazione.

Risultati

- System Manager modifica la proprietà del controller del volume. L'I/O verso il volume viene ora indirizzato attraverso questo percorso I/O.
- Il volume potrebbe non utilizzare il nuovo percorso I/O finché il driver multipath non si riconfigura per riconoscere il nuovo percorso. Questa operazione richiede in genere meno di cinque minuti.

Elimina un volume in SANtricity System Manager

In genere, si eliminano i volumi se sono stati creati con parametri o capacità errati, non soddisfano più le esigenze di configurazione dello storage o sono immagini Snapshot non più necessarie per il backup o il test delle applicazioni.

L'eliminazione di un volume aumenta la capacità libera nel pool o nel gruppo di volumi. È possibile selezionare uno o più volumi da eliminare.

Prima di iniziare

Per i volumi che si intende eliminare, assicurarsi di quanto segue:

- Tutti i dati sono sottoposti a backup.
- Tutte le operazioni di Input/Output (I/O) sono interrotte.
- Tutti i dispositivi e i file system sono smontati.

Informazioni su questa attività

Non è possibile eliminare un volume che presenta una delle seguenti condizioni:

- Il volume è in fase di inizializzazione.
- Il volume è in fase di ricostruzione.
- Il volume fa parte di un gruppo di volumi che contiene un'unità che sta subendo un'operazione di copyback.
- Il volume è in fase di un'operazione di modifica, come una modifica delle dimensioni del segmento, a meno che il volume non sia ora nello stato Failed.
- Il volume detiene un qualsiasi tipo di prenotazione persistente.
- Il volume è un volume di origine o un volume di destinazione in un Copy Volume che ha uno stato di Pending, In Progress o Failed.

L'eliminazione di un volume comporta la perdita di tutti i dati presenti su tali volumi.

Quando un volume supera una determinata dimensione (attualmente 128 TB) l'eliminazione viene eseguita in background e lo spazio liberato potrebbe non essere immediatamente disponibile.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Fai clic su **Delete**.

   Viene visualizzata la finestra di dialogo Delete Volumes.

3. Seleziona uno o più volumi che desideri eliminare e conferma che vuoi eseguire l'operazione.
4. Fai clic su **Delete**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutte le immagini Snapshot, le pianificazioni e i volumi Snapshot associati.
- Rimuove qualsiasi relazione di mirroring.
- Aumenta lo spazio libero nel pool o nel gruppo di volumi.

Modifica il limite di capacità allocata per un thin volume in SANtricity System Manager

Per i volumi thin in grado di allocare spazio su richiesta, è possibile modificare il limite che limita la capacità allocata a cui un volume thin può espandersi automaticamente.

È inoltre possibile modificare la percentuale oltre la quale viene inviato un avviso (superamento della soglia di allarme) all'area Notifiche nella pagina iniziale quando un volume thin si avvicina al limite di capacità allocata. È possibile scegliere di attivare o disattivare questa notifica di avviso.

Questa funzionalità non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

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

Quando si modificano il limite di capacità allocata e la soglia di avviso di un volume thin, è necessario tenere conto dello spazio che verrà consumato sia dai dati utente del volume sia dai dati dei servizi di copia.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona la scheda **Thin Volume Monitoring**.

   Viene visualizzata la vista Thin Volume Monitoring.

3. Seleziona il volume sottile che desideri modificare, quindi seleziona **Change Limit**.

   Viene visualizzata la finestra di dialogo Modifica limite. Il limite di capacità allocato e l'impostazione della

soglia di avviso per il volume thin selezionato vengono visualizzati in questa finestra di dialogo.

4. Modifica il limite di capacità assegnata e la soglia di avviso secondo necessità.

Dettagli del campo

Impostazione	Descrizione
Modifica il limite di capacità assegnata a…	La soglia oltre la quale le operazioni di scrittura falliscono, impedendo al volume thin di consumare risorse aggiuntive. Questa soglia è una percentuale della capacità dichiarata del volume.
Avvisami quando… (soglia di allarme)	Seleziona la check box se desideri che il sistema generi un avviso quando un thin volume si avvicina al limite di capacità allocata. L'avviso viene inviato all'area Notifiche nella pagina iniziale. Questa soglia è una percentuale della dimensione di capacità dichiarata del volume. Deselezionare la check box per disattivare la notifica di avviso della soglia di avvertimento.

5. Fare clic su **Save**.

Gestisci le impostazioni

Modificare le impostazioni di un volume in SANtricity System Manager

È possibile modificare le impostazioni di un volume, come il nome, l'assegnazione all'host, la dimensione del segmento, la priorità di modifica, la cache e così via.

Prima di iniziare

Il volume che si desidera modificare è in stato Optimal.

> Alcune operazioni potrebbero non essere disponibili mentre sono in corso modifiche alle impostazioni del volume

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona il volume che desideri modificare, quindi seleziona **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni volume. Le impostazioni di configurazione del volume selezionato vengono visualizzate in questa finestra di dialogo.

3. Seleziona la scheda **Basic** per modificare il nome del volume e l'assegnazione dell'host.

Dettagli del campo

Impostazione	Descrizione
Nome	Visualizza il nome del volume. Modifica il nome di un volume quando quello attuale non è più significativo o appropriato.
Capacità	Visualizza la capacità dichiarata e allocata per il volume selezionato. La capacità dichiarata e la capacità allocata coincidono per i volumi thick, ma sono diverse per i volumi thin. Per un volume thick, lo spazio fisicamente allocato è uguale allo spazio dichiarato all'host. Per un volume thin, la capacità dichiarata è la capacità dichiarata all'host, mentre la capacità allocata è la quantità di spazio su disco attualmente allocata per la scrittura dei dati.
Pool / Gruppo di volumi	Visualizza il nome e il livello RAID del pool o del gruppo di volumi. Indica se il pool o il gruppo di volumi è secure-capable e secure-enabled.
Host	Visualizza l'assegnazione del volume. Si assegna un volume a un host o a un cluster di host in modo che sia possibile accedervi per le operazioni di I/O. Questa assegnazione garantisce a un host o a un cluster di host l'accesso a un volume specifico o a più volumi in un array di storage. • **Assegnato a** — Identifica l'host o il cluster che ha accesso al volume selezionato. • **LUN** — Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzamento che un host utilizza per accedere a un volume. Il volume viene presentato all'host come capacità sotto forma di LUN. Ogni host ha il proprio spazio di indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi diversi. Per le interfacce NVMe, questa colonna visualizza Namespace ID. Un namespace è uno storage NVM formattato per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che corrisponde a un volume nell'array di storage. Il namespace ID è l'identificatore univoco del controller NVMe per il namespace e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.

Impostazione	Descrizione
Identificatori	Visualizza gli identificativi per il volume selezionato. • **Identificatore mondiale (WWID)** — Un identificatore esadecimale univoco per il volume. • **Identificatore univoco esteso (EUI)** — Un identificatore EUI-64 per il volume. • **Identificativo del sottosistema (SSID)** — L'identificativo del sottosistema dell'array di storage di un volume.

4. Seleziona la scheda **Advanced** per modificare ulteriori impostazioni di configurazione per un volume in un pool o in un gruppo di volumi.

Dettagli del campo

Impostazione	Descrizione
Informazioni sull'applicazione e sul carico di lavoro	Durante la creazione del volume, puoi creare carichi di lavoro specifici per l'applicazione o altri carichi di lavoro. Se applicabile, per il volume selezionato vengono visualizzati il nome del carico di lavoro, il tipo di applicazione e il tipo di volume. È possibile modificare il nome del carico di lavoro, se lo si desidera.
Impostazioni Quality of Service	**Disabilita definitivamente Data Assurance** — Questa impostazione viene visualizzata solo se il volume è abilitato per Data Assurance (DA). DA verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati dai controller alle unità. Utilizzare questa opzione per disabilitare definitivamente DA sul volume selezionato. Quando è disabilitata, DA non può essere riabilitata su questo volume. **Abilita il controllo di ridondanza pre-lettura** — Questa impostazione viene visualizzata solo se il volume è un volume thick. I controlli di ridondanza pre-lettura determinano se i dati su un volume sono coerenti ogni volta che viene eseguita una lettura. Un volume con questa funzione abilitata restituisce errori di lettura se i dati vengono determinati come incoerenti dal firmware del controller.
Proprietà del controller	Definisce il controller che è designato come controller proprietario, o primario, del volume. La gestione dei controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per il totale degli I/O.

Impostazione	Descrizione
Dimensionamento del segmento	Mostra l'impostazione per la dimensione del segmento, che viene visualizzata solo per i volumi in un gruppo di volumi. È possibile modificare la dimensione del segmento per ottimizzare le prestazioni. **Transizioni consentite per le dimensioni dei segmenti** — System Manager determina le transizioni di dimensione del segmento che sono consentite. Le dimensioni dei segmenti che rappresentano transizioni inappropriate rispetto alla dimensione corrente del segmento non sono disponibili nell'elenco a discesa. Le transizioni consentite sono solitamente il doppio o la metà della dimensione corrente del segmento. Ad esempio, se la dimensione corrente 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 abilitata** — È possibile specificare una dimensione del segmento di 4 KiB per i volumi con Cache SSD abilitata. Assicurarsi di selezionare la dimensione del segmento di 4 KiB solo per i volumi con Cache SSD abilitata che gestiscono operazioni di I/O a blocchi di piccole dimensioni (ad esempio, dimensioni di blocchi I/O di 16 KiB o inferiori). Le prestazioni potrebbero risentirne se si seleziona 4 KiB come dimensione del segmento per i volumi con Cache SSD abilitata che gestiscono operazioni sequenziali a blocchi di grandi dimensioni. **Tempo necessario per modificare la dimensione del segmento** — Il tempo necessario per modificare la dimensione del segmento di un volume dipende da queste variabili: • Il carico I/O dall'host • La priorità di modifica del volume • Il numero di unità nel gruppo di volumi • Il numero di canali drive • La potenza di elaborazione dei controller degli array di storage Quando si modifica la dimensione del segmento di un volume, le prestazioni di I/O vengono influenzate, ma i dati rimangono disponibili.
Priorità di modifica	Mostra l'impostazione per la priorità di modifica, che appare solo per i volumi in un gruppo di volumi. La priorità di modifica definisce la quantità di tempo di elaborazione allocata alle 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. Sposta le barre di scorrimento per selezionare un livello di priorità. **Livelli di priorità di modifica** — Il livello di priorità più basso favorisce le prestazioni del sistema, ma l'operazione di modifica richiede più tempo. Il livello di priorità più alto favorisce l'operazione di modifica, ma le prestazioni del sistema potrebbero essere compromesse.

Impostazione	Descrizione
Caching	Mostra l'impostazione di caching, che puoi modificare per influire sulle prestazioni I/O complessive di un volume.
Cache SSD	Mostra l'impostazione Cache SSD, che è possibile abilitare sui volumi compatibili come modo per migliorare le prestazioni in sola lettura. I volumi sono compatibili se condividono le stesse funzionalità di Drive Security e Data Assurance. **La funzionalità Cache SSD utilizza uno o più dischi a stato solido (SSD) per implementare una cache di lettura**. Le prestazioni delle applicazioni sono migliorate grazie ai tempi di lettura più rapidi degli SSD. Poiché la cache di lettura si trova nell'array di storage, la cache viene condivisa tra tutte le applicazioni che utilizzano l'array di storage. È sufficiente selezionare il volume che si desidera mettere in cache e la memorizzazione nella cache sarà automatica e dinamica.

5. Fare clic su **Save**.

   System Manager modifica le impostazioni del volume in base alle selezioni.

Dopo aver finito

Selezionare **Home › Visualizza operazioni in corso** per visualizzare lo stato di avanzamento delle operazioni di modifica attualmente in esecuzione per il volume selezionato.

Modificare le impostazioni del carico di lavoro in SANtricity System Manager

È possibile modificare il nome di un workload e visualizzarne il tipo di applicazione associato. Modificare il nome di un workload quando quello attuale non è più significativo o appropriato.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona la scheda **Applications & Workloads**.

   Viene visualizzata la vista Applications & Workloads.

3. Seleziona il workload che desideri modificare, quindi seleziona **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Applications & Workloads Settings.

4. **Facoltativo:** Modifica il nome del workload fornito dall'utente.
5. Fare clic su **Save**.

Modificare le impostazioni della cache per un volume in SANtricity System Manager

È possibile modificare le impostazioni della cache di lettura e della cache di scrittura per influire sulle prestazioni I/O complessive di un volume.

Informazioni su questa attività

Tenete a mente queste linee guida quando modificate le impostazioni della cache per un volume:

- Dopo aver aperto la finestra di dialogo Modifica impostazioni cache, potresti visualizzare 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 si sta caricando, quando un controller è stato rimosso o se il controller ha rilevato una discrepanza nelle dimensioni della cache. Dopo che la condizione è stata risolta, le proprietà della cache selezionate nella finestra di dialogo diventano attive. Se le proprietà della cache selezionate non diventano attive, contattare il supporto tecnico.

- È possibile modificare le impostazioni della cache per un singolo volume o per più volumi su un array di storage. È possibile modificare le impostazioni della cache per tutti i volumi standard o per tutti i volumi thin contemporaneamente.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona un volume qualsiasi, quindi seleziona **Altro › Modifica impostazioni cache**.

   Viene visualizzata la finestra di dialogo Modifica impostazioni cache. Tutti i volumi sull'array di storage vengono visualizzati in questa finestra di dialogo.

3. Seleziona la scheda **Basic** per modificare le impostazioni della cache di lettura e della cache di scrittura.

   Dettagli del campo

Impostazione della cache	Descrizione
Cache di lettura	La cache di lettura è un buffer che memorizza i dati letti dalle unità. I dati per un'operazione di lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando la necessità di accedere alle unità. I dati rimangono nella cache di lettura finché non vengono svuotati.
Cache di scrittura	La cache di scrittura è un buffer che memorizza i dati provenienti dall'host che non sono ancora stati scritti sulle unità. I dati rimangono nella cache di scrittura finché non vengono scritti sulle unità. La cache di scrittura può aumentare le prestazioni di I/O. La cache viene svuotata automaticamente dopo che la **Write caching** è stata disabilitata per un volume.

4. Seleziona la scheda **Advanced** per modificare le impostazioni avanzate per i volumi thick. Le impostazioni avanzate della cache sono disponibili solo per i volumi thick.

Dettagli del campo

Impostazione della cache	Descrizione
Precaricamento dinamico della cache di lettura	Il precaricamento dinamico della cache di lettura consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i blocchi di dati da un'unità alla cache. Questo caching aumenta la probabilità che le future richieste di dati possano essere soddisfatte dalla cache. Il precaricamento dinamico della cache di lettura è importante per le applicazioni multimediali che utilizzano I/O sequenziale. La velocità e la quantità di dati precaricati nella cache si regolano automaticamente in base alla velocità e alla dimensione delle richieste di lettura dell'host. L'accesso casuale non comporta il precaricamento dei dati nella cache. Questa funzionalità non si applica quando il caching di lettura è disabilitato. Per un volume thin, il precaricamento dinamico della cache di lettura è sempre disabilitato e non può essere modificato.
Cache di scrittura senza batteria	L'impostazione cache di scrittura senza batterie consente alla cache di scrittura di continuare anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta della cache di scrittura senza batterie non è generalmente raccomandata, perché i dati potrebbero andare persi in caso di perdita di alimentazione. In genere, la cache di scrittura viene disattivata temporaneamente dal controller fino a quando le batterie non sono cariche o una batteria guasta viene sostituita. **Possibile perdita di dati** — Se si seleziona questa opzione e non si dispone di un alimentatore universale di protezione, si potrebbero perdere dati. Inoltre, si potrebbero perdere dati se non si dispone di batterie per il controller e si abilita l'opzione **Write caching without batteries**. Questa impostazione è disponibile solo se è stata abilitata la cache di scrittura. Questa impostazione non è disponibile per i volumi thin.
Cache di scrittura con mirroring	La cache di scrittura con mirroring si verifica quando i dati scritti nella cache di un controller vengono scritti anche nella 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 la cache di scrittura è abilitata e sono presenti due controller. La cache di scrittura con mirroring è l'impostazione predefinita alla creazione del volume. Questa impostazione è disponibile solo se è stata abilitata la cache di scrittura. Questa impostazione non è disponibile per i volumi thin.

5. Fai clic su **Salva** per modificare le impostazioni della cache.

Modificare le impostazioni di scansione dei supporti per un volume in SANtricity System Manager

La scansione dei supporti è un'operazione in background che analizza tutti i dati e le informazioni di ridondanza presenti nel volume. Utilizzare questa opzione per abilitare o disabilitare le impostazioni di scansione dei supporti per uno o più volumi, oppure per modificarne la durata.

Prima di iniziare

Comprendi quanto segue:

- Le scansioni dei supporti vengono eseguite in modo continuo a una velocità costante, in base alla capacità da scansionare e alla durata della scansione. Le scansioni in background possono essere temporaneamente sospese da un'attività in background a priorità più elevata (ad esempio, la ricostruzione), ma riprenderanno alla stessa velocità costante.
- Un volume viene scansionato solo quando l'opzione di scansione dei supporti è abilitata per l'array di storage e per quel volume. Se il controllo di ridondanza è anche abilitato 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 di ridondanza è abilitata per impostazione predefinita per ogni volume al momento della sua creazione.
- Se durante la scansione si verifica un errore irreversibile del supporto di memorizzazione, i dati verranno riparati utilizzando le informazioni di ridondanza, se disponibili.

  Ad esempio, le informazioni sulla ridondanza sono disponibili nei volumi RAID 5 ottimali o nei volumi RAID 6 che sono ottimali o hanno solo un disco guasto. Se l'errore irreversibile non può essere riparato utilizzando le informazioni sulla ridondanza, il blocco di dati verrà aggiunto al registro dei settori illeggibili. Sia gli errori del supporto correggibili che quelli non correggibili vengono segnalati nel registro eventi.

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

Il periodo di scansione dei supporti predefinito è impostato su 120 giorni.

Informazioni su questa attività

Le scansioni dei supporti rilevano e riparano gli errori sui blocchi del disco che vengono letti raramente dalle applicazioni. Ciò può prevenire la perdita di dati in caso di guasto di un'unità, poiché i dati delle unità guaste vengono ricostruiti utilizzando le informazioni di ridondanza e i dati provenienti da altre unità nel gruppo o pool di volumi.

È possibile eseguire le seguenti azioni:

- Abilita o disabilita la scansione dei supporti in background per l'intero array di archiviazione
- Modifica la durata della scansione per l'intero array di storage
- Attiva o disattiva la scansione dei supporti per uno o più volumi
- Abilitare o disabilitare il controllo di ridondanza per uno o più volumi

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona un volume qualsiasi, quindi seleziona **More › Change media scan settings**.

   Viene visualizzata la finestra di dialogo Modifica impostazioni scansione supporti unità. Tutti i volumi

presenti nell'array di storage vengono visualizzati in questa finestra di dialogo.

3. Per abilitare la scansione dei supporti, selezionare la check box **Scansiona i supporti nel corso di…**.

   Disabilitare la check box della scansione dei supporti sospende tutte le impostazioni di scansione dei supporti.

4. Specifica il numero di giorni durante i quali desideri che venga eseguita la scansione dei supporti.
5. Seleziona la check box **Media Scan** per ogni volume su cui desideri eseguire una scansione dei supporti.

   System Manager abilita l'opzione Controllo ridondanza per ogni volume su cui si sceglie di eseguire una scansione dei supporti. Se ci sono singoli volumi per i quali non si desidera eseguire un controllo di ridondanza, deselezionare la check box **Redundancy Check**.

6. Fare clic su **Save**.

   System Manager applica le modifiche alle scansioni dei supporti in background in base alla tua selezione.

Utilizzare i servizi di copia

Scopri di più su Copy Volume in SANtricity System Manager

La funzione Copia volume consente di creare una copia point-in-time di un volume creando due volumi separati, il volume di origine e il volume di destinazione, sullo stesso storage array.

Questa funzione esegue una copia byte per byte dal volume di origine al volume di destinazione, rendendo i dati sul volume di destinazione identici ai dati sul volume di origine.

Copia dei dati per un accesso più ampio

Quando cambiano i requisiti di storage per un volume, è possibile utilizzare la funzione Copy Volume per copiare i dati da pool o gruppi di volumi che utilizzano drive di capacità inferiore a pool o gruppi di volumi che utilizzano drive di capacità superiore. Ad esempio, è possibile utilizzare la funzione Copy Volume per eseguire le seguenti operazioni:

- Sposta i dati su drive più grandi.
- Passa a unità con un tasso di trasferimento dei dati più elevato.
- Passa a unità che utilizzano nuove tecnologie per prestazioni superiori.
- Modificare un volume sottile in un volume spesso.

I volumi di origine e di destinazione della copia devono avere le stesse dimensioni dei blocchi logici/indirizzabili dall'host (dimensione del settore) riportate.

Le dimensioni dei blocchi di volume segnalate sono:

- **Dimensione del blocco nativo** – la dimensione del blocco del volume corrisponde alla dimensione del blocco dell'unità, ovvero 512 o 4K.
- **Dimensione del blocco emulata 512** - le unità sono da 4K ma la dimensione del blocco riportata è 512.

Modificare un volume thin in un volume thick

Se si desidera convertire un volume sottile in un volume spesso, utilizzare l'operazione Copy Volume per creare una copia del volume sottile. La destinazione di un'operazione Copy Volume è sempre un volume spesso.

System Manager non offre la possibilità di creare volumi con thin provisioning. Se si desidera creare volumi con thin provisioning, utilizzare la Command Line Interface (CLI).

Backup dei dati

La funzione Copia volume consente di eseguire il backup di un volume copiando i dati da un volume a un altro volume sullo stesso storage array. È possibile utilizzare il volume di destinazione come backup del volume di origine, per testare il sistema o per eseguire il backup su un altro dispositivo, come un disco a nastro.

Ripristina i dati del volume Snapshot nel volume base

Se è necessario ripristinare i dati sul volume di base dal volume Snapshot associato, è possibile utilizzare la funzione Copy Volume per copiare i dati dal volume Snapshot al volume di base. È possibile creare una copia del volume dei dati presenti sul volume Snapshot e quindi copiare i dati sul volume di base.

Volumi di origine e di destinazione

La tabella seguente specifica i tipi di volumi che possono essere utilizzati come volume di origine e volume di destinazione con la funzione Copy Volume.

Tipo di volume	Volume sorgente della copia del volume offline	Volume di origine della copia volume online	Volume di destinazione online e offline
Volume thick in un pool	Sì	Sì	Sì
Volume thick in un gruppo di volumi	Sì	Sì	Sì
Volume sottile	Sì[1]	Sì	No
Volume Snapshot	Sì[2]	No	No
Volume base Snapshot	Sì	Sì	No
volume primario dello specchio remoto	Sì[3]	Sì	No

[1] Il volume di destinazione deve avere una capacità pari o superiore alla capacità riportata del volume sottile.

[2] Non è possibile utilizzare la copia del volume Snapshot fino al completamento dell'operazione di copia online.

[3] Se il volume di origine è un volume primario, la capacità del volume di destinazione deve essere uguale o superiore alla capacità utilizzabile del volume di origine.

Scopri i tipi di operazioni di copia del volume nel software SANtricity

È possibile eseguire un'operazione di Copy Volume o un'operazione di Copy Volume . Un'operazione offline legge i dati da un volume di origine e li copia in un volume di destinazione. Un'operazione online utilizza un volume snapshot come origine e ne copia i dati in un volume di destinazione.

Per garantire l'integrità dei dati, tutte le attività di I/O sul volume di destinazione vengono sospese durante entrambi i tipi di operazione Copy Volume. Questa sospensione si verifica perché lo stato dei dati sul volume di destinazione non è coerente fino al completamento della procedura.

Le operazioni di copia del volume offline e online sono descritte di seguito.

Operazione Offline Copy Volume

La relazione offline Copy Volume è tra un volume di origine e un volume di destinazione. Una copia offline legge i dati dal volume di origine e li copia su un volume di destinazione, sospendendo tutti gli aggiornamenti al volume di origine durante la copia in corso. Tutti gli aggiornamenti al volume di origine vengono sospesi per evitare che vengano create incoerenze cronologiche sul volume di destinazione.

Cosa devi sapere sulle operazioni di copia offline	
Richieste di lettura e scrittura	• I volumi sorgente che partecipano a una copia offline sono disponibili per attività di I/O di sola lettura mentre un'operazione di Copy Volume ha lo stato In Progress o Pending. • Le richieste di scrittura sono consentite dopo che la copia offline è stata completata. • Per evitare messaggi di errore relativi alla protezione da scrittura, non accedere a un volume di origine che partecipa a un'operazione di Copy Volume con stato In Progress.
file system journaling	• Se il volume di origine è stato formattato con un file system journaling, qualsiasi tentativo di inviare una richiesta di lettura al volume di origine potrebbe essere rifiutato dai controller dell'array di storage e potrebbe comparire un messaggio di errore. • Il driver del file system con journaling invia una richiesta di scrittura prima di tentare di inviare la richiesta di lettura. Il controller rifiuta la richiesta di scrittura e la richiesta di lettura potrebbe non essere inviata a causa della richiesta di scrittura rifiutata. Questa condizione potrebbe causare la visualizzazione di un messaggio di errore che indica che il volume di origine è protetto da scrittura. • Per evitare che si verifichi questo problema, non tentare di accedere a un volume di origine che partecipa a una copia offline mentre l'operazione Copy Volume ha lo stato In Progress.

Operazione Online Copy Volume

La relazione di Copy Volume online si instaura tra un volume snapshot e un volume di destinazione. È possibile avviare un'operazione di Copy Volume mentre il volume di origine è online e disponibile per la scrittura dei dati. Questa funzione si ottiene creando uno snapshot del volume e utilizzando lo snapshot come volume di origine effettivo per la copia.

Quando si avvia un'operazione di Copy Volume per un volume di origine, System Manager crea un'immagine snapshot del volume di base e una relazione di copia tra l'immagine snapshot del volume di base e un volume di destinazione. L'utilizzo dell'immagine snapshot come volume di origine consente all'array di storage di continuare a scrivere sul volume di origine mentre la copia è in corso.

Durante un'operazione di copia online, si verifica un impatto sulle prestazioni a causa della procedura copy-on-write. Al termine della copia online, le prestazioni del volume di base vengono ripristinate.

Cosa devi sapere sulle operazioni di copia online	
Che tipo di volumi si possono utilizzare?	• Il volume per il quale viene creata l'immagine point-in-time è noto come volume base e deve essere un volume standard o un volume thin sull'array di storage. • Un volume di destinazione può essere un volume standard in un gruppo di volumi o un volume standard in un pool. Un volume di destinazione non può essere un volume thin o un volume base in un gruppo di snapshot. • È possibile utilizzare la funzione online Copy Volume per copiare i dati da un volume thin a un volume standard in un pool che si trova nello stesso storage array. Ma non è possibile utilizzare la funzione Copy Volume per copiare i dati da un volume standard a un volume thin.
Prestazioni del volume di base	• Se il volume snapshot utilizzato come origine della copia è attivo, le prestazioni del volume di base risultano compromesse a causa delle operazioni di copy-on-write. Al termine della copia, lo snapshot viene disabilitato e le prestazioni del volume di base vengono ripristinate. Anche se lo snapshot è disabilitato, il volume di capacità riservata e la relazione di copia rimangono invariati.
Tipi di volumi creati	• Un volume snapshot e un volume di capacità riservata vengono creati durante l'operazione di copia online. • Il volume snapshot non è un volume effettivo contenente dati; si tratta piuttosto di un riferimento ai dati che erano contenuti su un volume in un momento specifico. • Per ogni snapshot acquisito, viene creato un volume di capacità riservato per contenere i dati relativi allo snapshot. Il volume di capacità riservato viene utilizzato esclusivamente per gestire l'immagine dello snapshot.
volume di capacità riservato	• Prima che un blocco di dati sul volume di origine venga modificato, il contenuto del blocco da modificare viene copiato nel volume di capacità riservata per la conservazione. • Poiché il volume di capacità riservata memorizza copie dei dati originali in quei blocchi di dati, le ulteriori modifiche a quei blocchi di dati vengono scritte solo nel volume di origine. • L'operazione di copia online utilizza meno spazio su disco rispetto a una copia fisica completa perché nel volume di capacità riservata vengono memorizzati solo i blocchi di dati che sono stati modificati dal momento dello snapshot.

Copia un volume in SANtricity System Manager

È possibile copiare i dati da un volume a un altro volume nello stesso array di storage e creare un duplicato fisico point-in-time (clone) di un volume di origine.

Prima di iniziare

- Tutte le attività di I/O verso il volume di origine e il volume di destinazione devono essere interrotte.
- Tutti i file system presenti sul volume di origine e sul volume di destinazione devono essere smontati.
- Se hai utilizzato il volume di destinazione in un'operazione di copia del volume in precedenza, non hai più bisogno di quei dati o li hai già sottoposti a backup.

Informazioni su questa attività

Il volume di origine è il volume che accetta le operazioni di I/O dell'host e memorizza i dati delle applicazioni. Quando si avvia una Copy Volume, i dati dal volume di origine vengono copiati integralmente nel volume di destinazione.

Il volume di destinazione è un volume standard che mantiene una copia dei dati del volume di origine. Il volume di destinazione è identico al volume di origine al termine dell'operazione di copia del volume. Il volume di destinazione deve avere una capacità uguale o superiore a quella del volume di origine; tuttavia, può avere un livello RAID diverso.

Maggiori informazioni sulle copie online e offline

Copia online

Una copia online crea una copia point-in-time di qualsiasi volume all'interno di un array di storage, mentre è ancora possibile scrivere sul volume durante la copia in corso. Questa funzione viene ottenuta creando una Snapshot del volume e utilizzando la Snapshot come vero volume sorgente per la copia. Il volume per il quale viene creata l'immagine point-in-time è noto come base volume e può essere un volume standard o un thin volume nell'array di storage.

Copia offline

Una copia offline legge i dati dal volume di origine e li copia in un volume di destinazione, sospendendo tutti gli aggiornamenti al volume di origine durante la copia in corso. Tutti gli aggiornamenti al volume di origine vengono sospesi per evitare la creazione di incoerenze cronologiche sul volume di destinazione. La relazione di copia del volume offline è tra un volume di origine e un volume di destinazione.

Un'operazione di copia del volume sovrascrive i dati sul volume di destinazione e rende non riusciti tutti i volumi Snapshot associati al volume di destinazione, se presenti.

Passaggi

1. Selezionare **Storage › Volumes**.
2. Seleziona il volume che desideri utilizzare come origine per l'operazione Copy Volume, quindi seleziona **Copy Services › Copy volume**.

   Viene visualizzata la finestra di dialogo Copy Volume-Select Target.

3. Seleziona il volume di destinazione su cui desideri copiare i dati.

   La tabella visualizzata in questa finestra di dialogo elenca tutti i volume di destinazione idonei.

4. Utilizzare la barra di scorrimento per impostare la priorità di copia per l'operazione Copy Volume.

   La priorità di copia determina la quantità di risorse di sistema utilizzate per completare l'operazione Copy Volume rispetto alle richieste di I/O del servizio.

   Ulteriori informazioni sui tassi di priorità di copia

   Esistono cinque tassi di priorità di copia:

   - Più basso
   - Basso
   - Medio
   - Alto
   - Più alto

   Se la priorità di copia è impostata sul tasso di trasferimento dei dati più basso, l'attività di I/O ha la priorità e l'operazione Copy Volume richiede più tempo. Se la priorità di copia è impostata sul tasso di trasferimento dei dati più alto, l'operazione Copy Volume ha la priorità, ma l'attività di I/O per lo storage array potrebbe essere influenzata.

5. Seleziona se desideri creare una copia online o una copia offline. Per creare una copia online, seleziona la check box **Mantieni il volume di origine online durante l'operazione di copia**.
6. Eseguire una delle seguenti operazioni:
   - Per eseguire un'operazione di copia *online*, fare clic su **Avanti** per continuare alla finestra di dialogo **Riserva capacità**.
   - Per eseguire un'operazione di copia offline, fare clic su **Fine** per avviare la copia offline.
7. Se hai scelto di creare una copia online, imposta la capacità riservata necessaria per archiviare dati e altre informazioni per la copia online, quindi fai clic su **Fine** per avviare la copia online.

   La tabella dei volumi candidati visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copy service e oggetto di storage. Non è direttamente leggibile dall'host.

   Assegnare la capacità riservata utilizzando le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base e di solito questa capacità è sufficiente.
   - La capacità riservata, tuttavia, varia a seconda del numero di modifiche apportate ai dati originali. Più a lungo un oggetto di storage è attivo, maggiore dovrebbe essere la capacità riservata.

Risultati

System Manager copia tutti i dati dal volume di origine al volume di destinazione. Al termine dell'operazione di copia del volume, il volume di destinazione diventa automaticamente di sola lettura per gli host.

Dopo aver finito

Selezionare **Home › Visualizza operazioni in corso** per visualizzare l'avanzamento dell'operazione Copy Volume. Questa operazione può essere lunga e potrebbe influire sulle prestazioni del sistema.

Eseguire un’operazione di copia del volume in SANtricity System Manager

È possibile visualizzare un’operazione di Copy Volume in corso e interrompere, modificare la priorità, ricopiare o cancellare un’operazione di Copy Volume.

Passaggi

1. Seleziona **Home › Visualizza operazioni in corso**.

   Viene visualizzata la finestra di dialogo Operations in Progress.

2. Individua l’operazione Copy Volume su cui desideri intervenire, quindi fai clic sul collegamento nella colonna **Actions** per eseguire una delle seguenti azioni.

   Leggere tutti i testi di avviso forniti nelle finestre di dialogo, in particolare quando si interrompe un’operazione.

Azione	Descrizione
Arresta	È possibile interrompere un’operazione Copy Volume mentre lo stato dell’operazione è In Progress, Pending o Failed. Quando la Copy Volume viene interrotta, tutti gli host mappati hanno accesso in scrittura al volume di origine. Se vengono scritti dati sul volume di origine, i dati sul target volume non corrispondono più ai dati sul volume di origine.
Modifica priorità	È possibile modificare la priorità di un’operazione Copy Volume mentre l’operazione ha uno stato di In corso per selezionare la velocità con cui un’operazione Copy Volume viene completata.
Ricopia	È possibile ricopiare un volume quando si è interrotta un’operazione di Copy Volume e si desidera riavviarla oppure quando un’operazione di Copy Volume non è riuscita o si è interrotta. L’operazione di Copy Volume ricomincia dall’inizio. L’azione di ricopia sovrascrive i dati esistenti sul volume di destinazione e rende non riusciti tutti i volumi Snapshot associati al volume di destinazione, se presenti.
Chiaro	È possibile rimuovere l’operazione Copia volume mentre l’operazione ha uno stato di In corso, In sospeso o Non riuscito. Assicurati di voler eseguire questa operazione prima di selezionare **Cancella**. Non viene visualizzata alcuna finestra di dialogo di conferma.

Domande frequenti su volumi e carichi di lavoro per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è un volume?

Un volume è un container in cui applicazioni, database e file system memorizzano i dati. È il componente logico creato per consentire all'host di accedere allo storage sull'array di storage.

Un volume viene creato a partire dalla capacità disponibile in un pool o in un gruppo di volumi. Un volume ha una capacità definita. Sebbene un volume possa essere costituito da più unità, un volume appare come un singolo componente logico per l'host.

Perché visualizzo un errore di sovraallocazione della capacità quando ho capacità libera sufficiente in un gruppo di volumi per creare volumi?

Il gruppo di volumi selezionato potrebbe avere una o più aree di capacità libera. Un'area di capacità libera è la capacità libera che può risultare dall'eliminazione di un volume o dal mancato utilizzo di tutta la capacità libera 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 è limitata all'area di capacità libera più grande in quel 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 10 GiB, il volume più grande che è possibile creare è 10 GiB.

Se un gruppo di volumi dispone di aree di capacità libera, il grafico del gruppo di volumi contiene un collegamento che indica il numero di aree di capacità libera esistenti. Seleziona il collegamento per visualizzare un pop-over che indica la capacità di ciascuna area.

Consolidando la capacità libera, è possibile creare volumi aggiuntivi a partire dalla quantità massima di capacità libera in un gruppo di volumi. È possibile consolidare la capacità libera esistente su un gruppo di volumi selezionato utilizzando uno dei seguenti metodi:

- Quando viene rilevata almeno un'area di capacità libera per un gruppo di volumi, il suggerimento "Consolida capacità libera" viene visualizzato nella pagina iniziale, nell'area Notifiche. Fai clic sul collegamento **Consolida capacità libera** per avviare la finestra di dialogo.
- È inoltre possibile selezionare **Pool & Volume Groups › Attività non comuni › Consolida capacità libera del gruppo di volumi** per avviare la finestra di dialogo.

Se si desidera utilizzare una specifica area di capacità libera anziché l'area di capacità libera più grande, utilizzare la Command Line Interface (CLI).

In che modo il carico di lavoro selezionato influisce sulla creazione di volumi?

Durante la creazione del volume, ti vengono richieste informazioni sull'utilizzo di un carico di lavoro. Il sistema utilizza queste informazioni per creare una configurazione del volume ottimale per te, che può essere modificata secondo necessità. Facoltativamente, puoi saltare questo passaggio nella sequenza di creazione del volume.

Un carico di lavoro è un oggetto di archiviazione che supporta un'applicazione. Puoi definire uno o più carichi di lavoro, o istanze, per applicazione. Per alcune applicazioni, il sistema configura il carico di lavoro per contenere volumi con caratteristiche di volume sottostanti simili. Queste caratteristiche di volume sono ottimizzate in base al tipo di applicazione che il carico di lavoro supporta. Ad esempio, se crei un carico di lavoro che supporta un'applicazione Microsoft SQL Server e poi crei volumi per quel carico di lavoro, le caratteristiche di volume sottostanti sono ottimizzate per supportare Microsoft SQL Server.

- **Specifico per l'applicazione** — Quando si creano volumi utilizzando un carico di lavoro specifico per un'applicazione, il sistema potrebbe consigliare una configurazione del volume ottimizzata per ridurre al minimo la contesa tra l'I/O del carico di lavoro dell'applicazione e altro traffico proveniente dall'istanza

dell'applicazione. Le caratteristiche del volume, come il tipo di I/O, la dimensione del segmento, la proprietà del controller e la cache di lettura e scrittura, vengono automaticamente consigliate e ottimizzate per i carichi di lavoro creati per i seguenti tipi di applicazione.

  - Microsoft® SQL Server™
  - Microsoft® server Exchange™
  - Applicazioni di videosorveglianza
  - VMware ESXi™ (per volumi da utilizzare con Virtual Machine File System)

    È possibile esaminare la configurazione del volume consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliati dal sistema utilizzando la finestra di dialogo Add/Edit Volumes.

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

Perché questi volumi non sono associati a un workload?

I volumi non sono associati a un workload se sono stati creati tramite la command line interface (CLI) o se sono stati migrati (importati/esportati) da un diverso storage array.

Perché non posso eliminare il carico di lavoro selezionato?

Questo carico di lavoro è costituito da un gruppo di volumi creati tramite interfaccia a riga di comando (CLI) o migrati (importati/esportati) da un array di storage diverso. Di conseguenza, i volumi in questo carico di lavoro non sono associati a un carico di lavoro specifico per applicazione, quindi il carico di lavoro non può essere eliminato.

In che modo i carichi di lavoro specifici dell'applicazione mi aiutano a gestire il mio array di storage?

Le caratteristiche di volume del carico di lavoro specifico della tua applicazione determinano come il carico di lavoro interagisce con i componenti del tuo array di storage e aiutano a determinare le prestazioni del tuo ambiente in una data configurazione.

Un'applicazione è un software come SQL Server o server Exchange. Si definiscono uno o più carichi di lavoro per supportare ciascuna applicazione.

In che modo la fornitura di queste informazioni contribuisce alla creazione dello storage?

Le informazioni sul carico di lavoro vengono utilizzate per ottimizzare le caratteristiche del volume, come il tipo di I/O, la dimensione del segmento e la cache di lettura/scrittura per il carico di lavoro selezionato. Queste caratteristiche ottimizzate determinano il modo in cui il carico di lavoro interagisce con i componenti dell'array di storage.

In base alle informazioni sul carico di lavoro fornite, System Manager crea i volumi appropriati e li colloca nei pool o gruppi di volumi disponibili attualmente esistenti nel sistema. Il sistema crea i volumi e ne ottimizza le caratteristiche in base alle migliori pratiche correnti per il carico di lavoro selezionato.

Prima di completare la creazione dei volumi per un determinato carico di lavoro, è possibile rivedere la configurazione dei volumi consigliata e modificare, aggiungere o eliminare i volumi e le caratteristiche consigliati dal sistema tramite la finestra di dialogo Add/Edit Volumes.

Consultare la documentazione specifica della propria applicazione per informazioni sulle best practice.

Cosa devo fare per riconoscere la capacità ampliata?

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'espansione del volume. Tuttavia, alcuni potrebbero non farlo. Se il tuo sistema operativo non riconosce automaticamente la capacità del volume espanso, potrebbe essere necessario eseguire una nuova scansione del disco o riavviare.

Dopo aver aumentato la capacità del volume, è necessario incrementare manualmente le dimensioni del file system in modo che corrispondano. Come farlo dipende dal file system che si sta utilizzando.

Consultare la documentazione del sistema operativo host per ulteriori dettagli.

Perché non vedo tutti i miei pool e/o gruppi di volume?

Qualsiasi pool o gruppo di volumi verso cui non puoi spostare il volume non viene visualizzato nell'elenco.

I pool o i gruppi di volume non sono idonei per nessuno dei seguenti motivi:

- Le funzionalità di Data Assurance (DA) di un pool o di un gruppo di volumi pool non corrispondono.
- Un pool o un gruppo di volumi è in uno stato non ottimale.
- La capacità di un pool o di un gruppo di volumi è troppo piccola.

Che cos'è la dimensione del segmento?

Un segmento rappresenta la quantità di dati in kilobyte (KiB) memorizzata su un'unità prima che l'array di storage si sposti sull'unità successiva nello stripe (gruppo RAID). La dimensione del segmento si applica solo ai gruppi di volumi, non ai pool.

La dimensione del segmento è definita dal numero di blocchi di dati che contiene. Quando si determina la dimensione del segmento, è necessario sapere quale tipo di dati verrà memorizzato in un volume. Se un'applicazione utilizza tipicamente letture e scritture piccole e casuali (IOPS), una dimensione del segmento più piccola funziona generalmente meglio. In alternativa, se l'applicazione effettua letture e scritture grandi e sequenziali (throughput), una dimensione del segmento maggiore è generalmente migliore.

Sia che un'applicazione utilizzi piccole operazioni di lettura e scrittura casuali, sia operazioni di lettura e scrittura sequenziali di grandi dimensioni, l'array di storage offre prestazioni migliori se la dimensione del segmento è maggiore della dimensione tipica del blocco di dati. Questo normalmente rende più facile e veloce per le unità accedere ai dati, il che è importante per migliori prestazioni dell'array di storage.

Ambienti in cui le prestazioni IOPS sono importanti

In un ambiente con un elevato numero di operazioni di I/O al secondo (IOPS), l'array di storage offre prestazioni migliori se si utilizza una dimensione di segmento maggiore rispetto alla dimensione tipica del blocco di dati ("chunk") letto/scritto su un drive. Ciò garantisce che ogni chunk venga scritto su un disco singolo.

Ambienti in cui il throughput è importante

In un ambiente di throughput, la dimensione del segmento dovrebbe essere una frazione esatta del numero

totale di dischi per i dati e della dimensione tipica dei chunk di dati (dimensione I/O). Questo distribuisce i dati come un'unica stripe sui dischi del gruppo di volumi, portando a letture e scritture più veloci.

Che cos'è la proprietà preferita del controller?

La proprietà del controller preferito definisce il controller che è designato come controller proprietario, o primario, del volume.

La gestione dei controller è molto importante e deve essere pianificata con attenzione. I controller devono essere bilanciati il più possibile per il totale degli I/O.

Ad esempio, se un controller legge principalmente blocchi di dati sequenziali di grandi dimensioni e l'altro controller gestisce blocchi di dati di piccole dimensioni con frequenti operazioni di lettura e scrittura, i carichi sono molto diversi. Sapere quali volumi contengono quale tipo di dati consente di bilanciare equamente i trasferimenti di I/O su entrambi i controller.

Quando dovrei utilizzare la selezione "Assegna host in seguito"?

Se si desidera velocizzare 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: un processo di inizializzazione in background tramite Immediate Available Format (IAF) oppure un processo offline.

Quando si mappa un volume a un host, si forza qualsiasi volume in fase di inizializzazione in quel gruppo a passare all'inizializzazione in background. Questo processo di inizializzazione in background consente operazioni di I/O simultanee sull'host, che a volte possono richiedere molto tempo.

Quando nessuno dei volumi in un gruppo di volumi è mappato, viene eseguita l'inizializzazione offline. Il processo offline è molto più veloce del processo in background.

Cosa devo sapere sui requisiti della dimensione del blocco host?

Per i sistemi EF300 e EF600, è possibile configurare un volume per supportare una dimensione del blocco di 512 byte o di 4KiB (anche detta "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 la dimensione del blocco volume, leggere le seguenti limitazioni e linee guida.

- Alcuni sistemi operativi e macchine virtuali (in particolare VMware, al momento) richiedono una dimensione del blocco di 512 byte e non supportano 4KiB, quindi assicurati di conoscere i requisiti dell'host prima di creare un volume. In genere, puoi ottenere le migliori prestazioni impostando un volume per presentare una dimensione del blocco di 4KiB; tuttavia, assicurati che il tuo host consenta blocchi da 4KiB (o "4Kn").
- Il tipo di drive che si seleziona per il pool o il gruppo di volumi determina anche quali dimensioni dei blocchi di volume sono supportate, come segue:
  - Se si crea un gruppo di volumi utilizzando unità che scrivono in 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 in blocchi da 4KiB, è possibile creare volumi con blocchi da 512 byte o da 4KiB.
- Se l'array dispone di una scheda di interfaccia verso gli 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 una specifica implementazione hardware.

- Non è possibile modificare una dimensione di blocco una volta impostata. Se è necessario modificare una dimensione di blocco, è necessario eliminare il volume e ricrearlo.

Host e cluster di host

Scopri host e cluster di host nel software SANtricity

È possibile configurare host e cluster di host, che definiscono le connessioni tra l'array di storage e i server di dati.

Che cosa sono gli host e i cluster di host?

Un host è un server che invia I/O a un volume su un array di storage. Un host cluster è un gruppo di host, che puoi creare per assegnare gli stessi volumi a più host.

Per saperne di più:

- "Terminologia host"
- "Accesso ai volumi"
- "Numero massimo di LUN"

Come si configurano gli host e i cluster di host?

Per definire le connessioni host, puoi andare su **Storage › Hosts** per configurare manualmente l'host. Se desideri che due o più host condividano l'accesso allo stesso set di volumi, puoi quindi definire un cluster e assegnare i volumi a quel cluster.

Per saperne di più:

- "Creazione manuale host"
- "Come vengono assegnati i volumi agli host e ai cluster di host"
- "Flusso di lavoro per la creazione dell'host e l'assegnazione del volume"
- "Crea host manualmente"
- "Crea cluster host"
- "Assegna volumi agli host"

Informazioni correlate

Scopri di più sulle attività relative agli host:

- "Imposta bilanciamento del carico automatico"
- "Imposta la segnalazione della connettività host"
- "Modifica il tipo host predefinito"

Concetti

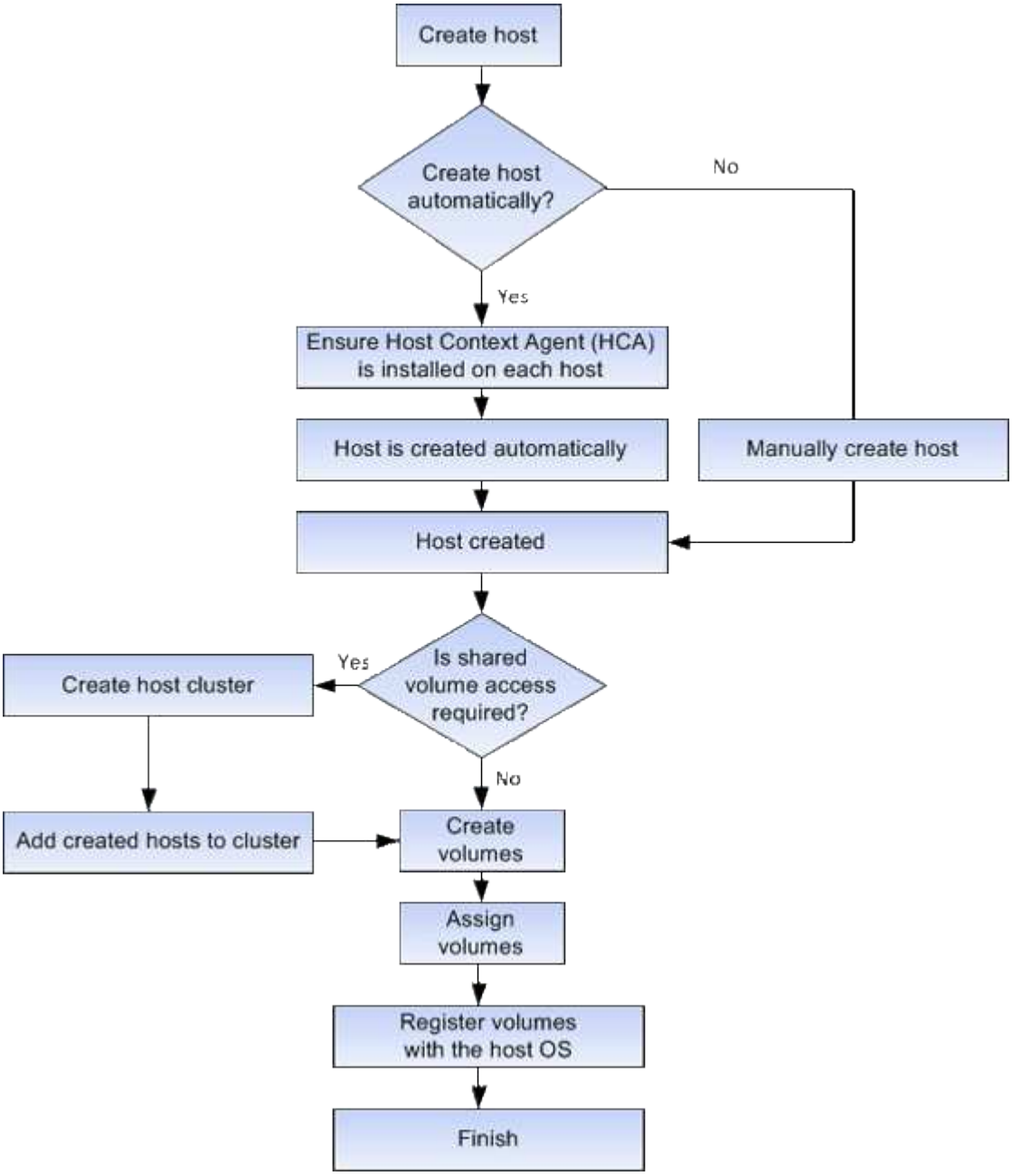
Scopri la terminologia relativa agli host nel software SANtricity

Scopri come si applicano i termini host al tuo storage array.

Componente	Definizione
Host	Un host è un server che invia I/O a un volume su un array di storage.
Nome host	L'host name deve corrispondere al nome di sistema dell'host.
Cluster host	Un cluster di host è un gruppo di host. Si crea un cluster di host per semplificare l'assegnazione degli stessi volumi a più host.
Protocollo di interfaccia verso gli host	Un protocollo di interfaccia verso gli host è la connessione (come Fibre Channel, iSCSI, ecc.) tra i controller e gli host.
HBA o Network Interface Card (NIC)	Un host bus adapter (HBA) è una scheda che risiede in un host e contiene una o più porte host.
Porta host	Una porta host è una porta su un host bus adapter (HBA) che fornisce la connessione fisica a un controller e viene utilizzata per le operazioni di I/O.
Identificatore della porta host	Un identificatore di porta host è un nome univoco a livello mondiale associato a ciascuna porta host su un host bus adapter (HBA). • Gli identificatori delle porte host iSCSI (Internet Small Computer System Interface) devono avere una lunghezza compresa tra 1 e 233 caratteri. Gli identificatori delle porte host iSCSI vengono visualizzati nel formato IQN standard (ad esempio, `iqn.xxx.com.xxx:8b3ad`). • Gli identificatori di porta host non-iSCSI, come Fibre Channel e Serial Attached SCSI (SAS), vengono visualizzati separati da due punti dopo ogni due caratteri (ad esempio, `xx:yy:zz`). Gli identificatori di porta host Fibre Channel devono avere 16 caratteri.
Tipo di sistema operativo host	Il tipo di sistema operativo host è un'impostazione di configurazione che definisce il modo in cui i controller nell'array di storage reagiscono alle operazioni di I/O a seconda del sistema operativo (o variante) dell'host. Questo viene anche talvolta chiamato *host type* in breve.
Porta host del controller	Una porta host del controller è una porta sul controller che fornisce la connessione fisica a un host ed è utilizzata per le operazioni di I/O.
LUN	Un numero di unità logica (LUN) è il numero assegnato allo spazio di indirizzi che un host utilizza 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 indirizzamento LUN. Pertanto, lo stesso LUN può essere utilizzato da host diversi per accedere a volumi differenti.

Come funzionano la creazione degli host e l'assegnazione dei volumi in SANtricity System Manager

La figura seguente illustra come configurare l'accesso all'host.



Scopri la creazione manuale di host in SANtricity System Manager

La creazione di un host è uno dei passaggi necessari per consentire all'array di storage di identificare gli host ad esso collegati e per autorizzare l'accesso I/O ai volumi. È possibile creare un host solo manualmente.

Creazione manuale

La creazione manuale degli host consente di garantire che gli identificatori delle porte host rilevati dai controller dello storage array siano associati correttamente agli host.

Durante la creazione manuale di un host, si associano gli identificatori di porta dell'host selezionandoli da un elenco o inserendoli manualmente. Dopo aver creato un host, è possibile assegnargli volumi o aggiungerlo a un host cluster se si prevede di condividere l'accesso ai volumi.

Come vengono assegnati i volumi agli host e ai cluster di host nel software SANtricity

Affinché un host o un cluster di host possa inviare I/O a un volume, è necessario assegnare il volume all'host o al cluster di host.

È possibile selezionare un host o un cluster di host quando si crea un volume oppure assegnare un volume a un host o a un cluster di host in un secondo momento. Un cluster di host è un gruppo di host. Si crea un cluster di host per facilitare l'assegnazione degli stessi volumi a più host.

L'assegnazione dei volumi agli host è flessibile e consente di soddisfare le specifiche esigenze di storage.

- **Host autonomo, non facente parte di un cluster di host** — È possibile assegnare un volume a un singolo host. Il volume può essere accessibile solo da quell'host.
- **Host cluster** — È possibile assegnare un volume a un host cluster. Il volume può essere accessibile da tutti gli host dell'host cluster.
- **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, il volume può essere accessibile solo dal singolo host e non da altri host nel cluster di host.

Quando si creano i volumi, i numeri di unità logica (LUN) vengono assegnati automaticamente. Il LUN funge da "indirizzo" tra l'host e il controller durante le operazioni di I/O. È possibile modificare i LUN dopo la creazione del volume.

Accedere ai volumi in SANtricity System Manager

Un volume di accesso è un volume configurato in fabbrica sull'array di storage che viene utilizzato per la comunicazione con l'array di storage e l'host tramite la connessione I/O dell'host. Il volume di accesso richiede un Logical Unit Number (LUN).

Il volume di accesso viene utilizzato nel seguente caso:

- **Gestione in banda** — Il volume di accesso viene utilizzato per una connessione in banda per gestire l'array di storage. Questo può essere fatto solo se si gestisce l'array di storage con la command line interface (CLI).

> La gestione in banda tramite il volume Access non è disponibile per i sistemi storage E4000, EF600/EF600C o EF300/EF300C.

Un volume di accesso viene creato automaticamente la prima volta che si assegna un volume a un host. Ad esempio, se si assegnano Volume_1 e Volume_2 a un host, quando si visualizzano i risultati di tale assegnazione, si vedono tre volumi (Volume_1, Volume_2 e Access).

Se non si creano automaticamente host o non si gestisce un array di storage in-band tramite CLI, non è necessario il volume di accesso ed è possibile liberare la LUN eliminando il volume di accesso. Questa operazione rimuove l'assegnazione volume-LUN e tutte le connessioni di gestione in-band all'host.

Scopri il numero massimo di LUN nel software SANtricity

L'array di storage ha un numero massimo di logical unit numbers (LUN) che possono essere utilizzati per ciascun host.

Il numero massimo dipende dal sistema operativo dell'host. L'array di storage tiene traccia del numero di LUN utilizzati. Se si tenta di assegnare un volume a un host che supera il numero massimo di LUN, l'host non può accedere al volume.

Scopri il tipo di sistema operativo host predefinito nel software SANtricity

Il tipo di host predefinito viene utilizzato dall'array di storage quando gli host sono inizialmente connessi. Definisce come i controller dell'array di storage lavorano con il sistema operativo dell'host quando si accede ai volumi.

È possibile modificare il tipo di host se è necessario cambiare il modo in cui l'array di storage opera in relazione agli host ad esso collegati. In genere, si modifica il tipo di host predefinito prima di collegare gli host all'array di storage o quando si collegano host aggiuntivi.

Tenete a mente queste linee guida:

- Se tutti gli host che si intende connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), allora modificare il tipo di host per farlo corrispondere al sistema operativo.
- Se si prevede di connettere all'array di storage host con sistemi operativi diversi (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo della maggior parte degli host.

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

- Se la maggior parte degli host connessi ha una combinazione di diversi sistemi operativi, modificare il tipo di host in Factory Default.

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo VMware e altri tre eseguono un sistema operativo Linux, è necessario selezionare Factory Default come tipo di sistema operativo host predefinito.

Configura l'accesso host

Creare manualmente un host in SANtricity System Manager

Per gli host che non possono essere rilevati automaticamente, è possibile creare un host manualmente. La creazione di un host è uno dei passaggi necessari per consentire all'array di storage di sapere quali host sono collegati e per autorizzare l'accesso I/O ai volumi.

Informazioni su questa attività

Tieni a mente queste linee guida quando crei un host:

- È necessario definire le porte identificative dell'host che sono associate all'host.
- Assicurati di fornire lo stesso nome del nome di sistema assegnato all'host.

- Questa operazione non avrà successo se il nome scelto è già in uso.
- La lunghezza del nome non può superare 30 caratteri.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Fare clic su **Crea › Host**.

   Viene visualizzata la finestra di dialogo Create Host.

3. Seleziona le impostazioni per l'host come appropriato.

Dettagli del campo

Impostazione	Descrizione
Nome	Digita un nome per il nuovo host.
Tipo di sistema operativo host	Seleziona il sistema operativo che è in esecuzione sul nuovo host dall'elenco a discesa.
Tipo di interfaccia verso gli host	(Facoltativo) Se l'array di storage supporta più di un tipo di interfaccia verso gli host, seleziona il tipo di interfaccia verso gli host che desideri utilizzare.
Porte host	Eseguire una delle seguenti operazioni: • **Seleziona l'interfaccia I/O** In genere, le porte host dovrebbero aver effettuato l'accesso ed essere disponibili nell'elenco a discesa. È possibile selezionare gli identificativi delle porte 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'utilità HBA o l'utilità iSCSI initiator per trovare gli identificatori di porta host e associarli all'host. È possibile inserire manualmente gli identificatori della porta host oppure copiarli/incollarli dall'utility (uno alla volta) nel campo **Host ports**. È necessario selezionare un identificatore di porta host alla volta per associarlo all'host, ma è possibile continuare a selezionare tutti gli identificatori che sono associati all'host. Ciascun identificatore viene visualizzato nel campo **Host ports**. Se necessario, è anche possibile rimuovere un identificatore selezionando la **X** accanto ad esso.

Impostazione	Descrizione
CHAP initiator	(Facoltativo) Se hai selezionato o inserito manualmente una porta host con un iSCSI IQN e desideri richiedere che un host che tenta di accedere all'array di storage si autentichi utilizzando il Challenge Handshake Authentication Protocol (CHAP), seleziona la check box **CHAP initiator**. Per ogni porta host iSCSI selezionata o inserita manualmente, procedi come segue: • Inserire lo stesso segreto CHAP impostato su ciascun iSCSI initiator per l'autenticazione CHAP. Se si utilizza il metodo di autenticazione CHAP reciproca (autenticazione bidirezionale che consente a un host di autenticarsi presso l'array di storage e a un array di storage di autenticarsi presso l'host), è necessario impostare il segreto CHAP anche per l'array di storage durante la configurazione iniziale o modificando le impostazioni. • Lascia il campo vuoto se non richiedi l'autenticazione dell'host. Attualmente, l'unico metodo di autenticazione iSCSI utilizzato da System Manager è CHAP.

4. Fai clic su **Create**.

Risultati

Dopo che l'host è stato creato correttamente, il sistema crea un nome predefinito per ogni porta host configurata per l'host (etichetta utente).

L'alias predefinito è `<Hostname_Port Number>`. Ad esempio, l'alias predefinito per la prima porta creata per `host IPT is IPT_1`.

Creare un cluster host in SANtricity System Manager

Si crea un cluster host quando due o più host necessitano di accesso I/O agli stessi volumi.

Informazioni su questa attività

Tieni a mente queste linee guida quando crei un cluster host:

- Questa operazione non viene avviata a meno che non siano disponibili due o più host per creare il cluster.
- Gli host nei cluster host possono avere sistemi operativi diversi (eterogenei).
- Gli host NVMe nei cluster di host non possono essere combinati con host non NVMe.
- Per creare un volume con Data Assurance (DA) abilitato, la connessione host che si intende utilizzare deve supportare DA.

  Se una qualsiasi delle connessioni host sui controller nel tuo storage array non supporta DA, gli host associati non possono accedere ai dati sui volumi abilitati per DA.

- Questa operazione non avrà successo se il nome scelto è già in uso.
- La lunghezza del nome non può superare 30 caratteri.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Selezionare **Create › Host Cluster**.

   Viene visualizzata la finestra di dialogo Create Host Cluster.

3. Selezionare le impostazioni per il cluster host come appropriato.

   Dettagli del campo

Impostazione	Descrizione
Nome	Digita il nome per il nuovo cluster host.
Selezionare gli host con cui condividere l'accesso al volume	Seleziona due o più host dall'elenco a discesa. Nell'elenco verranno visualizzati solo gli host che non fanno già parte di un cluster.

4. Fai clic su **Create**.

   Se gli host selezionati sono collegati a tipi di interfaccia con funzionalità Data Assurance (DA) diverse, viene visualizzata una finestra di dialogo con il messaggio che DA non sarà disponibile sul cluster host. Questa indisponibilità impedisce che volumi con DA abilitato vengano aggiunti 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 le unità. L'utilizzo di DA per il nuovo volume garantisce che eventuali errori vengano rilevati.

Risultati

Il nuovo cluster host appare nella tabella con gli host assegnati nelle righe sottostanti.

Assegna i volumi agli host in SANtricity System Manager

È necessario assegnare un volume a un host o a un cluster di host affinché possa essere utilizzato per le operazioni di I/O. Tale assegnazione garantisce a un host o a un cluster di host l'accesso a uno o più volumi in un array di storage.

Informazioni su questa attività

Tenete presenti queste linee guida quando assegnate i volumi agli host:

- È possibile assegnare un volume a un solo host o host cluster alla volta.
- I volumi assegnati sono condivisi tra i controller nell'array di storage.
- Lo stesso numero di unità logica (LUN) non può essere utilizzato due volte da un host o da un host cluster per accedere a un volume. È necessario utilizzare un LUN univoco.
- Per i nuovi gruppi di volumi, se si attende che tutti i volumi siano stati creati e inizializzati prima di assegnarli a un host, il tempo di inizializzazione dei volumi si riduce. Tenere presente che, una volta mappato un volume associato al gruppo di volumi, i volumi torneranno alla procedura di inizializzazione più

lenta. È possibile verificare l'avanzamento dell'inizializzazione dal **Home › Operazioni in corso**.

L'assegnazione di un volume non riesce in queste condizioni:

- Tutti i volumi sono assegnati.
- Il volume è già assegnato a un altro host o host cluster.

La possibilità di assegnare un volume non è disponibile in queste condizioni:

- Non esistono host o host cluster validi.
- Non sono stati definiti identificatori di porta host per l'host.
- Tutte le assegnazioni di volume sono state definite.

Tutti i volumi non assegnati vengono visualizzati durante questa operazione, ma le funzioni per gli host con o senza Data Assurance (DA) si applicano come segue:

- Per un host compatibile con DA, puoi selezionare volumi che sono abilitati DA o non abilitati DA.
- Per un host che non è compatibile con DA, se si seleziona un volume che è abilitato DA, viene visualizzato un avviso che indica che il sistema deve disattivare automaticamente DA sul volume prima di assegnare il volume all'host.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona l'host o il cluster a cui desideri assegnare i volumi, quindi fai clic su **Assign Volumes**.

   Viene visualizzata una finestra di dialogo che elenca tutti i volumi che possono essere assegnati. È possibile ordinare una qualsiasi delle colonne o digitare qualcosa nella casella **Filtro** per facilitare la ricerca di volumi specifici.

3. Seleziona la check box accanto a ciascun volume che desideri assegnare o seleziona la check box nell'intestazione della tabella per selezionare tutti i volumi.
4. Fai clic su **Assign** per completare l'operazione.

Risultati

Dopo aver assegnato correttamente uno o più volumi a un host o a un host cluster, il sistema esegue le seguenti azioni:

- Il volume assegnato riceve il prossimo 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 negli elenchi dei volumi associati all'host.

Gestisci host e cluster

Modificare il tipo di host predefinito in SANtricity System Manager

Utilizzare l'impostazione "Cambia sistema operativo host predefinito" per modificare il tipo di host predefinito a livello di storage array. In genere, si modifica il tipo di host predefinito prima di connettere host allo storage array o quando si connettono host aggiuntivi.

Informazioni su questa attività

Tenete a mente queste linee guida:

- Se tutti gli host che si intende connettere all'array di storage hanno lo stesso sistema operativo (ambiente host omogeneo), allora modificare il tipo di host per farlo corrispondere al sistema operativo.
- Se si prevede di connettere all'array di storage host con sistemi operativi diversi (ambiente host eterogeneo), modificare il tipo di host in modo che corrisponda al sistema operativo della maggior parte degli host.

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

- Se la maggior parte degli host connessi ha una combinazione di diversi sistemi operativi, modificare il tipo di host in Factory Default.

  Ad esempio, se si collegano otto host diversi all'array di storage e due di questi host eseguono un sistema operativo Windows, tre eseguono un sistema operativo VMware e altri tre eseguono un sistema operativo Linux, è necessario selezionare Factory Default come tipo di sistema operativo host predefinito.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive** e poi fai clic su **Modifica tipo di sistema operativo host predefinito**.
3. Seleziona il tipo di sistema operativo host che vuoi utilizzare come predefinito.
4. Fai clic su **Change**.

Annulla l'assegnazione dei volumi in SANtricity System Manager

Rimuovi l'assegnazione dei volumi dagli host o dai cluster di host se non hai più bisogno dell'accesso I/O a quel volume dall'host o dal cluster di host.

Informazioni su questa attività

Tenete presenti queste linee guida quando rimuovete l'assegnazione di un volume:

- Se si sta rimuovendo l'ultimo volume assegnato da un host cluster e l'host cluster contiene anche host con volumi assegnati specifici, assicurarsi di rimuovere o spostare tali assegnazioni prima di rimuovere l'ultima assegnazione per l'host cluster.
- Se un cluster host, un host o una porta host sono assegnati a un volume che è registrato nel sistema operativo, è necessario cancellare questa registrazione prima di poter rimuovere questi nodi.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona l'host o host cluster che desideri modificare, quindi fai clic su **Annulla assegnazione volumi**.

   Viene visualizzata una finestra di dialogo che mostra tutti i volumi attualmente assegnati.

3. Seleziona la check box accanto a ciascun volume che desideri rimuovere dall'assegnazione oppure seleziona la check box nell'intestazione della tabella per selezionare tutti i volumi.
4. Fai clic su **Unassign**.

Risultati

- I volumi che sono stati non assegnati sono disponibili per una nuova assegnazione.
- Finché le modifiche non vengono configurate sull'host, il volume è ancora riconosciuto dal sistema operativo host.

Eliminare un host o un cluster in SANtricity System Manager

È possibile eliminare un host o un cluster host.

Informazioni su questa attività

Tenete presenti queste linee guida quando eliminate un host o un cluster di host:

- Tutte le assegnazioni di volumi specifici vengono eliminate e i volumi associati sono disponibili per una nuova assegnazione.
- Se l'host fa parte di un cluster di host che ha assegnazioni specifiche proprie, il cluster di 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 tutti gli altri host o identificatori di porta host associati ereditano le assegnazioni predefinite.
- Tutti gli identificatori di porta host che erano associati all'host diventano indefiniti.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona l'host o il cluster che desideri eliminare, quindi fai clic su **Elimina**.

   Viene visualizzata la finestra di dialogo di conferma.

3. Conferma di voler eseguire l'operazione, quindi fai clic su **Delete**.

Risultati

Se si elimina un host, il sistema esegue le seguenti azioni:

- 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.
- Riporta tutti gli identificatori di porta host associati all'host a uno stato non associato.

Se si elimina un cluster host, il sistema esegue le seguenti azioni:

- 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 eventuali identificatori di porta host associati agli host a uno stato non associato.

Impostare la segnalazione della connettività host in SANtricity System Manager

È possibile abilitare la segnalazione della connettività host in modo che l'array di storage monitori continuamente la connessione tra i controller e gli host configurati, e quindi ti avvisi se la connessione viene interrotta. Questa funzione è abilitata per impostazione predefinita.

Informazioni su questa attività

Se si disabilita la segnalazione della connettività host, il sistema non monitora più la connettività o i problemi del driver multipath con un host connesso all'array di storage.

> La disabilitazione della segnalazione della connettività host disabilita anche il bilanciamento del carico automatico, che monitora e bilancia l'utilizzo delle risorse del controller.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive**, quindi fai clic su **Abilita/Disabilita report connettività host**.

   Il testo sotto questa opzione indica se è attualmente abilitata o disabilitata.

   Si apre una finestra di dialogo di conferma.
3. Fai clic su **Sì** per continuare.

   Selezionando questa opzione, si alterna la funzione tra abilitata/disabilitata.

Gestisci le impostazioni

Modificare le impostazioni di un host in SANtricity System Manager

È possibile modificare il nome, il tipo di host operating system e i cluster host associati per un host.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona l'host che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata una finestra di dialogo che mostra le impostazioni host correnti.
3. Se non è già selezionata, fai clic sulla scheda **Properties**.
4. Modifica le impostazioni come appropriato.

Dettagli del campo

Impostazione	Descrizione
Nome	È possibile modificare il nome fornito dall'utente per l'host. Specificare un nome per l'host è obbligatorio.
cluster host associato	Puoi scegliere una delle seguenti opzioni: • **Nessuno** — L'host rimane un host autonomo. Se l'host era associato a un cluster, 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 che hai definito.

5. Fare clic su **Save**.

Modificare le impostazioni per un cluster host in SANtricity System Manager

È possibile modificare il nome del cluster host oppure aggiungere o rimuovere host in un cluster host.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona il cluster host che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata una finestra di dialogo che mostra le impostazioni correnti del cluster host.

3. Modificare le impostazioni del cluster host in base alle necessità.

   Dettagli del campo

Impostazione	Descrizione
Nome	È possibile specificare il nome fornito dall'utente per il cluster host. Specificare un nome per un cluster è obbligatorio.
Host associati	Per aggiungere un host, fai clic sulla casella **Associated Hosts** e seleziona un host name dall'elenco a discesa. Non è possibile inserire manualmente un host name. Per eliminare un host, fai clic sulla **X** accanto al host name.

4. Fare clic su **Save**.

Modificare gli identificatori della porta host per un host in SANtricity System Manager

Modifica gli identificatori di porta host quando desideri cambiare l'etichetta utente su un identificatore di porta host, aggiungere un nuovo identificatore di porta host all'host o eliminare un identificatore di porta host dall'host.

Informazioni su questa attività

Quando si modificano gli identificatori della porta host, tenere presenti le seguenti linee guida:

- **Aggiungi** — Quando aggiungi una porta host, associ l'identificativo della porta host all'host che hai creato per connetterti al tuo array di storage. Puoi inserire manualmente le informazioni sulla porta utilizzando un'utilità host bus adapter (HBA).
- **Modifica** — È possibile modificare le porte host per spostare (associare) una porta host a un host diverso. Potresti aver spostato l'adattatore bus host o l'iSCSI initiator su un host diverso, quindi devi spostare (associare) la porta host al nuovo host.
- **Elimina** — Puoi eliminare le porte host per rimuovere (disassociare) le porte host da un host.

Passaggi

1. Seleziona **Storage › Hosts**.
2. Seleziona l'host a cui saranno associate le porte, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Se si desidera aggiungere porte a un host in un cluster di host, espandere il cluster di host e selezionare l'host desiderato. Non è possibile aggiungere porte a livello di cluster di host.

   Viene visualizzata una finestra di dialogo che mostra le impostazioni host correnti.

3. Fai clic sulla scheda **Host Ports**.

   La finestra di dialogo mostra gli identificatori di porta host correnti.

4. Modificare le impostazioni dell'identificativo della porta host come appropriato.

Impostazione	Descrizione
Porta host	Puoi scegliere una delle seguenti opzioni: • **Aggiungi** — Utilizzare Aggiungi per associare un nuovo identificatore di porta host all'host. La lunghezza del nome dell'identificatore di porta host è determinata dalla tecnologia dell'interfaccia verso gli host. I nomi degli identificatori di porta host Fibre Channel e Infiniband devono avere 16 caratteri. I nomi degli identificatori di porta host iSCSI hanno una lunghezza massima di 223 caratteri. La porta deve essere univoca. Non è consentito un numero di porta già configurato. • **Cancella** — Utilizzare Cancella per rimuovere (disassociare) un identificatore di porta host. L'opzione Cancella non rimuove fisicamente la porta host. Questa opzione rimuove l'associazione tra la porta host e l'host. A meno che non si rimuova l'adattatore bus host o l'iSCSI initiator, la porta host viene comunque riconosciuta dal controller. Se si elimina un identificatore di porta host, questo non è più associato a tale host. Inoltre, l'host perde l'accesso a qualsiasi volume assegnato 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. Non è consentito un nome di etichetta già configurato.
Segreto CHAP	Appare solo per host iSCSI. È possibile impostare o modificare il segreto CHAP per gli iniziatori (host iSCSI). System Manager utilizza il metodo Challenge Handshake Authentication Protocol (CHAP), che convalida l'identità dei target e degli initiator durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa chiamata segreto CHAP.

5. Fare clic su **Save**.

Domande frequenti sui sistemi host e cluster host per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cosa sono gli host e i cluster di host?

Un host è un server che invia operazioni di I/O a un volume su un array di storage. Un cluster di host è un gruppo di host. Si crea un cluster di host per semplificare l'assegnazione degli stessi volumi a più host.

Definisci un host separatamente. Può essere un'entità indipendente oppure essere aggiunto a un cluster di host. Puoi assegnare volumi a un singolo host, oppure un host può far parte di un cluster di host che condivide l'accesso a uno o più volumi con altri host nel cluster di host.

Il cluster host è un'entità logica che si crea in SANtricity System Manager. È necessario aggiungere gli host al cluster host prima di poter assegnare i volumi.

Perché dovrei creare un cluster host?

È necessario creare un cluster di host se si desidera che due o più host condividano l'accesso allo stesso set di volumi. Normalmente, sui singoli host è installato un software di clustering per coordinare l'accesso ai volumi.

Come faccio a sapere quale tipo di sistema operativo host è corretto?

Il campo Tipo di sistema operativo host contiene il sistema operativo dell'host. Puoi selezionare il tipo di host consigliato dall'elenco a discesa.

I tipi di host visualizzati nell'elenco a discesa dipendono dal modello dell'array di storage e dalla versione del firmware. Le versioni più recenti mostrano per prime le opzioni più comuni, che sono le più probabilmente appropriate. La presenza in questo elenco non implica che l'opzione sia completamente supportata.

Per ulteriori informazioni sul supporto host, consultare il "Tool NetApp Interoperability Matrix".

Nell'elenco potrebbero comparire alcuni dei seguenti tipi di host:

Tipo di sistema operativo host	Sistema operativo (OS) e driver multipath
Linux DM-MP (Kernel 3.10 o successivo)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath Device Mapper con un Kernel 3.10 o successivo.
VMware ESXi	Supporta i sistemi operativi VMware ESXi che eseguono l'architettura Native Multipathing Plug-in (NMP) utilizzando il modulo VMware integrato Storage Array Type Policy SATP_ALUA.
Windows (cluster o non cluster)	Supporta configurazioni Windows in cluster o non in cluster che non eseguono il driver di multipathing ATTO.
ATTO Cluster (tutti i sistemi operativi)	Supporta tutte le configurazioni cluster che utilizzano il driver multipathing di ATTO Technology, Inc.
Linux (Veritas DMP)	Supporta i sistemi operativi Linux utilizzando una soluzione di multipathing Veritas DMP.
Linux (ATTO)	Supporta i sistemi operativi Linux utilizzando un driver di multipathing di ATTO Technology, Inc.
Mac OS (ATTO)	Supporta le versioni di Mac OS che utilizzano un driver di multipathing di ATTO Technology, Inc.
Windows (ATTO)	Supporta i sistemi operativi Windows utilizzando un driver di multipathing di ATTO Technology, Inc.
IBM SVC	Supporta una configurazione IBM SAN Volume Controller.

Tipo di sistema operativo host	Sistema operativo (OS) e driver multipath
Impostazioni di fabbrica	Riservato per l'avvio iniziale dell'array di storage. Se il tipo di sistema operativo host è impostato su Factory Default, modificarlo in modo che corrisponda al sistema operativo host e al driver multipath in esecuzione sull'host connesso.
Linux DM-MP (Kernel 3.9 o precedente)	Supporta i sistemi operativi Linux che utilizzano una soluzione di failover multipath Device Mapper con un Kernel 3.9 o precedente.
Window Clustered (obsoleto)	Se il tipo di sistema operativo host è impostato su questo valore, utilizzare invece l'impostazione Windows (clustered o non-clustered).

Cosa sono gli HBA e le porte adapter?

Un adattatore bus host (HBA) è una scheda che risiede in un host e contiene una o più porte host. Una porta host è una porta su un adattatore bus host (HBA) che fornisce la connessione fisica a un controller e viene utilizzata per le operazioni di I/O.

Le porte dell'adattatore sull'HBA sono chiamate porte host. La maggior parte degli HBA ha una o due porte host. L'HBA ha un World Wide Identifier (WWID) univoco e ogni porta host dell'HBA ha un WWID univoco. Gli identificatori delle porte host vengono utilizzati per associare l'HBA appropriato all'host fisico quando si crea manualmente l'host tramite SANtricity System Manager.

Come faccio ad associare le porte host a un host?

Se si crea manualmente un host, è necessario innanzitutto utilizzare l'apposita utility per l'host bus adapter (HBA) disponibile sull'host per determinare gli identificatori della porta host associati a ciascun HBA installato nell'host.

Quando si dispone di queste informazioni, selezionare gli identificatori della porta host che hanno effettuato l'accesso all'array di storage dall'elenco fornito nella finestra di dialogo Crea host.

Assicurati di selezionare gli identificatori di porta host appropriati per l'host che stai creando. Se associ gli identificatori di porta host errati, potresti causare un accesso indesiderato da parte di un altro host a questi dati.

Come si creano i segreti CHAP?

Se si configura l'autenticazione Challenge Handshake Authentication Protocol (CHAP) su qualsiasi host iSCSI connesso all'array di storage, è necessario reinserire quel segreto CHAP dell'initiator per ciascun host iSCSI.

Per fare ciò, puoi utilizzare System Manager sia come parte dell'operazione Create Host sia tramite l'opzione View/Edit Settings.

Se si utilizza l'autenticazione reciproca CHAP, è necessario definire anche un segreto CHAP di destinazione per l'array di storage nella pagina Impostazioni e reinserire tale segreto CHAP di destinazione su ciascun host iSCSI.

Qual è il cluster predefinito?

Il cluster predefinito è un'entità definita dal sistema che consente a qualsiasi identificatore di porta host non

associato che abbia effettuato 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 host specifico, ma è fisicamente installata in un host e ha effettuato l'accesso all'array di storage.

> Se si desidera che gli host abbiano accesso specifico a determinati volumi nell'array di storage, non si deve utilizzare il cluster predefinito. È invece necessario associare gli identificatori di porta degli host ai rispettivi host. Questa operazione può essere eseguita manualmente durante l'operazione di creazione dell'host. Successivamente, si assegnano i volumi a un singolo host o a un cluster di host.

Dovresti utilizzare *solo* il cluster predefinito in situazioni particolari in cui l'ambiente di storage esterno consente a tutti gli host e a tutti gli identificatori di porta host connessi all'array di storage di accedere a tutti i volumi (modalità all-access) senza dover necessariamente rendere noti gli host all'array di storage o all'interfaccia utente.

Inizialmente, è possibile assegnare volumi solo al cluster predefinito tramite l'interfaccia a riga di comando (CLI). Tuttavia, dopo aver assegnato almeno un volume al cluster predefinito, questa entità (denominata Default Cluster) viene visualizzata nell'interfaccia utente, dove è possibile gestire questa entità.

Che cos'è la segnalazione della connettività host?

Quando la segnalazione della connettività host è abilitata, l'array di storage monitora continuamente la connessione tra i controller e gli host configurati e ti avvisa se la connessione viene interrotta.

Potrebbero verificarsi interruzioni della connessione in caso di cavo allentato, danneggiato o mancante, oppure in presenza di altri problemi con l'host. In queste situazioni, il sistema potrebbe visualizzare un messaggio di Recovery Guru:

- **Ridondanza host persa** — Si apre se uno dei controller non può comunicare con l'host.
- **Tipo host non corretto** — Si apre se il tipo dell'host è specificato in modo errato sull'array di storage, il che potrebbe causare problemi di failover.

Potrebbe essere opportuno disabilitare la segnalazione della connettività host in situazioni in cui il riavvio di un controller potrebbe richiedere più tempo del timeout di connessione. La disabilitazione di questa funzione sopprime i messaggi di Recovery Gurus.

> La disabilitazione della segnalazione della connettività host disabilita anche il bilanciamento del carico automatico, che monitora e bilancia l'utilizzo delle risorse del controller. Tuttavia, se si riabilita la segnalazione della connettività host, la funzionalità di bilanciamento del carico automatico non viene riattivata automaticamente.

Istantanee

Scopri gli snapshot in SANtricity System Manager

La funzione Snapshot consente di creare immagini point-in-time dei volumi dell'array di storage da utilizzare per il backup o per i test.

Cosa sono le immagini Snapshot?

Un'immagine snapshot è una copia logica dei dati di un volume, acquisita in un point-in-time. Come un punto di ripristino, le immagini snapshot consentono di tornare a un set di dati noto e funzionante. Sebbene l'host

possa accedere all'immagine snapshot, non può leggerla o scriverci direttamente.

Per saperne di più:

- "Come funziona l'archiviazione delle snapshot"
- "Terminologia Snapshot"
- "Volumi di base, capacità riservata e gruppi di Snapshot"
- "Programmazioni Snapshot e gruppi di coerenza"
- "Volumi Snapshot"

Come si creano le Snapshot?

È possibile creare manualmente un'immagine Snapshot da un volume di base o da un gruppo di coerenza Snapshot. Questa procedura è disponibile dal **Storage › Snapshots**.

Per saperne di più:

- "Requisiti e linee guida per le Snapshot"
- "Flusso di lavoro per la creazione di immagini Snapshot e volumi"
- "Crea un'immagine Snapshot"
- "Pianifica immagini Snapshot"
- "Crea un gruppo di coerenza Snapshot"
- "Crea un volume Snapshot"

Come posso ripristinare i dati da uno snapshot?

Il *rollback* è il processo di restituzione dei dati in un volume di base a un punto precedente nel tempo. È possibile eseguire il rollback dei dati di uno snapshot dal **Storage › Snapshots**.

Per saperne di più:

- "Rollback Snapshot"
- "Avvia un rollback dell'immagine Snapshot per un volume di base"
- "Avvia un rollback dell'immagine snapshot per un membro del gruppo di coerenza"

Informazioni correlate

Scopri di più sulle attività relative agli snapshot:

- "Modifica la capacità riservata per un volume snapshot"
- "Modifica la capacità riservata per un gruppo di snapshot"

Concetti

Come funziona l'archiviazione degli Snapshot nel software SANtricity

La funzione Snapshot utilizza la tecnologia copy-on-write per memorizzare le immagini snapshot e utilizzare la capacità riservata allocata.

Come vengono utilizzate le immagini Snapshot

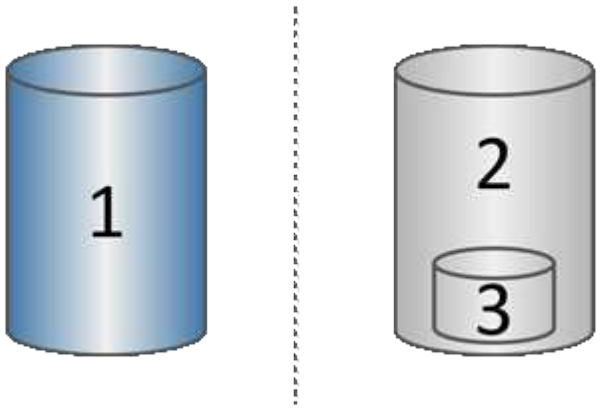
Un'immagine Snapshot è una copia logica di sola lettura del contenuto di un volume, acquisita in un determinato point-in-time. Puoi utilizzare le Snapshot per proteggere dalla perdita di dati.

Le immagini Snapshot sono utili anche per gli ambienti di test. Creando una copia virtuale dei dati, è possibile testare i dati utilizzando lo snapshot senza modificare il volume effettivo. Inoltre, gli host non hanno accesso in scrittura alle immagini Snapshot, quindi i tuoi snapshot sono sempre una risorsa di backup sicura.

Creazione di Snapshot

Quando vengono create le Snapshot, la funzione Snapshot memorizza i dati dell'immagine come segue:

- Quando viene creata un'immagine Snapshot, questa corrisponde esattamente al volume di base. La funzione Snapshots utilizza tecnologia copy-on-write. Dopo la creazione dello Snapshot, la prima scrittura su un blocco o un insieme di blocchi del volume di base comporta la copia dei dati originali nella capacità riservata prima della scrittura dei nuovi dati sul volume di base.
- Le Snapshot successive includono solo i blocchi di dati modificati. Prima che i dati vengano sovrascritti sul volume di base, la funzione Snapshot utilizza la tecnologia copy-on-write per salvare le immagini necessarie dei settori interessati nella capacità riservata alle Snapshot.



[1] Volume base (capacità del disco fisico); [2] Snapshots (capacità del disco logico); [3] Capacità riservata (capacità del disco fisico)

- La capacità riservata memorizza i blocchi di dati originali per le porzioni del volume di base che sono state modificate dopo la creazione dello snapshot e include un indice per tenere traccia delle modifiche. In genere, la dimensione della capacità riservata è predefinita al 40 percento del volume di base. (Se hai bisogno di una maggiore capacità riservata, puoi aumentare la capacità riservata.)
- Le immagini Snapshot vengono memorizzate in un ordine specifico, in base alla loro data e ora. Solo l'immagine Snapshot più vecchia di un volume di base è disponibile per la cancellazione manuale.

Ripristino Snapshot

Per ripristinare i dati su un volume di base, puoi utilizzare un volume Snapshot o un'immagine Snapshot:

- **Snapshot volume** — Se devi recuperare file eliminati, crea un volume snapshot da un'immagine snapshot valida e assegnalo all'host.
- **Snapshot image** — Se è necessario ripristinare un volume di base a un point-in-time, utilizzare un'immagine snapshot precedente per ripristinare i dati sul volume di base.

Scopri la terminologia relativa agli Snapshot nel software SANtricity

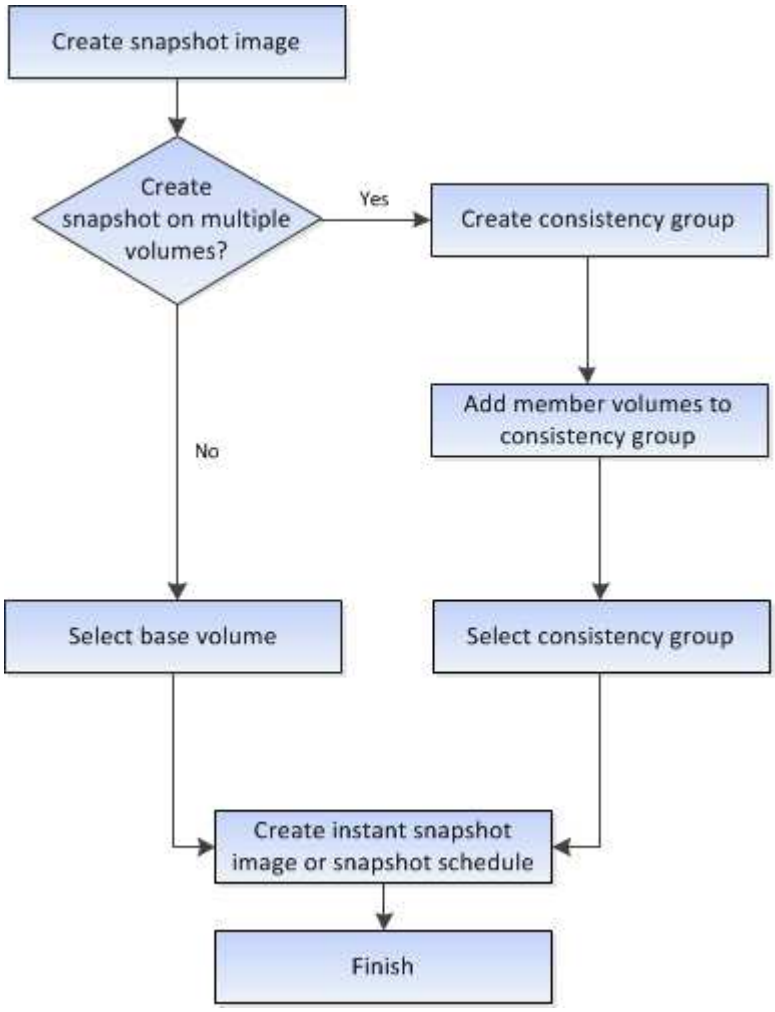
Scopri come si applicano i termini relativi agli snapshot al tuo array di storage.

Termine	Descrizione
Funzione Snapshot	La funzione Snapshot viene utilizzata per creare e gestire immagini dei volumi.
Immagine Snapshot	Un'immagine Snapshot è una copia logica dei dati di un volume, acquisita in un point-in-time. Come un punto di ripristino, le immagini Snapshot consentono di tornare a un set di dati funzionante. Sebbene l'host possa accedere all'immagine Snapshot, non può leggerla o scriverci direttamente.
Volume base	Il volume di base è la sorgente da cui viene creata un'immagine Snapshot. Può essere un volume thick o thin e viene in genere assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un pool di dischi.
Volume Snapshot	Un volume snapshot consente all'host di accedere ai dati nell'immagine snapshot. Il volume snapshot contiene una propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine snapshot originale.
Gruppo Snapshot	Un gruppo di snapshot è una raccolta di immagini snapshot da un singolo volume di base.
volume di capacità riservato	Un volume di capacità riservata tiene traccia di quali blocchi di dati del volume di base vengono sovrascritti e del contenuto conservato di tali blocchi.
calendario di Snapshot	Una pianificazione di Snapshot è una tabella di marcia per la creazione automatica di immagini Snapshot. Tramite la pianificazione, puoi controllare la frequenza di creazione delle immagini.
Gruppo di coerenza Snapshot	Un gruppo di coerenza snapshot è una raccolta di volumi che vengono trattati come un'unica entità quando viene creata un'immagine snapshot. Ciascuno di questi volumi ha la propria immagine snapshot, ma tutte le immagini vengono create nello stesso momento.
Volume membro del gruppo di coerenza Snapshot	Ogni volume appartenente a un gruppo di coerenza snapshot viene definito volume membro. Quando si aggiunge un volume a un gruppo di coerenza snapshot, System Manager crea automaticamente un nuovo gruppo snapshot che corrisponde a questo volume membro.
Rollback	Il rollback è il processo di restituzione dei dati in un volume di base a un precedente point-in-time.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copia del servizio e oggetto di archiviazione. Non è direttamente leggibile dall'host.

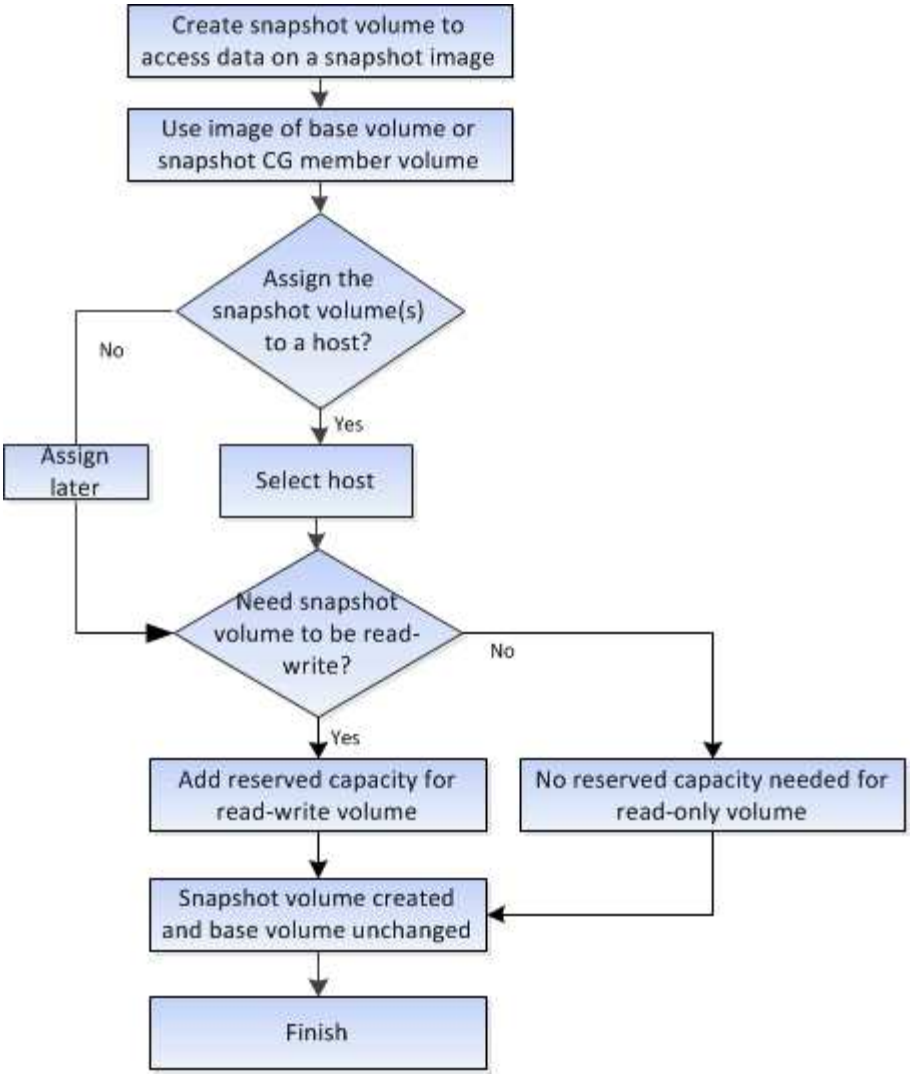
Come funziona la creazione di immagini Snapshot e volumi Snapshot in SANtricity System Manager

In SANtricity System Manager, puoi creare immagini Snapshot e volumi Snapshot seguendo questi passaggi.

Flusso di lavoro per la creazione di immagini Snapshot



Flusso di lavoro per la creazione di volumi Snapshot



Requisiti e linee guida per gli snapshot in SANtricity System Manager

Quando si creano e si utilizzano snapshot, esaminare i seguenti requisiti e linee guida.

Immagini Snapshot e gruppi di Snapshot

- Ciascuna immagine Snapshot è associata a un solo gruppo di Snapshot.
- Un gruppo di snapshot viene creato la prima volta che si crea un'immagine snapshot pianificata o istantanea per un oggetto associato. Questo crea capacità riservata.

  È possibile visualizzare i gruppi di snapshot dalla pagina Pool & gruppi di volumi.

- Le immagini Snapshot programmate non vengono create quando l'array di storage è offline o spento.
- Se si elimina un gruppo di Snapshot che ha una pianificazione di Snapshot, anche la pianificazione di Snapshot viene eliminata.
- Se si dispone di un volume snapshot che non è più necessario, è possibile riutilizzarlo, insieme a qualsiasi capacità riservata associata, invece di eliminarlo. Questo crea un volume snapshot diverso dello stesso volume di base. È possibile riassociare il volume snapshot o il volume snapshot del gruppo di coerenza snapshot alla stessa immagine snapshot o a un'immagine snapshot diversa, purché l'immagine snapshot sia nello stesso volume di base.

Gruppo di coerenza Snapshot

- Un gruppo di coerenza Snapshot contiene un gruppo Snapshot per ogni volume che è membro del gruppo di coerenza Snapshot.
- È possibile associare un gruppo di coerenza Snapshot a una sola pianificazione.
- Se si elimina un gruppo di coerenza Snapshot che ha una pianificazione Snapshot, anche la pianificazione Snapshot viene eliminata.
- Non è possibile gestire singolarmente un gruppo di snapshot associato a un gruppo di coerenza di snapshot. Al contrario, è necessario eseguire le operazioni di gestione (creazione di un'immagine snapshot, eliminazione di un'immagine snapshot o di un gruppo di snapshot e ripristino di un'immagine snapshot) a livello del gruppo di coerenza di snapshot.

Volume base

- Un volume snapshot deve avere le stesse impostazioni di Data Assurance (DA) e di sicurezza del volume base associato.
- Non è possibile creare un volume snapshot di un volume base guasto.
- Se il volume di base risiede su un gruppo di volumi, i volumi membri di qualsiasi gruppo di coerenza Snapshot associato possono risiedere su un pool o su un gruppo di volumi.
- Se un volume di base risiede su un pool, tutti i volumi membri di qualsiasi gruppo di coerenza Snapshot associato devono risiedere sullo stesso pool del volume di base.

Capacità riservata

- La capacità riservata è associata a un solo volume base.
- L'utilizzo di una pianificazione può generare un numero elevato di immagini Snapshot. Assicurati di disporre di una capacità riservata sufficiente per Snapshot pianificate.
- Il volume di capacità riservato per un gruppo di coerenza Snapshot deve avere le stesse impostazioni di Data Assurance (DA) e di sicurezza del volume base associato per il volume membro del gruppo di coerenza Snapshot.

Immagini Snapshot in sospeso

La creazione dell'immagine Snapshot potrebbe rimanere in stato "In sospeso" nelle seguenti condizioni:

- Il volume di base che contiene questa immagine Snapshot è membro di un gruppo mirror asincrono.
- Il volume di base è attualmente in fase di sincronizzazione. La creazione dell'immagine Snapshot viene completata non appena l'operazione di sincronizzazione è terminata.

Numero massimo di snapshot

- Se un volume è membro di un gruppo di coerenza snapshot, System Manager crea un gruppo snapshot per quel volume membro. Questo gruppo snapshot viene conteggiato nel numero massimo consentito di gruppi snapshot per volume base.
- Se si tenta di creare un'immagine Snapshot su un gruppo di Snapshot o su un gruppo di coerenza Snapshot, ma il gruppo associato ha raggiunto il numero massimo di immagini Snapshot, sono disponibili due opzioni:
  - Abilita l'eliminazione automatica per il gruppo di Snapshot o il gruppo di coerenza Snapshot.
  - Elimina manualmente una o più immagini Snapshot dal gruppo di Snapshot o dal gruppo di coerenza Snapshot e riprova l'operazione.

Eliminazione automatica

Se il gruppo di snapshot o il gruppo di coerenza degli snapshot è abilitato per l'eliminazione automatica, System Manager elimina l'immagine snapshot più vecchia quando il sistema ne crea una nuova per il gruppo.

Operazione di rollback

- Non è possibile eseguire le seguenti azioni durante un'operazione di rollback:
  - Elimina l'immagine Snapshot utilizzata per il rollback.
  - Crea una nuova immagine Snapshot per un volume di base che partecipa a un'operazione di rollback.
  - Modifica la policy Repository-Full del gruppo di Snapshot associato.
- Non è possibile avviare un'operazione di rollback quando una di queste operazioni è in corso:
  - Espansione della capacità (aggiunta di capacità a un pool o volume group)
  - Espansione del volume (aumento della capacità di un volume)
  - Modifica del livello RAID per un gruppo di volumi
  - Modifica della dimensione del segmento per un volume
- Non è possibile avviare un'operazione di rollback se il volume di base partecipa a una copia del volume.
- Non è possibile avviare un'operazione di rollback se il volume di base è un volume secondario in un mirror remoto.
- Un'operazione di rollback non riesce se una qualsiasi della capacità utilizzata nel volume del repository snapshot associato presenta settori illeggibili.

Scopri volumi di base, capacità riservata e gruppi di snapshot in SANtricity System Manager

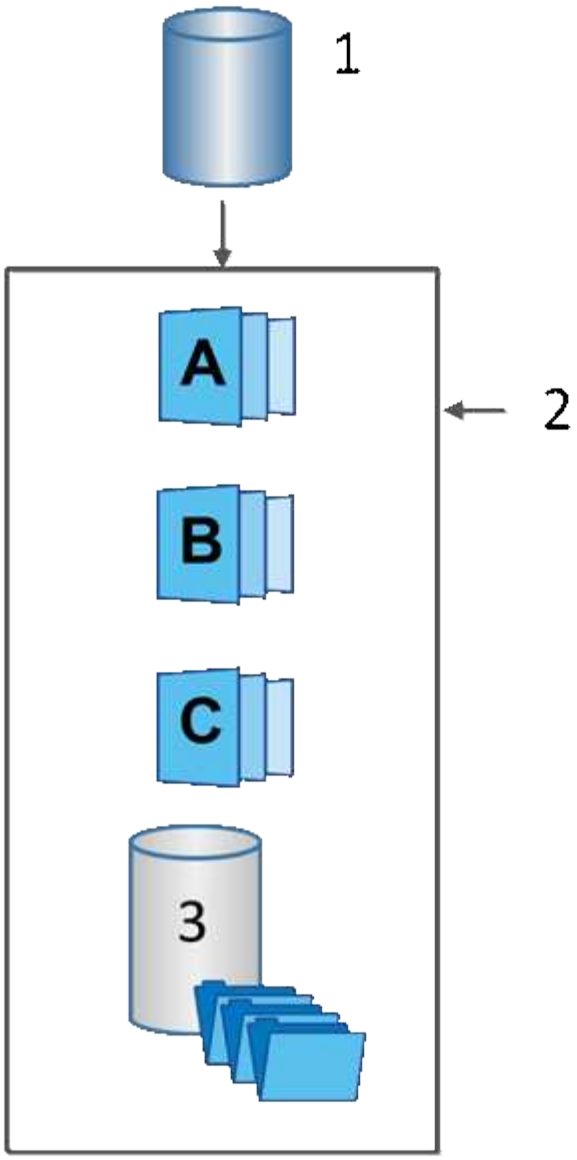
La funzionalità Snapshot utilizza volumi di base, capacità riservata e gruppi di Snapshot.

Volumi di base

Un *volume di base* è il volume utilizzato come sorgente per un'immagine Snapshot. Un volume di base può essere un volume spesso o un volume sottile e può risiedere in un pool o in un gruppo di volumi.

Per acquisire snapshot del volume di base, è possibile creare un'immagine istantanea in qualsiasi momento oppure automatizzare il processo definendo una pianificazione regolare per le snapshot.

La figura seguente mostra la relazione tra gli oggetti Snapshot e il volume di base.



[1] Volume base; [2] Oggetti Snapshot nel gruppo (immagini e capacità riservata); [3] Capacità riservata per il gruppo Snapshot.

Capacità riservata e gruppi di Snapshot

System Manager organizza le immagini snapshot in *gruppi di snapshot*. Quando System Manager stabilisce il gruppo di snapshot, crea automaticamente la *capacità riservata* associata per contenere le immagini snapshot del gruppo e per tenere traccia delle modifiche successive agli snapshot aggiuntivi.

Se il volume base si trova in un gruppo di volumi, la capacità riservata può essere collocata in un pool o in un gruppo di volumi. Se il volume base si trova in un pool, la capacità riservata deve essere collocata nello stesso pool del volume base.

I gruppi di Snapshot non richiedono alcuna azione da parte dell'utente, ma è possibile modificare la capacità riservata su un gruppo di Snapshot in qualsiasi momento. Inoltre, potrebbe essere richiesto di creare capacità riservata quando vengono soddisfatte le seguenti condizioni:

- Ogni volta che si crea uno snapshot di un volume di base che non dispone ancora di un gruppo di

snapshot, System Manager crea automaticamente un gruppo di snapshot. Questa operazione crea anche capacità riservata per il volume di base, utilizzata per archiviare le immagini snapshot successive.

- Ogni volta che si crea una pianificazione di snapshot per un volume di base, System Manager crea automaticamente un gruppo di snapshot.

Eliminazione automatica

Quando si lavora con gli snapshot, utilizzare l'opzione predefinita per avere l'eliminazione automatica attivata. L'eliminazione automatica cancella automaticamente l'immagine snapshot più vecchia quando il gruppo di snapshot raggiunge il limite di 32 immagini. Se si disattiva l'eliminazione automatica, i limiti del gruppo di snapshot verranno eventualmente superati e sarà necessario intervenire manualmente per configurare le impostazioni del gruppo di snapshot e gestire la capacità riservata.

Scopri le pianificazioni di Snapshot e i gruppi di coerenza degli Snapshot in SANtricity System Manager

Utilizzare i calendari di Snapshot per la raccolta delle immagini Snapshot e utilizzare i gruppi di coerenza di Snapshot per gestire più volumi di base.

Per gestire facilmente le operazioni di Snapshot per i volumi di base, puoi utilizzare le seguenti funzionalità:

- **Snapshot schedule** — Automatizza le Snapshot per un singolo volume di base.
- **Gruppo di coerenza Snapshot** — Gestisci più volumi di base come un'unica entità.

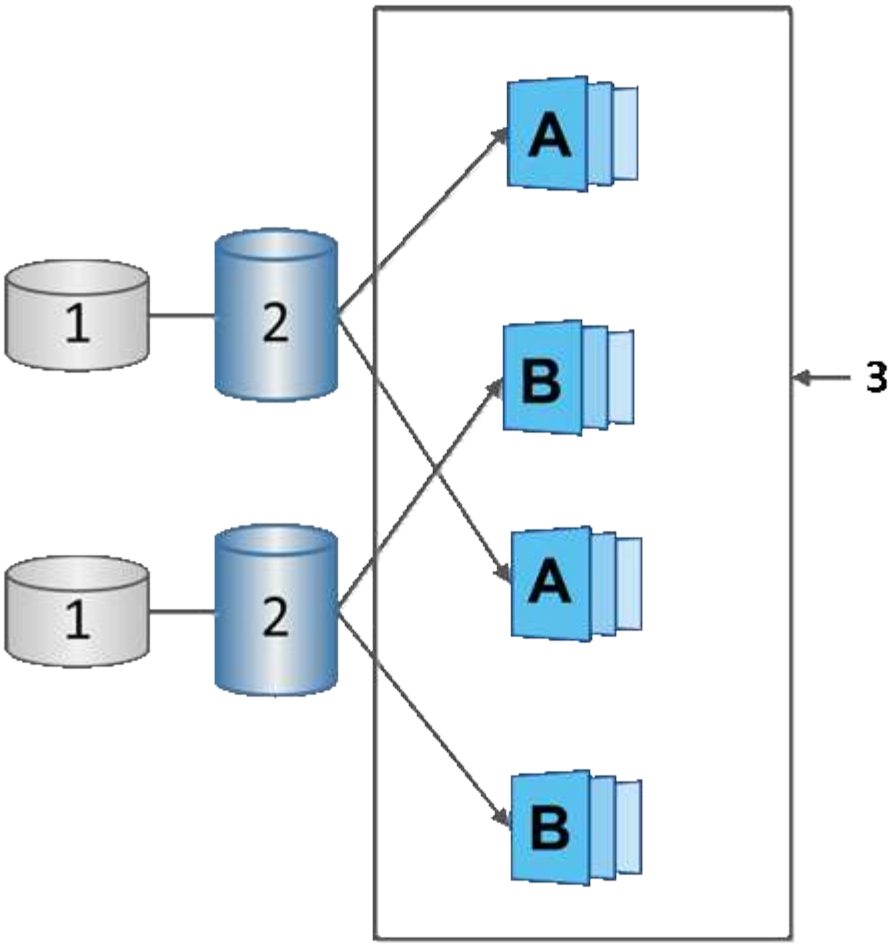
calendario di Snapshot

Se si desidera acquisire automaticamente snapshot per un volume di base, è possibile creare un calendario. Ad esempio, è possibile definire un calendario che acquisisca immagini snapshot ogni sabato a mezzanotte, il primo di ogni mese o in qualsiasi data e ora si decida. Dopo che è stato raggiunto il massimo di 32 snapshot per un singolo calendario, è possibile sospendere gli snapshot pianificati, creare ulteriore capacità riservata o eliminare gli snapshot. Gli snapshot possono essere eliminati manualmente o automatizzando il processo di eliminazione. Dopo che un'immagine snapshot viene eliminata, ulteriore capacità riservata sarà disponibile per il riutilizzo.

Gruppo di coerenza Snapshot

Si crea un gruppo di coerenza snapshot quando si desidera garantire che le immagini snapshot vengano acquisite contemporaneamente su più volumi. Le azioni sulle immagini snapshot vengono eseguite sull'intero gruppo di coerenza snapshot. Ad esempio, è possibile pianificare snapshot sincronizzati di tutti i volumi con lo stesso timestamp. I gruppi di coerenza snapshot sono ideali per le applicazioni che si estendono su più volumi, come le applicazioni di database che memorizzano i log su un volume e i file del database su un altro volume.

I volumi inclusi in un gruppo di coerenza di snapshot sono chiamati volumi membri. Quando si aggiunge un volume a un gruppo di coerenza, System Manager crea automaticamente una nuova capacità riservata che corrisponde a quel volume membro. È possibile definire un calendario per creare automaticamente un'immagine Snapshot di ciascun volume membro.



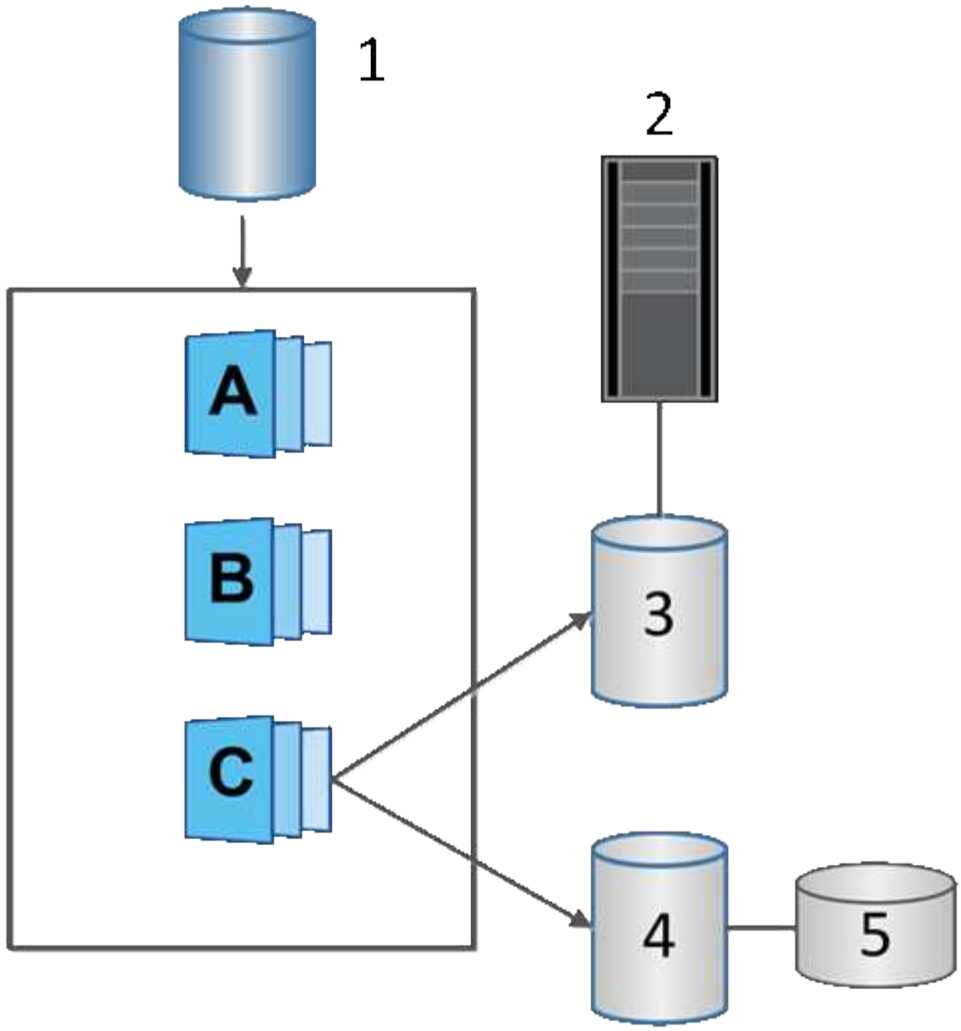
[1] Capacità riservata; [2] Volume membro; [3] Immagini Snapshot del gruppo di coerenza

Scopri i volumi Snapshot nel software SANtricity

È possibile creare un volume Snapshot e assegnarlo a un host se si desidera leggere o scrivere dati Snapshot. Il volume Snapshot condivide le stesse caratteristiche del volume base (livello RAID, caratteristiche di I/O e così via).

Quando si crea un volume Snapshot, è possibile designarlo come *di sola lettura* o *accessibile in lettura e scrittura*.

Quando si creano volumi Snapshot di sola lettura, non è necessario aggiungere capacità riservata. Quando si creano volumi Snapshot di lettura/scrittura, è necessario aggiungere capacità riservata per fornire l'accesso in scrittura.



[1] Volume base; [2] Host; [3] Volume Snapshot di sola lettura; [4] Volume Snapshot di lettura/scrittura; [5] Capacità riservata

Scopri il rollback degli snapshot nel software SANtricity

Un'operazione di rollback riporta un volume di base a uno stato precedente, determinato dallo Snapshot selezionato.

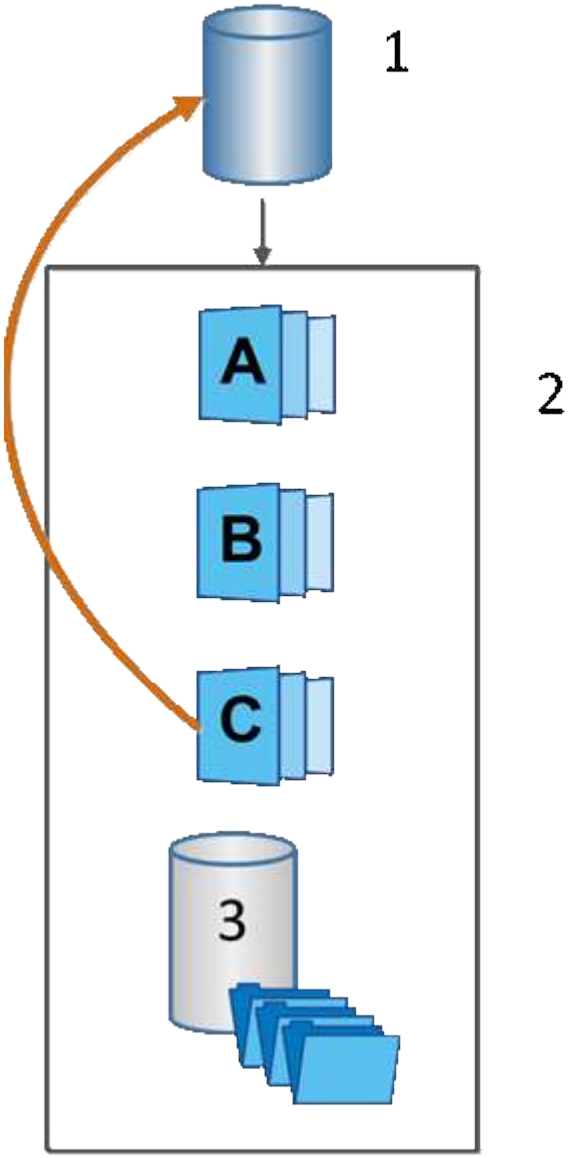
Per il rollback, è possibile selezionare un'immagine Snapshot da una delle seguenti fonti:

- **Rollback dell'immagine Snapshot**, per un ripristino completo di un volume di base.
- **Ripristino del gruppo di coerenza Snapshot**, che può essere utilizzato per ripristinare uno o più volumi.

Durante il rollback, la funzionalità Snapshot preserva tutte le immagini snapshot nel gruppo. Consente inoltre all'host di accedere al volume di base durante questo processo, se necessario per le operazioni di I/O.

Quando viene avviato un rollback, un processo in background analizza gli indirizzi di blocco logici (LBA) del volume di base e quindi trova i dati copy-on-write nell'immagine snapshot del rollback da ripristinare. Poiché il volume di base è accessibile dall'host per letture e scritture, e tutti i dati precedentemente scritti sono immediatamente disponibili, il volume di capacità riservata deve essere sufficientemente grande da contenere tutte le modifiche mentre il rollback è in corso. Il trasferimento dei dati continua come operazione in

background fino al completamento del rollback.



[1] Volume base; [2] Oggetti Snapshot in un gruppo; [3] Capacità riservata del gruppo Snapshot

Crea Snapshot e oggetti Snapshot

Crea un'immagine Snapshot in SANtricity System Manager

È possibile creare manualmente un'immagine Snapshot da un volume di base o da un gruppo di coerenza Snapshot. Questa operazione è anche chiamata *instant snapshot* o *instant image*.

Prima di iniziare

- Il volume di base deve essere ottimale.
- Il disco deve essere ottimale.

- Il gruppo di snapshot non può essere designato come “reserved.”
- Il volume di capacità riservata deve avere le stesse impostazioni di Data Assurance (DA) del volume base associato per il gruppo di Snapshot.

Passaggi

1. Esegui una delle seguenti azioni per creare un’immagine Snapshot:
   - Selezionare **Storage › Volumes**. Selezionare l’oggetto (base volume o snapshot consistency group), quindi selezionare **Copy Services › Create instant snapshot**.
   - Selezionare **Storage › Snapshots**. Selezionare la scheda **Snapshot Images** e quindi selezionare **Create › Instant snapshot**.

     Viene visualizzata la finestra di dialogo Crea Snapshot Image. Selezionare l’oggetto (volume di base o gruppo di coerenza snapshot), quindi fare clic su **Avanti**. Se è già stata creata una precedente immagine snapshot per il volume o il gruppo di coerenza snapshot, il sistema crea immediatamente la snapshot istantanea. Altrimenti, se questa è la prima volta che viene creata un’immagine snapshot per il volume o il gruppo di coerenza snapshot, viene visualizzata la finestra di dialogo Conferma creazione Snapshot Image.

2. Fai clic su **Crea** per accettare la notifica che è necessaria la capacità riservata e per procedere alla fase Reserve Capacity.

   Viene visualizzata la finestra di dialogo Reserve Capacity.

3. Utilizza la casella di selezione per regolare la percentuale di capacità, quindi fai clic su **Next** per accettare il volume candidato evidenziato nella tabella.

   Viene visualizzata la finestra di dialogo Edit Settings.

4. Seleziona le impostazioni per l’immagine Snapshot come appropriato e conferma di voler eseguire l’operazione.

Dettagli del campo

Impostazione	Descrizione
Impostazioni dell'immagine Snapshot	Limite delle immagini Snapshot
Mantieni selezionata la check box se desideri che le immagini Snapshot vengano eliminate automaticamente dopo il limite specificato; usa la spinner box per modificare il limite. Se deselezioni questa check box, la creazione di immagini Snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservata**
Avvisami quando…	Utilizzare il selettore a rotella per regolare la percentuale al punto in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di Snapshot sta per essere piena. Quando la capacità riservata per il gruppo di Snapshot supera la soglia specificata, utilizzare la notifica anticipata per aumentare la capacità riservata o per eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Politica per la piena capacità riservata	Scegli una delle seguenti policy: • **Elimina l'immagine Snapshot più vecchia** — Il sistema elimina automaticamente l'immagine Snapshot più vecchia nel gruppo di Snapshot, liberando la capacità riservata dell'immagine Snapshot per il riutilizzo all'interno del gruppo. • **Rifiuta le scritture sul volume base** — Quando la capacità riservata raggiunge la percentuale massima definita, il sistema rifiuta qualsiasi richiesta di scrittura I/O sul volume base che ha attivato l'accesso alla capacità riservata.

Risultati

- System Manager visualizza la nuova immagine Snapshot nella tabella Immagini Snapshot. La tabella elenca la nuova immagine in base al timestamp e al volume di base o al gruppo di coerenza Snapshot associato.
- La creazione di Snapshot potrebbe rimanere nello stato "In sospeso" a causa delle seguenti condizioni:
  - Il volume di base che contiene questa immagine Snapshot è membro di un gruppo mirror asincrono.

- Il volume di base è attualmente in fase di sincronizzazione. La creazione dell'immagine Snapshot viene completata non appena l'operazione di sincronizzazione è terminata.

Pianifica le immagini Snapshot in SANtricity System Manager

Si crea un calendario di Snapshot per abilitare il ripristino in caso di un problema con il volume di base e per eseguire backup programmati. Gli Snapshot dei volumi di base o dei gruppi di coerenza di Snapshot possono essere creati su base giornaliera, settimanale o mensile, in qualsiasi momento della giornata.

Prima di iniziare

Il volume di base deve essere Optimal.

Informazioni su questa attività

Questa procedura descrive come creare un calendario di Snapshot per un gruppo di coerenza Snapshot o un volume di base esistente.

> È inoltre possibile creare un calendario di Snapshot contemporaneamente alla creazione di un'immagine Snapshot di un volume di base o di un gruppo di coerenza Snapshot.

Passaggi

1. Eseguire una delle seguenti azioni per creare un calendario di Snapshot:
   - Selezionare **Storage › Volumes**.

     Selezionare l'oggetto (volume o gruppo di coerenza snapshot) per questo calendario di Snapshot, quindi selezionare **Copy Services › Crea calendario di Snapshot**.

   - Selezionare **Storage › Snapshots**.

     Seleziona la scheda **Schedules** e poi fai clic su **Create**.

2. Selezionare l'oggetto (volume o gruppo di coerenza di snapshot) per questo calendario di Snapshot, quindi fare clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Crea calendario di Snapshot.

3. Eseguire una delle seguenti azioni:
   - **Utilizzare un calendario di Snapshot definito in precedenza da un altro oggetto Snapshot**.

     Assicurati che le opzioni avanzate siano visualizzate. Fai clic su **Mostra altre opzioni**. Fai clic su **Importa Schedule**, seleziona l'oggetto con il calendario che desideri importare e quindi fai clic su **Importa**.

   - **Modifica le opzioni di base o avanzate**.

     Nell'angolo in alto a destra della finestra di dialogo, fai clic su **Mostra altre opzioni** per visualizzare tutte le opzioni, e poi consulta la tabella seguente.

Dettagli del campo

Campo	Descrizione
Impostazioni di base	Seleziona giorni
Seleziona i singoli giorni della settimana per le immagini Snapshot.	Ora di inizio
Dal menu a tendina, seleziona un nuovo orario di inizio per le Snapshot giornaliere (le opzioni sono disponibili con incrementi di mezz'ora). L'orario di inizio predefinito è mezz'ora avanti rispetto all'ora corrente.	Fuso orario
Dal menu a discesa, seleziona il fuso orario del tuo array.	**Impostazioni avanzate**
Giorno/mese	Scegli una delle seguenti opzioni: • **Giornaliero/Settimanale** — Seleziona i singoli giorni per le Snapshot di sincronizzazione. Puoi anche selezionare la check box **Seleziona tutti i giorni** in alto a destra se desideri un calendario giornaliero. • **Mensile/Annuale** — Seleziona i singoli mesi per le Snapshot di sincronizzazione. Nel campo **Giorno/i**, inserisci i giorni del mese in cui devono avvenire le sincronizzazioni. I valori validi sono da **1** a **31** e **Last**. Puoi separare più giorni con una virgola o un punto e virgola. Usa un trattino per le date inclusive. Ad esempio: 1,3,4,10-15,Last. Puoi anche selezionare la check box **Select all months** in alto a destra se desideri un calendario mensile.
Ora di inizio	Dal menu a tendina, seleziona un nuovo orario di inizio per le Snapshot giornaliere (le opzioni sono disponibili con incrementi di mezz'ora). L'orario di inizio predefinito è mezz'ora avanti rispetto all'ora corrente.
Fuso orario	Dal menu a discesa, seleziona il fuso orario del tuo array.
Snapshot al giorno / Tempo tra Snapshot	Seleziona il numero di immagini di Snapshot da creare al giorno. Se ne selezioni più di una, seleziona anche l'intervallo di tempo tra le immagini di Snapshot. Per più immagini di Snapshot, assicurati di disporre di una capacità riservata adeguata.

Campo	Descrizione
Creare un'immagine Snapshot adesso?	Seleziona questa check box per creare un'istantanea in aggiunta alle immagini automatiche che stai programmando.
Data di inizio/fine o nessuna data di fine	Inserisci la data di inizio per l'avvio delle sincronizzazioni. Inserisci anche una data di fine oppure seleziona **No end date**.

4. Eseguire una delle seguenti azioni:
   - Se l'oggetto è un gruppo di coerenza Snapshot, fai clic su **Crea** per accettare le impostazioni e creare il calendario di Snapshot.
   - Se l'oggetto è un volume, fai clic su **Avanti** per allocare la capacità riservata per le immagini Snapshot.

     La tabella dei volumi candidati visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copy service e oggetto di storage. Non è direttamente leggibile dall'host.
5. Utilizzare la casella di selezione per allocare la capacità riservata per le immagini Snapshot. Eseguire una delle seguenti azioni:
   - **Accetta le impostazioni predefinite.**

     Utilizza questa opzione consigliata per allocare la capacità riservata per le immagini Snapshot con le impostazioni predefinite.
   - **Assegna le tue impostazioni di capacità riservata per soddisfare le tue esigenze di archiviazione dati.**

     Se modifichi l'impostazione predefinita della capacità riservata, fai clic su **Aggiorna candidati** per aggiornare l'elenco dei candidati per la capacità riservata che hai specificato.

     Assegnare la capacità riservata utilizzando le seguenti linee guida:
     - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base. Di solito questa capacità è sufficiente.
     - La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sui volumi e della quantità e durata della raccolta delle immagini Snapshot.
6. Fai clic su **Avanti**.

   Viene visualizzata la finestra di dialogo Edit Settings.
7. Modifica le impostazioni del calendario di Snapshot secondo necessità, quindi fai clic su **Fine**.

Dettagli del campo

Impostazione	Descrizione
Limite di immagini Snapshot	Abilita l'eliminazione automatica delle immagini Snapshot quando…
Mantieni selezionata la check box se desideri che le immagini Snapshot vengano eliminate automaticamente dopo il limite specificato; usa la spinner box per modificare il limite. Se deselezioni questa check box, la creazione di immagini Snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservata**
Avvisami quando…	Utilizzare il selettore a rotella per regolare la percentuale al punto in cui il sistema invia una notifica di avviso quando la capacità riservata per un calendario sta per esaurirsi. Quando la capacità riservata per il calendario supera la soglia specificata, utilizzare l'avviso anticipato per aumentare la capacità riservata o per eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Politica per la piena capacità riservata	Scegli una delle seguenti policy: • **Elimina l'immagine Snapshot più vecchia** — Il sistema elimina automaticamente l'immagine Snapshot più vecchia, liberando la capacità riservata per le Snapshot per il riutilizzo all'interno del gruppo di Snapshot. • **Rifiuta le scritture sul volume base** — Quando la capacità riservata raggiunge la percentuale massima definita, il sistema rifiuta qualsiasi richiesta di scrittura I/O sul volume base che ha attivato l'accesso alla capacità riservata.

Crea un gruppo di coerenza snapshot in SANtricity System Manager

Per garantire di avere copie coerenti, è possibile creare un set di più volumi denominato *gruppo di coerenza snapshot*.

Questo gruppo consente di creare snapshot di tutti i volumi contemporaneamente per garantire la coerenza. Ogni volume che appartiene a un gruppo di coerenza snapshot viene definito *volume membro*. Quando si aggiunge un volume a un gruppo di coerenza snapshot, il sistema crea automaticamente un nuovo gruppo di

snapshot che corrisponde a questo volume membro.

Informazioni su questa attività

La sequenza di creazione del gruppo di coerenza Snapshot consente di selezionare i volumi membri del gruppo e di allocare capacità ai volumi membri.

La procedura per creare un gruppo di coerenza Snapshot si articola in più fasi.

Passaggio 1: Aggiungi membri al gruppo di coerenza Snapshot

Seleziona i membri per specificare una raccolta di volumi che compongono il gruppo di coerenza Snapshot. Qualsiasi azione eseguita sul gruppo di coerenza Snapshot si estende uniformemente ai volumi membri selezionati.

Prima di iniziare

I volumi dei membri devono essere Optimal.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Consistency Groups**.
3. Selezionare menu:Crea [Snapshot consistency group].

   Viene visualizzata la finestra di dialogo Crea gruppo di coerenza Snapshot.
4. Selezionare il/i volume/i da aggiungere come volumi membri al gruppo di coerenza Snapshot.
5. Fai clic su **Avanti** e vai a Passaggio 2: Riserva la capacità per il gruppo di coerenza Snapshot.

Passaggio 2: Riserva la capacità per il gruppo di coerenza Snapshot

Associa la capacità riservata al gruppo di coerenza Snapshot. System Manager suggerisce i volumi e la capacità in base alle proprietà del gruppo di coerenza Snapshot. Puoi accettare la configurazione di capacità riservata consigliata o personalizzare lo storage allocato.

Informazioni su questa attività

Nella finestra di dialogo Capacità riservata, la tabella dei volumi candidati visualizza solo i candidati che supportano la capacità riservata specificata. La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copy service e oggetto di storage. Non è direttamente leggibile dall'host.

Passaggi

1. Utilizzare la casella di selezione per allocare la capacità riservata per il gruppo di coerenza Snapshot. Eseguire una delle seguenti azioni:
   - **Accetta le impostazioni predefinite**.

     Utilizza questa opzione consigliata per allocare la capacità riservata per ciascun volume membro con le impostazioni predefinite.
   - **Assegna le tue impostazioni di capacità riservata per soddisfare le tue esigenze di archiviazione dati.**

     Assegna la capacità riservata utilizzando le seguenti linee guida.
     - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base. Di

solito questa capacità è sufficiente.

- La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sui volumi e della quantità e durata della raccolta delle immagini Snapshot.

2. **Facoltativo:** Se modifichi l'impostazione predefinita della capacità riservata, fai clic su **Aggiorna candidati** per aggiornare l'elenco dei candidati per la capacità riservata specificata.
3. Fai clic su **Avanti** e vai a Passaggio 3: Modifica delle impostazioni per il gruppo di coerenza Snapshot.

Passaggio 3: Modifica delle impostazioni per il gruppo di coerenza Snapshot

Accetta o scegli le impostazioni di eliminazione automatica e le soglie di avviso della capacità riservata per il gruppo di coerenza Snapshot.

Informazioni su questa attività

La sequenza di creazione del gruppo di coerenza Snapshot consente di selezionare i volumi membri del gruppo e di allocare capacità ai volumi membri.

Passaggi

1. Accetta o modifica le impostazioni predefinite per il gruppo di coerenza Snapshot, secondo necessità.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del gruppo di coerenza Snapshot	Nome
Specificare il nome per il gruppo di coerenza Snapshot.	Abilita l'eliminazione automatica delle immagini Snapshot quando…
Mantieni selezionata la check box se desideri che le immagini Snapshot vengano eliminate automaticamente dopo il limite specificato; usa la spinner box per modificare il limite. Se deselezioni questa check box, la creazione di immagini Snapshot si interrompe dopo 32 immagini.	**Impostazioni di capacità riservata**
Avvisami quando…	Utilizzare il selettore a rotella per regolare la percentuale al punto in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di coerenza Snapshot sta per esaurirsi. Quando la capacità riservata per il gruppo di coerenza Snapshot supera la soglia specificata, utilizzare la notifica preventiva per aumentare la capacità riservata o per eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.
Politica per la piena capacità riservata	Scegli una delle seguenti policy: • **Elimina l'immagine snapshot più vecchia** — Il sistema elimina automaticamente l'immagine snapshot più vecchia nel gruppo di coerenza snapshot, liberando la capacità riservata all'immagine snapshot per il riutilizzo all'interno del gruppo. • **Rifiuta le scritture sul volume base** — Quando la capacità riservata raggiunge la percentuale massima definita, il sistema rifiuta qualsiasi richiesta di scrittura I/O sul volume base che ha attivato l'accesso alla capacità riservata.

2. Dopo aver verificato la configurazione del gruppo di coerenza Snapshot, fare clic su **Fine**.

Creare un volume Snapshot in SANtricity System Manager

Si crea un volume Snapshot per consentire all'host di accedere a un'immagine Snapshot di un volume o di un gruppo di coerenza Snapshot. È possibile designare il volume Snapshot come di sola lettura o di lettura/scrittura.

Informazioni su questa attività

La sequenza di creazione del volume snapshot consente di creare un volume snapshot da un'immagine snapshot e offre opzioni per allocare capacità riservata se il volume è in lettura/scrittura. Un volume snapshot può essere designato come uno dei seguenti:

- Un volume snapshot di sola lettura fornisce a un'applicazione host l'accesso in lettura a una copia dei dati contenuti nell'immagine snapshot, ma senza la possibilità di modificare l'immagine snapshot. Un volume snapshot di sola lettura non dispone di capacità riservata associata.
- Un volume snapshot di lettura/scrittura fornisce all'applicazione host l'accesso in scrittura a una copia dei dati contenuti nell'immagine snapshot. Dispone di una propria capacità riservata che viene utilizzata per salvare eventuali modifiche successive apportate dall'applicazione host al volume di base senza influire sull'immagine snapshot di riferimento.

Il processo per creare un volume Snapshot è una procedura in più fasi.

Passaggio 1: Esaminare i membri per un volume di Snapshot

Selezionare un'immagine Snapshot di un volume base o un gruppo di coerenza Snapshot. Se si seleziona un'immagine Snapshot di un gruppo di coerenza Snapshot, i volumi membri del gruppo di coerenza Snapshot vengono visualizzati per la revisione.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.
3. Seleziona **Create**.

   Viene visualizzata la finestra di dialogo Crea Snapshot Volume.

4. Seleziona l'immagine Snapshot (volume o gruppo di coerenza Snapshot) che desideri convertire in un volume Snapshot, quindi fai clic su **Avanti**. Utilizza una voce di testo nel campo **Filtro** per restringere l'elenco.

   Se la selezione riguarda un'immagine Snapshot di un gruppo di coerenza Snapshot, viene visualizzata la finestra di dialogo Review Members.

   Nella finestra di dialogo Review Members, esamina l'elenco dei volumi selezionati per la conversione in volumi Snapshot, quindi fai clic su **Next**.

5. Vai a Passaggio 2: Assegna il volume Snapshot all'host.

Passaggio 2: Assegna il volume Snapshot all'host

Seleziona un host specifico o un cluster di host da assegnare al volume Snapshot. Questa assegnazione garantisce a un host o a un cluster di host l'accesso al volume Snapshot. Puoi scegliere di assegnare un host in un secondo momento, se necessario.

Prima di iniziare

- Host o cluster di host validi sono presenti nella pagina Host.
- Gli identificatori della porta host devono essere stati definiti per l'host.
- Prima di creare un volume abilitato per DA, verificare che la connessione host pianificata supporti la funzionalità Data Assurance (DA). Se una qualsiasi delle connessioni host sui controller nell'array di storage non supporta DA, gli host associati non possono accedere ai dati sui volumi abilitati per DA.

Informazioni su questa attività

Quando si assegnano i volumi, tenere a mente queste linee guida:

- Il sistema operativo di un host può avere limiti specifici su quanti volumi l'host può accedere.
- È possibile definire un'assegnazione host per ogni volume Snapshot nell'array di archiviazione.
- I volumi assegnati sono condivisi tra i controller nell'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 Snapshot. È necessario utilizzare un LUN univoco.

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

Passaggi

1. Nella finestra di dialogo **Assegna a host**, seleziona l'host o il cluster di host che desideri assegnare al nuovo volume. Se desideri creare il volume senza assegnare un host, seleziona **Assegna in seguito** dall'elenco a discesa.
2. Seleziona la modalità di accesso. Scegli una delle seguenti:
   - **Lettura/scrittura** — Questa opzione fornisce all'host l'accesso in lettura/scrittura al volume Snapshot e richiede capacità riservata.
   - **Sola lettura** — Questa opzione fornisce all'host l'accesso in sola lettura al volume Snapshot e non richiede capacità riservata.
3. Fai clic su **Avanti** e scegli una delle seguenti opzioni:
   - Se il volume Snapshot è in lettura/scrittura, viene visualizzata la finestra di dialogo Rivedi capacità. Vai a Passaggio 3: Riservare capacità per un volume Snapshot.
   - Se il volume Snapshot è di sola lettura, viene visualizzata la finestra di dialogo Modifica priorità. Vai a Passaggio 4: Modificare le impostazioni per un volume Snapshot.

Passaggio 3: Riservare capacità per un volume Snapshot

Associa la capacità riservata a un volume snapshot di lettura/scrittura. System Manager suggerisce i volumi e la capacità in base alle proprietà del volume di base o del gruppo di coerenza snapshot. Puoi accettare la configurazione di capacità riservata consigliata o personalizzare lo storage allocato.

Informazioni su questa attività

È possibile aumentare o diminuire la capacità riservata per il volume snapshot in base alle necessità. Se si scopre che la capacità riservata per lo snapshot è superiore al necessario, è possibile ridurne le dimensioni per liberare spazio necessario ad altri volumi logici.

Passaggi

1. Utilizza la casella di selezione per allocare la capacità riservata per il volume Snapshot.

   La tabella Volume Candidate visualizza solo i candidati che supportano la capacità riservata specificata.

Eseguire una delle seguenti azioni:

- **Accetta le impostazioni predefinite**.

  Utilizza questa opzione consigliata per allocare la capacità riservata per il volume Snapshot con le impostazioni predefinite.

- **Imposta le tue impostazioni di capacità riservata per soddisfare le tue esigenze di archiviazione dati**.

  Se modifichi l'impostazione predefinita della capacità riservata, fai clic su **Aggiorna candidati** per aggiornare l'elenco dei candidati per la capacità riservata che hai specificato.

  Assegna la capacità riservata utilizzando le seguenti linee guida.

  - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base e di solito questa capacità è sufficiente.
  - La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sui volumi e della quantità e durata della raccolta delle immagini Snapshot.

2. **Facoltativo:** Se si sta creando il volume Snapshot per un gruppo di coerenza Snapshot, l'opzione "Change candidate" viene visualizzata nella tabella Reserved Capacity Candidates. Fare clic su **Change candidate** per selezionare un candidato alternativo di capacità riservata.
3. Fai clic su **Avanti** e vai a Passaggio 4: Modificare le impostazioni per un volume Snapshot.

Passaggio 4: Modificare le impostazioni per un volume Snapshot

Modifica le impostazioni di un volume Snapshot, come il nome, la cache, le soglie di avviso per la capacità riservata e così via.

Informazioni su questa attività

È possibile aggiungere il volume alla Cache SSD come metodo per migliorare le prestazioni in sola lettura. La Cache SSD è costituita da un insieme di unità SSD che vengono raggruppate logicamente nell'array di archiviazione.

Passaggi

1. Accetta o modifica le impostazioni del volume Snapshot come appropriato.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del volume Snapshot	Nome
Specificare il nome per il volume Snapshot.	Abilita Cache SSD
Scegli questa opzione per abilitare la cache in sola lettura sugli SSD.	**Impostazioni di capacità riservata**
Avvisami quando…	**Viene visualizzato solo per un volume Snapshot di lettura/scrittura**. Utilizzare il selettore a rotella per regolare la percentuale al punto in cui il sistema invia una notifica di avviso quando la capacità riservata per un gruppo di Snapshot sta per essere piena. Quando la capacità riservata per il gruppo di Snapshot supera la soglia specificata, utilizzare la notifica anticipata per aumentare la capacità riservata o per eliminare gli oggetti non necessari prima che lo spazio rimanente si esaurisca.

2. Rivedi la configurazione del volume Snapshot. Fai clic su **Back** per apportare eventuali modifiche.
3. Quando sei soddisfatto della configurazione del volume Snapshot, fai clic su **Finish**.

Gestisci le pianificazioni Snapshot

Modifica le impostazioni per un calendario di Snapshot in SANtricity System Manager

Per un calendario di Snapshot, è possibile modificare gli orari di raccolta automatica o la frequenza di raccolta.

Informazioni su questa attività

È possibile importare le impostazioni da un calendario di Snapshot esistente oppure modificarle in base alle proprie esigenze.

Poiché un calendario di Snapshot è associato a un gruppo di Snapshot o a un gruppo di coerenza di Snapshot, la capacità riservata potrebbe essere influenzata dalle modifiche alle impostazioni del calendario.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Schedules**.
3. Seleziona il calendario di Snapshot che desideri modificare, quindi fai clic su **Modifica**.

   Viene visualizzata la finestra di dialogo Edit Snapshot Schedule.

4. Eseguire una delle seguenti operazioni:
   - **Utilizza un calendario definito in precedenza da un altro oggetto Snapshot** — fai clic su **Importa calendario**, seleziona l'oggetto con il calendario che desideri importare e quindi fai clic su **Importa**.
   - **Modifica le impostazioni del calendario** — Fai riferimento ai dettagli del campo qui sotto.

     Dettagli del campo

Impostazione	Descrizione
Giorno/mese	Scegli una delle seguenti opzioni: • **Giornaliero/Settimanale** — Seleziona i singoli giorni per le Snapshot di sincronizzazione. Puoi anche selezionare la check box **Seleziona tutti i giorni** in alto a destra se desideri un calendario giornaliero. • **Mensile/Annuale** — Seleziona i singoli mesi per le Snapshot di sincronizzazione. Nel campo **Giorno/i**, inserisci i giorni del mese in cui devono avvenire le sincronizzazioni. I valori validi sono da **1** a **31** e **Last**. Puoi separare più giorni con una virgola o un punto e virgola. Usa un trattino per le date inclusive. Ad esempio: 1,3,4,10-15,Last. Puoi anche selezionare la check box **Select all months** in alto a destra se desideri un calendario mensile.
Ora di inizio	Dal menu a tendina, seleziona un nuovo orario di inizio per le Snapshot giornaliere. Le opzioni sono disponibili con incrementi di mezz'ora. L'orario di inizio predefinito è mezz'ora avanti rispetto all'ora corrente.
Fuso orario	Dal menu a discesa, seleziona il fuso orario del tuo array di storage.
Snapshot al giorno Intervallo tra le Snapshot	Seleziona il numero di immagini di Snapshot da creare al giorno. Se si selezionano più punti di ripristino, selezionare anche l'intervallo di tempo tra i punti di ripristino. Per più punti di ripristino, assicurarsi di disporre di una capacità di riserva adeguata.
Data di inizio Data di fine Nessuna data di fine	Inserisci la data di inizio per l'avvio delle sincronizzazioni. Inserisci anche una data di fine oppure seleziona **No end date**.

5. Fare clic su **Save**.

Attivare e sospendere una pianificazione snapshot in SANtricity System Manager

È possibile sospendere temporaneamente la raccolta programmata di immagini snapshot quando è necessario risparmiare spazio di storage. Questo metodo è più efficiente rispetto all'eliminazione e alla successiva ricreazione della pianificazione degli snapshot.

Informazioni su questa attività

Lo stato della pianificazione degli snapshot rimane sospeso finché non si utilizza l'opzione **Attiva** per riprendere l'attività di snapshot pianificata.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Se non è già visualizzata, fai clic sulla scheda **Schedules**.

   Gli orari sono elencati sulla pagina.

3. Seleziona una pianificazione di snapshot attiva che desideri sospendere, quindi fai clic su **Attiva / Sospendi**.

   Lo stato della colonna State cambia in **Sospeso** e la pianificazione degli snapshot interrompe la raccolta di tutte le immagini snapshot.

4. Per riprendere la raccolta delle immagini snapshot, seleziona la pianificazione di snapshot sospesa che desideri riprendere, quindi fai clic su **Attiva/Sospendi**.

   Lo stato della colonna State cambia in **Active**.

Eliminare una pianificazione di Snapshot in SANtricity System Manager

Se non desideri più raccogliere immagini Snapshot, puoi eliminare una pianificazione Snapshot esistente.

Informazioni su questa attività

Quando si elimina una pianificazione di snapshot, le immagini snapshot associate non vengono eliminate insieme ad essa. Se si pensa che la raccolta di immagini snapshot possa essere ripresa in futuro, è meglio sospendere la pianificazione di snapshot anziché eliminarla.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Schedules**.
3. Seleziona la pianificazione Snapshot che desideri eliminare e conferma l'operazione.

Risultati

Il sistema rimuove tutti gli attributi di pianificazione dal volume base o dal gruppo di coerenza Snapshot.

Gestisci le immagini Snapshot

Visualizza le impostazioni dell'immagine Snapshot in SANtricity System Manager

È possibile visualizzare le proprietà, lo stato, la capacità riservata e gli oggetti associati assegnati a ciascuna immagine Snapshot.

Informazioni su questa attività

Gli oggetti associati a una snapshot includono il volume di base o il gruppo di coerenza snapshot per cui questa snapshot è un punto di ripristino, il gruppo snapshot associato e tutti i volumi snapshot creati dalla snapshot. Utilizzare le impostazioni snapshot per determinare se si desidera copiare o convertire la snapshot.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Images**.
3. Seleziona l'immagine Snapshot che desideri visualizzare, quindi fai clic su **Visualizza impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni immagine Snapshot.

4. Visualizza le impostazioni per l'immagine Snapshot.

Avvia il rollback dell'immagine Snapshot per un volume base in SANtricity System Manager

È possibile eseguire un'operazione di rollback per modificare il contenuto di un volume di base in modo che corrisponda al contenuto salvato in un'immagine Snapshot.

L'operazione di rollback non modifica il contenuto delle immagini Snapshot associate al volume di base.

Prima di iniziare

- È disponibile una capacità riservata sufficiente per avviare un'operazione di rollback.
- L'immagine Snapshot selezionata è Optimal e il volume selezionato è Optimal.
- Il volume selezionato non ha un'operazione di rollback già in corso.

Informazioni su questa attività

La sequenza di avvio del rollback consente di avviare il rollback su un'immagine Snapshot di un volume di base, offrendo al contempo opzioni per aggiungere capacità di storage. Non è possibile avviare più di un'operazione di rollback per un volume di base alla volta.

> L'host può accedere immediatamente al nuovo volume di base ripristinato, ma il volume di base esistente non consente all'host l'accesso in lettura e scrittura dopo l'inizio del rollback. È possibile creare uno Snapshot del volume di base poco prima di avviare il rollback per preservare il volume di base precedente al rollback ai fini del ripristino.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Seleziona la scheda **Snapshot Images**.
3. Seleziona l'immagine Snapshot, quindi seleziona menu: Rollback[Start].

   Viene visualizzata la finestra di dialogo Confirm Start Rollback.

4. **Opzionale:** Selezionare l'opzione per **Increase Capacity** se necessario.

   Viene visualizzata la finestra di dialogo Increase Reserved Capacity.

   a. Utilizzare la casella spinner per regolare la percentuale di capacità.

      Se non è disponibile capacità libera nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage presenta Unassigned Capacity, è possibile aggiungere capacità. È possibile creare un nuovo pool o volume group e quindi riprovare questa operazione utilizzando la nuova capacità libera su quel pool o volume group.

   b. Fai clic su **Increase**.

5. Conferma che desideri eseguire questa operazione, quindi fai clic su **Rollback**.

Risultati

System Manager esegue le seguenti azioni:

- Ripristina il volume con il contenuto salvato sull'immagine Snapshot selezionata.
- Rende i volumi ripristinati immediatamente disponibili per l'accesso da parte dell'host. Non è necessario attendere il completamento dell'operazione di rollback.

Dopo aver finito

Selezionare **Home › Visualizza operazioni in corso** per visualizzare l'avanzamento dell'operazione di rollback.

Se l'operazione di rollback non va a buon fine, l'operazione viene sospesa. È possibile riprendere l'operazione sospesa e, se non ha ancora successo, seguire la procedura di Recovery Guru per correggere il problema oppure contattare il supporto tecnico.

Avvia il rollback dell'immagine Snapshot per i volumi membri del gruppo di coerenza Snapshot in SANtricity System Manager

È possibile eseguire un'operazione di rollback per modificare il contenuto dei volumi membri del gruppo di coerenza Snapshot in modo che corrisponda al contenuto salvato in un'immagine Snapshot.

L'operazione di rollback non modifica il contenuto delle immagini Snapshot associate al gruppo di coerenza Snapshot.

Prima di iniziare

- È disponibile una capacità riservata sufficiente per avviare un'operazione di rollback.
- L'immagine Snapshot selezionata è Optimal e il volume selezionato è Optimal.
- Il volume selezionato non ha un'operazione di rollback già in corso.

Informazioni su questa attività

La sequenza di avvio del rollback consente di avviare il rollback su un'immagine Snapshot di un gruppo di coerenza Snapshot, offrendo opzioni per aggiungere capacità di storage. Non è possibile avviare più di un'operazione di rollback per un gruppo di coerenza Snapshot alla volta.

> L'host ha accesso immediato ai nuovi volumi ripristinati, ma i volumi membri esistenti non consentono più l'accesso in lettura e scrittura all'host dopo l'avvio del rollback. È possibile creare un'immagine Snapshot dei volumi membri poco prima di avviare il rollback per preservare i volumi base pre-rollback a scopo di ripristino.

La procedura per avviare il rollback di un'immagine Snapshot di un gruppo di coerenza Snapshot è composta da più fasi.

Passaggio 1: Seleziona i membri

È necessario selezionare i volumi membro da ripristinare.

Passaggi

1. Selezionare **Storage › Snapshots**.

2. Seleziona la scheda **Snapshot Images**.
3. Selezionare l'immagine Snapshot del gruppo di coerenza Snapshot, quindi selezionare **Rollback › Start**.

   Viene visualizzata la finestra di dialogo Start Rollback.

4. Selezionare il volume o i volumi membro.
5. Fai clic su **Avanti** e scegli una delle seguenti opzioni:
   - Se uno qualsiasi dei volumi membro selezionati è associato a più di un oggetto di capacità riservata che memorizza immagini Snapshot, viene visualizzata la finestra di dialogo Rivedi capacità. Vai a Fase 2: Revisione della capacità.
   - Se nessuno dei volumi membro selezionati è associato a più di un oggetto di capacità riservata che memorizza immagini Snapshot, viene visualizzata la finestra di dialogo Modifica priorità. Vai a Passaggio 3: Modifica priorità.

Fase 2: Revisione della capacità

Se hai selezionato volumi membro associati a più di un oggetto di capacità riservata, come un gruppo di Snapshot e un volume di capacità riservata, puoi rivedere e aumentare la capacità riservata per il/i volume/i ripristinato/i.

Passaggi

1. Accanto a qualsiasi volume membro con capacità riservata molto bassa (o pari a zero), fare clic sul collegamento **Aumenta capacità** nella colonna **Modifica**.

   Viene visualizzata la finestra di dialogo Increase Reserved Capacity.

2. Utilizza la spinner box per regolare la percentuale di capacità, quindi fai clic su **Increase**.

   Se non è disponibile capacità libera nel pool o nel gruppo di volumi che contiene l'oggetto di storage selezionato e l'array di storage presenta Unassigned Capacity, è possibile aggiungere capacità. È possibile creare un nuovo pool o volume group e riprovare questa operazione utilizzando la nuova capacità libera su quel pool o volume group.

3. Fai clic su **Avanti** e vai a Passaggio 3: Modifica priorità.

   Viene visualizzata la finestra di dialogo Edit Priority.

Passaggio 3: Modifica priorità

È possibile modificare la priorità dell'operazione di rollback, se necessario.

Informazioni su questa attività

La priorità di rollback determina quante risorse di sistema vengono dedicate all'operazione di rollback a scapito delle prestazioni del sistema.

Passaggi

1. Utilizza il cursore per regolare la priorità di rollback secondo necessità.
2. Conferma che desideri eseguire questa operazione, quindi fai clic su **Fine**.

Risultati

System Manager esegue le seguenti azioni:

- Ripristina i volumi membri del gruppo di coerenza Snapshot con il contenuto salvato sull'immagine Snapshot selezionata.
- Rende i volumi ripristinati immediatamente disponibili per l'accesso da parte dell'host. Non è necessario attendere il completamento dell'operazione di rollback.

Dopo aver finito

Selezionare **Home › Visualizza operazioni in corso** per visualizzare l'avanzamento dell'operazione di rollback.

Se l'operazione di rollback non va a buon fine, l'operazione viene sospesa. È possibile riprendere l'operazione sospesa e, se non ha ancora successo, seguire la procedura di Recovery Guru per correggere il problema oppure contattare il supporto tecnico.

Riprendi un rollback dell'immagine Snapshot in SANtricity System Manager

Se si verifica un errore durante un'operazione di rollback di un'immagine Snapshot, l'operazione viene automaticamente sospesa. È possibile riprendere un'operazione di rollback che si trova in stato di sospensione.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Images**.
3. Evidenzia il rollback in pausa, quindi seleziona **Rollback › Resume**.

   L'operazione riprende.

Risultati

System Manager esegue le seguenti azioni:

- Se l'operazione di rollback riprende correttamente, puoi visualizzare lo stato di avanzamento dell'operazione di rollback nella finestra Operazioni in corso.
- Se l'operazione di rollback non va a buon fine, l'operazione si interrompe nuovamente. È possibile seguire la procedura di Recovery Guru per risolvere il problema oppure contattare il supporto tecnico.

Annulla il rollback dell'immagine Snapshot in SANtricity System Manager

È possibile annullare un rollback attivo in corso (che sta copiando dati), un rollback in sospeso (in una coda in attesa delle risorse per iniziare) o un rollback che è stato messo in pausa a causa di un errore.

Informazioni su questa attività

Quando si annulla un'operazione di rollback in corso, il volume di base torna a uno stato inutilizzabile e appare come failed. Pertanto, considera di annullare un'operazione di rollback solo quando esistono opzioni di ripristino per il ripristino del contenuto del volume di base.

> Se il gruppo di snapshot in cui risiede l'immagine snapshot contiene una o più immagini snapshot eliminate automaticamente, l'immagine snapshot utilizzata per l'operazione di rollback potrebbe non essere disponibile per rollback futuri.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Images**.
3. Seleziona il rollback attivo o in pausa, quindi seleziona **Rollback › Cancel**.

   Viene visualizzata la finestra di dialogo Confirm Cancel Rollback.

4. Fai clic su **Yes** per confermare.

Risultati

System Manager interrompe l'operazione di rollback. Il volume di base è utilizzabile ma potrebbe contenere dati incoerenti o non integri.

Dopo aver finito

Dopo aver annullato un'operazione di rollback, è necessario eseguire una delle seguenti azioni:

- Reinizializza il contenuto del volume base.
- Eseguire una nuova operazione di rollback per ripristinare il volume di base utilizzando la stessa immagine Snapshot utilizzata nell'operazione di Cancel Rollback oppure un'immagine Snapshot diversa per eseguire la nuova operazione di rollback.

Eliminare un'immagine Snapshot in SANtricity System Manager

Si eliminano le immagini snapshot per rimuovere l'immagine snapshot più vecchia da un gruppo di snapshot o da un gruppo di coerenza snapshot.

Informazioni su questa attività

È possibile eliminare una singola immagine Snapshot oppure eliminare immagini Snapshot da gruppi di coerenza Snapshot che hanno lo stesso timestamp di creazione. È anche possibile eliminare immagini Snapshot da un gruppo di Snapshot.

Non è possibile eliminare un'immagine Snapshot se non è l'immagine Snapshot più vecchia per il volume di base associato o il gruppo di coerenza Snapshot.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Images**.
3. Seleziona l'immagine Snapshot che desideri eliminare e conferma di voler eseguire l'operazione.

   Se hai selezionato un'immagine Snapshot di un gruppo di coerenza Snapshot, seleziona ciascun volume membro che desideri eliminare e conferma di voler eseguire l'operazione.

4. Fai clic su **Delete**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina l'immagine Snapshot dallo storage array.
- Rilascia la capacità riservata per il riutilizzo all'interno del gruppo di snapshot o del gruppo di coerenza snapshot.

- Disabilita tutti i volumi Snapshot associati che esistono per l'immagine Snapshot eliminata.
- Da un'eliminazione di un gruppo di coerenza Snapshot, sposta qualsiasi volume membro associato all'immagine Snapshot eliminata allo stato Arrestato.

Gestisci i gruppi di coerenza Snapshot

Aggiungi un volume membro a un gruppo di coerenza Snapshot in SANtricity System Manager

È possibile aggiungere un nuovo volume membro a un gruppo di coerenza snapshot esistente. Quando si aggiunge un nuovo volume membro, è necessario riservare la capacità anche per il volume membro.

Prima di iniziare

- Il volume membro deve essere Optimal.
- Il gruppo di coerenza snapshot deve avere meno del numero massimo di volumi consentiti (come definito dalla configurazione).
- Ciascun volume di capacità riservata deve avere le stesse impostazioni di Data Assurance (DA) e sicurezza del volume membro associato.

Informazioni su questa attività

È possibile aggiungere volumi standard o volumi thin al gruppo di coerenza snapshot. Il volume di base può risiedere in un pool o in un gruppo di volumi.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Consistency Groups**.

   La tabella viene visualizzata e mostra tutti i gruppi di coerenza snapshot associati all'array di storage.

3. Seleziona il gruppo di coerenza snapshot che desideri modificare, quindi fai clic su **Add Members**.

   Viene visualizzata la finestra di dialogo Add Members.

4. Seleziona il/i volume/i membro/i che vuoi aggiungere, quindi fai clic su **Next**.

   Viene visualizzata la fase Reserve Capacity. La tabella Volume Candidate mostra solo i candidati che supportano la reserved capacity specificata.

5. Utilizzare la casella di selezione per allocare la capacità riservata per il volume membro. Eseguire una delle seguenti azioni:
   - **Accetta le impostazioni predefinite.**

     Utilizza questa opzione consigliata per allocare la capacità riservata al volume membro con le impostazioni predefinite.

   - **Assegna le tue impostazioni di capacità riservata per soddisfare le tue esigenze di archiviazione dati.**

     Se modifichi l'impostazione predefinita della capacità riservata, fai clic su **Aggiorna candidati** per aggiornare l'elenco dei candidati per la capacità riservata che hai specificato.

Assegna la capacità riservata utilizzando le seguenti linee guida.

- L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base e di solito questa capacità è sufficiente.
- La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sui volumi e della quantità e durata della raccolta delle immagini Snapshot.

6. Fai clic su **Fine** per aggiungere i volumi member.

Rimuovere un volume membro da un gruppo di coerenza Snapshot in SANtricity System Manager

È possibile rimuovere un volume membro da un gruppo di coerenza snapshot esistente.

Informazioni su questa attività

Quando si rimuove un volume membro da un gruppo di coerenza snapshot, System Manager elimina automaticamente gli oggetti Snapshot associati a tale volume membro.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Consistency Groups**.
3. Espandere il gruppo di coerenza Snapshot che si desidera modificare selezionando il segno più (+) accanto ad esso.
4. Seleziona il volume membro che desideri rimuovere, quindi fai clic su **Remove**.
5. Conferma che desideri eseguire l'operazione, quindi fai clic su **Rimuovi**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutte le immagini Snapshot e i volumi Snapshot associati al volume membro.
- Elimina il gruppo Snapshot associato al volume membro.
- Il volume membro non viene altrimenti modificato o eliminato.

Modificare le impostazioni per un gruppo di coerenza di Snapshot in SANtricity System Manager

Modifica le impostazioni per un gruppo di coerenza Snapshot quando desideri cambiarne il nome, le impostazioni di eliminazione automatica o il numero massimo di immagini Snapshot consentite.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Consistency Groups**.
3. Seleziona il gruppo di coerenza Snapshot che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Snapshot Consistency Group Setting.

4. Modificare le impostazioni per il gruppo di coerenza Snapshot come appropriato.

Dettagli del campo

Impostazione	Descrizione
Impostazioni del gruppo di coerenza Snapshot	Nome
È possibile modificare il nome del gruppo di coerenza Snapshot.	Eliminazione automatica
Mantieni selezionata la check box se desideri che le immagini Snapshot vengano eliminate automaticamente dopo il limite specificato; usa la spinner box per modificare il limite. Se deselezioni questa check box, la creazione di immagini Snapshot si interrompe dopo 32 immagini.	Limite delle immagini Snapshot
È possibile modificare il numero massimo di immagini Snapshot consentite per un gruppo di Snapshot.	calendario di Snapshot
Questo campo indica se un calendario di Snapshot è associato al gruppo di coerenza Snapshot.	**Oggetti associati**
Volumi membri	È possibile visualizzare la quantità di volumi membro associati al gruppo di coerenza Snapshot.

5. Fare clic su **Save**.

Eliminare un gruppo di coerenza Snapshot in SANtricity System Manager

È possibile eliminare i gruppi di coerenza Snapshot non più necessari.

Prima di iniziare

Confermare che le immagini di tutti i volumi membri non sono più necessarie per il backup o per scopi di test.

Informazioni su questa attività

Questa operazione elimina tutte le immagini Snapshot o le pianificazioni associate al gruppo di coerenza Snapshot.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Consistency Groups**.
3. Seleziona il gruppo di coerenza Snapshot che desideri eliminare, quindi seleziona **Uncommon Tasks › Delete**.

   Viene visualizzata la finestra di dialogo Conferma eliminazione gruppo di coerenza Snapshot.

4. Conferma che vuoi eseguire questa operazione, quindi fai clic su **Cancella**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutte le immagini Snapshot e i volumi Snapshot esistenti dal gruppo di coerenza Snapshot.
- Elimina tutte le immagini snapshot associate che esistono per ciascun volume membro nel gruppo di coerenza snapshot.
- Elimina tutti i volumi Snapshot associati che esistono per ciascun volume membro nel gruppo di coerenza Snapshot.
- Elimina tutta la capacità riservata associata per ciascun volume membro nella snapshot consistency group (se selezionato).

Gestisci i volumi Snapshot

Converti il volume Snapshot in modalità di lettura/scrittura in SANtricity System Manager

È possibile convertire un volume Snapshot di sola lettura o un volume Snapshot di un gruppo di coerenza Snapshot in modalità di lettura-scrittura, se necessario.

Un volume Snapshot convertito in modalità di lettura e scrittura contiene una propria capacità riservata. Questa capacità viene utilizzata per salvare eventuali modifiche successive apportate dall'applicazione host al volume di base, senza influire sull'immagine Snapshot di riferimento.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.

   Viene visualizzata la tabella Snapshot Volumes, che mostra tutti i volumi snapshot associati all'array di storage.

3. Seleziona il volume Snapshot di sola lettura che desideri convertire, quindi fai clic su **Converti in lettura/scrittura**.

   La finestra di dialogo Convert to Read/Write viene visualizzata con il passaggio **Reserve Capacity** attivato. La tabella Volume Candidate mostra solo i candidati che supportano la reserved capacity specificata.

4. Per allocare la capacità riservata per il volume Snapshot di lettura/scrittura, eseguire una delle seguenti

operazioni:

- **Accetta le impostazioni predefinite** — Utilizza questa opzione consigliata per allocare la capacità riservata per il volume Snapshot con le impostazioni predefinite.
- **Assegna le tue impostazioni di capacità riservata per soddisfare le tue esigenze di archiviazione dati** — Assegna la capacità riservata seguendo le seguenti linee guida.
  - L'impostazione predefinita per la capacità riservata è il 40% della capacità del volume base e di solito questa capacità è sufficiente.
  - La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sul volume.

5. Seleziona **Avanti** per rivedere o modificare le impostazioni.

   Viene visualizzata la finestra di dialogo Edit Settings.

6. Accetta o specifica le impostazioni per il volume Snapshot come appropriato, quindi seleziona **Fine** per convertire il volume Snapshot.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di capacità riservata	Avvisami quando…

Modificare le impostazioni del volume per un volume Snapshot in SANtricity System Manager

È possibile modificare le impostazioni di un volume snapshot o di un volume snapshot di un gruppo di coerenza snapshot per rinominarlo, abilitare o disabilitare la cache SSD oppure modificare l'host, il cluster o l'assegnazione del numero di unità logica (LUN).

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Fai clic sulla scheda **Snapshot Volumes**.
3. Seleziona il volume Snapshot che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni volume Snapshot.

4. Visualizza o modifica le impostazioni per il volume Snapshot come appropriato.

Dettagli del campo

Impostazione	Descrizione
Volume Snapshot	Nome
È possibile modificare il nome per il volume snapshot.	Assegnato a
È possibile modificare l'assegnazione dell'host o del cluster host per il volume Snapshot.	LUN
È possibile modificare l'assegnazione LUN per il volume Snapshot.	Cache SSD
È possibile abilitare/disabilitare la cache di sola lettura sui dischi a stato solido (SSDs).	**Oggetti associati**
Immagine Snapshot	È possibile visualizzare le immagini Snapshot associate al volume Snapshot. Un'immagine Snapshot è una copia logica dei dati del volume, acquisita in un determinato point-in-time. Analogamente a un punto di ripristino, le immagini Snapshot consentono di tornare a un set di dati funzionante. Sebbene l'host possa accedere all'immagine Snapshot, non può leggerla o scriverci direttamente.
Volume base	È possibile visualizzare il volume di base associato al volume Snapshot. Un volume di base è la fonte da cui viene creata un'immagine Snapshot. Può essere un volume thick o con thin provisioning e in genere viene assegnato a un host. Il volume di base può risiedere in un gruppo di volumi o in un disk pool.
Gruppo Snapshot	È possibile visualizzare il gruppo di snapshot associato al volume di snapshot. Un gruppo di snapshot è una raccolta di immagini snapshot provenienti da un singolo volume di base.

Copia un volume Snapshot in SANtricity System Manager

È possibile eseguire un processo Copy Volume su un volume Snapshot o su un volume Snapshot di un gruppo di coerenza Snapshot.

Informazioni su questa attività

È possibile copiare un volume Snapshot sul volume di destinazione come in una normale operazione di Copy Volume. Tuttavia, i volumi Snapshot non possono rimanere online durante il processo di Copy Volume.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.

   Viene visualizzata la tabella Snapshot Volumes, che mostra tutti i volumi snapshot associati all'array di storage.

3. Seleziona il volume Snapshot che desideri copiare, quindi seleziona **Copy Volume**.

   Viene visualizzata la finestra di dialogo Copia volume, che richiede di selezionare un volume di destinazione.

4. Seleziona il volume di destinazione da utilizzare come destinazione della copia, quindi fai clic su **Fine**.

Ricreare un volume snapshot in SANtricity System Manager

È possibile ricreare un volume snapshot o un volume snapshot di un gruppo di coerenza snapshot precedentemente disabilitato. Ricreare un volume snapshot richiede meno tempo rispetto a crearne uno nuovo.

Prima di iniziare

- Il volume snapshot deve trovarsi nello stato Optimal o Disabled.
- Tutti i volumi snapshot membri devono essere nello stato Disabled prima di poter ricreare il volume snapshot del gruppo di coerenza snapshot.

Informazioni su questa attività

Non è possibile ricreare un singolo volume snapshot membro; è possibile ricreare solo il volume snapshot della snapshot del gruppo di coerenza complessivo.

> Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot fa parte di una relazione di copia online, non è possibile eseguire l'opzione di ricreazione sul volume.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.

   Viene visualizzata la tabella Snapshot Volumes, che mostra tutti i volumi snapshot associati all'array di storage.

3. Seleziona il volume Snapshot che desideri ricreare, quindi seleziona **Uncommon Tasks › Recreate**.

   Viene visualizzata la finestra di dialogo Ricrea volume Snapshot.

4. Seleziona una delle seguenti opzioni:
   - **Un'immagine snapshot esistente creata dal volume <name>**

     Selezionare questa opzione per indicare un'immagine Snapshot esistente da cui ricreare il volume Snapshot.

- **Una nuova immagine (istantanea) snapshot del volume <name>**

  Seleziona questa opzione per creare una nuova immagine Snapshot da cui ricreare il volume Snapshot.

5. Fai clic su **Recreate**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutti `write` i dati su qualsiasi volume repository di snapshot associato.
- I parametri del volume Snapshot o del volume snapshot del gruppo di coerenza snapshot rimangono invariati rispetto ai parametri del volume precedentemente disabilitati.
- Mantiene i nomi originali per il volume Snapshot o il volume Snapshot del gruppo di coerenza Snapshot.

Disabilitare un volume Snapshot in SANtricity System Manager

È possibile disabilitare un volume Snapshot o un volume Snapshot in un gruppo di coerenza Snapshot quando non è più necessario o si desidera interromperne temporaneamente l'utilizzo.

Informazioni su questa attività

Utilizzare l'opzione Disabilita se si verifica una delle seguenti condizioni:

- Hai terminato con il volume Snapshot o con il volume Snapshot del gruppo di coerenza Snapshot per il momento.
- Si intende ricreare il volume snapshot o il volume snapshot del gruppo di coerenza snapshot (designato come lettura-scrittura) in un secondo momento e si desidera conservare la capacità riservata associata in modo da non doverla creare di nuovo.
- Si desidera aumentare le prestazioni dell'array di storage interrompendo l'attività di scrittura su un volume Snapshot di lettura/scrittura.

Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot è designato come lettura-scrittura, questa opzione consente anche di interrompere qualsiasi ulteriore attività di scrittura sul volume di capacità riservata associato. Se si decide di ricreare il volume snapshot o il volume snapshot del gruppo di coerenza snapshot, è necessario scegliere un'immagine snapshot dallo stesso volume di base.

> Se il volume snapshot o il volume snapshot del gruppo di coerenza snapshot fa parte di una relazione di copia online, non è possibile eseguire l'opzione Disable sul volume.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.

   System Manager visualizza tutti i volumi Snapshot associati all'array di storage.

3. Seleziona il volume snapshot che desideri disabilitare, quindi seleziona **Uncommon Tasks › Disable**.
4. Conferma che desideri eseguire l'operazione, quindi fai clic su **Disabilita**.

Risultati

- Il volume Snapshot rimane associato al suo volume di base.
- Il volume Snapshot mantiene il suo World Wide Name (WWN).
- Se in lettura-scrittura, il volume snapshot mantiene la capacità riservata associata.
- Il volume snapshot conserva tutte le assegnazioni host e l'accesso. Tuttavia, le richieste di lettura e scrittura non riescono.
- Il volume snapshot perde la sua associazione con la sua immagine snapshot.

Eliminare un volume Snapshot in SANtricity System Manager

È possibile eliminare un volume Snapshot o un volume Snapshot di un gruppo di coerenza Snapshot che non è più necessario per scopi di backup o test delle applicazioni software.

È inoltre possibile specificare se si desidera eliminare il volume di capacità riservata snapshot associato a `read-write` volume snapshot oppure mantenerlo come volume non assegnato.

Informazioni su questa attività

L'eliminazione di un volume di base comporta l'eliminazione automatica di qualsiasi volume Snapshot o volume Snapshot del gruppo di coerenza associato. Non è possibile eliminare un volume Snapshot che si trova in una copia del volume con stato **In Progress**.

Passaggi

1. Selezionare **Storage › Snapshots**.
2. Selezionare la scheda **Snapshot Volumes**.

   System Manager visualizza tutti i volumi Snapshot associati all'array di storage.

3. Seleziona il volume snapshot che desideri eliminare, quindi seleziona **Uncommon Tasks › Delete**.
4. Conferma di voler eseguire l'operazione, quindi fai clic su **Delete**.

Risultati

System Manager esegue le seguenti azioni:

- Elimina tutti i volumi snapshot membri (per un volume snapshot di un gruppo di coerenza snapshot).
- Rimuove tutte le assegnazioni host associate.

Domande frequenti sulle Snapshot per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Perché non vedo tutti i miei volumi, host o cluster di host?

I volumi Snapshot con un volume base abilitato DA non possono essere assegnati a un host che non è Data Assurance (DA) compatibile. È necessario disabilitare DA sul volume base prima che un volume Snapshot possa essere assegnato a un host che non è DA compatibile.

Considera le seguenti linee guida per l'host a cui stai assegnando il volume Snapshot:

- Un host non è compatibile con DA se è connesso al sistema storage tramite un'interfaccia I/O non

compatibile con DA.

- Un cluster host non è compatibile con DA se ha almeno un membro host che non è compatibile con DA.

> Non è possibile disabilitare DA su un volume associato a snapshot (gruppi di coerenza, gruppi di snapshot, immagini snapshot e volumi snapshot), copie di volume e mirror. Tutta la capacità riservata associata e tutti gli oggetti snapshot devono essere eliminati prima di poter disabilitare DA sul volume di base.

Che cos'è un'immagine Snapshot?

Un'immagine Snapshot è una copia logica del contenuto di un volume, acquisita in un determinato momento. Le immagini Snapshot utilizzano uno spazio di storage minimo.

I dati delle immagini Snapshot vengono memorizzati come segue:

- Quando viene creata un'immagine Snapshot, questa corrisponde esattamente al volume di base. Dopo la creazione dello Snapshot, alla prima richiesta di scrittura per un blocco o un insieme di blocchi sul volume di base, i dati originali vengono copiati nella capacità riservata allo Snapshot prima che i nuovi dati vengano scritti sul volume di base.
- Le Snapshot successive includono solo i blocchi di dati che sono stati modificati da quando è stata creata la prima immagine Snapshot. Ogni successiva operazione di copy-on-write salva i dati originali che stanno per essere sovrascritti sul volume di base nella capacità riservata alle Snapshot prima che i nuovi dati vengano scritti sul volume di base.

Perché utilizzare immagini Snapshot?

È possibile utilizzare gli snapshot per proteggere da e consentire il ripristino dopo la perdita o la corruzione accidentale o dolosa dei dati.

Seleziona un volume di base o un gruppo di volumi di base, chiamato snapshot consistency group, e quindi acquisisci immagini Snapshot in uno o più dei seguenti modi:

- È possibile creare un'immagine Snapshot di un singolo volume di base o un gruppo di coerenza Snapshot composto da più volumi di base.
- È possibile acquisire Snapshot manualmente oppure creare una pianificazione per un volume di base o un gruppo di coerenza Snapshot per acquisire automaticamente immagini Snapshot periodiche.
- È possibile creare un volume Snapshot accessibile dall'host di un'immagine Snapshot.
- È possibile eseguire un'operazione di rollback per ripristinare un'immagine Snapshot.

Il sistema conserva più immagini Snapshot come punti di ripristino che puoi utilizzare per tornare a set di dati noti e funzionanti in momenti specifici. La possibilità di tornare indietro offre protezione contro la cancellazione accidentale dei dati e la corruzione dei dati.

Che tipo di volumi possono essere utilizzati per le Snapshot?

Solo i volumi standard e i volumi thin possono essere utilizzati per archiviare le immagini Snapshot. I volumi non standard non possono essere utilizzati. Il volume di base può risiedere su un pool o un gruppo di volumi.

Perché dovrei creare un gruppo di coerenza Snapshot?

Si crea un gruppo di coerenza Snapshot quando si desidera garantire che le immagini Snapshot vengano acquisite contemporaneamente su più volumi.

Ad esempio, un database composto da più volumi che devono rimanere coerenti ai fini del ripristino richiederebbe un gruppo di coerenza Snapshot per raccogliere Snapshot coordinati di tutti i volumi e utilizzarli per ripristinare l'intero database.

I volumi inclusi in un gruppo di coerenza Snapshot sono chiamati *volumi membri*.

È possibile eseguire le seguenti operazioni Snapshot su un gruppo di coerenza Snapshot:

- Crea un'immagine Snapshot di un gruppo di coerenza Snapshot per ottenere immagini simultanee dei volumi membri.
- Crea una pianificazione per il gruppo di coerenza Snapshot per acquisire automaticamente immagini simultanee periodiche dei volumi membri.
- Crea un volume Snapshot accessibile dall'host di un'immagine di un gruppo di coerenza Snapshot.
- Eseguire un'operazione di rollback per un gruppo di coerenza Snapshot.

Che cos'è un volume Snapshot e quando necessita di capacità riservata?

Un volume Snapshot consente all'host di accedere ai dati nell'immagine Snapshot. Il volume Snapshot contiene una propria capacità riservata, che salva eventuali modifiche al volume di base senza influire sull'immagine Snapshot originale. Le immagini Snapshot non sono accessibili in lettura o scrittura dagli host. Se si desidera leggere o scrivere sui dati Snapshot, creare un volume Snapshot e assegnarlo a un host.

È possibile creare due tipi di volumi Snapshot. Il tipo di volume Snapshot determina se utilizza la capacità riservata.

- **Sola lettura** — Un volume Snapshot creato come sola lettura fornisce a un'applicazione host l'accesso in lettura a una copia dei dati contenuti nell'immagine Snapshot. Un volume Snapshot di sola lettura non utilizza capacità riservata.
- **Lettura-scrittura** — Un volume Snapshot creato come lettura-scrittura consente di apportare modifiche al volume Snapshot senza influire sull'immagine Snapshot di riferimento. Un volume Snapshot lettura-scrittura utilizza capacità riservata per memorizzare queste modifiche. È possibile convertire un volume Snapshot di sola lettura in lettura-scrittura in qualsiasi momento.

Che cos'è un gruppo di Snapshot?

Un gruppo di Snapshot è una raccolta di immagini Snapshot point-in-time di un singolo volume di base associato.

System Manager organizza le immagini Snapshot in *gruppi di Snapshot*. I gruppi di Snapshot non richiedono alcuna azione da parte dell'utente, ma è possibile modificare la capacità riservata su un gruppo di Snapshot in qualsiasi momento. Inoltre, potrebbe essere richiesto di creare capacità riservata quando vengono soddisfatte le seguenti condizioni:

- Ogni volta che si crea una Snapshot di un volume di base che non dispone ancora di un gruppo di Snapshot, System Manager crea automaticamente un gruppo di Snapshot. Questo crea capacità riservata per il volume di base, utilizzata per archiviare le immagini Snapshot successive.
- Ogni volta che si crea una pianificazione di snapshot per un volume di base, System Manager crea automaticamente un gruppo di snapshot.

Perché dovrei disabilitare un volume Snapshot?

È possibile disabilitare un volume Snapshot quando si desidera assegnare un volume Snapshot diverso

all'immagine Snapshot. È possibile riservare il volume Snapshot disabilitato per un utilizzo successivo.

Se non hai più bisogno del volume Snapshot o del volume Snapshot del gruppo di coerenza e non intendi ricrearlo in un secondo momento, dovresti eliminare il volume anziché disabilitarlo.

Che cos'è lo stato Disabilitato?

Un volume Snapshot con stato Disabilitato non è attualmente assegnato a un'immagine Snapshot. Per abilitare il volume Snapshot, è necessario utilizzare l'operazione di re-create per assegnare una nuova immagine Snapshot al volume Snapshot disabilitato.

Le caratteristiche del volume Snapshot sono definite dall'immagine Snapshot ad esso assegnata. L'attività di lettura e scrittura viene sospesa su un volume Snapshot in stato Disabled.

Perché dovrei sospendere una pianificazione di Snapshot?

Quando una pianificazione viene sospesa, la creazione delle immagini Snapshot programmate non viene eseguita. È possibile mettere in pausa una pianificazione di Snapshot per risparmiare spazio di storage e quindi riprendere le Snapshot programmate in un secondo momento.

Se non hai bisogno della pianificazione Snapshot, dovresti eliminarla invece di sospenderla.

Mirroring

Panoramica

Scopri il mirroring asincrono nel software SANtricity

La funzionalità di mirroring asincrono fornisce un meccanismo a livello di controller, basato su firmware, per la replica dei dati tra un array di storage locale e un array di storage remoto.

Che cos'è il mirroring asincrono?

La *mirroring asincrona* cattura lo stato del volume primario in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato man mano che la larghezza di banda lo consente. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, non appena le risorse di rete diventano disponibili.

Il mirroring asincrono viene creato per singolo volume, ma gestito a livello di gruppo, consentendo di associare un distinto volume mirrorato remoto a qualsiasi volume primario su un determinato storage array. Questo tipo di mirroring è ideale per soddisfare la domanda di operazioni non-stop e, in generale, è molto più efficiente in termini di rete per i processi periodici.

Per saperne di più:

- "Come funziona il mirroring asincrono"
- "Terminologia relativa al mirroring asincrono"
- "Stato dello specchio asincrono"
- "Proprietà del volume"

- "Cambio di ruolo di un mirror consistency group"

Come si configura il mirroring asincrono?

È necessario utilizzare l'interfaccia di Unified Manager per eseguire la configurazione iniziale del mirroring tra gli array. Una volta configurato, è possibile gestire le coppie mirrorate e i gruppi di coerenza in System Manager.

Per saperne di più:

- "Requisiti per l'utilizzo del mirroring asincrono"
- "Flusso di lavoro per il mirroring asincrono di un volume"
- "Creare una coppia speculare asincrona (in Unified Manager)"

Informazioni correlate

Scopri di più sui concetti relativi al mirroring asincrono:

- "Cosa devi sapere prima di creare un mirror consistency group"
- "Cosa devi sapere prima di creare una coppia mirrorata"
- "In che modo il mirroring asincrono differisce dal mirroring sincrono"

Scopri il mirroring sincrono nel software SANtricity

La funzionalità di mirroring sincrono fornisce replica dei dati in real-time tra array di storage su una distanza remota.

Questa funzionalità non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Che cos'è il mirroring sincrono?

Il mirroring sincrono replica i volumi di dati in real-time per garantire disponibilità continua. I controller degli array di storage gestiscono l'operazione di mirroring, che è trasparente per le macchine host e le applicazioni software.

Questo tipo di mirroring è ideale per scopi di continuità operativa, come il disaster recovery.

Per saperne di più:

- "Come funziona il mirroring sincrono"
- "Terminologia del mirroring sincrono"
- "Stato del mirroring sincrono"
- "Proprietà del volume"
- "Cambio di ruolo tra volumi in una coppia mirrorata"

Come si configura il mirroring sincrono?

È necessario utilizzare l'interfaccia di Unified Manager per eseguire la configurazione iniziale del mirroring tra gli array. Una volta configurato, è possibile gestire le coppie mirrorate in System Manager.

Per saperne di più:

- "Requisiti per l'utilizzo del mirroring sincrono"
- "Flusso di lavoro per il mirroring sincrono di un volume"
- "Creare una coppia sincrona mirrorata (in Unified Manager)"

Informazioni correlate

Scopri di più sui concetti relativi al mirroring sincrono:

- "Cosa devi sapere prima di creare una coppia mirrorata"
- "In che modo il mirroring asincrono differisce dal mirroring sincrono"

Concetti asincroni

Come funziona il mirroring asincrono in SANtricity System Manager

Il mirroring asincrono copia i volumi di dati su richiesta o secondo una pianificazione, riducendo al minimo o evitando i tempi di inattività che potrebbero derivare da danneggiamento o perdita di dati.

La replica asincrona cattura lo stato del volume primario in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato man mano che la larghezza di banda lo consente. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, non appena le risorse di rete diventano disponibili.

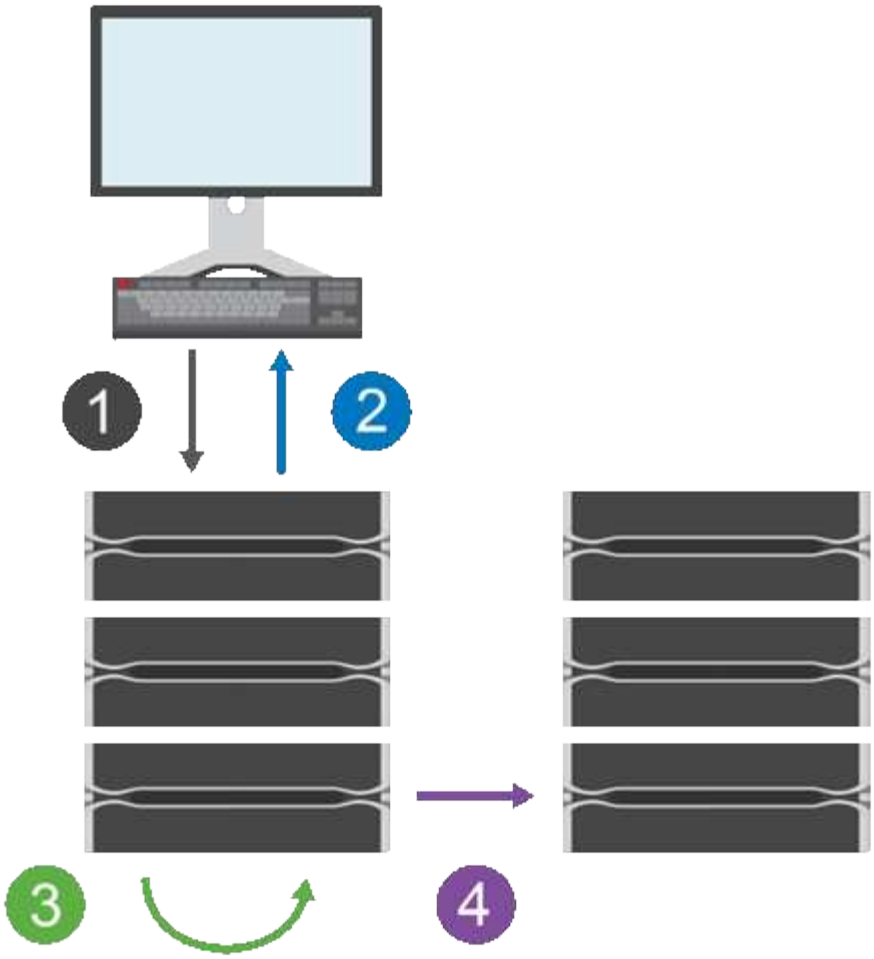
Questo tipo di mirroring è ideale per soddisfare la domanda di operazioni non-stop e, in generale, è molto più efficiente in termini di rete per processi periodici, come copia di backup e archiviazione. I motivi per utilizzare il mirroring asincrono includono i seguenti:

- Consolidamento dei backup remoti.
- Proteggi da disastri locali o su vasta scala.
- Sviluppo e test di applicazioni su un'immagine point-in-time di dati live.

Sessione di mirroring asincrono

Il mirroring asincrono cattura lo stato del volume primario in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine. Il mirroring asincrono consente di aggiornare immediatamente il sito primario e di aggiornare il sito secondario man mano che la larghezza di banda lo consente. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, quando le risorse di rete diventano disponibili.

Ci sono quattro fasi principali in una sessione di mirroring asincrono attiva.



1. Un'operazione di scrittura avviene innanzitutto sull'array di archiviazione del volume primario.
2. Lo stato dell'operazione viene restituito all'host.
3. Tutte le modifiche sul volume primario vengono registrate e tracciate.
4. Tutte le modifiche vengono inviate all'array di archiviazione del volume secondario come processo in background.

Questi passaggi vengono ripetuti secondo gli intervalli di sincronizzazione definiti o i passaggi possono essere ripetuti manualmente se non sono definiti intervalli.

Il mirroring asincrono trasferisce i dati al sito remoto solo a intervalli prestabiliti, quindi l'I/O locale non risente quasi per niente delle connessioni di rete lente. Poiché questo trasferimento non è vincolato all'I/O locale, non influisce sulle prestazioni dell'applicazione. Pertanto, il mirroring asincrono può utilizzare connessioni più lente, come iSCSI, e funzionare su distanze maggiori tra i sistemi di storage locali e remoti.

Gli array di storage devono avere una versione minima del firmware pari a 7.84. (Possono ciascuno eseguire versioni diverse del sistema operativo.)

Gruppi di coerenza mirror e coppie mirror

Si crea un gruppo di coerenza mirror per stabilire la relazione di mirroring tra l'array di storage locale e l'array di storage remoto. La relazione di mirroring asincrono consiste in una coppia mirror: un volume primario su un array di storage e un volume secondario su un altro array di storage.

L'array di storage contenente il volume primario si trova solitamente nel sito primario e serve gli host attivi.

L’array di storage contenente il volume secondario si trova solitamente in un sito secondario e ospita una replica dei dati. Il volume secondario in genere contiene una copia di backup dei dati e viene utilizzato per il ripristino di emergenza.

Impostazioni di sincronizzazione

Quando si crea una coppia speculare, si definiscono anche la priorità di sincronizzazione e la politica di risincronizzazione che la coppia speculare utilizza per completare l’operazione di risincronizzazione dopo un’interruzione della comunicazione.

Quando si crea un gruppo di coerenza mirror, si definiscono anche la priorità di sincronizzazione e la politica di risincronizzazione per tutte le coppie mirror all’interno del gruppo. Le coppie mirror utilizzano la priorità di sincronizzazione e la politica di risincronizzazione per completare l’operazione di risincronizzazione dopo un’interruzione della comunicazione.

In una coppia con mirroring, i volumi primario e secondario possono desincronizzarsi quando l’array di storage del volume primario non è in grado di scrivere dati sul volume secondario. Questa condizione può essere causata dai seguenti problemi:

- Problemi di rete tra gli array di archiviazione locali e remoti.
- Un volume secondario non riuscito.
- La sincronizzazione viene sospesa manualmente sulla coppia mirrorata.
- Conflitto di ruolo del gruppo mirror.

È possibile sincronizzare i dati sull’array di storage remoto manualmente o automaticamente.

Capacità riservata e mirroring asincrono

La capacità riservata viene utilizzata per tenere traccia delle differenze tra il volume primario e il volume secondario quando la sincronizzazione non è in corso. Inoltre, tiene traccia delle statistiche di sincronizzazione per ciascuna coppia di volumi mirrorati.

Ogni volume in una coppia con mirroring richiede la propria capacità riservata.

Configurazione e gestione

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l’interfaccia di Unified Manager. Una volta abilitato il mirroring, è possibile gestire le coppie mirrorate e le impostazioni di sincronizzazione in System Manager.

Scopri la terminologia relativa al mirroring asincrono nel software SANtricity

Scopri come i termini relativi al mirroring asincrono si applicano al tuo array di storage.

Termine	Descrizione
Array di archiviazione locale	L’array di archiviazione locale è l’array di archiviazione su cui si sta operando. Quando nella colonna Ruolo locale viene visualizzato **Primary**, significa che l’array di storage contiene il volume che ricopre il ruolo primario nella relazione di mirroring. Quando nella colonna Ruolo locale viene visualizzato **Secondary**, significa che l’array di storage contiene il volume che ricopre il ruolo secondario nella relazione di mirroring.

Termine	Descrizione
Gruppo di coerenza mirror	Un gruppo di coerenza mirror è un container per una o più coppie mirror. Per le operazioni di mirroring asincrono, è necessario creare un gruppo di coerenza mirror.
Coppia specchiata	Una coppia speculare è composta da due volumi, un volume primario e un volume secondario. Nel mirroring asincrono, una coppia mirrorata appartiene sempre a un mirror consistency group. Le operazioni di scrittura vengono eseguite prima sul volume primario e poi replicate sul volume secondario. Ogni coppia mirrorata in un mirror consistency group condivide le stesse impostazioni di sincronizzazione.
Volume primario	Il volume primario di una coppia speculare è il volume di origine da sottoporre a mirroring.
array di storage remoto	L'array di storage remoto viene solitamente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copia del servizio e oggetto di archiviazione. Non è direttamente leggibile dall'host.
Cambio di ruolo	Il cambio di ruolo consiste nell'assegnare il ruolo primario al volume secondario e viceversa.
Volume secondario	Il volume secondario di una coppia speculare si trova solitamente in una sede secondaria e contiene una replica dei dati.
Sincronizzazione	La sincronizzazione avviene al momento della sincronizzazione iniziale tra l'array di storage locale e l'array di storage remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario si desincronizzano a seguito di un'interruzione della comunicazione. Quando il collegamento di comunicazione viene ripristinato, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Eseguire il mirroring di un volume in modo asincrono nel software SANtricity

Configuri il mirroring asincrono utilizzando il seguente flusso di lavoro.

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare l'array di storage locale come origine per il trasferimento dei dati.
   b. Crea o seleziona un gruppo di coerenza mirror esistente, che è un container per il volume primario sull'array locale e il volume secondario sull'array remoto. I volumi primario e secondario sono indicati come la "coppia mirrorata". Se stai creando il gruppo di coerenza mirror per la prima volta, specifichi se desideri eseguire sincronizzazioni manuali o pianificate.
   c. Seleziona un volume primario dall'array di storage locale, quindi determina la sua capacità riservata. La capacità riservata è la capacità fisica allocata da utilizzare per l'operazione di copia.

d. Selezionare un array di storage remoto come destinazione del trasferimento, un volume secondario e quindi determinarne la capacità riservata.

e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, questo trasferimento iniziale potrebbe richiedere diverse ore.

2. Verifica lo stato di avanzamento della sincronizzazione iniziale:

   a. In Unified Manager, avvia System Manager per l'array locale.

   b. In System Manager, visualizza lo stato dell'operazione di mirroring. Quando il mirroring è completo, lo stato della coppia mirrorata è "Ottimale".

3. **Facoltativo:** È possibile riprogrammare o eseguire manualmente i trasferimenti di dati successivi in System Manager. Solo i nuovi blocchi e i blocchi modificati vengono trasferiti dal volume primario al volume secondario.

> Grazie alla periodicità della replica asincrona, il sistema può consolidare i blocchi modificati e risparmiare larghezza di banda di rete. L'impatto sul throughput di scrittura e sulla latenza di scrittura è minimo.

Requisiti per l'utilizzo del mirroring asincrono nel software SANtricity

Se si intende utilizzare il mirroring asincrono, tenere presenti i seguenti requisiti.

Unified Manager

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Unified Manager viene installato su un sistema host insieme al Web Services Proxy.

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Array di archiviazione

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- I due array di storage devono essere rilevati in Unified Manager.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel o un'interfaccia iSCSI.

Connessioni supportate

Il mirroring asincrono può utilizzare connessioni FC o iSCSI, o entrambe, per la comunicazione tra sistemi storage locali e remoti. Al momento della creazione di un gruppo di coerenza mirror, l'amministratore può selezionare FC o iSCSI per quel gruppo se entrambe sono connesse all'array di storage remoto. Non è previsto alcun failover da un tipo di canale all'altro.

Il mirroring asincrono utilizza le porte I/O lato host dell'array di storage per trasferire i dati mirrorati dal lato primario al lato secondario.

- **Mirroring attraverso un'interfaccia Fibre Channel (FC)**

  Ciascun controller dell'array di storage dedica la sua porta host FC con il numero più alto alle operazioni di mirroring.

  Se il controller dispone sia di porte FC di base che di porte FC sulla scheda di interfaccia verso gli host (HIC), la porta con il numero più alto si trova sulla HIC. Qualsiasi host connesso alla porta dedicata viene disconnesso e non vengono accettate richieste di accesso host. Le richieste di I/O su questa porta sono accettate solo dai controller che partecipano alle operazioni di mirroring.

  Le porte di mirroring dedicate devono essere collegate a un ambiente FC fabric che supporti le interfacce directory service e name service. In particolare, FC-AL e point-to-point non sono supportati come opzioni di connettività tra i controller che partecipano alle relazioni di mirroring.

- **Mirroring tramite un'interfaccia iSCSI**

  A differenza di FC, iSCSI non richiede una porta dedicata. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare nessuna delle porte iSCSI front-end dell'array di storage al mirroring asincrono; tali porte sono condivise sia per il traffico di mirroring asincrono che per le connessioni I/O host-array.

  Il controller mantiene un elenco di sistemi di storage remoti con cui l'iSCSI initiator tenta di stabilire una sessione. La prima porta che riesce a stabilire una connessione iSCSI viene utilizzata per tutte le comunicazioni successive con tale array di storage remoto. Se la comunicazione fallisce, viene tentata una nuova sessione utilizzando tutte le porte disponibili.

  Le porte iSCSI sono configurate a livello di array su base porta per porta. La comunicazione tra controller per la messaggistica di configurazione e il trasferimento dei dati utilizza le impostazioni globali, incluse le impostazioni per:

  - VLAN: Sia il sistema locale che quello remoto devono avere la stessa impostazione VLAN per comunicare
  - porta di ascolto iSCSI
  - Frame jumbo
  - Priorità Ethernet

  > La comunicazione iSCSI tra i controller deve utilizzare una porta di connessione host e non la porta Ethernet di gestione.

  Il mirroring asincrono utilizza le porte I/O lato host dell'array di storage per trasferire dati mirrorati dal lato primario al lato secondario. Poiché il mirroring asincrono è pensato per reti a latenza più elevata e a basso costo, le connessioni iSCSI (e quindi basate su TCP/IP) sono particolarmente adatte. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare alcuna porta iSCSI front-end dell'array al mirroring asincrono; tali porte sono condivise sia per il traffico di mirroring asincrono che per le connessioni

I/O host-array.

E4000 non supporta il mirroring asincrono quando si utilizza il protocollo iSCSI.

Candidati al volume mirrorato

- Il livello RAID, i parametri di caching e la dimensione dei segmenti possono essere diversi sui volumi primario e secondario di una coppia con mirroring asincrono.

  Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona in mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie asincrone in mirroring non ammissibili non appariranno nell'elenco dei volumi disponibili.

- Il volume secondario deve essere almeno grande quanto il volume primario.
- Un volume può partecipare a una sola relazione mirror.
- I candidati volume devono condividere le stesse funzionalità di Data Security.
  - Se il volume primario è FIPS capable, il volume secondario deve essere FIPS capable.
  - Se il volume primario è FDE capable, anche il volume secondario deve essere FDE capable.
  - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.
- I volumi primari e secondari devono condividere lo stesso tipo di unità. La combinazione di unità NVMe e SAS tra volumi primari e secondari non è supportata.
- I volumi primari e secondari non devono avere la partizione delle risorse abilitata.

Capacità riservata

- È necessario un volume di capacità riservato sia per il volume primario che per il volume secondario in una coppia mirrorata per registrare le informazioni di scrittura e recuperare dai reset del controller e altre interruzioni temporanee.
- Poiché sia il volume primario che il volume secondario in una coppia mirrorata richiedono capacità riservata aggiuntiva, è necessario assicurarsi di disporre di capacità libera su entrambi gli array di storage nella relazione di mirror.
- Il volume di capacità riservata deve condividere lo stesso tipo di drive dei volumi mirror associati.
  - Se il volume di capacità riservata viene creato su unità NVMe, anche i suoi volumi mirrorati devono essere creati su unità NVMe.
  - Se il volume di capacità riservata viene creato su unità SAS, anche i suoi volumi mirrorati devono essere creati su unità SAS.

Funzione di sicurezza dell'unità

- Se si utilizzano unità con funzionalità di sicurezza, il volume primario e il volume secondario devono avere impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla autonomamente.
- Se si utilizzano unità compatibili con Secure, il volume primario e il volume secondario devono utilizzare lo stesso tipo di unità. Questa restrizione non è applicata; pertanto, è necessario verificarla autonomamente.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse

impostazioni DA.

Visualizza lo stato del mirror asincrono in SANtricity System Manager

Lo stato dello specchio definisce lo stato dei gruppi di coerenza dello specchio e delle coppie di volumi mirrorati.

Stato dei gruppi di coerenza mirror

Stato	Descrizione
Sincronizzazione (initial sync)	Lo stato di avanzamento della sincronizzazione iniziale dei dati completata tra le coppie di volume mirrorato. Durante una sincronizzazione iniziale, i volumi possono passare ai seguenti stati: Degradato/Non riuscito/Ottimale/Sconosciuto.
Sincronizzazione (sincronizzazione a intervalli)	Lo stato di avanzamento della sincronizzazione periodica dei dati completata tra le coppie di volume mirrorato.
Sistema sospeso	Sincronizzazione dei dati sospesa dal sistema storage su tutte le coppie mirrorate a livello del gruppo di coerenza mirror. Almeno una coppia mirrorata nel mirror consistency group si trova in uno stato Arrestato o Fallito.
Utente sospeso	Sincronizzazione dei dati sospesa dall'utente su tutte le coppie mirrorate a livello del gruppo di coerenza del mirror. Questo stato contribuisce a ridurre qualsiasi impatto sulle prestazioni dell'applicazione host che potrebbe verificarsi mentre tutti i dati modificati sull'array di storage locale vengono copiati sull'array di storage remoto.
In pausa	Il processo di sincronizzazione dei dati è stato temporaneamente sospeso a causa di un errore nell'accesso all'array di storage remoto.
Orfano	Un volume di coppia mirrorata orfano esiste quando un volume membro in un gruppo di mirror di coerenza è stato rimosso da un lato del gruppo di mirror di coerenza (sia dal lato primario che dal lato secondario), ma non dall'altro lato. I volumi di coppie mirrorate orfane vengono rilevati quando la comunicazione tra gli array viene ripristinata e i due lati della configurazione mirrorata riconciliano i parametri del mirror. È possibile rimuovere una coppia mirrorata per correggere lo stato di una coppia mirrorata orfana.

Stato	Descrizione
Cambio di ruolo in sospeso/in corso	Un cambio di ruolo tra i mirror consistency groups è in sospeso o in corso. Il cambio di ruolo (a ruolo primario o secondario) influisce su tutte le coppie mirrorate asincrone all'interno del gruppo di coerenza mirror selezionato. È possibile annullare una modifica di ruolo in sospeso, ma non una modifica di ruolo in corso.
Conflitto di ruolo	Si è verificato un conflitto di ruoli tra i gruppi di coerenza mirror a causa di un problema di comunicazione tra l'array di storage locale e l'array di storage remoto durante un'operazione di cambio di ruolo. Quando il problema di comunicazione è stato risolto, si verifica un Role Conflict. Utilizzare il Recovery Guru per recuperare da questo errore. Non è consentita una promozione forzata quando si risolve un conflitto di ruoli.

Stato delle coppie mirrorate

Lo stato di una coppia mirrorata indica se i dati sul volume primario e sul volume secondario sono sincronizzati.

Stato	Descrizione
Sincronizzazione	L'avanzamento della sincronizzazione iniziale o periodica dei dati che è stata completata tra le coppie speculari. Esistono due tipi di sincronizzazione: sincronizzazione iniziale e sincronizzazione periodica. L'avanzamento della sincronizzazione iniziale viene visualizzato anche nella finestra di dialogo Long Running Operations.
Ottimale	I volumi nella coppia speculare sono sincronizzati, il che indica che la connessione tra gli array di storage è operativa e ciascun volume si trova nelle condizioni di lavoro desiderate.
Incompleto	La coppia di mirroring asincrono è incompleta sull'array di storage remoto perché la sequenza di creazione della coppia di mirroring è stata avviata su un array di storage non supportato da System Manager e la coppia di mirroring non è stata completata sul volume secondario. Il processo di creazione della coppia con mirroring si completa quando un volume viene aggiunto al gruppo di coerenza mirror sull'array di storage remoto. Questo volume diventa il volume secondario nella coppia con mirroring asincrono. La coppia mirrorata viene completata automaticamente se l'array di storage remoto è gestito da System Manager.

Stato	Descrizione
Fallito	L'operazione di mirroring asincrono non può funzionare normalmente a causa di un errore con i volumi primari, i volumi secondari o la capacità riservata al mirroring.
Orfano	Un volume di coppia mirrorata orfano esiste quando un volume membro in un gruppo di mirror di coerenza è stato rimosso da un lato del gruppo di mirror di coerenza (sia dal lato primario che dal lato secondario), ma non dall'altro lato. I volumi di coppie mirror orfane vengono rilevati quando viene ripristinata la comunicazione tra i due array di storage e i due lati della configurazione mirror riconciliano i parametri del mirror. È possibile rimuovere una coppia mirrorata per correggere lo stato di una coppia mirrorata orfana.
Arrestato	La coppia speculare si trova nello stato Arrestato perché il gruppo di coerenza del mirror si trova nello stato di sospensione del sistema.

Scopri la proprietà dei volumi nel mirroring asincrono nel software SANtricity

È possibile modificare il proprietario del controller preferito in una coppia mirrorata.

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

Ad esempio, un volume primario è di proprietà del controller A, e poi si cambia il proprietario del controller assegnandolo al controller B. In questo caso, la successiva scrittura remota cambia il proprietario del controller del volume secondario da controller A a B. Poiché le modifiche di proprietà del controller sul lato secondario sono controllate dal lato primario, non richiedono alcun intervento particolare da parte dell'amministratore del sistema storage.

Reset del controller

Il ripristino di un controller provoca un cambio di proprietà del volume sul lato primario, dal proprietario del controller preferito al controller alternativo nel sistema storage.

A volte, una scrittura remota viene interrotta dal ripristino del controller o da un ciclo di accensione/spegnimento dell'array di storage prima che possa essere scritta sul volume secondario. Il controller non ha bisogno di eseguire una sincronizzazione completa della coppia con mirroring in questo caso.

Quando una scrittura remota viene interrotta durante un ripristino del controller, il nuovo proprietario del controller sul lato primario legge le informazioni memorizzate in un file di log nel volume di capacità riservata del proprietario del controller preferito. Il nuovo proprietario del controller copia quindi i blocchi di dati interessati dal volume primario al volume secondario, eliminando la necessità di una sincronizzazione completa dei volumi mirrorati.

Modificare i ruoli del gruppo di coerenza mirror nel software SANtricity

È possibile modificare il ruolo tra coppie mirrorate in un mirror consistency group. È possibile farlo declassando il mirror consistency group primario al ruolo secondario oppure promuovendo il mirror consistency group secondario al ruolo primario.

Esamina le seguenti informazioni relative all'operazione di cambio di ruolo:

- Il cambio di ruolo interessa tutte le coppie mirrorate all'interno del gruppo di coerenza mirror selezionato.
- Quando un mirror consistency group viene declassato al ruolo secondario, tutte le mirrored pairs all'interno di quel mirror consistency group vengono anch'esse declassate al ruolo secondario e viceversa.
- Quando il gruppo di coerenza mirror primario viene declassato al ruolo secondario, gli host a cui sono stati assegnati i volumi membri all'interno di tale gruppo non hanno più accesso in scrittura a tali volumi.
- Quando un gruppo di coerenza mirror viene promosso al ruolo primario, qualsiasi host che accede ai volumi membri all'interno di tale gruppo è ora in grado di scrivervi.
- Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, puoi forzare il cambio di ruolo sull'array di storage locale.

Forza cambio di ruolo

È possibile forzare un cambio di ruolo tra mirror consistency groups quando un problema di comunicazione tra l'array di storage locale e l'array di storage remoto impedisce la promozione dei volumi membri all'interno del secondary mirror consistency group o la retrocessione dei volumi membri all'interno del primary mirror consistency group.

È possibile forzare il gruppo di coerenza mirror sul lato secondario a passare al ruolo primario. Quindi l'host di ripristino può accedere ai volumi membri appena promossi all'interno di quel gruppo di coerenza mirror e le operazioni di business possono continuare.

Quando è consentita una promozione forzata e quando non è consentita?

La promozione forzata di un mirror consistency group è consentita solo se tutti i volumi membri del mirror consistency group sono stati sincronizzati e dispongono di punti di ripristino coerenti.

La promozione forzata di un gruppo di coerenza mirror non è consentita alle seguenti condizioni:

- Uno qualsiasi dei volumi membri di un mirror consistency group è in fase di sincronizzazione iniziale.
- Nessuno dei volumi membri di un gruppo di coerenza mirror possiede un'immagine point-in-time del punto di ripristino (ad esempio, a causa di un errore di capacità riservata piena).
- Il gruppo di coerenza mirror non contiene volumi membro.
- Il gruppo di coerenza mirror si trova negli stati Non riuscito, Cambio ruolo in sospeso o Cambio ruolo in corso, oppure se uno qualsiasi dei volumi membro associati o dei volumi di capacità riservata è non riuscito.

Conflitto di ruolo nel gruppo mirror

Quando viene risolto un problema di comunicazione tra gli array di storage locali e remoti, si verifica una condizione di Mirror Group Role Conflict. Utilizzare il Recovery Guru per ripristinare da questo errore. Non è consentita una promozione forzata durante la risoluzione di un conflitto di doppio ruolo.

Per evitare la condizione di Mirror Group Role Conflict e le conseguenti procedure di ripristino, attendere che la

connessione tra gli array di storage sia operativa prima di forzare il cambio di ruolo.

Stato di avanzamento del cambio di ruolo

Se due array di storage in una configurazione di mirroring si disconnettono, e il lato primario di un mirror consistency group viene forzatamente declassato a ruolo secondario, e il lato secondario di un mirror consistency group viene forzatamente promosso a ruolo primario, allora, al ripristino della comunicazione, i mirror consistency group su entrambi gli array di storage vengono posti nello stato Role-Change-In-Progress.

Il sistema completerà il processo di cambio ruolo trasferendo i registri delle modifiche, risincronizzando, impostando lo stato del gruppo di coerenza mirror a uno stato operativo normale e continuando con sincronizzazioni periodiche.

Concetti di sincronizzazione

Come funziona il mirroring sincrono in SANtricity System Manager

Il mirroring sincrono replica i volumi di dati in tempo reale per garantire disponibilità continua.

> La funzione di mirroring sincrono non è disponibile sull'array di storage EF600/EF600C o EF300/EF300C.

Il mirroring sincrono raggiunge un recovery point objective (RPO) di zero dati persi avendo una copia dei dati importanti disponibile se si verifica un disastro su uno dei due storage array. La copia è identica ai dati di produzione in ogni momento perché ogni volta che viene eseguita una scrittura sul volume primario, viene eseguita una scrittura anche sul volume secondario. L'host non riceve una conferma che la scrittura è stata eseguita con successo finché il volume secondario non viene aggiornato correttamente con le modifiche apportate al volume primario.

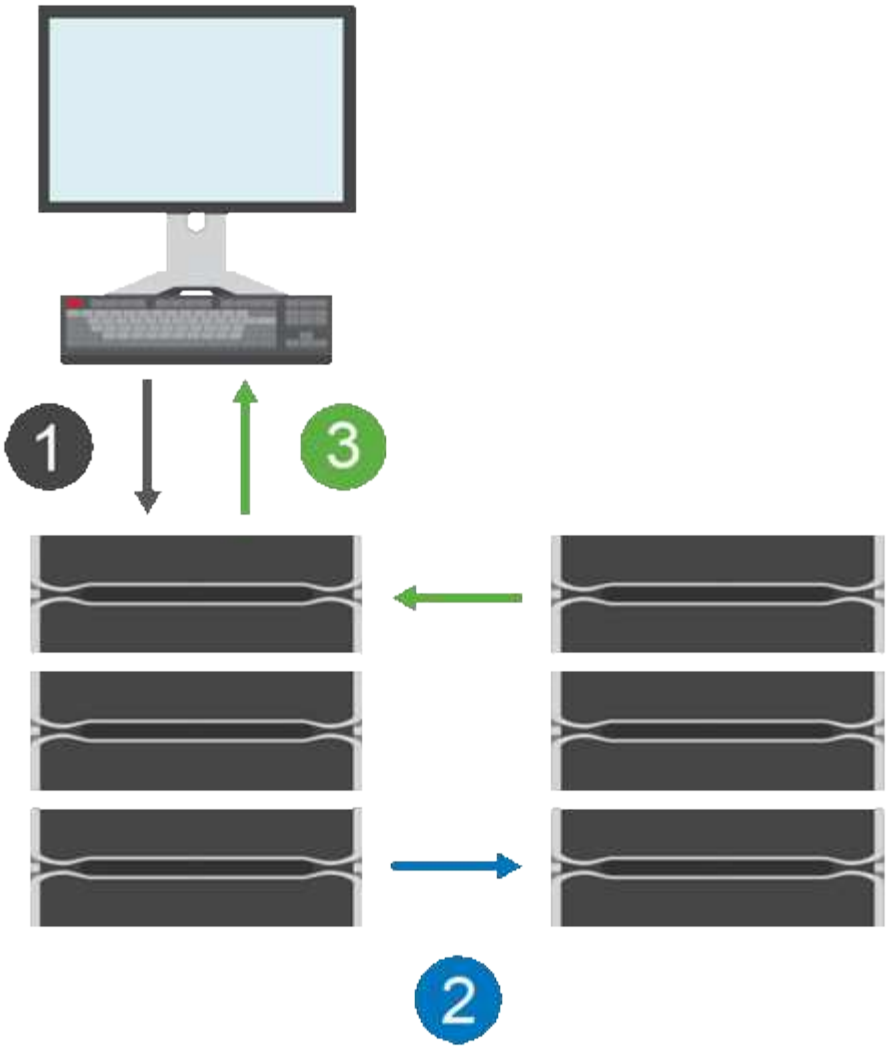
Questo tipo di mirroring è ideale per scopi di continuità operativa, come il disaster recovery.

Relazione di mirroring sincrono

Una relazione di mirroring sincrono consiste in un volume primario e un volume secondario su array di storage separati. L'array di storage contenente il volume primario si trova solitamente presso il sito primario e serve gli host attivi. L'array di storage contenente il volume secondario si trova solitamente presso un sito secondario e contiene una replica dei dati. Il volume secondario viene utilizzato se l'array di storage del volume primario non è disponibile a causa, ad esempio, di un'interruzione completa di corrente, di un incendio o di un guasto hardware presso il sito primario.

Sessione di mirroring sincrono

Il processo di configurazione del mirroring sincrono prevede la configurazione di volumi in coppie. Dopo aver creato una coppia con mirroring, composta da un volume primario su un array di storage e un volume secondario su un altro array di storage, è possibile avviare il mirroring sincrono. I passaggi del mirroring sincrono sono illustrati di seguito.



1. Arriva una scrittura dall'host.
2. L'operazione di scrittura viene confermata sul volume primario, propagata al sistema remoto e quindi confermata sul volume secondario.
3. L'array di storage del volume primario invia un messaggio di completamento I/O al sistema host *dopo* che entrambe le operazioni di scrittura sono state completate con successo.

La capacità riservata viene utilizzata per registrare informazioni sulla richiesta di scrittura in arrivo da un host.

Quando il controller proprietario corrente del volume primario riceve una richiesta di scrittura da un host, il controller registra prima le informazioni sulla scrittura nella capacità riservata del volume primario. Poi scrive i dati sul volume primario. Successivamente, il controller avvia un'operazione di scrittura remota per copiare i blocchi di dati interessati sul volume secondario nell'array di storage remoto.

Poiché l'applicazione host deve attendere che la scrittura avvenga sull'array di storage locale e attraverso la rete sull'array di storage remoto, è necessaria una connessione molto veloce tra l'array di storage locale e l'array di storage remoto per mantenere la relazione di mirroring senza ridurre eccessivamente le prestazioni di I/O locali.

Disaster recovery

Il mirroring sincrono mantiene una copia dei dati che è fisicamente distante dal sito in cui risiedono i dati. Se si verifica un disastro presso il sito primario, come un'interruzione di corrente o un'alluvione, i dati possono

essere rapidamente accessibili dal sito secondario.

Il volume secondario non è disponibile per le applicazioni host mentre l'operazione di mirroring sincrono è in corso, quindi, in caso di disastro nell'array di storage locale, è possibile eseguire il failover sull'array di storage remoto. Per eseguire il failover, promuovere il volume secondario al ruolo primario. Quindi l'host di ripristino può accedere al volume appena promosso e le operazioni di business possono continuare.

Impostazioni di sincronizzazione

Quando si crea una coppia speculare, si definiscono anche la priorità di sincronizzazione e la politica di risincronizzazione che la coppia speculare utilizza per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

Se il collegamento di comunicazione tra i due array di storage smette di funzionare, gli host continuano a ricevere conferme dall'array di storage locale, evitando una perdita di accesso. Quando il collegamento di comunicazione torna a funzionare, eventuali dati non replicati possono essere risincronizzati automaticamente o manualmente con l'array di storage remoto.

Se la risincronizzazione dei dati avviene automaticamente dipende dalla policy di risincronizzazione della coppia mirror. Una policy di risincronizzazione automatica consente alla coppia mirror di risincronizzarsi automaticamente quando il collegamento torna a funzionare. Una policy di risincronizzazione manuale richiede di riprendere manualmente la sincronizzazione dopo un problema di comunicazione. La risincronizzazione manuale è la policy consigliata.

È possibile modificare le impostazioni di sincronizzazione per una coppia con mirroring solo sull'array di storage che contiene il volume primario.

Dati non sincronizzati

I volumi primario e secondario si desincronizzano quando l'array di storage del volume primario non è in grado di scrivere dati sul volume secondario. Ciò può essere causato dai seguenti problemi:

- Problemi di rete tra gli array di storage locali e remoti
- Un volume secondario non riuscito
- Sincronizzazione sospesa manualmente sulla coppia mirrorata

Coppia speculare orfana

Un volume di coppia speculare orfano esiste quando un volume membro è stato rimosso da un lato (sia dal lato primario che dal lato secondario) ma non dall'altro lato.

I volumi di coppie mirrorate orfane vengono rilevati quando la comunicazione tra gli array viene ripristinata e i due lati della configurazione mirrorata riconciliano i parametri del mirror.

È possibile rimuovere una coppia mirrorata per correggere lo stato di una coppia mirrorata orfana.

Configurazione e gestione

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Una volta abilitato il mirroring, è possibile gestire le coppie mirrorate e le impostazioni di sincronizzazione in System Manager.

Scopri la terminologia del mirroring sincrono nel software SANtricity

Scopri come i termini del mirroring sincrono si applicano al tuo array di storage.

Termine	Descrizione
Array di archiviazione locale	L'array di archiviazione locale è l'array di archiviazione su cui si sta operando. Quando nella colonna Ruolo locale viene visualizzato **Primary**, significa che l'array di storage contiene il volume che ricopre il ruolo primario nella relazione di mirroring. Quando nella colonna Ruolo locale viene visualizzato **Secondary**, significa che l'array di storage contiene il volume che ricopre il ruolo secondario nella relazione di mirroring.
Coppia specchiata	Una coppia speculare è composta da due volumi, un volume primario e un volume secondario.
Volume primario	Il volume primario di una coppia speculare è il volume di origine da sottoporre a mirroring.
Obiettivo del punto di recupero (RPO)	Recovery Point Objective (RPO) rappresenta un obiettivo che indica la differenza considerata accettabile tra il volume primario e il volume secondario in una coppia mirrorata. Un RPO pari a zero indica che non può essere tollerata alcuna differenza tra il volume primario e il volume secondario. Un RPO maggiore di zero indica che il volume secondario è meno aggiornato o in ritardo rispetto al volume primario.
array di storage remoto	L'array di storage remoto viene solitamente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copia del servizio e oggetto di archiviazione. Non è direttamente leggibile dall'host.
Cambio di ruolo	Il cambio di ruolo consiste nell'assegnare il ruolo primario al volume secondario e viceversa.
Volume secondario	Il volume secondario di una coppia speculare si trova solitamente in una sede secondaria e contiene una replica dei dati.
Sincronizzazione	La sincronizzazione avviene al momento della sincronizzazione iniziale tra l'array di storage locale e l'array di storage remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario si desincronizzano a seguito di un'interruzione della comunicazione. Quando il collegamento di comunicazione viene ripristinato, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Eseguire il mirroring sincrono di un volume nel software SANtricity

Configuri il mirroring sincrono utilizzando il seguente flusso di lavoro.

Questa funzionalità non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Seleziona un array di storage locale come origine per il trasferimento dei dati.
   b. Selezionare un volume primario dall'array di storage locale.
   c. Selezionare un array storage remoto come destinazione per il trasferimento dei dati, quindi selezionare un volume secondario.
   d. Seleziona le priorità di sincronizzazione e risincronizzazione.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, questo trasferimento iniziale potrebbe richiedere diverse ore.
2. Verifica lo stato di avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avvia System Manager per l'array locale.
   b. In System Manager, visualizza lo stato dell'operazione di mirroring. Quando il mirroring è completo, lo stato della coppia mirrorata è "Ottimale". I due array tentano di rimanere sincronizzati durante le normali operazioni. Solo i nuovi blocchi e i blocchi modificati vengono trasferiti dal volume primario al volume secondario.
3. **Facoltativo:** È possibile modificare le impostazioni di sincronizzazione in System Manager.

Poiché la replica sincrona è continua, il collegamento di replica tra i due siti deve fornire una larghezza di banda sufficiente.

Requisiti per l'utilizzo del mirroring sincrono nel software SANtricity

Se si intende utilizzare il mirroring sincrono, è necessario tenere presenti i seguenti requisiti.

Unified Manager

Per abilitare e configurare il mirroring tra due array, è necessario utilizzare l'interfaccia di Unified Manager. Unified Manager viene installato su un sistema host insieme al Web Services Proxy.

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Array di archiviazione

Il mirroring sincrono non è disponibile sugli array di storage EF300/EF300C o EF600/EF600C.

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- I due array di storage devono essere rilevati in Unified Manager.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione

Ethernet configurata e deve essere connesso alla rete.

- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel.

Connessioni supportate

La comunicazione per il mirroring sincrono è supportata solo sui controller con porte host Fibre Channel (FC).

Il mirroring sincrono utilizza la porta host con il numero più alto su ciascun controller sia sull'array di storage locale che su quello remoto. La porta host 4 dell'adattatore bus host (HBA) del controller è in genere riservata alla trasmissione dei dati mirrorati.

Candidati al volume mirrorato

- Il livello RAID, i parametri di caching e la dimensione dei segmenti possono essere diversi sui volumi primario e secondario di una coppia di volumi con mirroring sincrono.
- I volumi primario e secondario in una coppia con mirroring sincrono devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Il volume secondario deve essere almeno grande quanto il volume primario.
- Solo il volume primario può avere snapshot associati e/o essere il volume di origine o di destinazione in un'operazione di copia del volume.
- Un volume può partecipare a una sola relazione mirror.
- Esistono dei limiti al numero di volumi supportati su un determinato array di storage. Assicurati che il numero di volumi configurati sul tuo array di storage sia inferiore al limite supportato. Quando il mirroring sincrono è attivo, i due volumi di capacità riservata che vengono creati vengono conteggiati nel limite dei volumi.

Capacità riservata

- La capacità riservata è necessaria per un volume primario e per un volume secondario per registrare le informazioni di scrittura e recuperare dai reset del controller e altre interruzioni temporanee.
- I volumi con capacità riservata vengono creati automaticamente quando il mirroring sincrono è attivato. Poiché sia il volume primario che il volume secondario in una coppia con mirroring richiedono capacità riservata, è necessario assicurarsi di disporre di capacità libera sufficiente su entrambi gli array di storage che partecipano alla relazione di mirroring sincrono.

Funzione di sicurezza dell'unità

- Se si utilizzano unità con funzionalità di sicurezza, il volume primario e il volume secondario devono avere impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla autonomamente.
- Se si utilizzano unità compatibili con Secure, il volume primario e il volume secondario devono utilizzare lo stesso tipo di unità. Questa restrizione non è applicata; pertanto, è necessario verificarla autonomamente.
  - Se il volume primario utilizza unità FDE (Full Disk Encryption), il volume secondario dovrebbe utilizzare unità FDE.

    - Se il volume primario utilizza unità convalidate secondo il Federal Information Processing Standards 140-2 (FIPS), il volume secondario dovrebbe utilizzare unità convalidate secondo il FIPS 140-2.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse impostazioni DA.

Scopri lo stato del mirroring sincrono in SANtricity System Manager

Lo stato di una coppia mirrorata sincrona indica se i dati sul volume primario e sul volume secondario sono sincronizzati. Lo stato del mirror è indipendente dallo stato dei componenti dei volumi nella coppia mirrorata.

Questa funzionalità non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Le coppie mirrorate sincrone possono avere uno dei seguenti stati:

- **Ottimale**

  Indica che i volumi nella coppia mirrorata sono sincronizzati, il che significa che la connessione fabric tra gli array di storage è operativa e ciascun volume si trova nelle condizioni di lavoro desiderate.

- **Sincronizzazione**

  Mostra l'avanzamento della sincronizzazione dei dati tra le coppie mirrorate. Questo stato verrà visualizzato anche durante la sincronizzazione iniziale.

  Dopo un'interruzione del collegamento di comunicazione, solo i blocchi modificati sul volume primario durante l'interruzione del collegamento vengono copiati sul volume secondario.

- **Non sincronizzato**

  Indica che l'array di storage del volume primario non è in grado di scrivere i dati in ingresso sull'array remoto. L'host locale può continuare a scrivere sul volume primario, ma le scritture remote non vengono eseguite. Diverse condizioni possono impedire all'array di storage del volume primario di scrivere i dati in ingresso sul volume secondario, ad esempio:

    - Il volume secondario non è accessibile.
    - L'array di storage remoto non è accessibile.
    - La connessione fabric tra gli array di storage non è accessibile.
    - Il volume secondario non può essere aggiornato con un nuovo World Wide Identifier (WWID).
- **Sospeso**

  Indica che l'operazione di mirroring sincrono è stata sospesa dall'utente. Quando una coppia mirrorata viene sospesa, non viene effettuato alcun tentativo di contattare il volume secondario. Tutte le scritture sul volume primario vengono registrate in modo permanente nei volumi di capacità riservata del mirror.

- **Non riuscito**

  Indica che l'operazione di mirroring sincrono non è in grado di funzionare normalmente a causa di un guasto al volume primario, al volume secondario o alla capacità riservata del mirror.

Scopri la proprietà dei volumi nel mirroring sincrono nel software SANtricity

È possibile modificare il proprietario del controller preferito in una coppia mirrorata.

> Questa funzione non è disponibile per il mirroring sincrono sui sistemi storage EF600/EF600C o EF300/EF300C.

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

Ad esempio, un volume primario è di proprietà del controller A, e poi si cambia il proprietario del controller assegnandolo al controller B. In questo caso, la successiva scrittura remota cambia il proprietario del controller del volume secondario da controller A a B. Poiché le modifiche di proprietà del controller sul lato secondario sono controllate dal lato primario, non richiedono alcun intervento particolare da parte dell'amministratore del sistema storage.

Reset del controller

Il ripristino di un controller provoca un cambio di proprietà del volume sul lato primario, dal proprietario del controller preferito al controller alternativo nel sistema storage.

A volte, una scrittura remota viene interrotta dal ripristino del controller o da un ciclo di accensione/spegnimento dell'array di storage prima che possa essere scritta sul volume secondario. Il controller non ha bisogno di eseguire una sincronizzazione completa della coppia con mirroring in questo caso.

Quando una scrittura remota viene interrotta durante un ripristino del controller, il nuovo proprietario del controller sul lato primario legge le informazioni memorizzate in un file di log nel volume di capacità riservata del proprietario del controller preferito. Il nuovo proprietario del controller copia quindi i blocchi di dati interessati dal volume primario al volume secondario, eliminando la necessità di una sincronizzazione completa dei volumi mirrorati.

Scopri le modifiche al ruolo del volume in una coppia mirrorata nel software SANtricity

È possibile modificare il ruolo tra i volumi in una coppia mirrorata. È possibile farlo declassando il volume primario al ruolo secondario o promuovendo il volume secondario al ruolo primario.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Esamina le seguenti informazioni relative all'operazione di cambio di ruolo:

- Quando un volume primario viene declassato al ruolo secondario, il volume secondario in quella coppia mirrorata viene promosso al ruolo primario e viceversa.
- Quando il volume primario viene declassato al ruolo secondario, gli host a cui era assegnato tale volume non hanno più accesso in scrittura a esso.
- Quando il volume secondario viene promosso al ruolo primario, tutti gli host che accedono a tale volume sono ora in grado di scrivere su di esso.

- Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, puoi forzare il cambio di ruolo sull'array di storage locale.

Forza cambio di ruolo

È possibile forzare un cambio di ruolo tra volumi in una coppia con mirroring quando un problema di comunicazione tra l'array di storage locale e l'array di storage remoto impedisce la promozione del volume secondario o la retrocessione del volume primario.

È possibile forzare il volume sul lato secondario a passare al ruolo primario. Successivamente, l'host di ripristino può accedere al volume appena promosso e le operazioni di business possono continuare.

> Quando l'array di storage remoto è stato ripristinato e tutti i problemi di comunicazione sono stati risolti, si verifica una condizione di conflitto Synchronous Mirroring - Primary Volume. I passaggi di ripristino includono la risincronizzazione dei volumi. Utilizzare il Recovery Guru per recuperare da questo errore.

Quando è consentita una promozione forzata e quando non è consentita?

La promozione forzata di un volume in una coppia mirrorata non è consentita alle seguenti condizioni:

- Uno qualsiasi dei volumi in una coppia mirrorata è in fase di sincronizzazione iniziale.
- La coppia mirrorata si trova negli stati Non riuscito, Cambio ruolo in sospeso o Cambio ruolo in corso, oppure se uno qualsiasi dei volumi di capacità riservata associati è non riuscito.

Stato di avanzamento del cambio di ruolo

Se due array di storage in una configurazione di mirroring si disconnettono, e il volume primario di una coppia di volumi mirrorati viene forzatamente declassato a ruolo secondario, e il volume secondario di una coppia di volumi mirrorati viene forzatamente promosso a ruolo primario, allora, quando la comunicazione viene ripristinata, i volumi su entrambi gli array di storage vengono posti nello stato Role-Change-In-Progress.

Il sistema completerà il processo di cambio ruolo trasferendo i registri delle modifiche, risincronizzando, riportando lo stato della coppia mirrorata a uno stato operativo normale e proseguendo con le sincronizzazioni.

Gestisci i gruppi di coerenza mirror asincroni

Test della comunicazione per i gruppi di coerenza mirror in SANtricity System Manager

È possibile testare il collegamento di comunicazione per diagnosticare eventuali problemi di comunicazione tra il sistema storage locale e il sistema storage remoto associato a un gruppo di coerenza mirror.

Prima di iniziare

Il gruppo di coerenza mirror che si desidera testare deve esistere sugli array di storage locali e remoti.

Informazioni su questa attività

È possibile eseguire quattro test diversi:

- **Connettività** — Verifica che i due controller abbiano un percorso di comunicazione. Il test di connettività invia un messaggio inter-array tra i sistemi storage e quindi verifica che il corrispondente mirror consistency group sul sistema storage remoto esista. Verifica inoltre che i volumi membri del mirror consistency group sul sistema storage remoto corrispondano ai volumi membri del mirror consistency

group sul sistema storage locale.

- **Latenza** — Invia un comando SCSI Test Unit a ciascun volume mirrorato sull'array di storage remoto associato al gruppo di coerenza mirror per testare la latenza minima, media e massima.
- **Larghezza di banda** — Invia due messaggi inter-array all'array di storage remoto per testare la larghezza di banda minima, media e massima, nonché la velocità di collegamento negoziata della porta sull'array che esegue il test.
- **Connessioni delle porte** — Mostra la porta utilizzata per il mirroring sul sistema storage locale e la porta che riceve i dati mirrorati sul sistema storage remoto.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups** e poi seleziona il mirror consistency group che desideri testare.
3. Seleziona **Test Communication**.

   Viene visualizzata la finestra di dialogo Test comunicazione.

4. Selezionare uno o più test di comunicazione da eseguire tra i sistemi storage locali e remoti associati al gruppo di coerenza mirror selezionato, quindi fare clic su **Test**.
5. Esamina le informazioni visualizzate nella finestra Risultati.

Stato del test di comunicazione	Descrizione
Normale senza errori	Il gruppo di coerenza mirror sta comunicando correttamente.
Stato superato (ma non normale)	Verifica eventuali problemi di rete o di connessione e riprova il test.
Stato non riuscito	Viene indicata la causa dell'errore. Consulta la Guida al ripristino per risolvere il problema.
Errore di connessione alla porta	Il problema potrebbe essere dovuto al fatto che l'array di storage locale non è connesso o non è possibile contattare l'array di storage remoto. Consultare la Recovery Guru per correggere il problema.

Risultati

Al termine del test di comunicazione, questa finestra di dialogo mostra uno stato Normale, uno stato Superato o uno stato Non superato.

Se il test di comunicazione restituisce uno stato di errore, il test continua a essere eseguito dopo la chiusura di questa finestra di dialogo finché la comunicazione tra i mirror consistency groups non viene ripristinata.

Sospendere o riprendere la sincronizzazione per i gruppi di coerenza mirrorati in SANtricity System Manager

È possibile sospendere o riprendere la sincronizzazione dei dati su tutte le coppie mirrorate all'interno di un mirror consistency group, operazione più efficiente rispetto alla sospensione o alla ripresa della sincronizzazione su singole coppie mirrorate.

Informazioni su questa attività

La sospensione e la ripresa della sincronizzazione dei gruppi contribuiscono a ridurre qualsiasi impatto sulle prestazioni dell'applicazione host, che potrebbe verificarsi mentre i dati modificati sull'array di archiviazione locale vengono copiati sull'array di archiviazione remoto.

Lo stato del mirror consistency group e delle sue coppie mirrorate rimane sospeso finché non si utilizza l'opzione Riprendi per riprendere l'attività di sincronizzazione.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella dei gruppi di coerenza mirror e vengono mostrati tutti i gruppi di coerenza mirror associati all'array di storage.

3. Seleziona il mirror consistency group che desideri sospendere o riattivare, quindi seleziona **More › Sospendi** oppure **More › Riattiva**.

   Il sistema visualizza una conferma.

4. Seleziona **Yes** per confermare.

Risultati

System Manager esegue le seguenti azioni:

- Sospende o riprende il trasferimento dei dati tra tutte le coppie mirrorate in un gruppo di coerenza mirror senza rimuovere la relazione di mirroring.
- Registra tutti i dati scritti sul lato primario del gruppo di coerenza mirror mentre il gruppo mirror è sospeso e scrive automaticamente i dati sul lato secondario del gruppo di coerenza mirror quando il gruppo mirror viene ripristinato. Non è necessaria una sincronizzazione completa.
- Per un gruppo di coerenza mirror *sospeso*, viene visualizzato **user-suspended** nella tabella Mirror Consistency Groups.
- Per un gruppo di coerenza mirror *riattivato*, i dati scritti sui volumi primari mentre il gruppo di coerenza mirror era sospeso vengono scritti immediatamente sui volumi secondari. La sincronizzazione periodica riprende se è stato impostato un intervallo di sincronizzazione automatica.

Modifica le impostazioni di sincronizzazione per un gruppo di coerenza mirror in SANtricity System Manager

È possibile modificare le impostazioni di sincronizzazione e le soglie di avviso che il gruppo di coerenza mirror sull'array di archiviazione locale utilizza quando i dati vengono inizialmente sincronizzati o quando i dati vengono risincronizzati durante le operazioni di mirroring asincrono.

Informazioni su questa attività

La modifica delle impostazioni di sincronizzazione influisce sulle operazioni di sincronizzazione di tutte le coppie speculari all'interno del mirror consistency group.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.

2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella dei gruppi di coerenza mirror e vengono mostrati tutti i gruppi di coerenza mirror associati all'array di storage.

3. Seleziona il mirror consistency group che desideri modificare, quindi seleziona **More › Edit Settings**.

   Il sistema visualizza la finestra di dialogo Edit Settings.

4. Modifica le impostazioni di sincronizzazione e di avviso come appropriato, quindi fai clic su **Salva**.

Dettagli del campo

Campo	Descrizione
Sincronizza le coppie speculari…	Specifica se desideri sincronizzare le coppie mirrorate sull'array di storage remoto manualmente o automaticamente. • **Manualmente** – Selezionare questa opzione per sincronizzare manualmente le coppie mirrorate sull'array di storage remoto. • **Automaticamente, ogni** – Seleziona questa opzione per sincronizzare automaticamente le coppie replicate sull'array di storage remoto specificando l'intervallo di tempo dall'inizio dell'aggiornamento precedente all'inizio del successivo aggiornamento. L'intervallo predefinito è 10 minuti.
Avvisami…	Se si imposta il metodo di sincronizzazione per avvenire automaticamente, configurare i seguenti avvisi: • **Sincronizzazione** – Imposta la durata di tempo dopo la quale System Manager invia un avviso che la sincronizzazione non è stata completata. • **Punto di ripristino remoto** – Imposta un limite di tempo trascorso il quale System Manager invia un avviso indicando che i dati del punto di ripristino sull'array di storage remoto sono precedenti al limite di tempo definito. Definisci il limite di tempo a partire dalla fine dell'aggiornamento precedente. • **Soglia di capacità riservata** – Definisci un valore di capacità riservata al quale System Manager invia un avviso che ti stai avvicinando alla soglia di capacità riservata. Definisci la soglia in percentuale rispetto alla capacità rimanente.

Risultati

System Manager modifica le impostazioni di sincronizzazione per ogni coppia mirrorata nel mirror consistency group.

Risincronizzare manualmente i gruppi di coerenza mirror in SANtricity System Manager

È possibile avviare manualmente la risincronizzazione per tutte le coppie mirrorate all'interno di un mirror consistency group.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group e vengono visualizzati tutti i mirror consistency group associati all'array di storage.

3. Seleziona il mirror consistency group che desideri risincronizzare, quindi seleziona **More › Risincronizza manualmente**.

   Il sistema visualizza una conferma.

4. Seleziona **Yes** per confermare.

Risultati

Il sistema esegue le seguenti azioni:

- Avvia la risincronizzazione dei dati su tutte le coppie mirrorate all'interno del mirror consistency group selezionato.
- Aggiorna i dati modificati dall'array di storage locale all'array di storage remoto.

Visualizza la quantità di dati non sincronizzati tra i gruppi di coerenza mirror in SANtricity System Manager

È possibile visualizzare la quantità di dati non sincronizzati tra i gruppi di coerenza mirror sull'array di storage locale e sull'array di storage remoto. Quando il gruppo di coerenza mirror si trova nello stato Non sincronizzato, non viene eseguita alcuna attività di mirroring.

Informazioni su questa attività

È possibile eseguire questa operazione quando il gruppo di coerenza mirror selezionato contiene coppie mirrorate e quando la sincronizzazione non è attualmente in corso.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group e vengono visualizzati tutti i mirror consistency group associati all'array di storage.

3. Fare clic su **Altro › Visualizza la quantità di dati non sincronizzati**.

   Se sono presenti dati non sincronizzati, i valori della tabella lo riflettono. La colonna della quantità di dati elenca la quantità di dati non sincronizzati in MiB.

Aggiorna gli indirizzi IP degli array di storage remoti in SANtricity System Manager

È possibile aggiornare l'indirizzo IP iSCSI per l'array di storage remoto per ristabilire la connessione con l'array di storage locale.

Prima di iniziare

Sia l'array di storage locale che quello remoto devono essere configurati per il mirroring asincrono utilizzando una connessione iSCSI.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   La tabella Mirror Consistency Group visualizza tutti i mirror consistency group associati allo storage array.

3. Seleziona il gruppo di coerenza mirror che desideri aggiornare, quindi seleziona **More › Aggiorna indirizzo IP remoto**.

   Il sistema visualizza la finestra di dialogo Update Remote IP Address.

4. Seleziona **Aggiorna** per aggiornare l'indirizzo IP iSCSI del tuo array di storage remoto.

Risultati

Il sistema reimposta l'indirizzo IP dell'array storage remoto per ristabilire la connessione con l'array storage locale.

Modifica il ruolo del gruppo di coerenza mirror in primario o secondario in SANtricity System Manager

È possibile modificare il ruolo tra i gruppi di coerenza mirror per scopi amministrativi o in caso di disastro sull'array di storage locale.

Informazioni su questa attività

I gruppi di coerenza mirror creati sull'array di storage locale hanno il ruolo primario. I gruppi di coerenza mirror creati sull'array di storage remoto hanno il ruolo secondario. Puoi declassare il gruppo di coerenza mirror locale a ruolo secondario oppure promuovere il gruppo di coerenza mirror remoto a ruolo primario.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group e vengono visualizzati tutti i mirror consistency group associati all'array di storage.

3. Seleziona il mirror consistency group per il quale desideri modificare il ruolo, quindi seleziona **More › Change role to <Primary | Secondary>**.

   Il sistema visualizza una conferma.

4. Conferma che desideri modificare il ruolo del mirror consistency group, quindi fai clic su **Change Role**.

> Il sistema visualizza la finestra di dialogo Impossibile contattare l'array di storage quando viene richiesta una modifica del ruolo, ma non è possibile contattare l'array di storage remoto. Fare clic su **Sì** per forzare la modifica del ruolo.

Risultati

System Manager esegue le seguenti azioni:

- La tabella Mirror Consistency Group visualizza lo stato "pending" o "in-progress" accanto al mirror consistency group che sta subendo la modifica del ruolo. Puoi annullare un'operazione di Role Change in sospeso facendo clic sul link **Cancel** presente nella cella della tabella.
- Se è possibile contattare il gruppo di coerenza mirror associato, i ruoli tra i gruppi di coerenza mirror cambiano. System Manager promuove il gruppo di coerenza mirror secondario a ruolo primario o retrocede il gruppo di coerenza mirror primario a ruolo secondario (a seconda della selezione). La modifica del ruolo ha effetto su tutte le coppie mirror all'interno del gruppo di coerenza mirror selezionato.

Eliminare un gruppo di coerenza mirror in SANtricity System Manager

È possibile eliminare i gruppi di coerenza mirror che non sono più necessari sull'array di archiviazione locale e sull'array di archiviazione remoto.

Prima di iniziare

Tutte le coppie mirrorate devono essere rimosse dal mirror consistency group.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirror Consistency Groups**.

   Viene visualizzata la tabella Mirror Consistency Group e vengono visualizzati tutti i mirror consistency group associati all'array di storage.

3. Seleziona il gruppo di coerenza mirror che desideri eliminare, quindi seleziona **Uncommon Tasks › Delete**.

   Il sistema visualizza una conferma.

4. Selezionare **Sì** per eliminare il gruppo di coerenza mirror.

Risultati

System Manager esegue le seguenti azioni:

- Elimina il gruppo di coerenza mirror sull'array di archiviazione locale per primo, quindi elimina il gruppo di coerenza mirror sull'array di archiviazione remoto.
- Rimuove il gruppo di coerenza mirror dalla tabella Mirror Consistency Group.

Dopo aver finito

Occasionalmente, può capitare che il gruppo di coerenza mirror venga eliminato correttamente dall'array di archiviazione locale, ma un errore di comunicazione impedisca l'eliminazione del gruppo di coerenza mirror dall'array di archiviazione remoto. In questo caso, è necessario accedere all'array di archiviazione remoto per eliminare il gruppo di coerenza mirror corrispondente.

Gestisci coppie mirrorate asincrone

Rimuovere le relazioni mirror asincrone in SANtricity System Manager

Si rimuove una coppia mirrorata per rimuovere la relazione di mirroring dal volume primario sull'array di storage locale e dal volume secondario sull'array di storage remoto.

Informazioni su questa attività

Esamina le seguenti informazioni sulle coppie mirrorate orfane:

- Una coppia mirrorata orfana esiste quando un volume membro in un gruppo mirror di coerenza è stato rimosso da un lato (sia dal lato del sistema storage locale che dal lato del sistema storage remoto) ma non dall'altro lato.
- Le coppie mirrorate orfane vengono rilevate quando viene ripristinata la comunicazione tra gli array e i due lati della configurazione mirrorata riconciliano i parametri del mirror.
- È possibile rimuovere una coppia mirrorata per correggere lo stato di una coppia mirrorata orfana.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirrored Pair**.

   Viene visualizzata la tabella Mirrored Pairs, che mostra tutte le coppie mirror associate all'array di storage.

3. Seleziona la coppia mirrorata che desideri rimuovere, quindi fai clic su **Remove**.
4. Conferma di voler rimuovere la coppia mirrorata, quindi fai clic su **Rimuovi**.

Risultati

System Manager esegue le seguenti azioni:

- Rimuove la relazione di mirroring dal mirror consistency group sull'array di storage locale e sull'array di storage remoto ed elimina la capacità riservata.
- Ripristina il volume primario e il volume secondario come volumi non mirrorati accessibili dall'host.
- Aggiorna il riquadro Mirroring asincrono con la rimozione della coppia mirrorata asincrona.

Aumentare la capacità riservata in SANtricity System Manager

È possibile aumentare la capacità riservata, ovvero la capacità fisicamente allocata utilizzata per qualsiasi operazione di copy service su un oggetto di archiviazione.

Per le operazioni di snapshot, in genere è il 40 percento del volume di base; per le operazioni di mirroring asincrono, in genere è il 20 percento del volume di base. In genere, si aumenta la capacità riservata quando si riceve un avviso che la capacità riservata dell'oggetto di archiviazione sta per esaurirsi.

Prima di iniziare

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

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

Informazioni su questa attività

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

- Gruppo Snapshot
- Volume Snapshot

- Volume membro del gruppo di coerenza
- Volume della coppia mirrorata

Utilizza una percentuale elevata se ritieni che il volume primario subirà molte modifiche o se la durata di una particolare operazione di copy service sarà molto lunga.

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

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la scheda **Reserved Capacity**.
3. Seleziona l'oggetto storage per cui desideri aumentare la capacità riservata, quindi fai clic su **Aumenta capacità**.

   Viene visualizzata la finestra di dialogo Increase Reserved Capacity.

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

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

5. Fai clic su **Increase**.

Risultati

System Manager esegue le seguenti azioni:

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

Modificare le impostazioni di capacità riservata per un volume di coppia mirror in SANtricity System Manager

È possibile modificare le impostazioni di un volume con mirroring per regolare la percentuale di soglia oltre la quale SANtricity System Manager invia una notifica di avviso quando la capacità riservata per un volume con mirroring sta per esaurirsi.

Passaggi

1. Selezionare **Storage › Pool & Volume Groups**.
2. Seleziona la scheda **Reserved Capacity**.
3. Seleziona il volume della coppia mirrored che desideri modificare, quindi fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Impostazioni capacità riservata Mirrored Pair Volume.

4. Modificare le impostazioni di capacità riservata per il volume della coppia mirrorata, se necessario.

Dettagli del campo

Impostazione	Descrizione
Avvisami quando…	Utilizzare il selettore a rotella per regolare il punto percentuale al quale System Manager invia una notifica di avviso quando la capacità riservata per una coppia mirror sta per esaurirsi. Quando la capacità riservata per la coppia mirror supera la soglia specificata, System Manager invia un avviso, consentendoti di aumentare la capacità riservata. La modifica dell'impostazione di avviso per una coppia mirrorata modifica l'impostazione di avviso per tutte le coppie mirrorate che appartengono allo stesso mirror consistency group.

5. Fai clic su **Salva** per applicare le modifiche.

Completare una coppia mirrorata per i volumi primari creati su un sistema legacy in SANtricity System Manager

Se hai creato un volume primario su un array di storage legacy che non può essere gestito da SANtricity System Manager, puoi creare il volume secondario su questo array con SANtricity System Manager.

Informazioni su questa attività

È possibile eseguire il mirroring asincrono tra array legacy che utilizzano un'interfaccia diversa e array più recenti che possono essere gestiti da System Manager.

- Se stai eseguendo il mirroring tra due array di storage che utilizzano System Manager, puoi saltare questa operazione perché hai già completato la coppia mirrorata nella sequenza di creazione della coppia mirrorata.
- Eseguire questa operazione sull'array di archiviazione remoto.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Seleziona la scheda **Mirrored Pair**.

   Viene visualizzata la tabella Mirrored Pairs, che mostra tutte le coppie mirror associate all'array di storage.
3. Individua il volume della coppia mirrorata con stato Incompleto, quindi fai clic sul collegamento **Complete mirrored pair** visualizzato nella colonna della coppia mirrorata.
4. Scegli se completare la sequenza di creazione della coppia mirrorata automaticamente o manualmente selezionando uno dei seguenti pulsanti di opzione:
   - **Automatic** — Crea un nuovo volume secondario.

     Accetta le impostazioni predefinite per il lato remoto della coppia con mirroring selezionando un pool o un gruppo di volumi esistente in cui desideri creare il volume secondario. Utilizza questa opzione

consigliata per allocare la capacità riservata per il volume secondario con le impostazioni predefinite.

- **Manual** — Selezionare un volume esistente.

  Definisci i tuoi parametri per il volume secondario.

  i. Fare clic su **Avanti** per selezionare il volume secondario.
  ii. Seleziona un volume esistente che desideri utilizzare come volume secondario e quindi fai clic su **Next** per allocare la capacità riservata.
  iii. Assegnare la capacità riservata. Eseguire una delle seguenti operazioni:
    - Accetta le impostazioni predefinite.

      L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume base e di solito questa capacità è sufficiente.

    - Assegna le tue impostazioni di capacità riservata per soddisfare le tue esigenze di storage dati relative al mirroring asincrono.

      La capacità necessaria varia a seconda della frequenza e della dimensione delle operazioni di I/O sul volume primario e della durata per cui è necessario mantenere la capacità. In generale, scegliere una capacità maggiore per la capacità riservata se si verifica una o entrambe le seguenti condizioni:

      - Intendi mantenere la coppia mirrorata per un lungo periodo di tempo.
      - Una percentuale elevata di blocchi di dati subirà modifiche sul volume primario a causa di un'intensa attività di I/O. Utilizza i dati storici sulle prestazioni o altre utilità del sistema operativo per aiutarti a determinare l'attività di I/O tipica sul volume primario.

5. Seleziona **Complete**.

Risultati

System Manager esegue le seguenti azioni:

- Crea il volume secondario sull'array di storage remoto e alloca la capacità riservata per il lato remoto della coppia mirrorata.
- Avvia la sincronizzazione iniziale tra l'array di archiviazione locale e l'array di archiviazione remoto.
- Se il volume di cui si esegue il mirroring è un volume thin, durante la sincronizzazione iniziale vengono trasferiti al volume secondario solo i blocchi allocati. Questo trasferimento riduce la quantità di dati che devono essere trasferiti per completare la sincronizzazione iniziale.
- Crea la capacità riservata per la coppia mirrorata sull'array di storage locale e sull'array di storage remoto.

Gestisci le coppie mirrorate sincronizzate

Verifica la comunicazione per il mirroring sincrono in SANtricity System Manager

È possibile testare la comunicazione tra un array di storage locale e un array di storage remoto per diagnosticare possibili problemi di comunicazione per una coppia mirrorata che partecipa al mirroring sincrono.

Informazioni su questa attività

Vengono eseguiti due test diversi:

- **Comunicazione** — Verifica che i due array di storage abbiano un percorso di comunicazione. Il test di comunicazione convalida che l'array di storage locale possa comunicare con l'array di storage remoto e che il volume secondario associato alla coppia mirrorata esista sull'array di storage remoto.
- **Latenza** — Invia un comando di test unità SCSI al volume secondario sull'array di storage remoto associato alla coppia con mirroring per testare la latenza minima, media e massima.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Seleziona la coppia mirrorata che desideri testare, quindi seleziona **Test Communication**.
3. Esamina le informazioni visualizzate nella finestra Risultati e, se necessario, segui l'azione correttiva indicata.

> Se il test di comunicazione fallisce, il test continua a essere eseguito dopo la chiusura di questa finestra di dialogo finché la comunicazione tra la coppia mirrorata non viene ripristinata.

Sospendere e riprendere la sincronizzazione per coppie mirrorate in SANtricity System Manager

È possibile utilizzare le opzioni Suspend e Resume per controllare quando sincronizzare i dati sul volume primario e sul volume secondario in una coppia con dati mirrorati.

Informazioni su questa attività

Se una coppia mirrorata viene sospesa manualmente, la coppia mirrorata non si sincronizzerà finché non verrà ripresa manualmente.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Seleziona la coppia mirrorata che desideri sospendere o riprendere, quindi seleziona **Altro › Sospendi** oppure **Altro › Riprendi**.

   Il sistema visualizza una conferma.
3. Seleziona **Yes** per confermare.

Risultati

System Manager esegue le seguenti azioni:

- Consente di sospendere o riprendere il trasferimento dei dati tra la coppia mirrorata senza rimuovere la relazione di mirroring.
- Per una coppia mirrorata sospesa:
  - Visualizza **Sospeso** nella tabella delle coppie mirrorate.
  - Registra tutti i dati che sono stati scritti sul volume primario della coppia con mirroring mentre la sincronizzazione è sospesa.
- Per una coppia mirrorata *ripristinata*, i dati vengono scritti automaticamente sul volume secondario della coppia mirrorata quando la sincronizzazione viene ripresa. Non è necessaria una sincronizzazione completa.

Modifica il ruolo tra i volumi in una coppia mirrorata in SANtricity System Manager

È possibile eseguire un'inversione di ruolo tra i due volumi di una coppia con mirroring che partecipano al mirroring sincrono. Questa operazione potrebbe essere necessaria per scopi amministrativi o in caso di disastro sull'array di storage locale.

Informazioni su questa attività

È possibile declassare il volume primario al ruolo secondario o promuovere il volume secondario al ruolo primario. Tutti gli host che accedono al volume primario hanno accesso in lettura/scrittura al volume. Quando il volume primario diventa un volume secondario, solo le scritture remote avviate dal controller primario vengono scritte sul volume.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Seleziona la coppia speculare che contiene i volumi per cui desideri modificare il ruolo, quindi seleziona **More › Change Role**.

   Il sistema visualizza una conferma.

3. Conferma che desideri modificare il ruolo dei volumi, quindi seleziona **Cambia ruolo**.

> Se l'array di storage locale non riesce a comunicare con l'array di storage remoto, il sistema visualizza la finestra di dialogo Cannot Contact Storage Array quando viene richiesta una modifica del ruolo, ma non è possibile contattare l'array di storage remoto. Fare clic su **Yes** per forzare la modifica del ruolo.

Risultati

System Manager esegue la seguente azione:

- Se è possibile contattare il volume associato nella coppia mirrorata, i ruoli tra i volumi cambiano. System Manager promuove il volume secondario nella coppia mirrorata al ruolo primario oppure declassa il volume primario nella coppia mirrorata al ruolo secondario (a seconda della selezione).

Modificare le impostazioni di sincronizzazione per una coppia mirrorata in SANtricity System Manager

È possibile modificare la priorità di sincronizzazione e la policy di risincronizzazione che la coppia mirror utilizza per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione.

Informazioni su questa attività

È possibile modificare le impostazioni di sincronizzazione per una coppia con mirroring solo sull'array di storage che contiene il volume primario.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Seleziona la coppia speculare che desideri modificare, quindi seleziona **More › Edit settings**.

   Il sistema visualizza la finestra di dialogo Visualizza/Modifica impostazioni.

3. Utilizza la barra di scorrimento per modificare la priorità di sincronizzazione.

La priorità di sincronizzazione determina quante risorse di sistema vengono utilizzate per completare l'operazione di risincronizzazione dopo un'interruzione della comunicazione rispetto alle richieste di I/O del servizio.

Ulteriori informazioni sulle velocità di sincronizzazione

Esistono cinque livelli di priorità di sincronizzazione:

- Più basso
- Basso
- Medio
- Alto
- Più alto

Se la priorità di sincronizzazione è impostata sul valore più basso, l'attività di I/O ha la priorità e l'operazione di risincronizzazione richiede più tempo. Se la priorità di sincronizzazione è impostata sul valore più alto, l'operazione di risincronizzazione ha la priorità, ma l'attività di I/O per l'array di storage potrebbe essere influenzata.

4. Modifica la policy di risincronizzazione come appropriato.

   È possibile risincronizzare le coppie mirrorate sull'array di archiviazione remoto manualmente o automaticamente.

   - **Manuale** (opzione consigliata) — Selezionare questa opzione per richiedere che la sincronizzazione venga ripresa manualmente dopo il ripristino della comunicazione con una coppia mirror. Questa opzione offre la migliore opportunità per il recupero dei dati.
   - **Automatico** — Selezionare questa opzione per avviare automaticamente la risincronizzazione dopo il ripristino della comunicazione con una coppia mirrorata.
5. Seleziona **Save**.

Rimuovere le relazioni di mirroring sincrono in SANtricity System Manager

Si rimuove una coppia mirrorata per rimuovere la relazione di mirroring dal volume primario sull'array di storage locale e dal volume secondario sull'array di storage remoto.

Informazioni su questa attività

È inoltre possibile rimuovere una coppia mirrorata per correggere lo stato di una coppia mirrorata orfana. Consultare le seguenti informazioni sulle coppie mirrorate orfane:

- Una coppia mirrorata orfana esiste quando un volume membro è stato rimosso da un lato (locale/remoto) ma non dall'altro lato.
- Le coppie mirrorate orfane vengono rilevate quando viene ripristinata la comunicazione tra gli array.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Seleziona la coppia mirrorata che desideri rimuovere, quindi seleziona il **Uncommon Tasks › Rimuovi**.

   Viene visualizzata la finestra di dialogo Remove Mirror Relationship.

3. Conferma di voler rimuovere la coppia mirrorata, quindi fai clic su **Rimuovi**.

Risultati

System Manager esegue le seguenti azioni:

- Rimuove la relazione di mirroring dalla coppia mirrorata sul sistema storage locale e sul sistema storage remoto.
- Ripristina il volume primario e il volume secondario come volumi non mirrorati accessibili dall'host.
- Aggiorna il riquadro Mirroring sincrono con la rimozione della coppia mirrorata sincrona.

Disattiva mirroring

Disattivare il mirroring asincrono in SANtricity System Manager

È possibile disattivare il mirroring asincrono sugli array di storage locali e remoti per ripristinare il normale utilizzo delle porte dedicate sugli array di storage.

Prima di iniziare

- Devi aver eliminato tutte le relazioni di mirror. Verifica che tutti i gruppi di coerenza di mirror e le coppie mirrorate siano stati eliminati dagli array di storage locali e remoti.
- L'array di storage locale e l'array di storage remoto devono essere collegati tramite una rete Fibre Channel o un'interfaccia iSCSI.

Informazioni su questa attività

Quando si disattiva il mirroring asincrono, non può verificarsi alcuna attività di mirroring sugli array di storage locali e remoti.

Passaggi

1. Selezionare **Storage › Asynchronous Mirroring**.
2. Selezionare **Uncommon Tasks › Deactivate**.

   Il sistema visualizza una conferma.

3. Seleziona **Yes** per confermare.

Risultati

- I canali host HBA del controller che erano dedicati alla comunicazione di mirroring asincrono ora possono accettare richieste di lettura e scrittura da host.
- Nessuno dei volumi in questo array di storage è in grado di partecipare a relazioni di mirror, né come volumi primari né come volumi secondari.

Disattivare il mirroring sincrono in SANtricity System Manager

È possibile disattivare la funzionalità di mirroring sincrono su un array di storage per ripristinare il normale utilizzo della porta host 4 dell'adattatore bus host (HBA), che era riservata per la trasmissione dei dati mirrorati.

Prima di iniziare

Devi aver eliminato tutte le relazioni di mirroring sincrono. Verifica che tutte le coppie mirrorate siano state

eliminate dall'array di storage.

Passaggi

1. Selezionare **Storage › Synchronous Mirroring**.
2. Selezionare **Uncommon Tasks › Deactivate**.

   Il sistema visualizza una conferma.

3. Seleziona **Yes** per confermare.

Risultati

- La porta host HBA 4 del controller, che era dedicata alla comunicazione di mirroring sincrono, ora può accettare richieste di lettura e scrittura dall'host.
- I volumi di capacità riservata sull'array di storage vengono eliminati.

Domande frequenti sul mirroring asincrono per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

In che modo il mirroring asincrono si differenzia dal mirroring sincrono?

La funzione di mirroring asincrono si differenzia dalla funzione di mirroring sincrono per un aspetto fondamentale: acquisisce lo stato del volume sorgente in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine.

Con il mirroring sincrono, lo stato del volume primario non viene acquisito in un determinato momento, ma riflette tutte le modifiche apportate al volume primario sul volume secondario. Il volume secondario è identico al volume primario in ogni istante perché, con questo tipo di mirroring, ogni volta che viene eseguita una scrittura sul volume primario, viene eseguita una scrittura anche sul volume secondario. L'host non riceve una conferma dell'avvenuta scrittura finché il volume secondario non viene aggiornato correttamente con le modifiche apportate al volume primario.

Con il mirroring asincrono, l'array di storage remoto non è completamente sincronizzato con l'array di storage locale, quindi se l'applicazione deve passare all'array di storage remoto a causa della perdita dell'array di storage locale, alcune transazioni potrebbero andare perse.

Confronto tra le funzionalità di mirroring:

Mirroring asincrono	Mirroring sincrono
Metodo di replica	• **Point-in-Time** Il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente. Le pianificazioni possono essere definite con una granularità di minuti. Il tempo minimo tra le sincronizzazioni è di 10 minuti.

Mirroring asincrono	Mirroring sincrono
• **Continuo** Il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura dell'host.	**Capacità riservata**
• **Multipli** È necessario un volume di capacità riservata per ogni coppia speculare.	• **Singolo** È richiesto un unico volume di capacità riservata per tutti i volumi mirrorati.
Comunicazione	• **iSCSI e Fibre Channel** Supporta le interfacce iSCSI e Fibre Channel tra gli array di storage.
• **Fibre Channel** Supporta solo interfacce Fibre Channel tra gli array di storage.	**Distanza**
• **Illimitato** Supporto per distanze praticamente illimitate tra l'array di storage locale e l'array di storage remoto, con la distanza in genere limitata solo dalle capacità della rete e dalla tecnologia di estensione del canale.	• **Limitato** In genere deve trovarsi entro circa 10 km (6.2 miglia) dall'array di storage locale per soddisfare i requisiti di latenza e prestazioni dell'applicazione.

Perché non posso accedere alla funzione di mirroring che ho scelto?

Il mirroring viene configurato nell'interfaccia SANtricity Unified Manager.

La funzione di mirroring sincrono non è disponibile sull'array di storage EF600/EF600C o EF300/EF300C.

Per abilitare e configurare il mirroring tra due array, verificare quanto segue:

- Il servizio Web Services Proxy deve essere in esecuzione. (Unified Manager è installato su un sistema host insieme al Web Services Proxy.)
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- I due storage array che si desidera utilizzare per il mirroring devono essere rilevati in Unified Manager.
- Unified Manager deve disporre di certificati SSL validi per gli array di storage. È possibile accettare un certificato autofirmato o installare certificati firmati da CA tramite Unified Manager.

Per le istruzioni di configurazione, vedere quanto segue:

- "Creare una coppia speculare asincrona (in Unified Manager)"
- "Creare una coppia sincrona mirrorata (in Unified Manager)"

Cosa devo sapere prima di creare un mirror consistency group?

Segui queste linee guida prima di creare un mirror consistency group.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Si crea un gruppo di coerenza in Unified Manager nella procedura guidata Crea coppie speculari.

Soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Assicurati inoltre di soddisfare i seguenti requisiti per gli array di storage:

- I due array di storage devono essere rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel o un'interfaccia iSCSI.

Mirroring asincrono - Cosa devo sapere prima di creare una coppia speculare?

Si configurano le coppie di mirror nell'interfaccia SANtricity Unified Manager e poi si gestiscono le coppie in SANtricity System Manager.

Prima di creare una coppia speculare, seguire queste linee guida.

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel o un'interfaccia iSCSI.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.

- Hai installato Web Services Proxy e Unified Manager. Le coppie speculari sono configurate nell'interfaccia di Unified Manager.
- I due array di storage vengono rilevati in Unified Manager.
- L'array di storage deve contenere almeno un mirror consistency group. Si crea un mirror consistency group in Unified Manager nella procedura guidata Create Mirrored Pairs.

Cosa devo sapere prima di aumentare la capacità riservata su un volume di coppia in mirroring?

In genere, si dovrebbe aumentare la capacità riservata quando si riceve un avviso che la capacità riservata per una coppia di mirroring sta per esaurirsi. È possibile aumentare la capacità riservata solo in incrementi di 8 GiB.

Per le operazioni di mirroring asincrono, la capacità riservata è in genere il 20 percento del volume di base. Scegli una capacità maggiore per la capacità riservata se esiste una o entrambe queste condizioni:

- Intendi mantenere la coppia mirrorata per un lungo periodo di tempo.
- Una percentuale elevata di blocchi di dati subirà modifiche sul volume primario a causa di un'intensa attività di I/O. Utilizza i dati storici sulle prestazioni o altre utilità del sistema operativo per aiutarti a determinare l'attività di I/O tipica sul volume primario.

È possibile aumentare la capacità riservata per una coppia di mirroring eseguendo una delle seguenti azioni:

- Regola la percentuale di capacità per un volume della coppia in mirroring selezionando **Storage › Pools and Volumes Groups** e poi facendo clic sulla scheda **Reserved Capacity**.
- Crea un nuovo volume utilizzando la capacità libera disponibile in un pool o in un gruppo di volumi.

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

Perché non posso aumentare la capacità riservata con la quantità richiesta?

È possibile aumentare la capacità riservata solo in incrementi di 4 GiB.

Esaminare le seguenti linee guida:

- È necessario disporre di una capacità libera sufficiente nel pool o nel gruppo di volumi affinché possa essere espanso se necessario.

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

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

Per le operazioni di mirroring asincrono la capacità riservata è in genere il 20 percento del volume di base. Utilizzare una percentuale più alta se si ritiene che il volume di base subirà molte modifiche o se la durata stimata dell'operazione di copy service di un oggetto storage sarà molto lunga.

Perché dovrei cambiare questa percentuale?

La capacità riservata è in genere pari al 40 percento del volume di base per le operazioni di snapshot e al 20 percento del volume di base per le operazioni di mirroring asincrono.

Di solito questa capacità è sufficiente. La capacità necessaria varia a seconda della frequenza e delle dimensioni delle scritture di I/O sul volume di base e di quanto tempo si intende utilizzare l'operazione di servizio di copia dell'oggetto di storage.

In generale, scegli una percentuale maggiore per la capacità riservata se sussistono una o entrambe queste condizioni:

- Se la durata dell'operazione di copy service di un particolare oggetto storage sarà molto lunga.
- Se una grande percentuale di blocchi di dati cambierà sul volume di base a causa di un'intensa attività di I/O. Utilizzare i dati storici sulle prestazioni o altre utility del sistema operativo per aiutare a determinare l'attività di I/O tipica del volume di base.

Perché vedo più di un candidato a capacità riservata?

Se in un pool o gruppo di volumi è presente più di un volume che soddisfa la percentuale di capacità selezionata per l'oggetto storage, verranno visualizzati più candidati.

È possibile aggiornare l'elenco dei candidati consigliati modificando la percentuale di spazio fisico dell'unità che si desidera riservare sul volume di base per le operazioni di copy service. I candidati migliori vengono visualizzati in base alla selezione effettuata.

Perché vedo valori Non disponibili visualizzati nella tabella?

La tabella elenca i valori Not Available quando i dati presenti sull'array di storage remoto non sono disponibili per essere visualizzati.

Per visualizzare i dati dell'array di storage remoto, avvia System Manager da Unified Manager.

Perché non vedo tutti i miei pool e gruppi di volumi?

Quando si crea un volume secondario per la coppia di mirroring asincrono, il sistema visualizza un elenco di tutti i pool e i gruppi di volumi idonei per quella coppia di mirroring asincrono. Qualsiasi pool o gruppo di volumi non idoneo all'uso non viene visualizzato in quell'elenco.

I pool o i gruppi di volumi potrebbero non essere idonei per uno dei seguenti motivi.

- Le capacità di sicurezza di un pool o di un gruppo di volumi non corrispondono.
- Un pool o un gruppo di volumi è in uno stato non ottimale.
- La capacità di un pool o di un gruppo di volumi è troppo piccola.

Mirroring asincrono - Perché non vedo tutti i volumi?

Quando si seleziona un volume primario per una coppia con mirroring, un elenco mostra tutti i volumi idonei.

I volumi che non sono idonei all'uso non vengono visualizzati in quell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è ottimale.

- Il volume partecipa già a una relazione di mirroring.
- Per i volumi sottili, l'auto-espansione deve essere abilitata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona in mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie asincrone in mirroring non ammissibili non appariranno nell'elenco dei volumi disponibili.

Mirroring asincrono - Perché non vedo tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario sull'array di storage remoto, un elenco mostra tutti i volumi idonei per quella coppia di mirroring.

Qualsiasi volume che non è idoneo all'uso non viene visualizzato in quell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume non è ottimale.
- Il volume partecipa già a una relazione di mirroring.
- Gli attributi del volume sottile tra il volume primario e il volume secondario non corrispondono.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse impostazioni DA.
  - Se il volume primario è abilitato per DA, il volume secondario deve essere abilitato per DA.
  - Se il volume primario non è abilitato per DA, il volume secondario non deve essere abilitato per DA.

Perché dovrei aggiornare l'indirizzo IP del mio array di storage remoto?

Aggiornare l'indirizzo IP dell'array di storage remoto quando l'indirizzo IP di una porta iSCSI cambia e l'array di storage locale non è in grado di comunicare con l'array di storage remoto.

Quando si stabilisce una relazione di mirroring asincrono con una connessione iSCSI, sia l'array di storage locale che quello remoto memorizzano un record dell'indirizzo IP dell'array di storage remoto nella configurazione di mirroring asincrono. Se l'indirizzo IP di una porta iSCSI cambia, l'array di storage remoto che tenta di utilizzare tale porta riscontra un errore di comunicazione.

L'array di storage con l'indirizzo IP modificato invia un messaggio a ciascun array di storage remoto associato ai gruppi di coerenza mirror configurati per il mirroring su una connessione iSCSI. Gli array di storage che ricevono questo messaggio aggiornano automaticamente il proprio indirizzo IP di destinazione remoto.

Se l'array di storage con l'indirizzo IP modificato non riesce a inviare il messaggio inter-array a un array di storage remoto, il sistema invia un avviso relativo al problema di connettività. Utilizza l'opzione Aggiorna indirizzo IP remoto per ristabilire la connessione con l'array di storage locale.

Domande frequenti sul mirroring sincrono per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

In che modo il mirroring asincrono si differenzia dal mirroring sincrono?

La funzione di mirroring asincrono si differenzia dalla funzione di mirroring sincrono per un aspetto fondamentale: acquisisce lo stato del volume sorgente in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine.

Con il mirroring sincrono, lo stato del volume primario non viene acquisito in un determinato momento, ma riflette tutte le modifiche apportate al volume primario sul volume secondario. Il volume secondario è identico al volume primario in ogni istante perché, con questo tipo di mirroring, ogni volta che viene eseguita una scrittura sul volume primario, viene eseguita una scrittura anche sul volume secondario. L'host non riceve una conferma dell'avvenuta scrittura finché il volume secondario non viene aggiornato correttamente con le modifiche apportate al volume primario.

Con il mirroring asincrono, l'array di storage remoto non è completamente sincronizzato con l'array di storage locale, quindi se l'applicazione deve passare all'array di storage remoto a causa della perdita dell'array di storage locale, alcune transazioni potrebbero andare perse.

Confronto tra le funzionalità di mirroring:

Mirroring asincrono	Mirroring sincrono
Metodo di replica	• **Point-in-Time** Il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente. Le pianificazioni possono essere definite con una granularità di minuti. Il tempo minimo tra le sincronizzazioni è di 10 minuti.
• **Continuo** Il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura dell'host.	**Capacità riservata**
• **Multipli** È necessario un volume di capacità riservata per ogni coppia speculare.	• **Singolo** È richiesto un unico volume di capacità riservata per tutti i volumi mirrorati.
Comunicazione	• **iSCSI e Fibre Channel** Supporta le interfacce iSCSI e Fibre Channel tra gli array di storage.
• **Fibre Channel** Supporta solo interfacce Fibre Channel tra gli array di storage.	**Distanza**

Mirroring asincrono	Mirroring sincrono
• **Illimitato** Supporto per distanze praticamente illimitate tra l'array di storage locale e l'array di storage remoto, con la distanza in genere limitata solo dalle capacità della rete e dalla tecnologia di estensione del canale.	• **Limitato** In genere deve trovarsi entro circa 10 km (6.2 miglia) dall'array di storage locale per soddisfare i requisiti di latenza e prestazioni dell'applicazione.

Mirroring sincrono - Perché non visualizzo tutti i miei volumi?

Quando si seleziona un volume primario per una coppia con mirroring, un elenco mostra tutti i volumi idonei.

I volumi che non sono idonei all'utilizzo non vengono visualizzati in tale elenco. I volumi potrebbero non essere idonei per uno qualsiasi dei seguenti motivi:

- Il volume è un volume non standard, come un volume Snapshot o un volume thin.
- Il volume non è ottimale.
- Il volume partecipa già a una relazione di mirroring.

Mirroring sincrono - Perché non visualizzo tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario sull'array di storage remoto, un elenco mostra tutti i volumi idonei per quella coppia di mirroring.

Qualsiasi volume che non è idoneo all'uso non viene visualizzato in quell'elenco. I volumi potrebbero non essere idonei per uno dei seguenti motivi:

- Il volume è un volume non standard, come un volume Snapshot o un volume thin.
- Il volume non è ottimale.
- Il volume partecipa già a una relazione di mirroring.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse impostazioni DA.
  - Se il volume primario è abilitato per DA, il volume secondario deve essere abilitato per DA.
  - Se il volume primario non è abilitato per DA, il volume secondario non deve essere abilitato per DA.

Mirroring sincrono - cosa devo sapere prima di creare una coppia speculare?

Si configurano le coppie di mirror nell'interfaccia SANtricity Unified Manager e poi si gestiscono le coppie in SANtricity System Manager.

Prima di creare una coppia mirror, segui queste linee guida:

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.

- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- Hai installato Web Services Proxy e Unified Manager. Le coppie speculari sono configurate nell'interfaccia di Unified Manager.
- I due array di storage vengono rilevati in Unified Manager.

Che impatto ha la priorità di sincronizzazione sulle velocità di sincronizzazione?

La priorità di sincronizzazione definisce la quantità di tempo di elaborazione allocata alle attività di sincronizzazione rispetto alle prestazioni del sistema.

Il controller proprietario del volume primario esegue questa operazione in background. Contemporaneamente, il controller proprietario elabora le scritture I/O locali sul volume primario e le relative scritture remote sul volume secondario. Poiché la risincronizzazione distoglie le risorse di elaborazione del controller dall'attività di I/O, la risincronizzazione può avere un impatto sulle prestazioni dell'applicazione host.

Tenete a mente queste linee guida per aiutarvi a determinare quanto tempo potrebbe richiedere una priorità di sincronizzazione e in che modo le priorità di sincronizzazione possono influire sulle prestazioni del sistema.

Informazioni sulle priorità di sincronizzazione

Queste tariffe prioritarie sono disponibili:

- Più basso
- Basso
- Medio
- Alto
- Più alto

La velocità di priorità più bassa supporta le prestazioni del sistema, ma la risincronizzazione richiede più tempo. La velocità di priorità più alta supporta la risincronizzazione, ma le prestazioni del sistema potrebbero essere compromesse.

Queste linee guida approssimativamente approssimano le differenze tra le priorità.

Tariffa prioritaria per la sincronizzazione completa	Tempo trascorso rispetto alla velocità di sincronizzazione più elevata
Più basso	Circa otto volte più a lungo rispetto al tasso di priorità più alto.
Basso	Circa sei volte più a lungo rispetto al tasso di priorità più alto.
Medio	Circa tre volte e mezzo più a lungo rispetto al tasso di priorità più alto.

Tariffa prioritaria per la sincronizzazione completa	Tempo trascorso rispetto alla velocità di sincronizzazione più elevata
Alto	Circa il doppio del tempo rispetto alla velocità di priorità più alta.

Le dimensioni del volume e i carichi di I/O dell'host influenzano i confronti dei tempi di sincronizzazione.

Perché è consigliato utilizzare una policy di sincronizzazione manuale?

Si consiglia la risincronizzazione manuale perché consente di gestire il processo di risincronizzazione in modo da offrire la migliore opportunità per il recupero dei dati.

Se si utilizza una policy di risincronizzazione automatica e si verificano problemi di comunicazione intermittenti durante la risincronizzazione, i dati sul volume secondario potrebbero essere temporaneamente danneggiati. Al termine della risincronizzazione, i dati vengono corretti.

Archiviazione remota

Scopri la funzionalità Remote Storage in SANtricity System Manager

Se disponi della funzionalità Remote Storage, puoi importare dati da un sistema storage remoto nel tuo storage array.

Che cos'è la funzione Remote Storage?

La funzione *Remote Storage* consente di importare dati da un sistema storage remoto a un sistema storage E-Series locale. Il sistema remoto può essere un altro sistema E-Series o un sistema di un altro fornitore. Questa funzione è utile quando si desidera semplificare la migrazione dei dati riducendo al minimo i tempi di inattività, ad esempio durante gli aggiornamenti delle apparecchiature.

Per utilizzare lo storage remoto, questa funzione deve essere abilitata nel Submodel ID (SMID).

Per saperne di più:

- "Come funziona lo storage remoto"
- "Terminologia Remote Storage"
- "Requisiti del sistema storage remoto"
- "Requisiti del volume dello storage remoto"

Come faccio a importare i dati con questa funzione?

Tramite la procedura guidata Remote Storage, è possibile associare un dispositivo di storage (la fonte per l'importazione dei dati) a un volume di destinazione sul sistema E-Series. Questa procedura guidata è disponibile dal **Storage › Remote storage**.

Per saperne di più:

- "Importa storage remoto"
- "Gestisci l'avanzamento dell'importazione dei dati"

Concetti

Come funziona lo storage remoto nel software SANtricity

La funzione Archiviazione remota consente di importare dati da un sistema storage remoto a un sistema storage E-Series locale. Questa funzione è utile quando si desidera semplificare la migrazione dei dati riducendo al minimo i tempi di inattività, ad esempio durante gli aggiornamenti delle apparecchiature.

Per configurare la funzionalità Remote Storage, è necessario impostare l'hardware e quindi utilizzare System Manager per creare un oggetto remote storage. Una volta completata questa configurazione, il processo di importazione avrà inizio.

Configurazione hardware

Utilizzare il seguente workflow per preparare i collegamenti hardware.

Questi passaggi sono descritti in dettaglio nella guida utente per la funzionalità Remote Storage, disponibile dal centro di documentazione E-Series e SANtricity all' "Panoramica dei volumi storage remoti", e nel "Rapporto tecnico sul sistema storage remoto".

SANtricity Remote Storage Volumes non è attualmente supportato sui sistemi E4000.

Sul sistema storage E-Series:

1. Assicurarsi che ogni controller disponga di una connessione iSCSI al sistema storage remoto. Con questa connessione, il sistema E-Series locale agisce come un iSCSI initiator che può essere configurato come host sul sistema remoto.
2. Crea un volume di destinazione per l'operazione di importazione. Assicurati che il volume abbia una capacità pari o superiore a quella del volume di origine sul sistema storage remoto, abbia una dimensione del blocco corrispondente e non sia mappato. Vedi "Crea volumi".
3. Recupera l'iSCSI Qualified Name (IQN) per il sistema E-Series locale dalla sua interfaccia System Manager. L'IQN verrà utilizzato successivamente per configurare il sistema E-Series locale come host sul sistema storage remoto. In System Manager, vai a: **Settings › System › iSCSI settings › Target IQN**.

Sul sistema storage remoto:

1. Configurare il sistema E-Series locale come host sul sistema remoto, utilizzando il suo IQN. Assicurarsi di impostare il tipo di host appropriato, come segue:
   - Se il sistema remoto è un modello E-Series, vedere "Panoramica degli host e dei cluster di host". Utilizzare un tipo host "Factory Default."
   - Se il sistema remoto è di un altro fornitore, selezionare un tipo di host appropriato in base alle opzioni disponibili.
2. Interrompere tutte le operazioni di I/O, smontare tutti i file system e rimuovere qualsiasi assegnazione a host o applicazioni per il volume di origine.
3. Assegna il volume al nuovo host locale del sistema storage E-Series appena creato.
4. Per il volume di origine selezionato, raccogliere le seguenti informazioni dal sistema storage remoto in modo che sia possibile creare l'importazione:
   - iSCSI Qualified Name (IQN)

- Indirizzo IP iSCSI
- Numero LUN del volume sorgente

Configurazione di System Manager

Utilizzare il seguente flusso di lavoro per creare un oggetto di storage remoto per l'importazione:

1. Utilizzando la procedura guidata Remote Storage nell'interfaccia System Manager, mappare un dispositivo di storage remoto (l'origine per l'importazione dei dati) a un volume di destinazione sul sistema E-Series. Quando si seleziona **Fine**, il processo di importazione ha inizio.
2. Monitora l'importazione dalla finestra di dialogo Visualizza operazioni o dal pannello Operazioni in corso. Se necessario, puoi anche mettere in pausa e riprendere il processo.
3. Facoltativamente, interrompere la connessione tra il volume di origine e il volume di destinazione al termine dell'importazione oppure mantenerla per importazioni future.

Scopri la terminologia relativa all'archiviazione remota nel software SANtricity

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

Termine	Descrizione
IQN	Identificatore iSCSI Qualified Name (IQN), che è un nome univoco per un iSCSI initiator o target.
LUN	Numero di unità logica, utilizzato per identificare un'unità logica che può essere presentata a un host per l'accesso.
sistema storage remoto	Il sistema storage in cui risiedono inizialmente i dati. Il sistema storage remoto può essere un modello E-Series o un sistema di un altro fornitore.
dispositivo di storage remoto	Il dispositivo fisico o logico in cui i dati vengono inizialmente memorizzati sul sistema remoto. In un sistema storage E-Series, questo viene definito "volume".
Oggetto storage remoto	Un oggetto contenente informazioni che consentono al sistema E-Series di identificare e connettersi al sistema storage remoto. Queste informazioni includono l'IQN e gli indirizzi IP del sistema storage remoto. L'oggetto storage remoto rappresenta la comunicazione tra il sistema storage remoto e il sistema E-Series.
Volume di storage remoto	Un volume standard del sistema E-Series che consente l'accesso ai dati a un dispositivo di storage remoto.
Volume	Un container in cui vengono memorizzati i dati. È il componente logico creato affinché l'host possa accedere ai dati.

Scopri i requisiti della funzionalità Remote Storage nel software SANtricity

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

Protocolli supportati

Sono supportati i seguenti protocolli:

- iSCSI
- IPv4

Per informazioni aggiornate sul supporto e la configurazione di E-Series, consultare la "Tool NetApp Interoperability Matrix".

Requisiti hardware

Il sistema storage E-Series deve includere:

- Due controller (duplex mode)
- Connessioni iSCSI per entrambi i controller E-Series per comunicare con il sistema storage remoto tramite una o più connessioni iSCSI
- SANtricity OS 11.71 o superiore
- Funzione Remote Storage abilitata nel Submodel ID (SMID)

Il sistema remoto può essere un sistema storage E-Series o un sistema di un altro fornitore. Deve includere:

- Interfacce compatibili con iSCSI

Restrizioni

La funzionalità di archiviazione remota presenta le seguenti limitazioni:

- Il mirroring deve essere disabilitato.
- Il volume di destinazione sul sistema E-Series non deve avere Snapshot.
- Il volume di destinazione sul sistema E-Series non deve essere mappato a nessun host prima dell'inizio dell'importazione.
- Il volume di destinazione sul sistema E-Series deve avere la gestione delle risorse disabilitata.
- La mappatura diretta del volume di storage remoto a un host o a più host non è supportata.
- Web Services Proxy non è supportato.
- I segreti CHAP iSCSI non sono supportati.
- SMcli non è supportato.
- VMware Datastore non è supportato.
- Solo un sistema storage nella coppia relazione/import può essere aggiornato alla volta quando è presente una coppia di import.

Scopri i requisiti dei volumi di storage remoto nel software SANtricity

I volumi utilizzati per le importazioni devono soddisfare i requisiti relativi a dimensioni, stato e altri criteri.

Volume di storage remoto

Il volume di origine di un'importazione è chiamato "remote storage volume". Questo volume deve soddisfare i

seguenti criteri:

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

Dopo l'inizio dell'importazione, il firmware del controller crea in background un volume di storage remoto. 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.

Dopo la creazione, il volume di storage remoto viene trattato come qualsiasi altro volume standard sul sistema E-Series, con le seguenti eccezioni:

- Possono essere utilizzati come proxy per il dispositivo di storage remoto.
- Non possono essere utilizzati come candidati per altre copie di volume o Snapshot.
- Non è possibile modificare l'impostazione Data Assurance mentre l'importazione è in corso.
- Non possono essere mappati su alcun host, perché sono riservati esclusivamente all'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 remoti. Il volume di storage remoto viene identificato in modo univoco utilizzando una combinazione dei seguenti elementi:

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

Candidati 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 pari o superiore al volume di storage remoto.
- Deve avere una dimensione del blocco uguale a quella del volume storage remoto.
- Deve avere uno stato valido (ottimale).
- Non è possibile avere nessuna delle seguenti relazioni: copia del volume, copie Snapshot, mirroring asincrono o sincrono.
- Non deve essere in corso alcuna operazione di riconfigurazione: Dynamic Volume Expansion, Dynamic Capacity Expansion, Dynamic Segment Size, Dynamic RAID Migration, Dynamic Capacity Reduction o Defragmentation.
- Non può essere mappato a un host prima che l'importazione inizi (tuttavia, può essere mappato dopo che l'importazione è stata completata).
- Impossibile avere Flash Read Cached (FRC) abilitato.

System Manager verifica automaticamente questi requisiti nell'ambito della procedura guidata Import Remote Storage. Solo i volumi che soddisfano tutti i requisiti vengono visualizzati per la selezione del volume di destinazione.

Gestire l’archiviazione remota

Importa storage remoto in SANtricity System Manager

Per avviare un’importazione dello storage da un sistema remoto a un sistema storage E-Series, utilizzare la procedura guidata Import Remote Storage.

Prima di iniziare

- Il sistema storage E-Series deve essere configurato per comunicare con il sistema storage remoto.

> La configurazione hardware è descritta nella guida utente per la funzionalità Remote Storage, disponibile presso il centro di documentazione E-Series e SANtricity all’indirizzo "Configura l’hardware", e in "Rapporto tecnico sul sistema storage remoto".

- Per il sistema storage remoto, raccogli le seguenti informazioni:
  - IQN iSCSI
  - Indirizzi IP iSCSI
  - Numero LUN del dispositivo di storage remoto (volume di origine)
- Per il sistema storage E-Series locale, creare o selezionare un volume da utilizzare per l’importazione dei dati. Vedere "Crea volumi". Il volume di destinazione deve soddisfare i seguenti requisiti:
  - Corrisponde alla dimensione del blocco del dispositivo di storage remoto (il volume di origine).
  - Ha una capacità pari o superiore a quella del dispositivo di storage remoto.
  - Ha uno stato di Optimal ed è disponibile.

Per un elenco completo dei requisiti, vedere "Requisiti dei volumi dello storage remoto".

- **Consigliato:** Eseguire il backup dei volumi sul sistema storage remoto prima di avviare il processo di importazione.

Informazioni su questa attività

In questa procedura, si crea una mappatura tra il dispositivo di storage remoto e un volume sul sistema storage E-Series locale. Quando si termina la configurazione, l’importazione inizia.

> Poiché numerose variabili possono influire sull’operazione di importazione e sui tempi di completamento, si consiglia di eseguire prima delle importazioni “test” di dimensioni ridotte. Utilizzate questi test per assicurarvi che tutte le connessioni funzionino come previsto e che l’operazione di importazione si completi in un tempo adeguato.

Passaggi

1. Selezionare **Storage › Remote storage**.
2. Fai clic su **Import Remote Storage**.

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

3. Nel **Passaggio 1a** del pannello Configura origine, immettere le informazioni di connessione. 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**.

Dettagli del campo

Impostazione	Descrizione
Nome	Inserisci un nome per il dispositivo di storage remoto per identificarlo nell'interfaccia System Manager. Un nome può contenere fino a 30 caratteri e può includere solo lettere, numeri e i seguenti caratteri speciali: trattino basso (_), trattino (-) e cancelletto (#). Un nome non può contenere spazi.
Proprietà della connessione iSCSI	Inserire le proprietà di connessione del dispositivo di storage remoto: • **iSCSI Qualified Name (IQN)**: Inserire l'iSCSI IQN. • **Indirizzo IP**: Inserisci l'indirizzo IPv4. • **Porta**: Inserire il numero di porta da utilizzare per le comunicazioni tra i dispositivi di origine e di destinazione. Il numero di porta predefinito è 3260.

Dopo aver fatto clic su **Avanti**, viene visualizzato il **Passaggio 1b** del pannello Configure Source.

4. Nel campo **LUN**, selezionare il numero LUN del dispositivo di storage remoto da utilizzare come origine, quindi fare clic su **Avanti**.

   Si apre il pannello 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 del blocco, della capacità o della disponibilità del volume.

5. Dalla tabella, selezionare un volume di destinazione sul sistema storage E-Series. Se necessario, utilizzare il cursore per modificare la priorità di importazione. Fare clic su **Avanti**. Confermare l'operazione nella finestra di dialogo successiva digitando `continue`, e quindi facendo clic su **Continua**.

   Se il volume di destinazione ha una capacità maggiore rispetto al 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 al termine dell'operazione di importazione e dopo la disconnessione.

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

6. Dal pannello Review, verifica che le impostazioni siano corrette, quindi fai clic su **Finish** per avviare l'importazione.

   Si apre un'altra finestra di dialogo che chiede se si desidera avviare un'altra importazione.

7. Se necessario, fai clic su **Sì** per creare un'altra importazione di storage remoto. Facendo clic su **Sì** si torna al **Passaggio 1a** del pannello Configura origine, dove puoi selezionare la configurazione esistente o aggiungerne una nuova. Se non vuoi creare un'altra importazione, fai 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 sul volume di destinazione durante questo processo, tali nuovi dati vengono propagati al dispositivo remoto (source volume).

8. Visualizza l'avanzamento dell'operazione nella finestra di dialogo Visualizza operazioni nel pannello Remote Storage.

Risultati

Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del sistema storage remoto, dall'impostazione della priorità per l'importazione e dal carico di I/O su entrambi i sistemi storage e sui relativi volumi.

Una volta completata l'importazione, il volume locale è una copia del dispositivo di storage remoto.

Dopo aver finito

Quando sei pronto a interrompere la relazione tra i due volumi, seleziona **Disconnetti** sull'oggetto di importazione dalla vista Operations In Progress. Una volta disconnessa la relazione, le prestazioni del volume locale tornano alla normalità e non sono più influenzate dalla connessione remota.

Gestire l'avanzamento delle importazioni dello storage remoto in SANtricity System Manager

Dopo l'inizio del processo di importazione, puoi visualizzarne l'avanzamento e intervenire su di esso.

Informazioni su questa attività

Per ogni operazione di importazione, la finestra di dialogo 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 possibile visualizzare le operazioni in corso anche dalla pagina Home (**Home › Show operations in progress**).

Passaggi

1. Dalla pagina Remote Storage, selezionare **View Operations**.

   Viene visualizzata la finestra di dialogo Operations in Progress.

2. Se lo si desidera, utilizzare i collegamenti nella colonna **Azioni** per interrompere e riprendere, cambiare la priorità o disconnettersi da un'operazione.
   - **Modifica priorità** — Seleziona **Modifica priorità** per modificare la priorità di elaborazione di un'operazione in corso o in sospeso. Applica una priorità all'operazione e poi fai clic su **OK**.
   - **Interrompi** — Seleziona **Interrompi** per mettere in pausa la copia dei dati dal dispositivo di storage remoto. La relazione tra la coppia di importazione rimane intatta ed è possibile selezionare **Riprendi** quando si è pronti a continuare l'operazione di importazione.
   - **Riprendi** — Seleziona **Riprendi** per iniziare un processo interrotto o non riuscito dal punto in cui si era fermato. Successivamente, applica una priorità all'operazione Riprendi e poi fai clic su **OK**. Questa operazione *non* riavvia l'importazione dall'inizio. Se vuoi riavviare il processo dall'inizio, devi selezionare **Disconnetti** e poi ricreare l'importazione tramite la procedura guidata Import Remote Storage.
   - **Disconnetti** — Seleziona **Disconnetti** per interrompere la relazione tra i volumi di origine e di destinazione per un'operazione di importazione che si è arrestata, completata o non è riuscita.

Modificare le impostazioni di connessione per lo storage remoto in SANtricity System Manager

È possibile modificare, aggiungere o eliminare le impostazioni di connessione per

qualsiasi configurazione dello storage remoto tramite l'opzione Visualizza/Modifica impostazioni.

Informazioni su questa attività

La modifica delle proprietà di connessione influirà sulle importazioni in corso. Per evitare interruzioni, apportare modifiche alle proprietà di connessione solo quando le importazioni non sono in esecuzione.

Passaggi

1. Selezionare **Storage › Remote storage**.
2. Dall'elenco, seleziona l'oggetto storage remoto che desideri modificare.
3. Fai clic su **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Remote Storage Settings.

4. Fai clic sulla scheda **Connection Properties**.

   Vengono visualizzati l'indirizzo IP e le impostazioni della porta configurati per l'importazione dello storage remoto.

5. Eseguire una delle seguenti azioni:
   - **Modifica** — Fare clic su **Modifica** accanto alla voce corrispondente per il remote storage object. Immettere l'indirizzo IP e/o le informazioni sulla porta aggiornate nei campi.
   - **Aggiungi** — Fai clic su **Aggiungi**, quindi inserisci il nuovo indirizzo IP e le informazioni sulla porta nei campi forniti. Fai clic su **Aggiungi** per confermare, quindi la nuova connessione appare nell'elenco degli oggetti di storage remoti.
   - **Elimina** — Seleziona la connessione desiderata dall'elenco e quindi fai clic su **Elimina**. Conferma l'operazione digitando `delete` nel campo apposito e quindi fai clic su **Elimina**. La connessione viene rimossa dall'elenco degli oggetti di storage remoti.
6. Fare clic su **Save**.

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

Rimuovere un oggetto storage remoto in SANtricity System Manager

Al termine di un'importazione, è possibile rimuovere un oggetto di storage remoto se non si desidera più che i dati vengano copiati tra i dispositivi locali e remoti.

Prima di iniziare

Assicurati che non siano presenti importazioni associate all'oggetto di storage remoto che intendi rimuovere.

Informazioni su questa attività

Quando si rimuove un oggetto storage remoto, le connessioni tra i dispositivi locali e remoti vengono rimosse.

Passaggi

1. Selezionare **Storage › Remote storage**.
2. Dall'elenco, seleziona l'oggetto storage remoto che desideri rimuovere.
3. Fai clic su **Remove**.

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

4. Conferma l'operazione digitando `remove` e quindi facendo clic su **Rimuovi**.

   L'oggetto storage remoto selezionato viene rimosso.

Domande frequenti sullo storage remoto per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa devo sapere prima di creare una connessione storage remota?

Per configurare la funzionalità Remote Storage, è necessario connettere direttamente il dispositivo remoto e i sistemi storage di destinazione tramite iSCSI.

Per configurare la connessione di sistema iSCSI, fare riferimento a:

- "Configurare le porte iSCSI"
- "Rapporto tecnico sul sistema storage remoto"

Perché mi viene richiesto di rimuovere i volumi remoti?

Quando raggiunge il numero massimo di volumi remoti, il sistema storage rileva automaticamente eventuali volumi remoti non utilizzati e ti chiede di rimuoverli.

In alcuni casi, i volumi remoti non utilizzati non vengono eliminati durante il processo di creazione. Prima di avviare ulteriori operazioni di importazione, verificare che i sistemi siano ottimali e che le connessioni di rete siano stabili.

Perché non visualizzo tutti i miei volumi sull'array di destinazione?

Quando si configura un'importazione per la funzionalità Remote Storage, è possibile che alcuni volumi non vengano visualizzati nell'elenco dei candidati di destinazione a causa delle dimensioni del blocco, della capacità o della disponibilità del volume.

Per apparire nell'elenco, i candidati volume devono avere:

- Capacità pari o superiore al volume remoto.
- Dimensione del blocco uguale a quella del volume remoto.
- Stato attuale di Optimal.

I volumi candidati sono esclusi dall'elenco se hanno:

- Una delle seguenti relazioni: copia volume, snapshot o mirroring.
- Operazione di riconfigurazione in corso.
- Mappatura verso un altro dispositivo (host o cluster host).
- Lettura cache flash abilitata.

Cosa devo sapere sul volume remoto durante un'importazione?

Quando si utilizza la funzionalità Remote Storage, tenere presente che il volume remoto è la fonte da cui hanno origine i dati.

Durante l'importazione, i dati vengono trasferiti dal volume remoto al volume di destinazione sul sistema storage di destinazione. Questi due volumi devono avere una dimensione di blocco corrispondente.

Cosa devo sapere prima di avviare un'importazione da un sistema storage remoto?

La funzione Remote Storage consente di copiare i dati da un sistema storage remoto a un volume su un sistema storage E-Series. Prima di utilizzare questa funzione, consultare le seguenti linee guida.

Configurazione

Prima di creare l'importazione dello storage remoto, è necessario completare le seguenti azioni e verificare le seguenti condizioni:

- Assicurarsi che ogni controller del sistema storage E-Series disponga di una connessione iSCSI al sistema storage remoto.
- Sul sistema storage E-Series locale, crea un volume di destinazione per l'operazione di importazione. Assicurati che il volume abbia una capacità pari o superiore a quella del volume di origine, abbia una dimensione del blocco che corrisponde a quella del volume di origine e non sia mappato. Vedi "Crea volumi".
- Configura il sistema storage E-Series come host sul sistema remoto utilizzando il suo iSCSI Qualified Name (IQN). Puoi visualizzare l'IQN da **Settings › System › iSCSI settings › Target IQN**. Assicurati inoltre di impostare il tipo di host appropriato in base al sistema in uso.
- Interrompere tutte le operazioni di I/O, smontare tutti i file system e rimuovere tutte le assegnazioni a host o applicazioni per il volume selezionato sul sistema storage remoto.
- Assegna il volume al sistema storage remoto al nuovo host del sistema storage E-Series locale.
- Raccogli le seguenti informazioni dal sistema storage remoto per poter creare l'importazione:
  - iSCSI Qualified Name (IQN)
  - Indirizzo IP iSCSI
  - Il numero LUN del dispositivo di storage remoto, da cui provengono i dati di origine
- Una volta avviato il processo di importazione, l'intero volume di destinazione locale viene sovrascritto con i dati copiati. Tutti i nuovi dati scritti sul volume di destinazione locale vengono propagati al volume sul dispositivo di storage remoto dopo la creazione dell'importazione. Pertanto, si consiglia di eseguire il backup dei volumi sul sistema storage remoto prima di avviare il processo di importazione.

processo di importazione

I seguenti passaggi descrivono il processo di importazione.

1. Accedere all'interfaccia di System Manager e quindi andare alla pagina **Remote Storage**. Selezionare **Import** per avviare una nuova creazione di importazione. Per istruzioni dettagliate, vedere "Importa storage remoto".

   Se si desidera eseguire un'importazione offline, non mappare il volume di destinazione fino al completamento dell'importazione.

2. Monitorare l'avanzamento dell'importazione.

   Una volta avviata l'importazione, il volume di destinazione può essere mappato. Il tempo necessario per completare l'operazione di importazione dipende dalle dimensioni del dispositivo di storage remoto (volume di origine), dall'impostazione della priorità per l'importazione e dal carico di I/O sia sui sistemi storage che sui relativi volumi.

Al termine dell'importazione, il volume di destinazione è un duplicato del volume di origine.

3. Quando sei pronto a interrompere la relazione di mappatura, esegui un **Disconnect** sull'oggetto di importazione dal pannello **Operations In Progress**.

Una volta disconnessa l'importazione, le prestazioni della destinazione locale tornano alla normalità e non sono più influenzate dalla connessione remota.

Restrizioni

La funzionalità di archiviazione remota presenta le seguenti limitazioni:

- Il mirroring deve essere disabilitato.
- Il volume di destinazione sul sistema E-Series non deve avere Snapshot.
- Il volume di destinazione sul sistema E-Series non deve essere mappato a nessun host prima dell'inizio dell'importazione.
- Il volume di destinazione sul sistema E-Series deve avere la gestione delle risorse disabilitata.
- La mappatura diretta del volume di storage remoto a un host o a più host non è supportata.
- Web Services Proxy non è supportato.
- I segreti CHAP iSCSI non sono supportati.
- SMcli non è supportato.
- VMware Datastore non è supportato.
- Solo un sistema storage nella coppia relazione/import può essere aggiornato alla volta quando è presente una coppia di import.

Informazioni aggiuntive

Ulteriori informazioni sulla funzionalità Remote Storage sono disponibili da "Rapporto tecnico sul sistema storage remoto".

Componenti hardware

Visualizza e gestisci i componenti hardware in SANtricity System Manager

È possibile verificare lo stato dei componenti nella pagina Hardware ed eseguire alcune funzioni relative a quei componenti.

Quali componenti posso gestire?

È possibile verificare lo stato dei componenti ed eseguire alcune funzioni relative a questi componenti:

- **Ripiani** — Un *ripiano* è un componente che contiene l'hardware per l'array di storage (controller, power/fan canisters e drive). I ripiani sono disponibili in tre dimensioni per ospitare fino a 12, 24 o 60 drive.
- **Controller** — Un *controller* è l'insieme di hardware e firmware che implementa le funzioni di array di storage e di gestione. Include la memoria cache, il supporto per le unità e le porte per le connessioni host.
- **Unità** — Un'unità può essere un disco rigido (HDD) o un'unità a stato solido (SSD). A seconda delle dimensioni dello shelf, è possibile installare fino a 12, 24 o 60 unità.

Per saperne di più:

- "Pagina hardware"
- "Terminologia hardware"

Come posso visualizzare i componenti hardware?

Accedete alla pagina Hardware, che fornisce una rappresentazione grafica dei componenti fisici dell'array di storage. Potete passare dalla visualizzazione anteriore a quella posteriore degli alloggiamenti dell'array selezionando la scheda **Drives** o **Controllers** in alto a destra nella visualizzazione degli alloggiamenti.

Per saperne di più:

- "Visualizza lo stato e le impostazioni dei componenti dello shelf"
- "Visualizza le impostazioni del controller"
- "Visualizza lo stato e le impostazioni dell'unità"

Informazioni correlate

Scopri di più sui concetti relativi all'hardware:

- "Stati del controller"
- "Stati dei dischi"
- "Protezione contro la perdita di shelf e protezione contro la perdita di drawer"

Concetti

Pagina hardware e componenti di SANtricity System Manager

La pagina Hardware fornisce una rappresentazione grafica dei componenti fisici dell'array di storage. Da qui è possibile verificare lo stato dei componenti ed eseguire alcune funzioni relative a tali componenti.

Shelf di espansione

Uno shelf è un componente che contiene l'hardware per lo storage array (controller, power/fan canister e drive). Esistono due tipi di shelf:

- **Shelf dei controller** — Contiene i drive, i contenitori di alimentazione/ventole e i controller.
- **Drive shelf** (o **shelf di espansione**) — Contiene unità disco, alloggiamenti per ventole/alimentazione e due moduli di input/output (IOM). Gli IOM, noti anche come moduli di servizio ambientale (ESM), includono porte SAS che collegano il drive shelf al controller shelf.

Sono disponibili shelf in tre dimensioni per ospitare fino a 12, 24 o 60 drive. Ogni shelf include un numero ID, che viene assegnato dal firmware del controller. L'ID appare in alto a sinistra nella vista dello shelf.

La visualizzazione dello shelf nella pagina Hardware mostra i componenti anteriori o posteriori. Puoi passare da una visualizzazione all'altra selezionando le schede **Drives** o **Controller** in alto a destra della visualizzazione dello shelf. Puoi anche selezionare **Show all front** o **Show all back** in fondo alla pagina. Le visualizzazioni anteriore e posteriore mostrano quanto segue:

- **Componenti anteriori** — Unità disco e alloggiamenti vuoti per unità disco.
- **Componenti posteriori** — Controller e contenitori di alimentazione/ventola (per controller shelves) oppure IOM e contenitori di alimentazione/ventola (per drive shelves).

È possibile eseguire le seguenti operazioni relative agli shelf di espansione:

- Accendi la luce di localizzazione dello shelf, in modo da poter individuare la posizione fisica dello shelf all'interno dell'armadio o del rack.
- Modifica il numero ID visualizzato nell'angolo in alto a sinistra della vista shelf.
- Visualizza le impostazioni dello shelf, come i tipi di drive installati e il numero di serie.
- Sposta le visualizzazioni degli shelf verso l'alto o verso il basso per adattarle alla disposizione fisica nello storage array.

Controllori

Un controller è l'insieme di hardware e firmware che implementa le funzioni di array di storage e di gestione. Include la cache, il supporto per i dischi e il supporto per l'interfaccia verso gli host.

È possibile eseguire le seguenti funzioni relative ai controller:

- Configura le porte di gestione per indirizzi IP e velocità.
- Configura le connessioni host iSCSI (se disponi di host iSCSI).
- Configura un server Network Time Protocol (NTP) e un server Domain Name System (DNS).
- Visualizza stato e impostazioni del controller.
- Consenti agli utenti dall'esterno della rete locale di avviare una sessione SSH e modificare le impostazioni del controller.
- Posizionare il controller offline, online o in modalità service.

Dischi

Il sistema di archiviazione può includere hard disk drive (HDD) o solid state drive (SSD). A seconda delle dimensioni dello shelf, è possibile installare fino a 12, 24 o 60 drive nello shelf.

È possibile eseguire le seguenti funzioni relative ai dischi:

- Accendi la spia di localizzazione del disco, in modo da poter individuare la posizione fisica del disco nello shelf.
- Visualizza lo stato e le impostazioni del disco.
- Riassegnare un disco (sostituire logicamente un disco guasto con un disco non assegnato) e, se necessario, ricostruire manualmente il disco.
- Contrassegna manualmente un drive per poterlo sostituire. (Contrassegnare un drive consente di copiarne il contenuto prima di sostituirlo.)
- Assegna o revoca l'assegnazione degli hot spare.
- Cancella le unità.

Scopri la terminologia hardware utilizzata nel software SANtricity

I seguenti termini hardware si applicano agli array di storage.

Terminologia generale relativa all'hardware:

Componente	Descrizione
Baia	Un alloggiamento è uno slot nello shelf in cui viene installato un drive o un altro componente.
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i drive e implementa le funzioni di System Manager.
shelf del controller	Uno shelf di controllo contiene un set di dischi e uno o più controller canister. Un controller canister contiene i controller, le schede di interfaccia verso gli host (HIC) e le batterie.
Unità	Un'unità disco è un dispositivo elettromeccanico o un dispositivo di memoria a stato solido che fornisce lo storage fisico per i dati.
Shelf di dischi	Uno shelf di dischi, detto anche shelf di espansione, contiene un insieme di dischi e due moduli di input/output (IOM). Gli IOM contengono porte SAS che collegano uno shelf di dischi a uno shelf controller o ad altri shelf di dischi.
IOM (ESM)	Un IOM è un modulo di input/output che include porte SAS per collegare lo shelf di dischi allo shelf di controller. Nei modelli di controller precedenti, l'IOM era denominato environmental service module (ESM).
Contenitore di alimentazione/ventola	Un power/fan canister è un'unità che si inserisce in uno shelf. Include un alimentatore e una ventola integrata.
SFP	Un SFP è un ricetrasmettitore Small Form-factor Pluggable (SFP).
Shelf	Un shelf è un contenitore installato in un cabinet o rack. Contiene i componenti hardware per lo storage array. Esistono due tipi di shelf: uno shelf controller e uno shelf drive. Uno shelf controller include controller e drive. Uno shelf drive include moduli di input/output (IOM) e drive.
matrice di archiviazione	Un array di storage comprende gli shelf, i controller, i drive, il software e il firmware.

Termini del controller:

Componente	Descrizione
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i drive e implementa le funzioni di System Manager.
shelf del controller	Uno shelf di controllo contiene un set di dischi e uno o più controller canister. Un controller canister contiene i controller, le schede di interfaccia verso gli host (HIC) e le batterie.
DHCP	Dynamic Host Configuration Protocol (DHCP) è un protocollo utilizzato nelle reti Internet Protocol (IP) per distribuire dinamicamente i parametri di configurazione della rete, come gli indirizzi IP.
DNS	Il Domain Name System (DNS) è un sistema di denominazione per i dispositivi connessi a Internet o a una rete privata. Il DNS server mantiene una directory di nomi di dominio e li traduce in indirizzi Internet Protocol (IP).
Configurazioni duplex	La configurazione duplex prevede due moduli controller all'interno dell'array di storage. I sistemi duplex sono completamente ridondanti per quanto riguarda controller, percorsi dei volumi logici e percorsi dei dischi. Se un controller si guasta, l'altro controller assume la gestione delle operazioni di I/O per mantenere la disponibilità. I sistemi duplex dispongono inoltre di ventole e alimentatori ridondanti.
Connessioni full-duplex / half-duplex	Full-duplex e half-duplex si riferiscono alle modalità di connessione. In modalità full-duplex, due dispositivi possono comunicare simultaneamente in entrambe le direzioni. In modalità half-duplex, i dispositivi possono comunicare in una direzione alla volta (un dispositivo invia un messaggio, mentre l'altro dispositivo lo riceve).
HIC	Una scheda di interfaccia verso gli host (HIC) può essere installata facoltativamente all'interno di un contenitore del controller. Le porte host integrate nel controller sono chiamate porte host baseboard. Le porte host integrate nella HIC sono chiamate porte HIC.
Risposta ICMP PING	Internet Control Message Protocol (ICMP) è un protocollo utilizzato dai sistemi operativi dei computer in rete per inviare messaggi. I messaggi ICMP determinano se un host è raggiungibile e quanto tempo impiegano i pacchetti per andare e tornare da tale host.
indirizzo MAC	Gli identificatori di controllo dell'accesso al mezzo (indirizzi MAC) vengono utilizzati da Ethernet per distinguere tra canali logici separati che collegano due porte sulla stessa interfaccia di rete di trasporto fisica.
client di management	Un client di gestione è il computer su cui è installato un browser per accedere a System Manager.

Componente	Descrizione
MTU	Una Maximum Transmission Unit (MTU) è la dimensione massima del pacchetto o del frame che può essere inviato in una rete.
NTP	Network Time Protocol (NTP) è un protocollo di rete per la sincronizzazione del clock tra sistemi informatici in reti dati.
Configurazioni simplex	Simplex è una configurazione a modulo controller singolo all'interno dell'array di storage. Un sistema simplex non offre ridondanza del controller o del percorso del disco, ma dispone di ventole e alimentatori ridondanti.
VLAN	Una virtual local area network (VLAN) è una rete logica che si comporta come se fosse fisicamente separata dalle altre reti supportate dagli stessi dispositivi (switch, router, ecc.).

Termini dei dischi:

Componente	Descrizione
DA	Data Assurance (DA) è una funzionalità che verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati dai controller alle unità. Data Assurance può essere abilitata a livello di pool o di gruppo di volumi, con host che utilizzano un'interfaccia I/O compatibile con DA, come Fibre Channel.
Funzione di sicurezza dell'unità	Drive Security è una funzionalità dell'array di storage che fornisce un ulteriore livello di sicurezza con unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Quando queste unità vengono utilizzate con la funzionalità Drive Security, richiedono una chiave di sicurezza per accedere ai loro dati. Quando le unità vengono rimosse fisicamente dall'array, non possono funzionare finché non vengono installate in un altro array; a quel punto, saranno in uno stato Security Locked finché non viene fornita la chiave di sicurezza corretta.
Shelf di dischi	Uno shelf di dischi, detto anche shelf di espansione, contiene un insieme di dischi e due moduli di input/output (IOM). Gli IOM contengono porte SAS che collegano uno shelf di dischi a uno shelf controller o ad altri shelf di dischi.
DULBE	Deallocated or Unwritten Logical Block Error (DULBE) è un'opzione sulle unità NVMe che consente all'array di storage EF300 o EF600 di supportare volumi con resource provisioning.
Unità FDE	Le unità Full Disk Encryption (FDE) eseguono la crittografia sul disco a livello hardware. Il disco rigido contiene un chip ASIC che crittografa i dati durante la scrittura e li decrittografa durante la lettura.
Unità FIPS	Le unità FIPS utilizzano i Federal Information Processing Standards (FIPS) 140-2 livello 2. Sono essenzialmente unità FDE che rispettano gli standard del governo degli Stati Uniti per garantire algoritmi e metodi di crittografia robusti. Le unità FIPS hanno standard di sicurezza più elevati rispetto alle unità FDE.
HDD	I dischi rigidi (HDDs) sono dispositivi di archiviazione dati che utilizzano piatti metallici rotanti con un rivestimento magnetico.
Unità hot spare	Gli hot spare fungono da unità di standby nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Sono unità perfettamente funzionanti che non contengono dati. Se un'unità si guasta nel gruppo di volumi, il controller ricostruisce automaticamente i dati dall'unità guasta su un hot spare.
NVMe	Non-Volatile Memory Express (NVMe) è un'interfaccia progettata per dispositivi di archiviazione basati su memoria flash, come le unità SSD. NVMe riduce l'I/O overhead e include miglioramenti delle performance rispetto alle precedenti interfacce per dispositivi logici.

Componente	Descrizione
SAS	Serial Attached SCSI (SAS) è un protocollo seriale punto-punto che collega i controller direttamente alle unità disco.
unità compatibili con la sicurezza	Le unità secure-capable possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS), che crittografano i dati durante la scrittura e li decrittografano durante la lettura. Queste unità sono considerate secure-*capable* perché possono essere utilizzate per una sicurezza aggiuntiva tramite la funzionalità Drive Security. Se la funzionalità Drive Security è abilitata per i gruppi di volumi e i pool utilizzati con queste unità, le unità diventano secure-*enabled*.
Unità con protezione abilitata	Le unità secure-enabled vengono utilizzate con la funzionalità Drive Security. Quando si abilita la funzionalità Drive Security e la si applica a un pool o a un gruppo di volumi su unità secure-capable, le unità diventano secure-enabled. L'accesso in lettura e scrittura è disponibile solo tramite un controller configurato con la chiave di sicurezza corretta. Questa maggiore sicurezza impedisce l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage.
SSD	Le unità a stato solido (SSD) sono dispositivi di archiviazione dati che utilizzano memoria a stato solido (flash) per memorizzare i dati in modo permanente. Le SSD emulano i dischi rigidi tradizionali e sono disponibili con le stesse interfacce che i dischi rigidi utilizzano.

Termini iSCSI:

Termine	Descrizione
CHAP	Il metodo Challenge Handshake Authentication Protocol (CHAP) convalida l'identità dei target e degli initiator durante la fase iniziale della connessione. L'autenticazione si basa su una chiave di sicurezza condivisa chiamata CHAP_secret_.
Controller	Un controller è costituito da una scheda, firmware e software. Controlla i drive e implementa le funzioni di System Manager.
DHCP	Dynamic Host Configuration Protocol (DHCP) è un protocollo utilizzato nelle reti Internet Protocol (IP) per distribuire dinamicamente i parametri di configurazione della rete, come gli indirizzi IP.
IB	InfiniBand (IB) è uno standard di comunicazione per la trasmissione di dati tra server dalle performance elevate e sistemi di archiviazione.
Risposta ICMP PING	Internet Control Message Protocol (ICMP) è un protocollo utilizzato dai sistemi operativi dei computer in rete per inviare messaggi. I messaggi ICMP determinano se un host è raggiungibile e quanto tempo impiegano i pacchetti per andare e tornare da tale host.
IQN	Un identificatore iSCSI Qualified Name (IQN) è un nome univoco per un iSCSI initiator o iSCSI target.
iSER	iSCSI Extensions for RDMA (iSER) è un protocollo che estende il protocollo iSCSI per il funzionamento su trasporti RDMA, come InfiniBand o Ethernet.
iSNS	Internet Storage Name Service (iSNS) è un protocollo che consente la discovery automatica, la gestione e la configurazione di dispositivi iSCSI e Fibre Channel su reti TCP/IP.
indirizzo MAC	Gli identificatori di controllo dell'accesso al mezzo (indirizzi MAC) vengono utilizzati da Ethernet per distinguere tra canali logici separati che collegano due porte sulla stessa interfaccia di rete di trasporto fisica.
Client di gestione	Un client di gestione è il computer su cui è installato un browser per accedere a System Manager.
MTU	Una Maximum Transmission Unit (MTU) è la dimensione massima del pacchetto o del frame che può essere inviato in una rete.
RDMA	Remote Direct Memory Access (RDMA) è una tecnologia che consente ai computer di una rete di scambiare dati nella memoria principale senza coinvolgere il sistema operativo di nessuno dei due computer.

Termine	Descrizione
Sessione di discovery senza nome	Quando l’opzione per le sessioni di discovery senza nome è abilitata, gli iSCSI initiator non sono tenuti a specificare l’IQN del target per recuperare le informazioni del controller.

Termini NVMe:

Termine	Descrizione
InfiniBand	InfiniBand (IB) è uno standard di comunicazione per la trasmissione di dati tra server dalle performance elevate e sistemi di archiviazione.
Spazio dei nomi	Un namespace è una memoria NVM formattata per l'accesso a blocchi. È analogo a un'unità logica in SCSI, che corrisponde a un volume nell'array di storage.
ID dello spazio dei nomi	L'ID dello spazio dei nomi è l'identificativo univoco del controller NVMe per lo spazio dei nomi e può essere impostato su un valore compreso tra 1 e 255. È analogo a un numero di unità logica (LUN) in SCSI.
NQN	NVMe Qualified Name (NQN) viene utilizzato per identificare il target di storage remoto (l'array di storage).
NVM	La memoria non volatile (NVM) è una memoria persistente utilizzata in molti tipi di dispositivi di archiviazione.
NVMe	Non-Volatile Memory Express (NVMe) è un'interfaccia progettata per dispositivi di archiviazione basati su memoria flash, come le unità SSD. NVMe riduce l'I/O overhead e include miglioramenti delle performance rispetto alle precedenti interfacce per dispositivi logici.
NVMe-oF	Non-Volatile Memory Express over Fabrics (NVMe-oF) è una specifica che consente ai comandi e ai dati NVMe di essere trasferiti su una rete tra un host e uno storage.
controller NVMe	Un controller NVMe viene creato durante il processo di connessione dell'host. Fornisce un percorso di accesso tra un host e i namespace nell'array di storage.
coda NVMe	Una coda viene utilizzata per trasmettere comandi e messaggi tramite l'interfaccia NVMe.
sottosistema NVMe	L'array di storage con una connessione host NVMe.
RDMA	L'accesso diretto alla memoria remota (RDMA) consente uno spostamento dei dati più diretto da e verso un server implementando un protocollo di trasporto nell'hardware della scheda di interfaccia di rete (NIC).
RoCE	RDMA over Converged Ethernet (RoCE) è un protocollo di rete che consente l'accesso diretto alla memoria remota (RDMA) su una rete Ethernet.

Termine	Descrizione
SSD	Le unità a stato solido (SSD) sono dispositivi di archiviazione dati che utilizzano memoria a stato solido (flash) per memorizzare i dati in modo permanente. Le SSD emulano i dischi rigidi tradizionali e sono disponibili con le stesse interfacce che i dischi rigidi utilizzano.

Gestisci i componenti dello shelf

Visualizza i componenti hardware in SANtricity System Manager

La pagina Hardware offre funzioni di ordinamento e filtro che rendono più facile trovare i componenti.

Passaggi

1. Seleziona **Hardware**.
2. Utilizzare le funzioni descritte nella tabella seguente per visualizzare i componenti hardware.

Funzione	Descrizione
Viste di dischi, controller e componenti	Per passare dalla visualizzazione anteriore a quella posteriore del ripiano, selezionare **Unità** o **Controller e componenti** dall'estrema destra (il collegamento visualizzato dipende dalla visualizzazione corrente). La visualizzazione **Unità** mostra le unità e gli alloggiamenti vuoti per le unità. La visualizzazione **Controller e componenti** mostra i controller, e gli eventuali moduli IOM (ESM), i contenitori di alimentazione/ventole o gli alloggiamenti vuoti per i controller. In fondo alla pagina, è anche possibile selezionare **Mostra tutte le unità**.
Filtri di visualizzazione dell'unità	Se l'array di storage contiene unità con diversi tipi di attributi fisici e logici, la pagina **Hardware** include filtri per la visualizzazione delle unità. Questi campi filtro consentono di individuare rapidamente unità specifiche limitando i tipi di unità visualizzati nella pagina. In **Mostra unità che sono…**, fai clic sul campo filtro a sinistra (per impostazione predefinita, mostra **Qualsiasi tipo di unità**) per visualizzare un elenco a discesa di attributi fisici (ad esempio, capacità e velocità). Fai clic sul campo filtro a destra (per impostazione predefinita, mostra **Ovunque nell'array di storage**) per visualizzare un elenco a discesa di attributi logici (ad esempio, assegnazione al gruppo di volumi). Puoi utilizzare questi filtri insieme o separatamente. Se l'array di storage contiene unità che condividono tutte gli stessi attributi fisici, il campo **Qualsiasi tipo di unità** a sinistra non viene visualizzato. Se le unità si trovano tutte nella stessa posizione logica, il campo **Ovunque nell'array di storage** a destra non viene visualizzato.
Legenda	I componenti vengono visualizzati in determinati colori per rappresentare i loro stati di ruolo. Per espandere e comprimere le descrizioni di questi stati, fare clic su **Legend**.

Funzione	Descrizione
Mostra i dettagli dell'icona di stato	Gli indicatori di stato possono includere descrizioni testuali per gli stati di disponibilità. Fai clic su **Mostra dettagli icona di stato** per mostrare o nascondere questo testo di stato.
Scaffale/icone scaffale	Ogni visualizzazione a scaffale fornisce un elenco di comandi correlati, insieme a proprietà e stato. Fai clic su **Shelf** per visualizzare un elenco a discesa di comandi. Puoi anche selezionare una delle icone nella parte superiore per visualizzare stato e proprietà dei singoli componenti: controller, IOM (ESM), alimentatori, ventole, temperatura, batterie e SFP.
Ordine degli shelf	È possibile riorganizzare gli scaffali nella pagina Hardware. Utilizzare le frecce su e giù in alto a destra di ogni visualizzazione dello scaffale per modificare l'ordine superiore/inferiore degli scaffali.

Mostra o nascondi lo stato dei componenti in SANtricity System Manager

È possibile visualizzare le descrizioni dello stato per unità, controller, ventole e alimentatori.

Passaggi

1. Seleziona **Hardware**.
2. Per visualizzare i componenti posteriori o anteriori:
   - Se desideri visualizzare il controller e i componenti del contenitore di alimentazione/ventola, ma vengono visualizzati i dischi, fai clic sulla scheda **Controllers & Components**.
   - Se desideri visualizzare le unità, ma vengono visualizzati i componenti controller e power/fan canister, fai clic sulla scheda **Drives**.
3. Per visualizzare o nascondere le descrizioni di stato dei pop-over:
   - Se desideri visualizzare una descrizione a comparsa delle icone di stato, fai clic su **Mostra dettagli icona di stato** in alto a destra nella vista shelf (seleziona la check box).
   - Per nascondere le descrizioni a comparsa, fai di nuovo clic su **Mostra dettagli icona di stato** (deseleziona la check box).
4. Se desideri visualizzare i dettagli completi dello stato, seleziona il componente nella vista a scaffale e poi seleziona **Visualizza impostazioni**.
5. Se desideri visualizzare le descrizioni dei componenti colorati, seleziona **Legend**.

Visualizza le viste anteriore e posteriore in SANtricity System Manager

La pagina Hardware può mostrare la vista frontale o la vista posteriore delle shelf.

Informazioni su questa attività

La vista posteriore mostra i controller/IOM e gli alloggiamenti power-fan. La vista frontale mostra le unità.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

La grafica cambia per mostrare i controller anziché le unità.

3. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

4. Facoltativamente, puoi selezionare **Mostra tutto il fronte** o **Mostra tutto il retro**, situato in fondo alla pagina.

Modificare l'ordine di visualizzazione degli shelf in SANtricity System Manager

È possibile modificare l'ordine dei ripiani visualizzati nella pagina Hardware per farlo corrispondere all'ordine fisico dei ripiani in un armadio.

Passaggi

1. Seleziona **Hardware**.
2. Dall'angolo in alto a destra di una visualizzazione dello shelf, seleziona le frecce su o giù per riorganizzare l'ordine degli shelf mostrati nella pagina Hardware.

Attivare la spia di localizzazione degli shelf in SANtricity System Manager

Per individuare la posizione fisica di uno shelf mostrato nella pagina Hardware, è possibile accendere la spia di localizzazione dello shelf.

Passaggi

1. Seleziona **Hardware**.
2. Selezionare l'elenco a discesa per il Controller Shelf o il Drive Shelf, quindi selezionare **Turn on locator light**.

   La spia luminosa di localizzazione del ripiano si accende.

3. Quando hai individuato fisicamente lo shelf, torna alla finestra di dialogo e seleziona **Turn off**.

Modificare gli ID degli shelf in SANtricity System Manager

L'ID dello scaffale è un numero che identifica in modo univoco uno scaffale nell'array di storage. Gli scaffali sono numerati consecutivamente, a partire da 00 o 01, in alto a sinistra di ciascuna visualizzazione dello scaffale.

Informazioni su questa attività

Il firmware del controller assegna automaticamente l'ID dello shelf, ma puoi modificare quel numero se vuoi creare uno schema di ordinamento diverso.

Passaggi

1. Seleziona **Hardware**.
2. Selezionare l'elenco a discesa per il Controller Shelf o il Drive Shelf, quindi selezionare **Change ID**.
3. Nella finestra di dialogo Change Shelf ID, seleziona l'elenco a discesa per visualizzare i numeri disponibili.

   Questa finestra di dialogo non visualizza gli ID attualmente assegnati agli shelf attivi.

4. Seleziona un numero disponibile, quindi fai clic su **Salva**.

   A seconda del numero selezionato, l'ordine degli scaffali potrebbe essere modificato nella pagina Hardware. Se desiderato, puoi utilizzare le frecce su/giù in alto a destra di ogni scaffale per riaggiustare l'ordine.

Visualizza lo stato e le impostazioni dei componenti dello shelf in SANtricity System Manager

La pagina Hardware fornisce stato e impostazioni per i componenti dello shelf, inclusi gli alimentatori, le ventole e le batterie.

Informazioni su questa attività

I componenti disponibili dipendono dal tipo di shelf:

- **Ripiano per unità** — Contiene un set di unità, contenitori di alimentazione/ventole, moduli di input/output (IOMs) e altri componenti di supporto in un unico ripiano.
- **Ripiano del controller** — Contiene un set di unità, uno o due controller canisters, power/fan canisters e altri componenti di supporto in un unico ripiano.

Passaggi

1. Seleziona **Hardware**.
2. Seleziona l'elenco a discesa per il Controller Shelf o il Drive Shelf, quindi seleziona **View Settings**.

   Si apre la finestra di dialogo Impostazioni componenti ripiano, con schede che mostrano lo stato e le impostazioni relative ai componenti del ripiano. A seconda del tipo di ripiano selezionato, alcune schede descritte nella tabella potrebbero non essere visualizzate.

Scheda	Descrizione
Shelf	La scheda **Shelf** mostra le seguenti proprietà: • **ID scaffale** — Identifica in modo univoco uno scaffale nell'array di archiviazione. Il firmware del controller assegna questo numero, ma puoi modificarlo selezionando **Scaffale › Cambia ID**. • **Shelf path redundancy** — Specifica se le connessioni tra lo shelf e il controller dispongono di metodi alternativi (Sì) o meno (No). • **Tipi di unità attuali** — Mostra il tipo di tecnologia integrata nelle unità (ad esempio, un'unità SAS che supporta la sicurezza). Se sono presenti più tipi di unità, vengono visualizzate entrambe le tecnologie. • **Numero di serie** — Mostra il numero di serie dello shelf.

Scheda	Descrizione
IOM (ESM)	La scheda **IOM (ESM)** mostra lo stato del modulo di input/output (IOM), chiamato anche modulo di servizio ambientale (ESM). Monitora lo stato dei componenti in un alloggiamento per unità e funge da punto di connessione tra l'alloggiamento delle unità e il controller. Lo stato può essere Ottimale, Failed, Ottimale (Miswire) o Uncertified. Altre informazioni includono la versione del firmware e la versione delle impostazioni di configurazione. Seleziona **Mostra altre impostazioni** per visualizzare le velocità di trasmissione dati massima e attuale e lo stato della comunicazione della scheda (Sì o No). È possibile visualizzare questo stato anche selezionando l'icona IOM, accanto all'elenco a discesa Shelf.
Alimentatori	La scheda **Alimentatori** mostra lo stato del contenitore dell'alimentatore e dell'alimentatore stesso. Lo stato può essere Ottimale, Guasto, Rimosso o Sconosciuto. Mostra anche il numero di parte dell'alimentatore. È possibile visualizzare questo stato anche selezionando l'icona Alimentatore, accanto all'elenco a discesa Shelf.
Ventole	La scheda **Ventole** mostra lo stato del contenitore della ventola e della ventola stessa. Lo stato può essere Ottimale, Guasto, Rimosso o Sconosciuto. È possibile visualizzare questo stato anche selezionando l'icona della ventola, accanto all'elenco a discesa Shelf.
Temperatura	La scheda **Temperatura** mostra lo stato della temperatura dei componenti del ripiano, come i sensori, i controller e le unità di alimentazione/ventilazione. Lo stato può essere Ottimale, Temperatura nominale superata, Temperatura massima superata o Sconosciuto. È possibile visualizzare questo stato anche selezionando l'icona Temperatura, accanto all'elenco a discesa Shelf.
Batterie	La scheda **Batterie** mostra lo stato delle batterie del controller. Lo stato può essere Ottimale, Guasta, Rimossa o Sconosciuto. Altre informazioni includono l'età della batteria, i giorni rimanenti prima della sostituzione, i cicli di apprendimento e le settimane tra un ciclo di apprendimento e l'altro. È possibile visualizzare questo stato anche selezionando l'icona Batterie, accanto all'elenco a discesa Shelf.

Scheda	Descrizione
SFP	La scheda **SFP** mostra lo stato dei ricetrasmettitori Small Form-factor Pluggable (SFP) sui controller. Lo stato può essere Ottimale, Non riuscito o Sconosciuto. Seleziona **Mostra altre impostazioni** per visualizzare il part number, il numero di serie e il vendor degli SFP. È possibile visualizzare questo stato anche selezionando l'icona SFP, accanto all'elenco a discesa Shelf.

3. Fare clic su **Close**.

Aggiorna i cicli di apprendimento della batteria in SANtricity System Manager

Un ciclo di apprendimento è un ciclo automatico per la calibrazione dell'indicatore intelligente della batteria. I cicli sono programmati per avviarsi automaticamente, nello stesso giorno e alla stessa ora, a intervalli di 8 settimane (per controller). Se si desidera impostare una pianificazione diversa, è possibile regolare i cicli di apprendimento.

Informazioni su questa attività

L'aggiornamento dei cicli di apprendimento influisce su entrambe le batterie del controller.

Passaggi

1. Seleziona **Hardware**.
2. Seleziona l'elenco a discesa per la Controller Shelf, quindi seleziona **Visualizza impostazioni**.
3. Seleziona la scheda **batteria**.
4. Seleziona **Aggiorna i cicli di apprendimento della batteria**.

   Si apre la finestra di dialogo Update Battery Learn Cycles.

5. Dai menu a tendina, seleziona un nuovo giorno e un orario.
6. Fare clic su **Save**.

Gestire i controller

Scopri gli stati del controller in SANtricity System Manager

È possibile impostare un controller in tre stati diversi: online, offline e service mode.

Stato online

Lo stato online è il normale stato operativo del controller. Significa che il controller funziona normalmente ed è disponibile per le operazioni di I/O.

Quando si mette un controller online, il suo stato viene impostato su optimal.

Stato offline

Lo stato offline viene in genere utilizzato per preparare un controller alla sostituzione quando sono presenti due controller nell'array di storage. Un controller può entrare nello stato offline in due modi: è possibile emettere un comando esplicito oppure il controller può guastarsi. Un controller può uscire dallo stato offline solo emettendo un altro comando esplicito o sostituendo il controller guasto. È possibile mettere un controller offline solo se sono presenti due controller nell'array di storage.

Quando un controller si trova nello stato offline, si verificano le seguenti condizioni:

- Il controller non è disponibile per I/O.
- Non è possibile gestire l'array di storage tramite quel controller.
- Tutti i volumi attualmente di proprietà di quel controller vengono spostati sull'altro controller.
- Il mirroring della cache è disabilitato e tutti i volumi sono impostati in modalità cache write through.

Modalità di servizio

La Service Mode viene in genere utilizzata solo dal supporto tecnico per spostare tutti i volumi dell'array di storage su un controller, in modo che l'altro controller possa essere diagnosticato. Un controller deve essere messo manualmente in Service Mode e deve essere rimesso manualmente online al termine dell'operazione di servizio.

Quando un controller è in modalità di servizio, si verificano le seguenti condizioni:

- Il controller non è disponibile per I/O.
- Il supporto tecnico può accedere al controller tramite la porta seriale o la connessione di rete per analizzare potenziali problemi.
- Tutti i volumi attualmente di proprietà di quel controller vengono spostati sull'altro controller.
- Il mirroring della cache è disabilitato e tutti i volumi sono impostati in modalità cache write through.

Scopri come viene assegnato l'indirizzo IP ai controller E-Series

Di default, i controller vengono forniti con DHCP abilitato su entrambe le porte di rete. È possibile assegnare indirizzi IP statici, utilizzare gli indirizzi IP statici predefiniti o utilizzare indirizzi IP assegnati tramite DHCP. È anche possibile utilizzare la configurazione automatica stateless IPv6.

> IPv6 è disabilitato per impostazione predefinita sui nuovi controller, ma puoi configurare gli indirizzi IP della porta di gestione utilizzando un metodo alternativo e poi abilitare IPv6 sulle porte di gestione utilizzando System Manager.

Quando la porta di rete si trova nello stato "link down", ovvero disconnessa da una LAN, il sistema segnala la propria configurazione come statica, visualizzando un indirizzo IP di 0.0.0.0 (versioni precedenti), oppure con DHCP abilitato senza alcun indirizzo IP segnalato (versioni successive). Dopo che la porta di rete si trova nello stato "link up" (ovvero connessa a una LAN), tenta di ottenere un indirizzo IP tramite DHCP.

Se il controller non riesce a ottenere un indirizzo DHCP su una determinata porta di rete, torna a un indirizzo IP predefinito, operazione che potrebbe richiedere fino a 3 minuti. Gli indirizzi IP predefiniti sono i seguenti:

```
Controller 1 (port 1): IP Address: 192.168.128.101
```

```
Controller 1 (port 2): IP Address: 192.168.129.101
```

```
Controller 2 (port 1): IP Address: 192.168.128.102
```

```
Controller 2 (port 2): IP Address: 192.168.129.102
```

Quando si assegnano gli indirizzi IP:

- Riservare la porta 2 sui controller per l'utilizzo da parte del Customer Support. Non modificare le impostazioni di rete predefinite (DHCP abilitato).
- Per impostare indirizzi IP statici per i controller E4000, E2800 ed E5700, utilizzare SANtricity System Manager. Per impostare indirizzi IP statici per i controller E2700 ed E5600, utilizzare SANtricity Storage Manager. Dopo che un indirizzo IP statico è stato configurato, rimane impostato attraverso tutti gli eventi di disconnessione/riconnessione del collegamento.
- Per utilizzare il DHCP per assegnare l'indirizzo IP al controller, connettere il controller a una rete in grado di elaborare le richieste DHCP. Utilizzare un lease DHCP permanente.

> Gli indirizzi predefiniti non vengono mantenuti in caso di interruzione della connessione. Quando una porta di rete su un controller è configurata per utilizzare DHCP, il controller tenta di ottenere un indirizzo DHCP a ogni evento di riattivazione della connessione, inclusi inserimenti del cavo, riavvii e cicli di alimentazione. Ogni volta che un tentativo DHCP fallisce, viene utilizzato l'indirizzo IP statico predefinito per quella porta.

Configura la porta di gestione in SANtricity System Manager

Il controller include una porta Ethernet utilizzata per la gestione del sistema. Se necessario, è possibile modificarne i parametri di trasmissione e gli indirizzi IP.

Informazioni su questa attività

Durante questa procedura, si seleziona la porta 1 e si determinano la velocità e il metodo di indirizzamento della porta. La porta 1 si connette alla rete dove il client di gestione può accedere al controller e System Manager.

> Non utilizzare la porta 2 su nessuno dei due controller. La porta 2 è riservata per il supporto tecnico.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller con la porta di gestione che desideri configurare.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Configura porte di gestione**.

   Si apre la finestra di dialogo Configure Management Ports.

5. Assicurati che la porta 1 sia visualizzata, quindi fai clic su **Avanti**.
6. Seleziona le impostazioni della porta di configurazione, quindi fai clic su **Next**.

   Dettagli del campo

Campo	Descrizione
Velocità e duplex mode	Mantieni l'impostazione Auto-negotiate se desideri che System Manager determini i parametri di trasmissione tra l'array di storage e la rete; oppure, se conosci la velocità e la modalità della tua rete, seleziona i parametri dall'elenco a discesa. Solo le combinazioni valide di velocità e duplex mode appaiono nell'elenco.
Abilita IPv4 / Abilita IPv6	Seleziona una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6.

   Se si seleziona **Abilita IPv4**, si apre una finestra di dialogo per la selezione delle impostazioni IPv4 dopo aver fatto clic su **Avanti**. Se si seleziona **Abilita IPv6**, si apre una finestra di dialogo per la selezione delle impostazioni IPv6 dopo aver fatto clic su **Avanti**. Se si selezionano entrambe le opzioni, si apre prima la finestra di dialogo per le impostazioni IPv4 e poi, dopo aver fatto clic su **Avanti**, si apre la finestra di dialogo per le impostazioni IPv6.

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

Dettagli del campo

Campo	Descrizione
Ottieni automaticamente la configurazione dal server DHCP	Seleziona questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Seleziona questa opzione e poi inserisci l'indirizzo IP del controller. (Se desiderato, puoi tagliare e incollare gli indirizzi nei campi.) Per IPv4, includi la subnet mask di rete e il gateway. Per IPv6, includi l'indirizzo IP instradabile e l'indirizzo IP del router. Se si modifica la configurazione dell'indirizzo IP, si perde il percorso di gestione verso l'array di storage. Se si utilizza SANtricity Unified Manager per gestire globalmente gli array nella rete, aprire l'interfaccia utente e andare al **Manage › Discover**. Se si utilizza SANtricity Storage Manager, è necessario rimuovere il dispositivo dalla Enterprise Management Window (EMW), aggiungerlo nuovamente all'EMW selezionando **Edit › Add Storage Array** e quindi immettere il nuovo indirizzo IP.

8. Fare clic su **Fine**.

Risultati

La configurazione della porta di gestione viene visualizzata nelle impostazioni del controller, scheda Management Ports.

Configurare gli indirizzi del server NTP in SANtricity System Manager

È possibile configurare una connessione al server NTP (Network Time Protocol) in modo che il controller interroghi periodicamente il server NTP per aggiornare il proprio orologio interno del tempo.

Prima di iniziare

- È necessario installare e configurare un server NTP nella propria rete.
- È necessario conoscere l'indirizzo del server NTP primario e di un eventuale server NTP di backup. Questi indirizzi possono essere fully qualified domain name, indirizzi IPv4 o indirizzi IPv6.

Se si immettono uno o più domain name per i server NTP, è necessario configurare anche un DNS server per risolvere l'indirizzo del server NTP. È necessario configurare il DNS server solo sui controller in cui è stato configurato NTP e fornito un domain name.

Informazioni su questa attività

NTP consente all'array di storage di sincronizzare automaticamente gli orologi del controller con un host esterno utilizzando Simple Network Time Protocol (SNTP). Il controller interroga periodicamente il server NTP configurato e poi utilizza i risultati per aggiornare il proprio orologio interno. Se solo un controller ha NTP

abilitato, il controller alternativo sincronizza periodicamente il proprio orologio con quello del controller che ha NTP abilitato. Se nessuno dei due controller ha NTP abilitato, i controller sincronizzano periodicamente i propri orologi tra loro.

> Non è necessario configurare NTP su entrambi i controller; tuttavia, farlo migliora la capacità dell'array di storage di rimanere sincronizzato durante guasti hardware o di comunicazione.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller che desideri configurare.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Configura server NTP**.

   Si apre la finestra di dialogo Configure Network Time Protocol (NTP) Server.

5. Seleziona **Voglio abilitare NTP sul Controller** (**A** o **B**).

   Ulteriori selezioni vengono visualizzate nella finestra di dialogo.

6. Seleziona una delle seguenti opzioni:
   - **Ottieni automaticamente gli indirizzi del server NTP dal server DHCP** — Gli indirizzi del server NTP rilevati vengono visualizzati.

     > Se l'array di archiviazione è configurato per utilizzare un indirizzo NTP statico, non vengono visualizzati server NTP.

   - **Specificare manualmente gli indirizzi dei server NTP** — Inserire l'indirizzo del server NTP primario e un indirizzo del server NTP di backup. Il server di backup è facoltativo. (Questi campi relativi agli indirizzi vengono visualizzati dopo aver selezionato il pulsante di opzione.) L'indirizzo del server può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
7. **Facoltativo:** Inserire le informazioni del server e le credenziali per l'autenticazione per un server NTP di backup.
8. Fare clic su **Save**.

Risultati

La configurazione del server NTP viene visualizzata nelle impostazioni del controller, scheda **DNS / NTP**.

Configurare gli indirizzi dei server DNS in SANtricity System Manager

Domain Name System (DNS) viene utilizzato per risolvere fully qualified domain names per i controller e un server NTP (Network Time Protocol). Le porte di gestione sull'array di storage possono supportare simultaneamente i protocolli IPv4 o IPv6.

Prima di iniziare

- È necessario installare e configurare un DNS server nella propria rete.

- Conosci l'indirizzo del DNS server primario e di un eventuale DNS server di backup. Questi indirizzi possono essere indirizzi IPv4 o IPv6.

Informazioni su questa attività

Questa procedura descrive come specificare un indirizzo DNS server primario e uno di backup. Il DNS server di backup può essere configurato facoltativamente per essere utilizzato se un DNS server primario si guasta.

> Se hai già configurato le porte di gestione dell'array di storage con Dynamic Host Configuration Protocol (DHCP) e hai uno o più DNS server o server NTP associati alla configurazione DHCP, allora non è necessario configurare manualmente DNS o NTP. In questo caso, l'array di storage dovrebbe aver già ottenuto automaticamente gli indirizzi dei server DNS/NTP. Tuttavia, dovresti comunque seguire le istruzioni riportate di seguito per aprire la finestra di dialogo e assicurarti che vengano rilevati gli indirizzi corretti.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Selezionare il controller da configurare.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Configure DNS server**.

   Si apre la finestra di dialogo Configura server Domain Name System (DNS).

5. Seleziona una delle seguenti opzioni:
   - **Ottieni automaticamente gli indirizzi del DNS server dal server DHCP** — Gli indirizzi del DNS server rilevati vengono visualizzati.

     > Se l'array di storage è configurato per utilizzare un indirizzo DNS statico, non vengono visualizzati server DNS.

   - **Specificare manualmente gli indirizzi dei DNS server** — Inserire un indirizzo DNS server primario e un indirizzo DNS server di backup. Il DNS server di backup è facoltativo. (Questi campi relativi agli indirizzi vengono visualizzati dopo aver selezionato il pulsante di opzione.) Questi indirizzi possono essere indirizzi IPv4 o IPv6.
6. Fare clic su **Save**.
7. Ripeti questi passaggi per l'altro controller.

Risultati

La configurazione DNS viene visualizzata nelle impostazioni del controller, nella scheda **DNS / NTP**.

Visualizza le impostazioni del controller in SANtricity System Manager

È possibile visualizzare informazioni su un controller, come lo stato delle interfacce verso gli host, delle interfacce delle unità e delle porte di gestione.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Eseguire una delle seguenti azioni per visualizzare le impostazioni del controller:
   - Fai clic sul controller per visualizzare il menu contestuale, quindi seleziona **View settings**.
   - Selezionare l'icona del controller (accanto all'elenco a discesa **Shelf**). Per le configurazioni duplex, selezionare **Controller A** o **Controller B** dalla finestra di dialogo, quindi fare clic su **Next**.

     Si apre la finestra di dialogo Impostazioni controller.

4. Seleziona le schede per spostarti tra le impostazioni delle proprietà.

   Alcune schede hanno un collegamento per **Mostra altre impostazioni** in alto a destra.

Dettagli del campo

Scheda	Descrizione
Base	Mostra lo stato del controller, il nome del modello, il codice del ricambio, la versione corrente del firmware e la versione della memoria statica ad accesso casuale non volatile (NVSRAM).
cache	Mostra le impostazioni della cache del controller, che includono la data cache, la processor cache e il cache backup device. Il cache backup device viene utilizzato per eseguire il backup dei dati nella cache se si perde l'alimentazione al controller. Lo stato può essere Ottimale, Non riuscito, Rimosso, Sconosciuto, Protetto da scrittura o Incompatibile.
Interfacce verso gli host	Mostra le informazioni sull'interfaccia verso gli host e lo stato del collegamento di ciascuna porta. L'interfaccia verso gli host è la connessione tra il controller e l'host, ad esempio Fibre Channel o iSCSI. La scheda di interfaccia verso gli host (HIC) si trova sulla scheda madre o in uno slot (bay). "Baseboard" indica che le porte HIC sono integrate nel controller. Le porte "slot" si trovano sulla HIC opzionale.
Interfacce di unità	Mostra le informazioni sull'interfaccia dell'unità e lo stato del collegamento di ciascuna porta. L'interfaccia dell'unità è la connessione tra il controller e le unità, come SAS.
Porte di gestione	Mostra i dettagli della porta di gestione, come l'host name utilizzato per accedere al controller e se è stato abilitato l'accesso remoto. La porta di gestione collega il controller e il client di gestione, dove è installato un browser per accedere a System Manager.
DNS / NTP	Mostra il metodo di indirizzamento e gli indirizzi IP per il DNS server e il server NTP, se questi server sono stati configurati in System Manager. Il Domain Name System (DNS) è un sistema di denominazione per i dispositivi connessi a Internet o a una rete privata. Il DNS server mantiene una directory di nomi di dominio e li traduce in indirizzi Internet Protocol (IP). Network Time Protocol (NTP) è un protocollo di rete per la sincronizzazione del clock tra sistemi informatici in reti dati.

5. Fare clic su **Close**.

Configura l'accesso remoto (SSH) in SANtricity System Manager

Abilitando l'accesso remoto, si consente agli utenti esterni alla rete locale di avviare una sessione SSH e accedere alle impostazioni del controller.

Per le versioni di SANtricity 11.74 e successive, puoi anche configurare l'autorizzazione multifattore (MFA) richiedendo agli utenti di inserire una chiave SSH e/o una password SSH. Per le versioni di SANtricity 11.73 e precedenti, questa funzionalità *non* include un'opzione per l'autorizzazione multifattore con chiavi SSH e password.

Rischio per la sicurezza — Per motivi di sicurezza, solo il personale di supporto tecnico dovrebbe utilizzare la funzione di accesso remoto.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller per cui desideri configurare l'accesso remoto.

   Viene visualizzato il menu contestuale del controller.

4. Selezionare **Configura accesso remoto (SSH)**. (Per SANtricity versioni 11.73 e precedenti, questa voce di menu è **Modifica accesso remoto**.)

   Si apre la finestra di dialogo per abilitare l'accesso remoto.

5. Seleziona la casella di controllo **Abilita accesso remoto**.

   Questa impostazione consente l'accesso remoto con tre opzioni di autorizzazione:

   - **Solo password**. Per questa opzione, hai finito e puoi cliccare su **Salva**. Se disponi di un sistema duplex, puoi abilitare l'accesso remoto sul secondo controller seguendo i passaggi precedenti.
   - **Chiave SSH o password**. Per questa opzione, procedi al passaggio successivo.
   - **Sia la password che la chiave SSH**. Per questa opzione, selezionare la casella di controllo **Richiedi chiave pubblica e password autorizzate per l'accesso remoto** e procedere al passaggio successivo.

6. Compila il campo **Authorized public key**. Questo campo contiene un elenco di chiavi pubbliche autorizzate, nel formato del file **authorized_keys** di OpenSSH.

   Quando si compila il campo **Authorized public key**, tenere presente le seguenti linee guida:

   - Il campo **Chiave pubblica autorizzata** si applica a entrambi i controller e deve essere configurato solo sul primo controller.
   - Il file **authorized_keys** deve contenere una sola chiave per riga. Le righe che iniziano con # e le righe vuote vengono ignorate. Per ulteriori informazioni sul formato del file, vedere "Configurazione delle chiavi autorizzate per OpenSSH".
   - Un file **authorized_keys** dovrebbe avere un aspetto simile al seguente esempio:

     ```
     ssh-rsa
     AAAAB3NzaC1yc2EAAAADAQABAAABAQDJlG20rYTk4ok+xFjkPHYp/R0LfJqEYDLXA5AJ4
     9w3DvAWLrUg+1CpNq76WSqmQBmoG9jgbcAB5ABGdswdeMQZHilJcu29iJ3OKKv6SlCulA
     j1tHymwtbdhPuipd2wIDAQAB
     ```

7. Quando hai finito, fai clic su **Save**.
8. Per i sistemi duplex, puoi abilitare l'accesso remoto sul secondo controller seguendo i passaggi sopra. Se configuri l'opzione sia per la password che per la chiave SSH, assicurati di selezionare nuovamente la casella di controllo **Require authorized public key and password for remote login**.
9. Dopo che il supporto tecnico ha completato la risoluzione dei problemi, puoi disabilitare l'accesso remoto tornando alla finestra di dialogo Configura accesso remoto e deselezionando la casella di controllo **Abilita accesso remoto**. Se l'accesso remoto è abilitato su un secondo controller, si apre una finestra di dialogo di conferma che consente di disabilitare l'accesso remoto anche su quest'ultimo.

   La disabilitazione dell'accesso remoto termina tutte le sessioni SSH attive e rifiuta qualsiasi nuova richiesta di accesso.

Metti online un controller in SANtricity System Manager

Se un controller si trova nello stato offline o in modalità di servizio, è possibile rimetterlo online.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic su un controller che si trova nello stato offline o in modalità di servizio.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Place online** e conferma di voler eseguire l'operazione.

Risultati

Il rilevamento di un percorso preferenziale ripristinato da parte del driver multipath può richiedere fino a 10 minuti.

Tutti i volumi originariamente di proprietà di questo controller vengono automaticamente riassegnati al controller non appena vengono ricevute richieste di I/O per ciascun volume. In alcuni casi, potrebbe essere necessario ridistribuire manualmente i volumi con il comando **Redistribute volumes**.

Metti un controller offline in SANtricity System Manager

Se richiesto, è possibile mettere un controller offline.

Prima di iniziare

- Il tuo array di storage deve avere due controller. Il controller che non stai mettendo offline deve essere online (nello stato ottimale).
- Assicurati che nessun volume sia in uso o che tu abbia installato un driver multipath su tutti gli host che utilizzano questi volumi.

Informazioni su questa attività

Non mettere un controller offline a meno che non ti venga richiesto dal Recovery Guru o dal supporto tecnico.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller che desideri mettere offline.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Place offline** e conferma di voler eseguire l'operazione.

Risultati

Potrebbero essere necessari diversi minuti prima che System Manager aggiorni lo stato del controller a offline. Non avviare altre operazioni finché lo stato non sarà stato aggiornato.

Mettere un controller in modalità di servizio in SANtricity System Manager

Se richiesto, è possibile mettere un controller in modalità service.

Prima di iniziare

- L'array di storage deve avere due controller. Il controller che non si intende mettere in modalità di servizio deve essere online (nello stato ottimale).
- Assicurati che nessun volume sia in uso o che tu abbia installato un driver multipath su tutti gli host che utilizzano questi volumi.

Mettere un controller in modalità di servizio potrebbe ridurne significativamente le prestazioni. Non mettere un controller in modalità di servizio a meno che non ti venga richiesto dal supporto tecnico.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller che desideri mettere in modalità di servizio.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Place in service mode** e conferma di voler eseguire l'operazione.

Reimposta (riavvia) un controller in SANtricity System Manager

Alcuni problemi richiedono un reset (riavvio) del controller. Puoi eseguire il reset del controller anche se non hai accesso fisico ad esso.

Prima di iniziare

- L’array di storage deve avere due controller. Il controller che non si sta reimpostando deve essere online (nello stato ottimale).
- Assicurati che nessun volume sia in uso o che tu abbia installato un driver multipath su tutti gli host che utilizzano questi volumi.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller che vuoi reimpostare.

   Viene visualizzato il menu contestuale del controller.

4. Seleziona **Reset** e conferma di voler eseguire l’operazione.

Gestisci le porte iSCSI

Configurare le porte iSCSI in SANtricity System Manager

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

Prima di iniziare

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

> Le impostazioni e le funzioni iSCSI vengono visualizzate solo se l’array di storage supporta iSCSI.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller con le porte iSCSI che desideri configurare.

   Viene visualizzato il menu contestuale del controller.

4. Selezionare **Configura porte iSCSI**.

   > L’opzione **Configura porte iSCSI** viene visualizzata solo se System Manager rileva porte iSCSI sul controller.

   Si apre la finestra di dialogo Configura porte iSCSI.

5. Nell’elenco a discesa, seleziona la porta che desideri configurare e quindi fai clic su **Avanti**.
6. Seleziona le impostazioni della porta di configurazione, quindi fai clic su **Next**.

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

Dettagli del campo

Impostazione della porta	Descrizione
Velocità della porta Ethernet configurata (visualizzata solo per alcuni tipi di Host Interface Cards)	Selezionare la velocità che corrisponde alla capacità di velocità del modulo SFP sulla porta.
Modalità Forward Error Correction (FEC) (presente solo per alcuni tipi di Host Interface Cards)	Se lo si desidera, selezionare una delle modalità FEC per la porta host specificata. La modalità Reed Solomon non supporta la velocità di porta di 25 Gbps.
Abilita IPv4 / Abilita IPv6	Seleziona una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. Se si desidera disabilitare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
Porta di ascolto TCP (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 che il controller utilizza per ascoltare i login iSCSI dagli iniziatori iSCSI host. La porta di ascolto predefinita è 3260. È necessario immettere 3260 o un valore compreso tra 49152 e 65535.
Dimensione MTU (disponibile cliccando su **Mostra altre impostazioni della porta**.)	Se necessario, inserire una nuova dimensione in byte per la Maximum Transmission Unit (MTU). La dimensione predefinita della Maximum Transmission Unit (MTU) è di 1500 byte per frame. È necessario inserire un valore compreso tra 1500 e 9000.
Abilita le risposte ICMP PING	Seleziona questa opzione per abilitare il protocollo Internet Control Message Protocol (ICMP). I sistemi operativi dei computer in rete utilizzano questo protocollo per inviare messaggi. Questi messaggi ICMP determinano se un host è raggiungibile e quanto tempo occorre per inviare e ricevere pacchetti da e verso tale host.

Se hai selezionato **Abilita IPv4**, si apre una finestra di dialogo per la selezione delle impostazioni IPv4 dopo aver fatto clic su **Avanti**. Se hai selezionato **Abilita IPv6**, si apre una finestra di dialogo per la selezione delle impostazioni IPv6 dopo aver fatto clic su **Avanti**. Se hai selezionato entrambe le opzioni, la

finestra di dialogo per le impostazioni IPv4 si apre per prima e, dopo aver fatto clic su **Avanti**, si apre la finestra di dialogo per le impostazioni IPv6.

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

   Dettagli del campo

Impostazione della porta	Descrizione
Ottieni automaticamente la configurazione	Seleziona questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Seleziona questa opzione e inserisci un indirizzo statico nei campi. (Se lo desideri, puoi copiare e incollare gli indirizzi nei campi.) Per IPv4, includi la subnet mask di rete e il gateway. Per IPv6, includi l'indirizzo IP instradabile e l'indirizzo IP del router.
Abilita il supporto VLAN (Disponibile facendo clic su **Mostra altre impostazioni**.)	Seleziona questa opzione per abilitare una VLAN e inserire il suo ID. Una VLAN è una rete logica che si comporta come se fosse fisicamente separata dalle altre reti locali (LAN) fisiche e virtuali supportate dagli stessi switch, dagli stessi router o da entrambi.
Abilita la priorità Ethernet (Disponibile facendo clic su **Mostra altre impostazioni**.)	Seleziona questa opzione per abilitare il parametro che determina la priorità di accesso alla rete. Utilizza il cursore per selezionare una priorità compresa tra 1 (più bassa) e 7 (più alta). In un ambiente di rete locale (LAN) condivisa, come Ethernet, molte stazioni potrebbero competere per l'accesso alla rete. L'accesso avviene secondo il principio "primo arrivato, primo servito". Due stazioni potrebbero tentare di accedere alla rete contemporaneamente, il che costringe entrambe le stazioni ad attendere prima di riprovare. Questo processo è ridotto al minimo per lo switched Ethernet, dove solo una stazione è connessa a una porta dello switch.

8. Fare clic su **Fine**.

Configurare l'autenticazione iSCSI in SANtricity System Manager

Per una maggiore sicurezza in una rete iSCSI, è possibile impostare l'autenticazione tra i controller (target) e gli host (iniziatori).

System Manager utilizza il metodo Challenge Handshake Authentication Protocol (CHAP), che convalida l'identità dei target e degli initiator durante il collegamento iniziale. L'autenticazione si basa su una chiave di sicurezza condivisa chiamata *CHAP secret*.

Prima di iniziare

È possibile impostare il segreto CHAP per gli iniziatori (host iSCSI) sia prima che dopo aver impostato il

segreto CHAP per i target (controller). Prima di seguire le istruzioni di questa attività, è necessario attendere che gli host abbiano prima stabilito una connessione iSCSI e poi impostare il segreto CHAP sui singoli host. Dopo che le connessioni sono state stabilite, i nomi IQN degli host e i relativi segreti CHAP vengono elencati nella finestra di dialogo per l'autenticazione iSCSI (descritta in questa attività) e non è necessario inserirli manualmente.

Informazioni su questa attività

È possibile selezionare uno dei seguenti metodi di autenticazione:

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

Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Impostazioni solo se l'array di storage supporta iSCSI.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In Impostazioni iSCSI, fare clic su **Configura autenticazione**.

   Viene visualizzata la finestra di dialogo Configura autenticazione, che mostra il metodo attualmente impostato. Mostra anche se a qualche host sono stati configurati segreti CHAP.

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

   Se la chiave segreta CHAP per il controller è stata configurata in precedenza, i caratteri nel campo vengono mascherati. Se necessario, puoi sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

5. Eseguire una delle seguenti operazioni:
   - Se stai configurando l'autenticazione unidirezionale, fai clic su **Fine**. La finestra di dialogo si chiude e hai terminato la configurazione.
   - Se stai configurando l'autenticazione , fai clic su **Avanti** per visualizzare la finestra di dialogo Configura Initiator CHAP.

6. Per l'autenticazione a due vie, inserire o confermare una CHAP secret per uno qualsiasi degli host iSCSI (gli iniziatori), che può essere composta da 12 a 57 caratteri ASCII stampabili. Se non si desidera configurare l'autenticazione a due vie per un host specifico, lasciare vuoto il campo Initiator CHAP Secret.

> Se la chiave segreta CHAP per un host è stata configurata in precedenza, i caratteri nel campo vengono mascherati. Se necessario, puoi sostituire i caratteri esistenti (i nuovi caratteri non vengono mascherati).

7. Fare clic su **Fine**.

Risultati

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

Abilitare le impostazioni di rilevamento iSCSI in SANtricity System Manager

È possibile abilitare le impostazioni relative al rilevamento dei dispositivi storage in una rete iSCSI.

Le impostazioni di individuazione della destinazione consentono di registrare le informazioni iSCSI dell'array di storage utilizzando il protocollo Internet Storage Name Service (iSNS) e di determinare se consentire sessioni di individuazione senza nome.

Prima di iniziare

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

Informazioni su questa attività

È possibile abilitare le seguenti impostazioni relative alla scoperta iSCSI:

- **Abilita il server iSNS per registrare una destinazione** — Quando abilitato, l'array di storage registra il proprio iSCSI Qualified Name (IQN) e le informazioni sulla porta dal server iSNS. Questa impostazione consente la scoperta iSNS, così che un initiator possa recuperare l'IQN e le informazioni sulla porta dal server iSNS.
- **Abilita sessioni di discovery senza nome** — Quando le sessioni di discovery senza nome sono abilitate, l'initiator (iSCSI host) non deve fornire l'IQN del target (controller) durante la sequenza di login per una connessione di tipo discovery. Quando sono disabilitate, gli host devono fornire l'IQN per stabilire una discovery-session con il controller. Tuttavia, l'IQN del target è sempre richiesto per una normale sessione (con I/O). La disabilitazione di questa impostazione può impedire agli host iSCSI non autorizzati di connettersi al controller utilizzando solo il suo indirizzo IP.

> Le impostazioni e le funzioni iSCSI vengono visualizzate nella pagina Impostazioni solo se l'array di storage supporta iSCSI.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **impostazioni iSCSI**, fare clic su **Visualizza/Modifica impostazioni di rilevamento destinazione**.

   Viene visualizzata la finestra di dialogo Impostazioni di individuazione della destinazione. Sotto il campo **Abilita server iSNS**…, la finestra di dialogo indica se il controller è già registrato.

3. Per registrare il controller, selezionare **Abilita il server iSNS per registrare il mio target** e quindi selezionare una delle seguenti:
   - **Ottieni automaticamente la configurazione dal server DHCP** — Seleziona questa opzione se desideri configurare il server iSNS utilizzando un server DHCP (Dynamic Host Configuration Protocol). Tieni presente che se utilizzi questa opzione, tutte le porte iSCSI sul controller devono essere configurate per utilizzare DHCP anche loro. Se necessario, aggiorna le impostazioni della porta iSCSI del controller per abilitare questa opzione.

     Affinché il server DHCP possa fornire l'indirizzo del server iSNS, è necessario configurare il server DHCP per utilizzare l'opzione 43 — "Vendor Specific Information." Questa opzione deve contenere l'indirizzo IPv4 del server iSNS nei byte di dati 0xa-0xd (10-13).

   - **Specifica manualmente la configurazione statica** — Seleziona questa opzione se desideri immettere un indirizzo IP statico per il server iSNS. (Se desiderato, puoi tagliare e incollare gli indirizzi nei campi.) Nel campo, immetti un indirizzo IPv4 o un indirizzo IPv6. Se hai configurato entrambi, IPv4 è l'impostazione predefinita. Immetti anche una porta di ascolto TCP (usa il valore predefinito di 3205 o immetti un valore compreso tra 49152 e 65535).
4. Per consentire all'array di storage di partecipare alle sessioni di unnamed discovery, selezionare **Enable unnamed discovery sessions**.
   - Quando questa funzione è abilitata, gli iSCSI initiator non sono tenuti a specificare l'IQN di destinazione per recuperare le informazioni del controller.
   - Quando disabilitato, le sessioni di rilevamento vengono impedite a meno che l'initiator non fornisca l'IQN di destinazione. La disabilitazione delle sessioni di rilevamento senza nome offre maggiore sicurezza.
5. Fare clic su **Save**.

Risultati

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

Visualizza i pacchetti di statistiche iSCSI in SANtricity System Manager

È possibile visualizzare i dati sulle connessioni iSCSI al proprio array di storage.

Informazioni su questa attività

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

I tipi di statistiche visualizzati in System Manager si basano sulle statistiche disponibili per il tuo storage array.

- **Ethernet MAC statistiche** — Fornisce statistiche per il media access control (MAC). MAC fornisce anche un meccanismo di indirizzamento chiamato indirizzo fisico o indirizzo MAC. L'indirizzo MAC è un indirizzo univoco assegnato a ciascun network adapter. L'indirizzo MAC aiuta a recapitare i pacchetti di dati a una destinazione all'interno della subnetwork.
- **Ethernet TCP/IP statistiche** — Fornisce statistiche per il TCP/IP, ovvero il Transmission Control Protocol (TCP) e l'Internet Protocol (IP) per il dispositivo iSCSI. Con TCP, le applicazioni sugli host di rete possono creare connessioni tra loro, tramite le quali possono scambiare dati in pacchetti. L'IP è un protocollo orientato ai dati che comunica dati attraverso una rete interconnessa a commutazione di pacchetto. Le

statistiche IPv4 e le statistiche IPv6 vengono mostrate separatamente.

- **Ethernet Kernel statistics** — Fornisce statistiche per i driver del kernel della piattaforma del dispositivo iSCSI. Le statistiche del kernel visualizzano dati di rete simili a quelli dell'opzione statistiche TCP/IP. Tuttavia, i dati delle statistiche del kernel vengono raccolti dai driver del kernel della piattaforma anziché direttamente dall'hardware iSCSI.
- **Statistiche Local Target/Initiator (Protocollo)** — Mostra le statistiche per l'iSCSI target, che fornisce accesso a livello di blocco ai suoi supporti di archiviazione, e mostra le statistiche iSCSI per l'array di storage quando viene utilizzato come initiator in operazioni di mirroring asincrone.
- **Statistiche degli stati operativi DCBX** — Visualizza gli stati operativi delle varie funzionalità di Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistiche** — Visualizza le statistiche LLDP Type Length Value (TLV).
- **DCBX TLV statistiche** — Visualizza le informazioni che identificano le porte host dell'array di storage in un ambiente Data Center Bridging (DCB). Queste informazioni vengono condivise con i peer di rete a scopo di identificazione e verifica delle funzionalità.

È possibile visualizzare ciascuna di queste statistiche come raw statistiche o come statistiche baseline. Le raw statistiche sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche baseline sono point-in-time statistiche raccolte a partire dal momento in cui è stato impostato il tempo di riferimento.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Selezionare **Visualizza pacchetti di statistiche iSCSI**.
3. Fai clic su una scheda per visualizzare i diversi set di statistiche.
4. Per impostare la baseline, fai clic su **Set new baseline**.

   L'impostazione della baseline definisce un nuovo punto di partenza per la raccolta delle statistiche. La stessa baseline viene utilizzata per tutte le statistiche iSCSI.

Visualizza le sessioni iSCSI in SANtricity System Manager

È possibile visualizzare informazioni dettagliate sulle connessioni iSCSI al proprio array di storage. Le sessioni iSCSI possono avvenire con host o array di storage remoti in una relazione di mirroring asincrono.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Selezionare **Visualizza/Termina iSCSI Sessions**.

   Viene visualizzato un elenco delle sessioni iSCSI attive.

3. **Facoltativo:** Per visualizzare ulteriori informazioni su una specifica sessione iSCSI, seleziona una sessione e quindi fai clic su **Visualizza dettagli**.

Dettagli del campo

Articolo	Descrizione
Session Identifier (SSID)	Una stringa esadecimale che identifica una sessione tra un iSCSI initiator e un iSCSI target. L'SSID è composto dall'ISID e dal TPGT.
Session ID dell'iniziatore (ISID)	La parte initiator dell'identificativo di sessione. L'initiator specifica l'ISID durante il login.
Target Portal Group	L'iSCSI target.
Tag del gruppo del portale di destinazione (TPGT)	La parte di destinazione dell'identificativo di sessione. Un identificatore numerico a 16 bit per un iSCSI target portal group.
Nome iSCSI initiator	Il nome univoco a livello mondiale dell'initiator.
Etichetta iSCSI initiator	L'etichetta utente impostata in System Manager.
Alias iSCSI dell'iniziatore	Un nome che può anche essere associato a un nodo iSCSI. L'alias consente a un'organizzazione di associare una stringa di facile utilizzo al nome iSCSI. Tuttavia, l'alias non è un sostituto del nome iSCSI. L'alias iSCSI dell'initiator può essere impostato solo sull'host, non in System Manager
Host	Un server che invia input e output all'array di archiviazione.
Connection ID (CID)	Un nome univoco per una connessione all'interno della sessione tra l'initiator e il target. L'initiator genera questo ID e lo presenta al target durante le richieste di accesso. L'ID di connessione viene presentato anche durante le disconnessioni che chiudono le connessioni.
Identificatore porta	La porta del controller associata alla connessione.
Indirizzo IP dell'iniziator	L'indirizzo IP dell'initiator.
Parametri di login negoziati	I parametri che vengono scambiati durante l'accesso della sessione iSCSI.
Metodo di autenticazione	La tecnica per autenticare gli utenti che desiderano accedere alla rete iSCSI. I valori validi sono **CHAP** e **None**.
Metodo digest dell'intestazione	La tecnica per mostrare i possibili valori dell'intestazione per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.

Articolo	Descrizione
Metodo di digest dei dati	La tecnica per mostrare i possibili valori dei dati per la sessione iSCSI. HeaderDigest e DataDigest possono essere **None** o **CRC32C**. Il valore predefinito per entrambi è **None**.
Connessioni massime	Il numero massimo di connessioni consentite per la sessione iSCSI. Il numero massimo di connessioni può essere compreso tra 1 e 4. Il valore predefinito è **1**.
Alias di destinazione	L'etichetta associata al target.
Alias dell'iniziator	L'etichetta associata all'initiator.
Indirizzo IP di destinazione	L'indirizzo IP del target per la sessione iSCSI. I nomi DNS non sono supportati.
R2T iniziale	Lo stato iniziale di disponibilità al trasferimento. Lo stato può essere **Yes** o **No**.
Durata massima burst	Il payload SCSI massimo in byte per questa sessione iSCSI. La lunghezza massima del burst può essere da 512 a 262,144 (256 KB). Il valore predefinito è **262,144 (256 KB)**.
Prima burst length	Il payload SCSI in byte per i dati non richiesti per questa sessione iSCSI. La lunghezza del primo burst può variare da 512 a 131,072 (128 KB). Il valore predefinito è **65,536 (64 KB)**.
Tempo di attesa predefinito	Il numero minimo di secondi da attendere prima di tentare di stabilire una connessione dopo la terminazione o il ripristino di una connessione. Il valore predefinito del tempo di attesa può essere compreso tra 0 e 3600. Il valore predefinito è **2**.
Tempo predefinito di conservazione	Il numero massimo di secondi in cui la connessione è ancora possibile dopo una terminazione della connessione o un reset della connessione. Il tempo di conservazione predefinito può essere da 0 a 3600. Il valore predefinito è **20**.
Massimo R2T in sospeso	Il numero massimo di "ready to transfers" in sospeso per questa iSCSI session. Il valore massimo di ready to transfer in sospeso può essere compreso tra 1 e 16. Il valore predefinito è **1**.
Livello di ripristino degli errori	Il livello di ripristino degli errori per questa sessione iSCSI. Il valore del livello di ripristino degli errori è sempre impostato su **0**.
Lunghezza massima del segmento di dati ricevuti	La quantità massima di dati che l'initiator o il target possono ricevere in qualsiasi unità dati di payload iSCSI (PDU).

Articolo	Descrizione
Nome target	Il nome ufficiale della destinazione (non l'alias). Il nome della destinazione nel formato *iqn*.
Nome initiator	Il nome ufficiale dell'initiator (non l'alias). Il nome dell'initiator che utilizza il formato *iqn* o *eui*.

4. **Facoltativo:** Per salvare il report in un file, fai clic su **Save**.

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

Termina la sessione iSCSI in SANtricity System Manager

È possibile terminare una sessione iSCSI non più necessaria. Le sessioni iSCSI possono avvenire con host o array di storage remoti in una relazione di mirroring asincrono.

Informazioni su questa attività

Potresti voler terminare una sessione iSCSI per i seguenti motivi:

- **Accesso non autorizzato** — Se un iSCSI initiator è connesso e non dovrebbe avere accesso, puoi terminare la sessione iSCSI per forzare l'iSCSI initiator dall'array di storage. L'iSCSI initiator potrebbe essersi connesso perché il metodo di autenticazione None era disponibile.
- **Interruzione del servizio** — Se è necessario arrestare un array di storage e si nota che gli iSCSI initiator sono ancora connessi, è possibile terminare le sessioni iSCSI per disconnettere gli iSCSI initiator dall'array di storage.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Selezionare **Visualizza/Termina iSCSI Sessions**.

   Viene visualizzato un elenco delle sessioni iSCSI attive.

3. Seleziona la sessione che vuoi terminare.
4. Fai clic su **End Session** e conferma di voler eseguire l'operazione.

Configurare iSER sulle porte InfiniBand in SANtricity System Manager

Se il controller include una porta iSER su InfiniBand, è possibile configurare la connessione di rete all'host.

Prima di iniziare

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

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller con la porta iSER su InfiniBand che desideri configurare.

   Viene visualizzato il menu contestuale del controller.

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

   Si apre la finestra di dialogo Configura iSER tramite porte InfiniBand.

5. Nell'elenco a discesa, seleziona la porta HIC che vuoi configurare, quindi inserisci l'indirizzo IP dell'host.
6. Fare clic su **Configure**.
7. Completa la configurazione, quindi reimposta la porta iSER su InfiniBand facendo clic su **Sì**.

Visualizza statistiche iSER over InfiniBand in SANtricity System Manager

Se il controller del tuo array di storage include una porta iSER su InfiniBand, puoi visualizzare i dati relativi alle connessioni host.

Informazioni su questa attività

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

- **Statistiche Local Target (Protocollo)** — Fornisce statistiche per l'iSER su InfiniBand target, che mostrano l'accesso a livello di blocco ai suoi supporti di memorizzazione.
- **iSER over InfiniBand Interface statistiche** — Fornisce statistiche per tutte le porte iSER sull'interfaccia InfiniBand, che include statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come raw statistiche o come statistiche baseline. Le raw statistiche sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche baseline sono point-in-time statistiche raccolte a partire dal momento in cui è stato impostato il tempo di riferimento.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Seleziona **Visualizza statistiche iSER su InfiniBand**.
3. Fai clic su una scheda per visualizzare i diversi set di statistiche.
4. **Facoltativo:** Per impostare la baseline, fare clic su **Set new baseline**.

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

Gestisci le porte NVMe

Scopri di più su NVMe e sul software SANtricity

Alcuni controller includono una porta per l'implementazione di NVMe (Non-Volatile

Memory Express) su fabric. NVMe consente una comunicazione dalle performance elevate tra gli host e l'array di storage.

Che cos'è NVMe?

NVM è l'acronimo di "Non-Volatile Memory" e si riferisce a una memoria persistente utilizzata in molti tipi di dispositivi di storage. *NVMe* (NVM Express) è un'interfaccia o un protocollo standardizzato progettato specificamente per la comunicazione multi-coda dalle performance elevate con dispositivi NVM.

Che cos'è NVMe over Fabrics?

NVMe over Fabrics (NVMe-oF) è una specifica tecnologica che consente ai comandi e ai dati basati su messaggi NVMe di essere trasferiti tra un computer host e lo storage tramite una rete. Un array di storage NVMe (chiamato *sottosistema*) può essere accessibile da un host utilizzando una fabric. I comandi NVMe sono abilitati e incapsulati in livelli di astrazione di trasporto sia sul lato host sia sul lato sottosistema. Questo estende l'interfaccia NVMe dalle performance elevate end-to-end dall'host allo storage e standardizza e semplifica il set di comandi.

Lo storage NVMe-oF viene presentato a un host come un dispositivo di storage a blocchi locale. Il volume (chiamato *namespace*) può essere montato su un file system come qualsiasi altro dispositivo di storage a blocchi. È possibile utilizzare la REST API, SMcli o SANtricity System Manager per configurare lo storage in base alle proprie esigenze.

Che cos'è un nome qualificato NVMe (NQN)?

Il nome qualificato NVMe (NQN) viene utilizzato per identificare il target di storage remoto. Il nome qualificato NVMe per l'array di storage viene sempre assegnato dal sottosistema e non può essere modificato. Esiste un solo nome qualificato NVMe per l'intero array. Il nome qualificato NVMe è limitato a 223 caratteri di lunghezza. Puoi confrontarlo con un iSCSI Qualified Name.

Che cos'è uno spazio dei nomi e un namespace ID?

Un namespace è l'equivalente di un'unità logica in SCSI, che corrisponde a un volume nell'array. L'ID del namespace (NSID) è equivalente a un numero di unità logica (LUN) in SCSI. L'NSID viene creato al momento della creazione del namespace e può essere impostato su un valore compreso tra 1 e 255.

Che cos'è un controller NVMe?

Analogamente a un SCSI I_T nexus, che rappresenta il percorso dall'iniziator dell'host al target del sistema storage, un controller NVMe creato durante il processo di connessione dell'host fornisce un percorso di accesso tra un host e i namespace nell'array di storage. Un NQN per l'host più un identificatore di porta host identificano in modo univoco un controller NVMe. Sebbene un controller NVMe possa essere associato a un solo host, può accedere a più namespace.

Configuri quali host possono accedere a quali namespace e imposti l'ID del namespace per l'host utilizzando SANtricity System Manager. Successivamente, quando viene creato il controller NVMe, viene creato l'elenco degli ID dei namespace accessibili dal controller NVMe, che viene utilizzato per configurare le connessioni consentite.

Configurare le porte NVMe su InfiniBand in SANtricity System Manager

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

Prima di iniziare

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

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

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller con la porta NVMe over InfiniBand che desideri configurare.

   Viene visualizzato il menu contestuale del controller.

4. Selezionare **Configura NVMe su InfiniBand ports**.

   Si apre la finestra di dialogo Configura NVMe su InfiniBand porte.

5. Seleziona la porta HIC che desideri configurare dall'elenco a discesa, quindi inserisci l'indirizzo IP.

   Se si sta configurando un array di storage EF600 con un HIC compatibile con 200Gb, questa finestra di dialogo visualizza due campi Indirizzo IP, uno per una porta fisica (esterna) e uno per una porta virtuale (interna). Si dovrebbe assegnare un indirizzo IP univoco a entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e all'HIC di raggiungere le massime prestazioni. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funzionerà a circa metà della sua velocità prevista.

6. Fare clic su **Configure**.
7. Completa la configurazione, quindi ripristina la porta NVMe over InfiniBand facendo clic su **Sì**.

Configurare le porte NVMe over RoCE in SANtricity System Manager

Se il controller include una connessione per NVMe su RoCE (RDMA over Converged Ethernet), puoi configurare le impostazioni della porta NVMe dalla pagina Hardware.

Prima di iniziare

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

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra le unità, fare clic sulla scheda **Controllers & Components**.

   La grafica cambia per mostrare i controller anziché le unità.

3. Fai clic sul controller con la porta NVMe over RoCE che desideri configurare.

Viene visualizzato il menu contestuale del controller.

4. Selezionare **Configura NVMe su porte RoCE**.

   La finestra di dialogo Configura NVMe su porte RoCE si apre.

5. Nell'elenco a discesa, seleziona la porta HIC che vuoi configurare.
6. Fai clic su **Avanti**.

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

   Dettagli del campo

Impostazione della porta	Descrizione
Velocità della porta Ethernet configurata	Selezionare la velocità che corrisponde alla capacità di velocità del modulo SFP sulla porta.
Abilita IPv4 / Abilita IPv6	Seleziona una o entrambe le opzioni per abilitare il supporto per le reti IPv4 e IPv6. Se si desidera disabilitare l'accesso alla porta, deselezionare entrambe le caselle di controllo.
Dimensione MTU (disponibile cliccando su **Mostra altre impostazioni della porta**.)	Se necessario, inserire una nuova dimensione in byte per la Maximum Transmission Unit (MTU). La dimensione predefinita della Maximum Transmission Unit (MTU) è di 1500 byte per frame. È necessario inserire un valore compreso tra 1500 e 9000.

   Se hai selezionato **Abilita IPv4**, si apre una finestra di dialogo per la selezione delle impostazioni IPv4 dopo aver fatto clic su **Avanti**. Se hai selezionato **Abilita IPv6**, si apre una finestra di dialogo per la selezione delle impostazioni IPv6 dopo aver fatto clic su **Avanti**. Se hai selezionato entrambe le opzioni, la finestra di dialogo per le impostazioni IPv4 si apre per prima e, dopo aver fatto clic su **Avanti**, si apre la finestra di dialogo per le impostazioni IPv6.

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

Dettagli del campo

Impostazione della porta	Descrizione
Ottieni automaticamente la configurazione	Seleziona questa opzione per ottenere la configurazione automaticamente.
Specificare manualmente la configurazione statica	Seleziona questa opzione, quindi inserisci un indirizzo statico nei campi. (Se desiderato, puoi tagliare e incollare gli indirizzi nei campi.) Per IPv4, includi la subnet mask di rete e il gateway. Per IPv6, includi l'indirizzo IP instradabile e l'indirizzo IP del router. Se stai configurando un array di storage EF600 con un HIC compatibile con 200Gb, questa finestra di dialogo visualizza due serie di campi per i parametri di rete, una per una porta fisica (esterna) e una per una porta virtuale (interna). Dovresti assegnare parametri univoci a entrambe le porte. Queste impostazioni consentono all'host di stabilire un percorso tra ciascuna porta e all'HIC di raggiungere le massime prestazioni. Se non assegni un indirizzo IP alla porta virtuale, l'HIC funzionerà a circa metà della sua velocità.

8. Fare clic su **Fine**.

Visualizza le statistiche NVMe over Fabrics in SANtricity System Manager

È possibile visualizzare i dati sulle connessioni NVMe over Fabrics al proprio storage array.

Informazioni su questa attività

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

- **Statistiche del sottosistema NVMe** — Mostra statistiche per il controller NVMe e la relativa coda. Il controller NVMe fornisce un percorso di accesso tra un host e i namespace nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti.
- **Statistiche interfaccia RDMA** — Fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, incluse statistiche sulle prestazioni e informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics.

È possibile visualizzare ciascuna di queste statistiche come raw statistiche o come statistiche baseline. Le raw statistiche sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche baseline sono point-in-time statistiche raccolte a partire dal momento in cui è stato impostato il tempo di riferimento.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Selezionare **Visualizza statistiche NVMe over Fabrics**.
3. **Facoltativo:** Per impostare la baseline, fare clic su **Set new baseline**.

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

Gestisci le unità

Scopri gli stati delle unità in SANtricity System Manager

SANtricity System Manager segnala vari stati per le unità.

Stati di accessibilità

Stato	Definizione
Bypassato	L’unità è fisicamente presente, ma il controller non può comunicare con essa su nessuna delle due porte.
Incompatibile	Si verifica una delle seguenti condizioni: • L’unità non è certificata per l’uso nell’array di archiviazione. • L’unità ha una dimensione del settore diversa. • L’unità contiene dati di configurazione inutilizzabili provenienti da una versione del firmware precedente o successiva.
Rimosso	L’unità è stata rimossa in modo improprio dallo storage array.
Presente	Il controller può comunicare con l’unità su entrambe le porte.
Non risponde	L’unità non risponde ai comandi.

Stati di ruolo

Stato	Definizione
Assegnato	L’unità è un membro di un pool o di un gruppo di volumi.
Hot spare in uso	L’unità viene attualmente utilizzata come sostituzione di un’unità che ha avuto un guasto. Gli hot spare vengono utilizzati solo nei gruppi di volumi, non nei pool.
Hot spare di standby	L’unità è pronta per essere utilizzata come sostituto di un’unità che ha avuto un guasto. Gli hot spare vengono utilizzati solo nei gruppi di volumi, non nei pool.
Non assegnato	L’unità non è membro di un pool o di un gruppo di volumi.

Stati di disponibilità

Stato	Definizione
Fallito	L'unità non funziona. I dati sull'unità non sono disponibili.
Guasto imminente	È stato rilevato che l'unità potrebbe guastarsi a breve. I dati sull'unità sono ancora disponibili.
Offline	L'unità non è disponibile per l'archiviazione dei dati solitamente perché fa parte di un gruppo di volumi in fase di esportazione o perché è in corso un aggiornamento del firmware.
Ottimale	L'unità funziona normalmente.

Scopri i dischi a stato solido (SSD) in SANtricity System Manager

Le unità a stato solido (SSD) sono dispositivi di archiviazione dati che utilizzano memoria a stato solido (flash) per memorizzare i dati in modo permanente. Le SSD emulano i dischi rigidi tradizionali e sono disponibili con le stesse interfacce che i dischi rigidi utilizzano.

Vantaggi degli SSD

I vantaggi delle SSD rispetto ai dischi rigidi includono:

- Avvio più rapido (nessuna fase di spin up)
- Latenza inferiore
- Operazioni di I/O al secondo (IOPS) più elevate
- Maggiore affidabilità con un minor numero di componenti mobili
- Minore consumo energetico
- Minore produzione di calore e minore necessità di raffreddamento

Identificazione degli SSD

Dalla pagina Hardware, puoi individuare gli SSD nella vista frontale dello shelf. Cerca gli alloggiamenti per unità che mostrano un'icona a forma di fulmine, che indica che è installato un SSD.

Gruppi di volume

Tutte le unità di un gruppo di volumi devono essere dello stesso tipo di supporto (tutte SSD o tutte unità rigide). I gruppi di volumi non possono contenere un mix di tipi di supporto o di tipi di interfaccia.

Caching

La cache di scrittura del controller è sempre abilitata per gli SSD. La cache di scrittura migliora le prestazioni e prolunga la durata dell'SSD.

Oltre alla cache del controller, è possibile implementare la funzionalità di cache SSD per migliorare le prestazioni complessive del sistema. Nella cache SSD, i dati vengono copiati dai volumi e archiviati su due volumi RAID interni (uno per controller).

Filtra la visualizzazione dei dischi in SANtricity System Manager

Se l'array di storage include dischi con diversi tipi di attributi fisici e logici, la pagina Hardware fornisce campi filtro che aiutano a limitare la visualizzazione dei dischi e a individuare dischi specifici.

Informazioni su questa attività

I filtri delle unità consentono di limitare la visualizzazione a determinati tipi di unità fisiche (ad esempio, tutte le SAS), con determinati attributi di sicurezza (ad esempio, secure-capable), in determinate posizioni logiche (ad esempio, Volume Group 1). È possibile utilizzare questi filtri insieme o separatamente.

> Se tutte le unità condividono gli stessi attributi fisici, il campo filtro **Mostra unità che sono…** non viene visualizzato. Se tutte le unità condividono gli stessi attributi logici, il campo filtro **Ovunque nell'array di archiviazione** non viene visualizzato.

Passaggi

1. Seleziona **Hardware**.
2. Nel primo campo filtro (sotto **Mostra unità che sono…**), fai clic sulla freccia a discesa per visualizzare i tipi di disco e gli attributi di sicurezza disponibili.

   I tipi di unità potrebbero includere:

   - Tipo di supporto drive (SSD, HDD)
   - Tipo di interfaccia dell'unità
   - Capacità del disco (dalla più alta alla più bassa)
   - Velocità del disco (dalla più alta alla più bassa) Gli attributi di sicurezza potrebbero includere:
   - Compatibile con la sicurezza
   - Abilitato alla sicurezza
   - Compatibile con DA (Data Assurance)
   - Conforme agli standard FIPS
   - Conforme a FIPS (FIPS 140-2)
   - Conforme a FIPS (FIPS 140-3)

     Se una qualsiasi di queste caratteristiche è identica per tutte le unità, non viene visualizzata nell'elenco a discesa. Ad esempio, se l'array di storage include tutte le unità SSD con interfacce SAS e velocità di 15000 RPM, ma alcune SSD hanno capacità diverse, l'elenco a discesa visualizza solo le capacità come opzione di filtro.

   Quando si seleziona un'opzione dal campo, le unità che non corrispondono ai criteri di filtro vengono visualizzate in grigio nella rappresentazione grafica.

3. Nella seconda casella di filtro, fai clic sulla freccia a discesa per visualizzare le posizioni logiche disponibili per i drive.

   > Se devi cancellare i criteri di filtro, seleziona **Clear** all'estrema destra delle caselle di filtro.

   Le posizioni logiche potrebbero includere:

- Pool
- Gruppi di volume
- Hot spare
- Cache SSD
- Non assegnato

  Quando si seleziona un'opzione dal campo, le unità che non corrispondono ai criteri di filtro vengono visualizzate in grigio nella rappresentazione grafica.

4. Facoltativamente, puoi selezionare **Attiva le luci di localizzazione** all'estrema destra dei campi filtro per accendere le luci di localizzazione per le unità visualizzate.

   Questa azione consente di individuare fisicamente le unità nell'array di archiviazione.

Attivare la spia di localizzazione dell'unità in SANtricity System Manager

Dalla pagina Hardware, puoi attivare la spia di localizzazione per trovare la posizione fisica di un'unità nell'array di storage.

Informazioni su questa attività

È possibile individuare singole unità o più unità mostrate nella pagina Hardware.

Passaggi

1. Seleziona **Hardware**.
2. Per individuare una o più unità, eseguire una delle seguenti operazioni:
   - **Unità singola** — Dalla rappresentazione grafica dello scaffale, individua l'unità che desideri posizionare fisicamente nell'array. (Se la rappresentazione grafica mostra i controller, fai clic sulla scheda **Unità**.) Fai clic sull'unità per visualizzare il relativo menu contestuale, quindi seleziona **Attiva la spia di localizzazione**.

     La spia di localizzazione dell'unità si accende. Quando hai individuato fisicamente l'unità, torna alla finestra di dialogo e seleziona **Turn off**.

   - **Unità multiple** — Nei campi filtro, seleziona un tipo di unità fisica dall'elenco a discesa a sinistra e un tipo di unità logica dall'elenco a discesa a destra. Il numero di unità che corrispondono ai tuoi criteri viene visualizzato all'estrema destra dei campi. Successivamente, puoi fare clic su **Attiva spie di localizzazione** oppure selezionare **Individua tutte le unità filtrate** dal menu contestuale. Quando hai individuato fisicamente le unità, torna alla finestra di dialogo e seleziona **Disattiva**.

Visualizza lo stato e le impostazioni dell'unità in SANtricity System Manager

È possibile visualizzare lo stato e le impostazioni delle unità, come il tipo di media, il tipo di interfaccia e la capacità.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Seleziona l’unità per la quale desideri visualizzare stato e impostazioni.

   Si apre il menu contestuale dell’unità.

4. Seleziona **View settings**.

   Si apre la finestra di dialogo Drive Settings.

5. Per visualizzare tutte le impostazioni, fai clic su **Mostra altre impostazioni** nell’angolo in alto a destra della finestra di dialogo.

Dettagli del campo

Impostazioni	Descrizione
Stato	Visualizza Ottimale, Offline, Guasto non critico e Guasto. Lo stato Ottimale indica la condizione di lavoro desiderata.
Modalità	Visualizza Assegnato, Non assegnato, Hot Spare Standby o Hot Spare in uso.
Posizione	Mostra il numero dello shelf e dello slot in cui si trova il drive.
Assegnato a/Può proteggere per/Proteggendo	Se l'unità è assegnata a un pool, a un gruppo di volumi o a una cache SSD, questo campo visualizza "Assegnato a". Il valore può essere un nome di pool, un nome di gruppo di volumi o un nome di cache SSD. Se l'unità è assegnata a un hot spare e la sua modalità è Standby, questo campo visualizza "Può proteggere per". Se l'hot spare può proteggere uno o più gruppi di volumi, i nomi dei gruppi di volumi vengono visualizzati. Se non può proteggere un gruppo di volumi, visualizza 0 gruppi di volumi. Se l'unità è assegnata a una hot spare e la sua modalità è In uso, questo campo visualizza "Protecting". Il valore corrisponde al nome del gruppo di volumi interessato. Se l'unità non è assegnata, questo campo non viene visualizzato.
Tipo di media	Visualizza il tipo di supporto di registrazione utilizzato dall'unità, che può essere un hard disk drive (HDD) o un solid state disk (SSD).
Percentuale di endurance utilizzata (mostrata solo se sono presenti unità SSD)	La quantità di dati scritti sull'unità fino ad oggi, divisa per il limite teorico totale di scrittura.
Tipo di interfaccia	Visualizza il tipo di interfaccia che l'unità utilizza, ad esempio SAS.
Ridondanza del percorso del disco	Mostra se le connessioni tra l'unità e il controller sono ridondanti (Sì) o no (No).
Capacità (GiB)	Mostra la capacità utilizzabile (capacità totale configurata) del drive.
Velocità (RPM)	Mostra la velocità in RPM (non viene visualizzata per SSD).
Tasso di trasferimento dei dati attuale	Mostra il tasso di trasferimento dei dati tra l'unità e il sistema di archiviazione.
Dimensione del settore logico (byte)	Mostra la dimensione del settore logico utilizzata dall'unità.

Impostazioni	Descrizione
Dimensione del settore fisico (byte)	Indica la dimensione del settore fisico utilizzata dall'unità. In genere, la dimensione del settore fisico è 4096 byte per i dischi rigidi.
Versione del firmware dell'unità	Mostra il livello di revisione del firmware dell'unità.
Identificatore mondiale	Mostra l'identificativo esadecimale univoco dell'unità.
ID prodotto	Mostra l'identificativo del prodotto, che viene assegnato dal produttore.
Numero di serie	Mostra il numero di serie dell'unità.
Produttore	Mostra il fornitore dell'unità.
Data di fabbricazione	Mostra la data in cui è stata costruita l'unità. Non disponibile per drive NVMe.
Compatibile con la sicurezza	Mostra se l'unità è secure-capable (Sì) o no (No). Le unità secure-capable possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS) (livello 140-2 o 140-3), che crittografano i dati durante la scrittura e li decrittografano durante la lettura. Queste unità sono considerate secure-*capable* perché possono essere utilizzate per una sicurezza aggiuntiva tramite la funzionalità Drive Security. Se la funzionalità Drive Security è abilitata per i gruppi di volumi e i pool utilizzati con queste unità, le unità diventano secure-*enabled*.
Abilitato alla sicurezza	Mostra se l'unità è abilitata alla sicurezza (Sì) o no (No). Le unità abilitate alla sicurezza vengono utilizzate con la funzione Drive Security. Quando si abilita la funzione Drive Security e poi si applica Drive Security a un pool o a un gruppo di volumi su unità secure-*capable*, le unità diventano secure-*enabled*. L'accesso in lettura e scrittura è disponibile solo tramite un controller configurato con la chiave di sicurezza corretta. Questa sicurezza aggiuntiva impedisce l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage.
Accessibile in lettura/scrittura	Indica se l'unità è accessibile in lettura/scrittura (Sì) o non (No).

Impostazioni	Descrizione
Identificatore della chiave di sicurezza dell'unità	Mostra la chiave di sicurezza per le unità con sicurezza abilitata. Drive Security è una funzionalità dell'array di storage che fornisce un ulteriore livello di sicurezza con unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Quando queste unità vengono utilizzate con la funzionalità Drive Security, richiedono una chiave di sicurezza per accedere ai loro dati. Quando le unità vengono rimosse fisicamente dall'array, non possono funzionare finché non vengono installate in un altro array; a quel punto, saranno in uno stato Security Locked finché non viene fornita la chiave di sicurezza corretta.
Data Assurance (DA) capace	Indica se la funzionalità Data Assurance (DA) è abilitata (Sì) o non lo è (No). Data Assurance (DA) è una funzionalità che verifica e corregge gli errori che potrebbero verificarsi durante il trasferimento dei dati attraverso i controller fino alle unità. Data Assurance può essere abilitata a livello di pool o di gruppo di volumi, con host che utilizzano un'interfaccia I/O compatibile con DA, come Fibre Channel.
DULBE compatibile	Indica se l'opzione per Deallocated or Unwritten Logical Block Error (DULBE) è abilitata (Sì) o no (No). DULBE è un'opzione sulle unità NVMe che consente all'array di storage EF300 o EF600 di supportare volumi con provisioning delle risorse.

6. Fare clic su **Close**.

Sostituire un drive logicamente in SANtricity System Manager

Se un'unità si guasta o si desidera sostituirla per qualsiasi altro motivo, è possibile sostituire logicamente l'unità guasta con un'unità non assegnata o con un hot spare completamente integrato.

Informazioni su questa attività

Quando si sostituisce logicamente un'unità, questa viene assegnata e diventa quindi un membro permanente del pool o del volume group associato.

Si utilizza l'opzione di sostituzione logica per sostituire i seguenti tipi di unità:

- Unità disco guaste
- Unità mancanti
- Unità SSD per le quali il Recovery Guru ti ha notificato che stanno per raggiungere la fine del loro ciclo di vita
- Dischi rigidi per i quali il Recovery Guru ti ha notificato un imminente guasto dell'unità
- Unità assegnate (disponibili solo per le unità in un gruppo di volumi, non in un pool)

Prima di iniziare

L'unità di ricambio deve possedere le seguenti caratteristiche:

- Nello stato ottimale

- Nello stato Non assegnato
- Stesse caratteristiche dell'unità che viene sostituita (tipo di supporto, tipo di interfaccia e così via)
- La stessa funzionalità FDE (consigliata, ma non obbligatoria)
- La stessa funzionalità DA (consigliata, ma non obbligatoria)

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Fai clic sull'unità che desideri sostituire logicamente.

   Viene visualizzato il menu contestuale dell'unità.

4. Fai clic su **Sostituisci logicamente**.
5. **Opzionale:** Seleziona la check box **Fail drive after it is replaced** per contrassegnare come non valida l'unità originale dopo la sua sostituzione.

   Questa check box è abilitata solo se l'unità assegnata originariamente non è guasta o mancante.

6. Dalla tabella **Select a replacement drive**, seleziona l'unità sostitutiva che desideri utilizzare.

   La tabella elenca solo le unità compatibili con l'unità che si sta sostituendo. Se possibile, selezionare un'unità che mantenga shelf loss protection e drawer loss protection.

7. Fai clic su **Replace**.

   Se l'unità originale è guasta o mancante, i dati vengono ricostruiti sull'unità sostitutiva utilizzando le informazioni di parità. Questa ricostruzione si avvia automaticamente. Le spie di segnalazione di guasto dell'unità si spengono e le spie di attività delle unità nel pool o nel gruppo di volumi iniziano a lampeggiare.

   Se l'unità originale non è guasta o mancante, i suoi dati vengono copiati sull'unità sostitutiva. Questa operazione di copia si avvia automaticamente. Al termine dell'operazione di copia, il sistema imposta l'unità originale sullo stato Non assegnata oppure, se la check box è stata selezionata, sullo stato Guasta.

Ricostruire manualmente un disco in SANtricity System Manager

La ricostruzione del disco singolo si avvia normalmente in automatico dopo la sostituzione di un disco singolo. Se la ricostruzione del disco singolo non si avvia automaticamente, puoi avviare la ricostruzione manualmente.

Eseguire questa operazione solo quando richiesto dal supporto tecnico o dal Recovery Guru.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Fai clic sul disco che desideri ricostruire manualmente.

   Viene visualizzato il menu contestuale dell'unità.

4. Seleziona **Reconstruct** e conferma di voler eseguire l'operazione.

Inizializzare (formattare) i dischi in SANtricity System Manager

Se si spostano unità assegnate da un array di storage a un altro, è necessario inizializzare (formattare) le unità prima di poterle utilizzare nel nuovo array di storage.

Informazioni su questa attività

L'inizializzazione rimuove le informazioni di configurazione precedenti da un'unità e la riporta allo stato Non assegnato. L'unità è quindi disponibile per essere aggiunta a un nuovo pool o gruppo di volumi nel nuovo storage array.

Utilizza l'operazione di inizializzazione dell'unità quando stai spostando un disco singolo. Non è necessario inizializzare le unità se stai spostando un intero gruppo di volumi da un array di storage a un altro.

> **Possibile perdita di dati** — Quando si inizializza un drive, tutti i dati presenti sul drive vengono persi. Eseguire questa operazione solo su indicazione del supporto tecnico.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Fai clic sul disco che desideri inizializzare.

   Viene visualizzato il menu contestuale dell'unità.

4. Seleziona **Initialize** e conferma di voler eseguire l'operazione.

Guasto manuale di un'unità in SANtricity System Manager

Se richiesto, è possibile eseguire manualmente il fail di un'unità.

Informazioni su questa attività

System Manager monitora le unità nell'array di storage. Quando rileva che un'unità sta generando molti errori, il Recovery Guru ti avvisa di un imminente guasto dell'unità. Se ciò accade e hai a disposizione un'unità sostitutiva, potresti voler contrassegnare come guasto l'unità per adottare un'azione preventiva. Se non hai un'unità sostitutiva disponibile, puoi attendere che l'unità si guasti da sola.

> **Possibile perdita di accesso ai dati** — Questa operazione potrebbe comportare la perdita di dati o la perdita di ridondanza dei dati. Eseguire questa operazione solo su indicazione del supporto tecnico o del Recovery Guru.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

La grafica cambia per mostrare le unità invece dei controller.

3. Fai clic sull'unità che desideri guastare.

   Viene visualizzato il menu contestuale dell'unità.

4. Seleziona **Fail**.
5. Mantieni selezionata la check box **Copia il contenuto dell'unità prima dell'errore**.

   L'opzione di copia appare solo per le unità assegnate e per i gruppi di volumi non RAID 0.

   Prima di rendere inutilizzabile l'unità, assicurati di copiarne il contenuto. A seconda della configurazione, potresti perdere tutti i dati o la ridondanza sul pool o sul gruppo di volumi associato se non copi prima il contenuto dell'unità.

   L'opzione di copia consente un ripristino del disco più rapido rispetto alla ricostruzione e riduce la possibilità di un errore del volume se un altro disco dovesse guastarsi durante l'operazione di copia.

6. Conferma che vuoi dichiarare l'errore dell'unità.

   Dopo che l'unità si è guastata, attendere almeno 60 secondi prima di rimuoverla.

Cancella le unità in SANtricity System Manager

È possibile utilizzare l'opzione Cancella per preparare un'unità non assegnata alla rimozione dal sistema. Questa procedura elimina i dati in modo permanente, garantendo che i dati non possano essere letti nuovamente.

Prima di iniziare

L'unità deve trovarsi in uno stato Unassigned.

Informazioni su questa attività

Utilizza l'opzione Cancella solo se desideri rimuovere definitivamente tutti i dati da un'unità. Se l'unità è abilitata alla sicurezza, l'opzione Cancella esegue una cancellazione crittografica e ripristina gli attributi di sicurezza dell'unità allo stato di secure-capable.

> La funzione Erase non supporta alcuni modelli di unità meno recenti. Se si tenta di cancellare uno di questi modelli, viene visualizzato un messaggio di errore.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Facoltativamente, è possibile utilizzare i campi filtro per visualizzare tutte le unità non assegnate nello shelf. Dall'elenco a discesa **Mostra unità che sono…**, selezionare **Non assegnate**.

   La visualizzazione a scaffale mostra solo le unità non assegnate; tutte le altre sono grigiate.

4. Per aprire il menu contestuale dell'unità, fai clic su un'unità che desideri cancellare. (Se desideri selezionare più unità, puoi farlo nella finestra di dialogo Cancella unità.)

Possibile perdita di dati — L'operazione di Erase non può essere annullata. Assicurati di selezionare le unità corrette durante la procedura.

5. Dal menu contestuale, seleziona **Erase**.

   Si apre la finestra di dialogo Erase Drives, che mostra tutte le unità idonee per un'operazione di cancellazione.

6. Se lo si desidera, selezionare ulteriori unità dalla tabella. Non è possibile selezionare *tutte* le unità; assicurarsi che una unità rimanga deselezionata.
7. Conferma l'operazione digitando `erase`, quindi fai clic su **Cancella**.

   Assicurati di voler continuare con questa operazione. Una volta cliccato su Sì nella finestra di dialogo successiva, l'operazione non potrà essere annullata.

8. Nella finestra di dialogo Estimated Completion Time, fare clic su **Yes** per continuare con l'operazione di cancellazione.

Risultati

L'operazione di Erase potrebbe richiedere da diversi minuti a diverse ore. Puoi visualizzare lo stato nel menu: Home[View Operations in Progress]. Quando l'operazione di Erase è completata, le unità sono disponibili per l'uso in un altro volume group o disk pool, oppure in un altro storage array.

Dopo aver finito

Se desideri utilizzare nuovamente l'unità, devi prima inizializzarla. Per farlo, seleziona **Inizializza** dal menu contestuale dell'unità.

Sblocca o reimposta le unità NVMe o FIPS bloccate in SANtricity System Manager

Se si inserisce una o più unità NVMe o FIPS bloccate in un array di storage, è possibile sbloccare i dati dell'unità aggiungendo il file della chiave di sicurezza associato alle unità. Se non si dispone di una chiave di sicurezza, è possibile eseguire un reset su ciascuna unità bloccata inserendo il relativo Physical Security ID (PSID) per resettare gli attributi di sicurezza e cancellare i dati dell'unità.

Prima di iniziare

- Per l'opzione Sblocca, assicurati che il file della chiave di sicurezza (con un'estensione di `.slk`) sia disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager). Devi inoltre conoscere la pass phrase associata alla chiave.
- Per l'opzione Reset, è necessario individuare il PSID su ciascuna unità che si desidera ripristinare. Per individuare il PSID, rimuovere fisicamente l'unità e individuare la stringa PSID (massimo 32 caratteri) sull'etichetta dell'unità, quindi reinstallare l'unità.

Informazioni su questa attività

Questa procedura descrive come sbloccare i dati nelle unità NVMe o FIPS importando un file di chiave di sicurezza nell'array di storage. Per le situazioni in cui la chiave di sicurezza non è disponibile, questa procedura descrive anche come eseguire un ripristino su un'unità bloccata.

Se l'unità è stata bloccata utilizzando un server di gestione delle chiavi esterno, selezionare **Settings › System › Security key management** in System Manager per configurare la gestione delle chiavi esterne e sbloccare l'unità.

È possibile accedere alla funzione di sblocco dalla pagina Hardware oppure dal **Settings › System › Security key management**. La procedura seguente fornisce istruzioni dalla pagina Hardware.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Seleziona l'unità NVMe o FIPS che desideri sbloccare o ripristinare.

   Si apre il menu contestuale dell'unità.

4. Seleziona **Sblocca** per applicare il file della chiave di sicurezza o **Ripristina** se non hai un file della chiave di sicurezza.

   Queste opzioni vengono visualizzate solo se si seleziona un'unità NVMe o FIPS bloccata.

   Durante un'operazione di Reset, tutti i dati vengono cancellati. Eseguire un Reset solo se non si dispone di una security key. Il Reset di un drive bloccato rimuove definitivamente tutti i dati presenti sul drive e ripristina i suoi attributi di sicurezza su "secure-capable", ma non abilitato. **Questa operazione non è reversibile.**

5. Eseguire una delle seguenti operazioni:
   a. **Sblocca**: Nella finestra di dialogo **Sblocca unità protetta**, fai clic su **Sfoglia** e quindi seleziona il file della chiave di sicurezza che corrisponde all'unità che desideri sbloccare. Successivamente, inserisci la pass phrase e poi fai clic su **Sblocca**.
   b. **Ripristina**: Nella finestra di dialogo **Ripristina unità bloccata**, immettere la stringa PSID nel campo e quindi digitare `RESET` per confermare. Fare clic su **Ripristina**.

      Per un'operazione di sblocco, è sufficiente eseguire questa operazione una sola volta per sbloccare tutte le unità NVMe o FIPS. Per un'operazione di ripristino, è necessario selezionare singolarmente ciascuna unità che si desidera ripristinare.

Risultati

L'unità è ora disponibile per l'utilizzo in un altro gruppo di volumi o pool di dischi, o in un altro array di storage.

Gestire i ricambi a caldo

Scopri le unità hot spare in SANtricity System Manager

Gli hot spare fungono da unità di standby nei gruppi di volumi RAID 1, RAID 5 o RAID 6 per SANtricity System Manager.

Si tratta di unità perfettamente funzionanti che non contengono dati. Se un'unità del gruppo di volumi si guasta, il controller ricostruisce automaticamente i dati dall'unità guasta su un'unità assegnata come hot spare.

Le hot spare non sono dedicate a specifici gruppi di volumi. Possono essere utilizzate per qualsiasi unità guasta nell'array di storage, a condizione che la hot spare e l'unità condividano queste caratteristiche:

- Capacità uguale (o capacità maggiore per l'hot spare)
- Stesso tipo di supporto (ad esempio, HDD o SSD)
- Stesso tipo di interfaccia (ad esempio, SAS)

Come identificare gli hot spare

È possibile assegnare hot spare tramite la procedura guidata di configurazione iniziale o dalla pagina Hardware. Per verificare se sono stati assegnati hot spare, accedere alla pagina Hardware e cercare gli alloggiamenti per unità visualizzati in rosa.

Come funziona la copertura hot spare

La copertura hot spare funziona nel seguente modo:

- Si riserva un'unità non assegnata come hot spare per gruppi di volumi RAID 1, RAID 5 o RAID 6.

> Gli hot spare non possono essere utilizzati per i pool, che hanno un metodo di protezione dei dati differente. Anziché riservare un'unità aggiuntiva, i pool riservano capacità di riserva (chiamata *preservation capacity*) all'interno di ciascuna unità del pool. Se un'unità si guasta in un pool, il controller ricostruisce i dati in quella capacità di riserva.

- Se un'unità all'interno di un gruppo di volumi RAID 1, RAID 5 o RAID 6 si guasta, il controller utilizza automaticamente i dati di ridondanza per ricostruire i dati dall'unità guasta. L'hot spare viene automaticamente sostituita all'unità guasta senza richiedere una sostituzione fisica.
- Quando si sostituisce fisicamente il disco guasto, viene eseguita un'operazione di copyback dall'hot spare al disco sostituito. Se si è designato l'hot spare come membro permanente di un gruppo di volumi, l'operazione di copyback non è necessaria.
- La disponibilità della tray loss protection e della drawer loss protection per un gruppo di volumi dipende dalla posizione delle unità che compongono il gruppo di volumi. La tray loss protection e la drawer loss protection potrebbero essere perse a causa di un'unità guasta e della posizione dell'hot spare drive. Per assicurarsi che la tray loss protection e la drawer loss protection non vengano compromesse, è necessario sostituire un'unità guasta per avviare il processo di copyback.
- Il volume dell'array di storage rimane online e accessibile durante la sostituzione dell'unità guasta, perché l'hot spare viene automaticamente sostituito all'unità guasta.

Considerazioni sulla capacità dell'hot spare

Seleziona un disco con una capacità pari o superiore alla capacità totale del disco che desideri proteggere. Ad esempio, se hai un disco da 18 GiB con una capacità configurata di 8 GiB, puoi utilizzare un disco da 9 GiB o superiore come hot spare. In generale, non assegnare un disco come hot spare a meno che la sua capacità non sia pari o superiore alla capacità del disco più grande nell'array di storage.

> Se non sono disponibili hot spare con la stessa capacità fisica, è possibile utilizzare un disco con capacità inferiore come hot spare se la "capacità utilizzata" del disco è uguale o inferiore alla capacità del disco hot spare.

Considerazioni relative ai tipi di media e di interfaccia

L'unità utilizzata come hot spare deve avere lo stesso tipo di supporto e di interfaccia delle unità che proteggerà. Ad esempio, un'unità HDD non può fungere da hot spare per unità SSD.

Considerazioni per le unità secure-capable

Un drive con funzionalità di sicurezza, come FDE o FIPS, può fungere da hot spare per drive con o senza funzionalità di sicurezza. Tuttavia, un drive che non è dotato di funzionalità di sicurezza non può fungere da hot spare per drive con funzionalità di sicurezza.

Quando si seleziona un'unità secure-enabled da utilizzare come hot spare, System Manager richiede di eseguire una Secure Erase prima di poter procedere. La Secure Erase ripristina gli attributi di sicurezza dell'unità a secure-capable, ma non secure-enabled.

> Quando si abilita la funzionalità Drive Security e poi si crea un pool o un gruppo di volumi da drive compatibili con la sicurezza, i drive diventano *secure-enabled*. L'accesso in lettura e scrittura è disponibile solo tramite un controller configurato con la chiave di sicurezza corretta. Questa maggiore sicurezza impedisce l'accesso non autorizzato ai dati su un drive fisicamente rimosso dall'array di storage.

Numero consigliato di hot spare

Se hai utilizzato la procedura guidata di configurazione iniziale per creare automaticamente hot spare, System Manager crea un hot spare ogni 30 dischi di un determinato tipo di supporto e di interfaccia. Altrimenti, puoi creare manualmente hot spare tra i gruppi di volumi nell'array di storage.

Assegna hot spare in SANtricity System Manager

È possibile assegnare una hot spare come unità di standby per una maggiore protezione dei dati nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Se un'unità si guasta in uno di questi gruppi di volumi, il controller ricostruisce i dati dall'unità guasta sulla hot spare.

Prima di iniziare

- È necessario creare gruppi di volumi RAID 1, RAID 5 o RAID 6. (Non è possibile utilizzare hot spare per i pool. Invece, un pool utilizza capacità di riserva presente in ciascun disco per la protezione dei dati.)
- Deve essere disponibile un'unità che soddisfi i seguenti criteri:
  - Non assegnato, con stato ottimale.
  - Stesso tipo di supporto delle unità presenti nel gruppo di volumi (ad esempio, SSDs).
  - Stesso tipo di interfaccia delle unità nel gruppo di volumi (ad esempio, SAS).
  - Capacità pari o superiore alla capacità utilizzata delle unità nel gruppo di volumi.

Informazioni su questa attività

Questa procedura descrive come assegnare manualmente un hot spare dalla pagina Hardware. La copertura consigliata è di due hot spare per set di unità.

> Gli hot spare possono anche essere assegnati dalla procedura guidata di configurazione iniziale. Puoi determinare se gli hot spare sono già assegnati cercando gli alloggiamenti delle unità mostrati in rosa nella pagina Hardware.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Seleziona un'unità non assegnata (mostrata in grigio) che desideri utilizzare come hot spare.

   Si apre il menu contestuale dell'unità.

4. Seleziona **Assegna hot spare**.

   Se l'unità è secure-enabled, si apre la finestra di dialogo Secure Erase Drive?. Per utilizzare un'unità secure-enabled come hot spare, è necessario prima eseguire un'operazione di Secure Erase per rimuovere tutti i dati e ripristinare gli attributi di sicurezza.

   > **Possibile perdita di dati** — Assicurati di aver selezionato l'unità corretta. Dopo aver completato l'operazione di Secure Erase, non puoi recuperare nessuno dei dati.

   Se l'unità **non** è abilitata per la protezione, si apre la finestra di dialogo Conferma assegnazione hot spare.

5. Rivedi il testo nella finestra di dialogo, e poi conferma l'operazione.

   L'unità viene visualizzata in rosa nella pagina Hardware, il che indica che ora è un hot spare.

Risultati

Se un'unità all'interno di un gruppo di volumi RAID 1, RAID 5 o RAID 6 si guasta, il controller utilizza automaticamente i dati di ridondanza per ricostruire i dati dall'unità guasta all'hot spare.

Annulla l'assegnazione degli hot spare in SANtricity System Manager

È possibile riportare un hot spare a un'unità non assegnata.

Prima di iniziare

Il hot spare deve trovarsi nello stato Optimal, Standby.

Informazioni su questa attività

Non è possibile rimuovere l'assegnazione di un hot spare che sta attualmente sostituendo un'unità guasta. Se l'hot spare non si trova nello stato Optimal, seguire le procedure di Recovery Guru per risolvere eventuali problemi prima di tentare di rimuovere l'assegnazione dell'unità.

Passaggi

1. Seleziona **Hardware**.
2. Se il grafico mostra i controller, fai clic sulla scheda **Drives**.

   La grafica cambia per mostrare le unità invece dei controller.

3. Seleziona l'hot spare (visualizzato in rosa) che desideri disassegnare.

   Se sul vano unità rosa sono presenti linee diagonali, la hot spare è attualmente in uso e non può essere disassegnata.

   Si apre il menu contestuale dell'unità.

4. Dall'elenco a discesa dell'unità, selezionare **Annulla assegnazione hot spare**.

   La finestra di dialogo mostra i gruppi di volumi interessati dalla rimozione di questo hot spare e se altri hot spare li stanno proteggendo.

5. Confermare l'operazione di annullamento dell'assegnazione.

Risultati

L'unità viene restituita a Unassigned (visualizzata in grigio).

Domande frequenti sullo shelf di storage per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è la shelf loss protection e la drawer loss protection?

La shelf loss protection e la drawer loss protection sono attributi dei pool e dei 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'involucro che contiene le unità disco oppure le unità disco e il controller. La protezione contro la perdita di shelf garantisce l'accessibilità ai dati sui volumi in un pool o gruppo di volumi in caso di perdita totale di comunicazione con uno shelf di dischi singolo. Un esempio di perdita totale di comunicazione potrebbe essere la perdita di alimentazione allo 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 di 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 contro la 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
Pool	Il pool deve includere dischi provenienti da almeno cinque shelf e in ogni shelf deve essere presente un numero uguale di dischi. La shelf loss protection non è applicabile agli shelf di elevata capacità; se il sistema contiene shelf di elevata capacità, fare riferimento alla Drawer Loss Protection.	5
RAID 6	Il gruppo di volumi contiene al massimo due dischi in uno shelf singolo.	3

Livello	Criteri per la protezione contro la perdita di shelf	Numero minimo di shelf richiesti
RAID 3 o RAID 5	Ciascun disco del gruppo di volumi è alloggiato in uno shelf separato.	3
RAID 1	Ciascun disco in una coppia RAID 1 deve essere collocato in uno shelf separato.	2
RAID 0	Impossibile ottenere la Shelf Loss Protection.	Non applicabile

Protezione contro la perdita del cassetto

Un cassetto è uno degli scomparti di uno shelf che si estrae per accedere ai dischi. Solo gli shelf di elevata capacità hanno cassetti. La protezione contro la perdita del cassetto garantisce l'accessibilità ai dati sui volumi in un pool o 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 al cassetto.

> La protezione contro la perdita di un cassetto non è garantita se un'unità si è già guastata nel pool o nel gruppo di volumi. In questa situazione, la perdita di accesso a un cassetto (e di conseguenza a un'altra unità nel pool o nel gruppo di volumi) comporta la perdita di dati.

I criteri per la protezione contro la perdita dei cassetti dipendono dal metodo di protezione, come descritto nella tabella seguente:

Livello	Criteri per la protezione contro la perdita dei drawer	Numero minimo di cassetti richiesti
Pool	I candidati per il pool devono includere dischi da tutti i cassetti e in ogni cassetto deve esserci un numero uguale di dischi. Il pool deve includere dischi provenienti da almeno cinque cassetti e deve esserci un numero uguale di dischi in ciascun cassetto. Uno shelf da 60 dischi può ottenere la Drawer Loss Protection quando il pool contiene 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 dischi. Incrementi in multipli di 5 possono essere aggiunti al pool dopo la creazione iniziale.	5

Livello	Criteri per la protezione contro la perdita dei drawer	Numero minimo di cassetti richiesti
RAID 6	Il gruppo di volumi contiene al massimo due drive in un singolo cassetto.	3
RAID 3 o RAID 5	Ciascun disco del gruppo di volumi è alloggiato in un cassetto separato.	3
RAID 1	Ciascun disco in una coppia speculare deve essere alloggiato in un cassetto separato.	2
RAID 0	Impossibile ottenere la Drawer Loss Protection.	Non applicabile

Che cosa sono i cicli di apprendimento della batteria?

Un ciclo di apprendimento è un ciclo automatico per la calibrazione dell'indicatore intelligente della batteria.

Un ciclo di apprendimento consiste in queste fasi:

- Scarica controllata della batteria
- periodo di riposo
- Carica

Le batterie vengono scaricate fino a una soglia predeterminata. Durante questa fase, l'indicatore di carica della batteria viene calibrato.

Un ciclo di apprendimento richiede questi parametri:

- Batterie completamente cariche
- Nessuna batteria surriscaldata

I cicli di apprendimento per i sistemi di controller duplex avvengono simultaneamente. Per i controller che dispongono di alimentazione di backup da più di una batteria o gruppo di celle della batteria, i cicli di apprendimento avvengono in sequenza.

I cicli di apprendimento sono programmati per avviarsi automaticamente a intervalli regolari, alla stessa ora e nello stesso giorno della settimana. L'intervallo tra i cicli è descritto in settimane.

Un ciclo di apprendimento potrebbe richiedere diverse ore per essere completato.

Domande frequenti sullo storage controller per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è l'auto-negotiation?

L'autonegoziazione è la capacità di un'interfaccia di rete di coordinare automaticamente i propri parametri di connessione (velocità e duplex) con un'altra interfaccia di rete.

La negoziazione automatica è generalmente l'impostazione preferita per la configurazione delle porte di gestione; tuttavia, se la negoziazione fallisce, le impostazioni dell'interfaccia di rete non corrispondenti possono influire negativamente sulle prestazioni della rete. Nei casi in cui tale condizione non sia accettabile, è necessario impostare manualmente le impostazioni dell'interfaccia di rete su una configurazione corretta. La negoziazione automatica viene eseguita dalle porte di gestione Ethernet del controller. La negoziazione automatica non viene eseguita dagli iSCSI host bus adapter.

Se la negoziazione automatica fallisce, il controller tenta di stabilire una connessione a 10BASE-T, half-duplex, che è il minimo comune denominatore.

Che cos'è l'autoconfigurazione degli indirizzi IPv6 senza stato?

Con l'autoconfigurazione stateless, gli host non ottengono indirizzi e altre informazioni di configurazione da un server.

L'autoconfigurazione stateless in IPv6 include indirizzi link-local, multicasting e il protocollo Neighbor Discovery (ND). IPv6 può generare l'ID dell'interfaccia di un indirizzo a partire dall'indirizzo del livello di collegamento dati sottostante.

L'autoconfigurazione senza stato e l'autoconfigurazione con stato si completano a vicenda. Ad esempio, l'host può utilizzare l'autoconfigurazione senza stato per configurare i propri indirizzi, ma utilizzare l'autoconfigurazione con stato per ottenere altre informazioni. L'autoconfigurazione con stato consente agli host di ottenere indirizzi e altre informazioni di configurazione da un server. Internet Protocol versione 6 (IPv6) definisce anche un metodo mediante il quale tutti gli indirizzi IP su una rete possono essere rinumerati contemporaneamente. IPv6 definisce un metodo per cui i dispositivi sulla rete possono configurare automaticamente il proprio indirizzo IP e altri parametri senza la necessità di un server.

I dispositivi eseguono questi passaggi quando utilizzano l'autoconfigurazione stateless:

1. **Genera un indirizzo link-local** — Il dispositivo genera un indirizzo link-local, che ha 10 bit, seguiti da 54 zeri e seguiti dall'ID dell'interfaccia a 64 bit.
2. **Verifica l'unicità di un indirizzo link-local** — Il nodo verifica che l'indirizzo link-local che genera non sia già in uso sulla rete locale. Il nodo invia un messaggio di richiesta di prossimità utilizzando il protocollo ND. In risposta, la rete locale ascolta un messaggio di annuncio di prossimità, che indica che un altro dispositivo sta già utilizzando l'indirizzo link-local. In tal caso, è necessario generare un nuovo indirizzo link-local oppure l'autoconfigurazione fallisce e si deve utilizzare un altro metodo.
3. **Assegna un indirizzo link-local** — Se il dispositivo supera il test di unicità, il dispositivo assegna l'indirizzo link-local alla sua interfaccia IP. L'indirizzo link-local può essere utilizzato per la comunicazione sulla rete locale ma non su Internet.
4. **Contattare il router** — Il nodo tenta di contattare un router locale per ottenere maggiori informazioni su come proseguire con la configurazione. Questo contatto avviene ascoltando i messaggi di annuncio del router inviati periodicamente dai router oppure inviando uno specifico messaggio di richiesta al router per ottenere informazioni su cosa fare dopo.
5. **Fornire indicazioni al nodo** — Il router fornisce al nodo indicazioni su come procedere con l'autoconfigurazione. In alternativa, il router indica all'host come determinare l'indirizzo Internet globale.
6. **Configura l'indirizzo globale** — L'host si configura con il suo indirizzo Internet univoco a livello globale. Questo indirizzo è generalmente formato da un prefisso di rete fornito all'host dal router.

Quale devo scegliere: DHCP o configurazione manuale?

Il metodo predefinito per la configurazione di rete è il Dynamic Host Configuration Protocol (DHCP). Utilizzare sempre questa opzione, a meno che la rete non disponga di un server DHCP.

Che cos'è un server DHCP?

Il Dynamic Host Configuration Protocol (DHCP) è un protocollo che automatizza l'assegnazione di un indirizzo Internet Protocol (IP).

A ciascun dispositivo connesso a una rete TCP/IP deve essere assegnato un indirizzo IP univoco. Questi dispositivi includono i controller nel sistema storage.

Senza DHCP, un amministratore di rete inserisce manualmente questi indirizzi IP. Con DHCP, quando un client deve avviare operazioni TCP/IP, il client invia una richiesta broadcast di informazioni sull'indirizzo. Il server DHCP riceve la richiesta, assegna un nuovo indirizzo per un periodo di tempo specificato, chiamato lease period, e invia l'indirizzo al client. Con DHCP, un dispositivo può avere un indirizzo IP diverso ogni volta che si connette alla rete. In alcuni sistemi, l'indirizzo IP del dispositivo può cambiare anche mentre il dispositivo è ancora connesso.

Come configuro il mio server DHCP?

È necessario configurare un server Dynamic Host Configuration Protocol (DHCP) per utilizzare indirizzi Internet Protocol (IP) statici per i controller nel sistema storage.

Gli indirizzi IP assegnati dal server DHCP sono generalmente dinamici e possono cambiare perché hanno un periodo di validità che scade. Alcuni dispositivi, ad esempio server e router, devono utilizzare indirizzi statici. I controller nel tuo storage array necessitano anch'essi di indirizzi IP statici.

Per informazioni su come assegnare indirizzi statici, consultare la documentazione per il server DHCP.

Perché devo modificare la configurazione di rete del controller?

È necessario impostare la configurazione di rete per ciascun controller—il suo indirizzo Internet Protocol (IP), la maschera di sottorete (subnet mask) e il gateway—quando si utilizza out-of-band management.

È possibile impostare la configurazione di rete utilizzando un server Dynamic Host Configuration Protocol (DHCP). Se non si utilizza un server DHCP, è necessario inserire la configurazione di rete manualmente.

Dove posso trovare la configurazione di rete?

È possibile ottenere l'indirizzo Internet Protocol (IP), la maschera di sottorete (subnet mask) e le informazioni sul gateway dal proprio amministratore di rete.

Queste informazioni sono necessarie quando si configurano le porte sui controller.

Che cosa sono le risposte ICMP PING?

Internet Control Message Protocol (ICMP) è uno dei protocolli della suite TCP/IP.

I `ICMP echo request` e i (`ICMP echo reply` messaggi sono comunemente noti come `ping` messaggi. `Ping` è uno strumento di risoluzione dei problemi utilizzato dagli amministratori di sistema per testare manualmente la connettività tra dispositivi di rete e anche per testare il ritardo di rete e la perdita di pacchetti. Il comando `ping` invia un `ICMP echo request` a un dispositivo sulla rete e il dispositivo risponde immediatamente con un (`ICMP echo reply`. A volte, la politica di sicurezza di rete di un'azienda richiede che

`ping` (`ICMP echo reply` sia disabilitato su tutti i dispositivi per renderli più difficili da individuare da parte di persone non autorizzate.

Quando devo aggiornare la configurazione della porta?

Aggiorna il server DHCP ogni volta che il server viene modificato o aggiornato e le informazioni DHCP relative all'array di storage corrente e all'array di storage che si desidera utilizzare sono cambiate.

In particolare, aggiorna la configurazione della porta o il server iSNS dal server DHCP quando sai che il server DHCP assegnerà indirizzi diversi.

> L'aggiornamento della configurazione di una porta è distruttivo per tutte le connessioni iSCSI su quella porta.

Cosa devo fare dopo aver configurato le porte di management?

Se hai modificato l'indirizzo IP dell'array di storage, potresti voler aggiornare la vista globale dell'array in SANtricity Unified Manager.

Per aggiornare la visualizzazione globale dell'array in Unified Manager, apri l'interfaccia e vai al **Manage › Discover**.

Se stai ancora utilizzando il SANtricity Storage Manager, vai alla Enterprise Management Window (EMW), dove devi rimuovere e aggiungere nuovamente il nuovo indirizzo IP.

Perché il sistema storage è in modalità non ottimale?

Un sistema storage in modalità non ottimale è dovuto a uno stato di configurazione di sistema non valido. Nonostante questo stato, il normale accesso I/O ai volumi esistenti è pienamente supportato; tuttavia, SANtricity System Manager proibirà alcune operazioni.

Un sistema storage potrebbe passare allo stato di Configurazione di sistema non valida per uno di questi motivi:

- Il controller non è conforme, probabilmente perché presenta un codice submodel ID (SMID) errato o perché ha superato il limite delle funzionalità premium.
- È in corso un'operazione di servizio interna, come ad esempio il download del firmware di un'unità.
- Il controller ha superato la soglia di errore di parità ed è andato in lockdown.
- Si è verificata una condizione di lockdown generale.

Domande frequenti sul protocollo iSCSI per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa succede quando utilizzo un server iSNS per la registrazione?

Quando si utilizzano le informazioni del server Internet Storage Name Service (iSNS), gli host (initiator) possono essere configurati per interrogare il server iSNS per recuperare informazioni dal target (controller).

Questa registrazione fornisce al server iSNS il nome qualificato iSCSI (IQN) e le informazioni sulla porta del controller, e consente le query tra gli initiator (host iSCSI) e i target (controller).

Quali metodi di registrazione sono supportati automaticamente per iSCSI?

L'implementazione iSCSI supporta sia il metodo di rilevamento Internet Storage Name Service (iSNS) sia l'utilizzo del comando Send Targets.

Il metodo iSNS consente il rilevamento iSNS tra gli initiator (host iSCSI) e i target (i controller). Si registra il controller di destinazione per fornire al server iSNS il nome qualificato iSCSI (IQN) del controller e le informazioni sulla porta.

Se non si configura iSNS, l'iSCSI host può inviare il comando Send Targets durante una sessione di rilevamento iSCSI. In risposta, il controller restituisce le informazioni sulla porta (ad esempio, il Target IQN, l'indirizzo IP della porta, la porta di ascolto e il Target Port Group). Questo metodo di rilevamento non è necessario se si utilizza iSNS, perché l'initiator può recuperare gli IP di destinazione dal server iSNS.

Come posso interpretare le statistiche iSER su InfiniBand?

La finestra di dialogo Visualizza statistiche iSER over InfiniBand mostra le statistiche locali del target (protocollo) e le statistiche dell'interfaccia iSER over InfiniBand (IB). Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche Local Target (Protocollo)** — Fornisce statistiche per l'iSER su InfiniBand target, che mostrano l'accesso a livello di blocco ai suoi supporti di memorizzazione.
- **Statistiche iSER over InfiniBand Interface** — Fornisce statistiche per tutte le porte iSER over InfiniBand sull'interfaccia InfiniBand, incluse le statistiche sulle prestazioni e le informazioni sugli errori di collegamento associate a ciascuna porta dello switch.

È possibile visualizzare ciascuna di queste statistiche come raw statistiche o come statistiche baseline. Le raw statistiche sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche baseline sono point-in-time statistiche raccolte a partire dal momento in cui è stato impostato il tempo di riferimento.

Cos'altro devo fare per configurare o diagnosticare iSER over InfiniBand?

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

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

Azione	Posizione
Configurare iSER sulle porte InfiniBand	1. Seleziona **Hardware**. 2. Seleziona la scheda **Controllers & Components**. 3. Seleziona un controller. 4. Selezionare **Configura iSER sulle porte InfiniBand**. o 1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **iSER over InfiniBand settings**, quindi seleziona **Configure iSER over InfiniBand Ports**.

Azione	Posizione
Visualizza statistiche iSER over InfiniBand	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **iSER over InfiniBand settings**, quindi seleziona **View iSER over InfiniBand Statistics**.

Cos'altro devo fare per configurare o diagnosticare iSCSI?

Le sessioni iSCSI possono avvenire con host o array di storage remoti in una relazione di mirroring asincrono. Le tabelle seguenti elencano le funzioni di SANtricity System Manager che è possibile utilizzare per configurare e gestire queste sessioni iSCSI.

Le impostazioni iSCSI sono disponibili solo se il tuo array di storage supporta iSCSI.

Configurare iSCSI

Azione	Posizione
Gestisci le impostazioni iSCSI	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **iSCSI settings** per visualizzare tutte le funzioni di gestione.
Configurare le porte iSCSI	1. Seleziona **Hardware**. 2. Seleziona la scheda **Controllers & Components**. 3. Seleziona un controller. 4. Selezionare **Configura porte iSCSI**.
Imposta il segreto CHAP host	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **iSCSI settings**, quindi seleziona **Configura autenticazione**. o 1. Seleziona **Storage › Hosts**. 2. Seleziona un host membro. 3. Fare clic su menu: Visualizza/Modifica impostazioni [Host Ports] tab.

Diagnosticare iSCSI

Azione	Posizione
Visualizzare o terminare le sessioni iSCSI	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **iSCSI settings**, quindi seleziona **View/End iSCSI Sessions**. o 1. Selezionare **Support › Support Center › Diagnostics** scheda. 2. Selezionare **Visualizza/Termina iSCSI Sessions**.
Visualizza statistiche iSCSI	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **impostazioni iSCSI**, quindi seleziona **Visualizza pacchetti di statistiche iSCSI**. o 1. Selezionare **Support › Support Center › Diagnostics** scheda. 2. Selezionare **Visualizza pacchetti di statistiche iSCSI**.

Domande frequenti sul protocollo NVMe per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Come si interpretano le statistiche NVMe over Fabrics?

La finestra di dialogo Visualizza statistiche NVMe over Fabrics mostra le statistiche per il sottosistema NVMe e l'interfaccia RDMA. Tutte le statistiche sono di sola lettura e non possono essere impostate.

- **Statistiche del sottosistema NVMe** — Mostra le statistiche relative al controller NVMe e alla sua coda. Il controller NVMe fornisce un percorso di accesso tra un host e i namespace nell'array di storage. È possibile esaminare le statistiche del sottosistema NVMe per elementi quali errori di connessione, ripristini e arresti. Per ulteriori informazioni su queste statistiche, fare clic su **Visualizza legenda per le intestazioni della tabella**.
- **Statistiche dell'interfaccia RDMA** — Fornisce statistiche per tutte le porte NVMe over Fabrics sull'interfaccia RDMA, incluse le statistiche sulle prestazioni e le informazioni sugli errori di collegamento associate a ciascuna porta dello switch. Questa scheda viene visualizzata solo quando sono disponibili porte NVMe over Fabrics. Per ulteriori informazioni sulle statistiche, fare clic su **Visualizza legenda per le intestazioni della tabella**.

È possibile visualizzare ciascuna di queste statistiche come raw statistiche o come statistiche baseline. Le raw statistiche sono tutte le statistiche raccolte dall'avvio dei controller. Le statistiche baseline sono point-in-time statistiche raccolte a partire dal momento in cui è stato impostato il tempo di riferimento.

Cos’altro devo fare per configurare o diagnosticare NVMe su InfiniBand?

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

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

Azione	Posizione
Configurare NVMe tramite InfiniBand porte	1. Seleziona **Hardware**. 2. Seleziona la scheda **Controllers & Components**. 3. Seleziona un controller. 4. Selezionare **Configura NVMe su InfiniBand ports**. o 1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **NVMe over InfiniBand settings**, quindi seleziona **Configure NVMe over InfiniBand Ports**.
Visualizza statistiche NVMe over InfiniBand	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **NVMe over InfiniBand settings**, quindi seleziona **Visualizza statistiche NVMe over Fabrics**.

Cos’altro devo fare per configurare o diagnosticare NVMe over RoCE?

È possibile configurare e gestire NVMe over RoCE dalle pagine Hardware e Impostazioni.

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

Azione	Posizione
Configura le porte NVMe over RoCE	1. Seleziona **Hardware**. 2. Seleziona la scheda **Controllers & Components**. 3. Seleziona un controller. 4. Selezionare **Configura NVMe su porte RoCE**. o 1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **NVMe over RoCE settings**, quindi seleziona **Configure NVMe over RoCE Ports**.

Azione	Posizione
Visualizza statistiche NVMe over Fabrics	1. Selezionare **Impostazioni › Sistema**. 2. Scorri verso il basso fino a **Impostazioni NVMe su RoCE**, quindi seleziona **Visualizza statistiche NVMe over Fabrics**.

Perché ci sono due indirizzi IP per una porta fisica?

Lo storage array EF600 può includere due HIC: uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. A ogni porta fisica accessibile dall'HIC esterno corrisponde una porta virtuale sull'HIC interno.

Per ottenere le massime prestazioni a 200Gb, è necessario assegnare un indirizzo IP univoco sia alla porta fisica che a quella virtuale, in modo che l'host possa stabilire connessioni con ciascuna. Se non si assegna un indirizzo IP alla porta virtuale, l'HIC funzionerà a circa metà della sua velocità massima.

Perché ci sono due serie di parametri per una porta fisica?

Lo storage array EF600 può includere due HIC: uno esterno e uno interno.

In questa configurazione, l'HIC esterno è collegato a un HIC interno ausiliario. A ogni porta fisica accessibile dall'HIC esterno corrisponde una porta virtuale sull'HIC interno.

Per ottenere le massime prestazioni a 200Gb, è necessario assegnare parametri sia alle porte fisiche che a quelle virtuali, in modo che l'host possa stabilire connessioni con ciascuna. Se non si assegnano parametri alla porta virtuale, l'HIC funzionerà a circa metà della sua velocità massima.

Domande frequenti sui dischi di storage per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è un hot spare?

Gli hot spare fungono da unità di standby nei gruppi di volumi RAID 1, RAID 5 o RAID 6. Sono unità perfettamente funzionanti che non contengono dati. Se un'unità si guasta nel gruppo di volumi, il controller ricostruisce automaticamente i dati dall'unità guasta su un hot spare.

Se un drive si guasta nell'array di storage, il drive hot spare viene automaticamente sostituito al drive guasto senza richiedere una sostituzione fisica. Se il drive hot spare è disponibile quando un drive si guasta, il controller utilizza i dati di ridondanza per ricostruire i dati dal drive guasto al drive hot spare.

Un'unità hot spare non è dedicata a uno specifico gruppo di volumi. Al contrario, puoi utilizzare un'unità hot spare per qualsiasi unità guasta nell'array di storage con la stessa capacità o una capacità inferiore. Un'unità hot spare deve essere dello stesso tipo di supporto (HDD o SSD) delle unità che protegge.

> Le unità hot spare non sono supportate nei pool. Invece delle unità hot spare, i pool utilizzano la capacità di preservazione all'interno di ciascuna unità che compone il pool.

Che cos'è la capacità di conservazione?

La capacità di conservazione è la quantità di capacità (numero di unità) che viene riservata in un pool per

supportare potenziali guasti delle unità.

Quando viene creato un pool, il sistema riserva automaticamente una quantità predefinita di capacità di conservazione a seconda del numero di unità nel pool.

I pool utilizzano la capacità di conservazione durante la ricostruzione, mentre i gruppi di volumi utilizzano hot spare drive per lo stesso scopo. Il metodo della capacità di conservazione rappresenta un miglioramento rispetto agli hot spare drive perché consente una ricostruzione più rapida. La capacità di conservazione è distribuita su più drive nel pool anziché su un solo drive nel caso di un hot spare drive, quindi non si è limitati dalla velocità o dalla disponibilità di un singolo drive.

Perché dovrei sostituire logicamente un'unità disco?

Se un'unità si guasta o si desidera sostituirla per qualsiasi altro motivo, e si dispone di un'unità non assegnata nell'array di storage, è possibile sostituire logicamente l'unità guasta con l'unità non assegnata. Se non si dispone di un'unità non assegnata, è possibile sostituire fisicamente l'unità.

I dati dall'unità originale vengono copiati o ricostruiti sull'unità sostitutiva.

Dove posso visualizzare lo stato di un drive in fase di ricostruzione?

È possibile visualizzare lo stato di ricostruzione dell'unità dalla dashboard Operations in Progress.

Dalla Home page, fai clic sul collegamento **Visualizza operazioni in corso** in alto a destra.

A seconda dell'unità, la ricostruzione completa potrebbe richiedere un tempo considerevole. Se la proprietà di un volume è cambiata, potrebbe essere necessaria una ricostruzione completa anziché una ricostruzione rapida.

Avvisi

Scopri gli avvisi in SANtricity System Manager

È possibile configurare SANtricity System Manager per inviare avvisi relativi agli array di storage tramite e-mail, trap SNMP e messaggi syslog.

Che cosa sono gli avvisi?

Alerts notificano agli amministratori eventi importanti che si verificano sull'array di storage. Gli eventi possono includere problemi come un guasto alla batteria, un componente che passa da Ottimale a Offline o errori di ridondanza nel controller. Tutti gli eventi Critical sono considerati "alertable", insieme ad alcuni eventi Warning e Informational.

Per saperne di più:

- "Come funzionano gli avvisi"
- "Terminologia degli avvisi"

Come si configurano gli avvisi?

È possibile configurare gli avvisi in modo che vengano inviati come messaggio a uno o più indirizzi e-mail, come trap SNMP a un server SNMP o come messaggio a un server syslog. La configurazione degli avvisi è disponibile dal **Impostazioni › Avvisi**.

Per saperne di più:

- "Configura il server di posta e i destinatari per gli avvisi"
- "Configura il server syslog per gli avvisi"
- "Configura gli avvisi SNMP"

Informazioni correlate

Scopri di più sui concetti relativi agli avvisi:

- "Panoramica del registro eventi"
- "Indicazioni temporali incoerenti"

Concetti

Come funzionano gli avvisi in SANtricity System Manager

Gli avvisi notificano agli amministratori gli eventi importanti che si verificano sull'array di storage. Gli avvisi possono essere inviati tramite email, trap SNMP e syslog.

Il processo di allerta funziona come segue:

1. Un amministratore configura uno o più dei seguenti metodi di avviso in System Manager:
   - **Email** — I messaggi vengono inviati agli indirizzi email.
   - **SNMP** — Le trap SNMP vengono inviate a un server SNMP.
   - **Syslog** — I messaggi vengono inviati a un syslog server.
2. Quando il monitor degli eventi dell'array di storage rileva un problema, scrive le informazioni relative a tale problema nel registro eventi (disponibile dal **Support › Event Log**). Ad esempio, i problemi possono includere eventi come un guasto della batteria, il passaggio di un componente dallo stato Optimal a Offline o errori di ridondanza nel controller.
3. Se il monitor degli eventi determina che l'evento è "alertable", invia una notifica utilizzando i metodi di allerta configurati (email, SNMP e/o syslog). Tutti gli eventi Critical sono considerati "alertable", insieme ad alcuni eventi Warning e Informational.

Configurazione degli avvisi

È possibile configurare gli avvisi tramite la procedura guidata di configurazione iniziale (solo per gli avvisi via e-mail) oppure dalla pagina Avvisi. Per verificare la configurazione corrente, andare su **Settings › Alerts**.

Il riquadro Avvisi visualizza la configurazione degli avvisi, che può essere una delle seguenti:

- Non configurato.
- Configurato; è impostato almeno un metodo di avviso. Per determinare quali metodi di avviso sono configurati, posizionare il cursore sul riquadro.

Informazioni sugli avvisi

Gli avvisi possono includere i seguenti tipi di informazioni:

- Nome dello storage array.
- Tipo di errore evento correlato a una voce del registro eventi.
- Data e ora in cui si è verificato l'evento.
- Breve descrizione dell'evento.

Gli avvisi syslog seguono lo standard di messaggistica RFC 5424.

Scopri la terminologia relativa agli avvisi nel software SANtricity

Scopri come si applicano i termini degli avvisi al tuo storage array.

Componente	Descrizione
Monitoraggio eventi	Il monitor degli eventi risiede sull'array di storage e viene eseguito come attività in background. Quando il monitor degli eventi rileva anomalie sull'array di storage, scrive informazioni sui problemi nel registro eventi. I problemi possono includere eventi come un guasto della batteria, un componente che passa da Ottimale a Offline o errori di ridondanza nel controller. Se il monitor degli eventi determina che l'evento è "alertable", invia quindi una notifica utilizzando i metodi di avviso configurati (email, SNMP e/o syslog). Tutti gli eventi Critical sono considerati "alertable", insieme ad alcuni eventi Warning e Informational.
Server di posta	Il server di posta viene utilizzato per l'invio e la ricezione di avvisi e-mail. Il server utilizza Simple Mail Transfer Protocol (SMTP).
SNMP	Simple Network Management Protocol (SNMP) è un protocollo standard Internet utilizzato per gestire e condividere informazioni tra dispositivi su reti IP.
Trappola SNMP	Una trap SNMP è una notifica inviata a un server SNMP. La trap contiene informazioni su problemi significativi relativi all'array di storage.
destinazione trap SNMP	Una destinazione trap SNMP è un indirizzo IPv4 o IPv6 del server su cui è in esecuzione un servizio SNMP.
Nome della community	Il nome della community è una stringa che funge da password per il/i server di rete in un ambiente SNMP.
File MIB	Il file MIB (Management Information Base) definisce i dati monitorati e gestiti nell'array di storage. Deve essere copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB è disponibile con il software System Manager sul sito di supporto.
Variabili MIB	Le variabili della Management Information Base (MIB) possono restituire valori come il nome dell'array di storage, la posizione dell'array e una persona di contatto in risposta a SNMP GetRequests.
syslog	Syslog è un protocollo utilizzato dai dispositivi di rete per inviare messaggi di evento a un server di logging.

Componente	Descrizione
UDP	User Datagram Protocol (UDP) è un protocollo di livello di trasporto che specifica un numero di porta di origine e di destinazione nelle intestazioni dei pacchetti.

Gestisci gli avvisi email

Configura il server di posta e i destinatari degli avvisi in SANtricity System Manager

Per configurare gli avvisi via email, è necessario specificare l'indirizzo del server di posta e gli indirizzi email dei destinatari. Sono consentiti fino a 20 indirizzi email.

Prima di iniziare

- L'indirizzo del server di posta deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6, oppure un fully qualified domain name.

> Per utilizzare un fully qualified domain name, è necessario configurare un DNS server su entrambi i controller. È possibile configurare un DNS server dalla pagina Hardware.

- L'indirizzo email da utilizzare come mittente dell'avviso deve essere disponibile. Questo è l'indirizzo che compare nel campo "Da" del messaggio di avviso. Un indirizzo del mittente è richiesto nel protocollo SMTP; senza di esso, si verifica un errore.
- L'indirizzo e-mail o gli indirizzi e-mail del destinatario o dei destinatari dell'avviso devono essere disponibili. Il destinatario è in genere un indirizzo per un amministratore di rete o un amministratore di storage. È possibile inserire fino a 20 indirizzi e-mail.

Informazioni su questa attività

Questa procedura descrive come configurare il mail server, inserire gli indirizzi email del mittente e dei destinatari e testare tutti gli indirizzi email inseriti dalla pagina Alerts.

> Gli avvisi e-mail possono anche essere configurati dalla procedura guidata di configurazione iniziale.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Email**.

   Se un server di posta elettronica non è ancora configurato, la scheda E-mail visualizza "Configura server di posta".

3. Seleziona **Configura Mail Server**.

   Si apre la finestra di dialogo Configure Mail Server.

4. Inserisci le informazioni del server di posta, quindi fai clic su **Salva**.
   - **Indirizzo del server di posta** — Inserire un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6 del server di posta.

Per utilizzare un fully qualified domain name, è necessario configurare un DNS server su entrambi i controller. È possibile configurare un DNS server dalla pagina Hardware.

- **Indirizzo del mittente email** — Inserisci un indirizzo email valido da utilizzare come mittente dell'email. Questo indirizzo appare nel campo "Da" del messaggio email.
- **Crittografia** — Se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. Altrimenti, selezionare **None**.
- **Nome utente e password** — Se necessario, inserire un nome utente e una password per l'autenticazione con il mittente in uscita e il server di posta.
- **Includi le informazioni di contatto nell'email** — Per includere le informazioni di contatto del mittente con il messaggio di avviso, seleziona questa opzione e poi inserisci un nome e un numero di telefono.

  Dopo aver cliccato su **Salva**, gli indirizzi email appaiono nella scheda Email della pagina Avvisi.

5. Seleziona **Add Emails**.

   Si apre la finestra di dialogo Add Emails.

6. Inserisci uno o più indirizzi email per i destinatari dell'avviso, quindi fai clic su **Aggiungi**.

   Gli indirizzi email compaiono nella pagina Alerts.

7. Se vuoi assicurarti che gli indirizzi email siano validi, fai clic su **Test All Emails** per inviare messaggi di prova ai destinatari.

Risultati

Dopo aver configurato gli avvisi e-mail, il monitor degli eventi invia messaggi e-mail ai destinatari specificati ogni volta che si verifica un evento segnalabile.

Modifica gli indirizzi email per gli avvisi in SANtricity System Manager

È possibile modificare gli indirizzi e-mail dei destinatari che ricevono avvisi e-mail.

Prima di iniziare

L'indirizzo email che si intende modificare deve essere definito nella scheda Email della pagina Avvisi.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Email**.
3. Dalla tabella **Email Address**, seleziona l'indirizzo che desideri modificare, quindi fai clic sull'icona **Edit** (matita) all'estrema destra.

   La riga diventa un campo modificabile.

4. Inserisci un nuovo indirizzo, quindi fai clic sull'icona **Salva** (segno di spunta).

   Se desideri annullare le modifiche, seleziona l'icona **Cancel** (X).

Risultati

La scheda Email della pagina Avvisi visualizza gli indirizzi email aggiornati.

Aggiungi indirizzi email per gli avvisi in SANtricity System Manager

È possibile aggiungere fino a 20 destinatari per gli avvisi e-mail.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Email**.
3. Seleziona **Add Emails**.

   Si apre la finestra di dialogo Add Emails.

4. Nel campo vuoto, inserisci un nuovo indirizzo email. Se desideri aggiungere più di un indirizzo, seleziona **Add another email** per aprire un altro campo.
5. Fai clic su **Add**.

Risultati

La scheda Email della pagina Avvisi visualizza i nuovi indirizzi email.

Elimina il server di posta o gli indirizzi email per gli avvisi in SANtricity System Manager

È possibile rimuovere il server di posta precedentemente definito in modo che gli avvisi non vengano più inviati agli indirizzi email, oppure è possibile rimuovere singoli indirizzi email.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Email**.
3. Dalla tabella, esegui una delle seguenti operazioni:
   - Per rimuovere un server di posta in modo che gli avvisi non vengano più inviati agli indirizzi e-mail, selezionare la riga per il server di posta.
   - Per rimuovere un indirizzo email in modo che gli avvisi non vengano più inviati a questo indirizzo, seleziona la riga dell'indirizzo email che desideri eliminare. Il pulsante **Elimina** in alto a destra della tabella diventa disponibile per la selezione.
4. Fai clic su **Delete** e conferma l'operazione.

Modifica il mail server per gli avvisi in SANtricity System Manager

È possibile modificare l'indirizzo del mail server e l'indirizzo del mittente e-mail utilizzati per gli avvisi e-mail.

Prima di iniziare

L'indirizzo del server di posta che si desidera modificare deve essere disponibile. L'indirizzo può essere un indirizzo IPv4 o IPv6, oppure un fully qualified domain name.

> Per utilizzare un fully qualified domain name, è necessario configurare un DNS server su entrambi i controller. È possibile configurare un DNS server dalla pagina Hardware.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Email**.
3. Seleziona **Configura Mail Server**.

   Si apre la finestra di dialogo Configure Mail Server.

4. Modifica l'indirizzo del server di posta, le informazioni del mittente e le informazioni di contatto.
   - **Indirizzo del mail server** — Modifica il fully qualified domain name, l'indirizzo IPv4 o l'indirizzo IPv6 del mail server.

     Per utilizzare un fully qualified domain name, è necessario configurare un DNS server su entrambi i controller. È possibile configurare un DNS server dalla pagina Hardware.

   - **Indirizzo del mittente email** — Modifica l'indirizzo email da utilizzare come mittente dell'email. Questo indirizzo appare nel campo "Da" del messaggio email.
   - **Includi le informazioni di contatto nell'email** — Per modificare le informazioni di contatto del mittente, seleziona questa opzione e poi modifica il nome e il numero di telefono.
5. Fare clic su **Save**.

Gestisci gli avvisi SNMP

Configura gli avvisi SNMP in SANtricity System Manager

Per configurare gli avvisi Simple Network Management Protocol (SNMP), è necessario identificare almeno un server a cui il monitor degli eventi dell'array di storage possa inviare trap SNMP. La configurazione richiede un nome di community o un nome utente e un indirizzo IP per il server.

Prima di iniziare

- È necessario configurare un server di rete con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), affinché il monitor degli eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (fino a 10 server sono consentiti).
- Il file management information base (MIB) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito di supporto NetApp:

  - Vai a "NetApp Supporto".
  - Fai clic sulla scheda **Downloads** e poi seleziona **Downloads**.
  - Fare clic su **E-Series SANtricity OS Controller Software**.
  - Seleziona **Download Latest Release**.
  - Accedi.
  - Accettare l'informativa di attenzione e il contratto di licenza.
  - Scorri verso il basso finché non vedi il file MIB per il tuo tipo di controller, quindi fai clic sul link per scaricare il file.

Informazioni su questa attività

Questa procedura descrive come identificare il server SNMP per le destinazioni delle trap e quindi testare la configurazione.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Durante la prima configurazione, la scheda SNMP visualizza "Configura Communities/Users."

3. Seleziona **Configure Communities/Users**.

   La finestra di dialogo Seleziona versione SNMP si apre.

4. Seleziona la versione SNMP per gli avvisi, **SNMPv2c** o **SNMPv3**.

   A seconda della selezione effettuata, si apre la finestra di dialogo Configure Communities oppure la finestra di dialogo Configure SNMPv3 Users.

5. Segui le istruzioni appropriate per SNMPv2c (communities) o SNMPv3 (users):
   - **SNMPv2c (communities)** — Nella finestra di dialogo Configura communities, inserire una o più stringhe di community per i server di rete. Un nome di community è una stringa che identifica un insieme noto di stazioni di gestione e viene tipicamente creato da un amministratore di rete. È composto esclusivamente da caratteri ASCII stampabili. È possibile aggiungere fino a 256 communities. Quando hai finito, fai clic su **Save**.
   - **SNMPv3 (utenti)** — Nella finestra di dialogo Configura SNMPv3 Users, fare clic su **Add** e quindi immettere le seguenti informazioni:
     - **Nome utente** — Inserire un nome per identificare l'utente, che può essere lungo fino a 31 caratteri.
     - **ID motore** — Selezionare l'ID motore, utilizzato per generare le chiavi di autenticazione e crittografia per i messaggi, e che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, si dovrebbe selezionare **Locale**. Se si dispone di una configurazione non standard, selezionare **Personalizzata**; verrà visualizzato un altro campo in cui è necessario immettere l'ID motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32.
     - **Credenziali di autenticazione** — Seleziona un protocollo di autenticazione, che garantisce l'identità degli utenti. Successivamente, inserisci una password di autenticazione, necessaria quando il protocollo di autenticazione viene impostato o modificato. La password deve essere lunga tra 8 e 128 caratteri.
     - **Credenziali di privacy** — Seleziona un protocollo di privacy, che viene utilizzato per crittografare il contenuto dei messaggi. Successivamente, inserisci una password di privacy, che è necessaria quando il protocollo di privacy viene impostato o modificato. La password deve essere compresa tra 8 e 128 caratteri. Quando hai terminato, fai clic su **Aggiungi** e poi su **Chiudi**.
6. Dalla pagina Alerts, con la scheda SNMP selezionata, fare clic su **Add Trap Destinations**.

   Si apre la finestra di dialogo Add Trap Destinations.

7. Inserisci una o più destinazioni trap, seleziona i nomi della community o i nomi utente associati e quindi fai clic su **Aggiungi**.
   - **Destinazione trap** — Inserire un indirizzo IPv4 o IPv6 del server su cui è in esecuzione un servizio SNMP.

- **Nome della community o nome utente** — Dal menu a tendina, seleziona il nome della community (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne hai definito solo uno, il nome appare già in questo campo.)
- **Invia trap di errore di autenticazione** — Seleziona questa opzione (la casella di controllo) se desideri avvisare la destinazione della trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di community o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, le destinazioni trap e i nomi associati vengono visualizzati nella scheda **SNMP** della pagina **Avvisi**.

8. Per assicurarti che una trap sia valida, seleziona una destinazione trap dalla tabella e poi fai clic su **Test Trap Destination** per inviare una trap di prova all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP al/ai server ogni volta che si verifica un evento segnalabile.

Aggiungi destinazioni trap per gli avvisi SNMP in SANtricity System Manager

È possibile aggiungere fino a 10 server per l'invio di trap SNMP.

Prima di iniziare

- Il server di rete che si desidera aggiungere deve essere configurato con un'applicazione di servizio SNMP. È necessario l'indirizzo di rete di questo server (un indirizzo IPv4 o IPv6), affinché il monitor degli eventi possa inviare messaggi trap a tale indirizzo. È possibile utilizzare più di un server (fino a 10 server sono consentiti).
- Il file management information base (MIB) è stato copiato e compilato sul server con l'applicazione del servizio SNMP. Questo file MIB definisce i dati monitorati e gestiti.

  Se non si dispone del file MIB, è possibile ottenerlo dal sito di supporto NetApp:

  - Vai a "NetApp Supporto".
  - Fai clic su **Downloads** e poi seleziona **Downloads**.
  - Fare clic su **E-Series SANtricity OS Controller Software**.
  - Seleziona **Download Latest Release**.
  - Accedi.
  - Accettare l'informativa di attenzione e il contratto di licenza.
  - Scorri verso il basso finché non vedi il file MIB per il tuo tipo di controller, quindi fai clic sul link per scaricare il file.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole attualmente definite vengono visualizzate nella tabella.

3. Seleziona **Add Trap Desinations**.

   Si apre la finestra di dialogo Add Trap Destinations.

4. Inserisci una o più destinazioni trap, seleziona i nomi della community o i nomi utente associati e quindi fai clic su **Aggiungi**.

- **Destinazione trap** — Inserire un indirizzo IPv4 o IPv6 del server su cui è in esecuzione un servizio SNMP.
- **Nome della community o nome utente** — Dal menu a tendina, seleziona il nome della community (SNMPv2c) o il nome utente (SNMPv3) per questa destinazione trap. (Se ne hai definito solo uno, il nome appare già in questo campo.)
- **Invia trap di errore di autenticazione** — Seleziona questa opzione (la casella di controllo) se desideri avvisare la destinazione trap ogni volta che una richiesta SNMP viene rifiutata a causa di un nome di community o di un nome utente non riconosciuto. Dopo aver fatto clic su **Aggiungi**, le destinazioni trap e i relativi nomi di community o nomi utente vengono visualizzati nella tabella.

5. Per assicurarti che una trap sia valida, seleziona una destinazione trap dalla tabella e poi fai clic su **Test Trap Destination** per inviare una trap di prova all'indirizzo configurato.

Risultati

Il monitor degli eventi invia trap SNMP al/ai server ogni volta che si verifica un evento segnalabile.

Configura le variabili SNMP MIB in SANtricity System Manager

Per gli avvisi SNMP, è possibile configurare facoltativamente le variabili Management Information Base (MIB) che appaiono nelle trap SNMP. Queste variabili possono restituire il nome dell'array di storage, la posizione dell'array e una persona di contatto.

Prima di iniziare

Il file MIB deve essere copiato e compilato sul server con l'applicazione del servizio SNMP.

Se non si dispone di un file MIB, è possibile ottenerlo come segue:

- Vai a "NetApp Supporto".
- Fai clic su **Downloads** e poi seleziona **Downloads**.
- Fare clic su **E-Series SANtricity OS Controller Software**.
- Seleziona **Download Latest Release**.
- Accedi.
- Accettare l'informativa di attenzione e il contratto di licenza.
- Scorri verso il basso finché non vedi il file MIB per il tuo tipo di controller, quindi fai clic sul link per scaricare il file.

Informazioni su questa attività

Questa attività descrive come definire le variabili MIB per le trap SNMP. Queste variabili possono restituire i seguenti valori in risposta a SNMP GetRequests:

- `sysName` (nome per l'array di archiviazione)
- `sysLocation` (posizione dell'array di archiviazione)
- `sysContact` (nome di un amministratore)

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

3. Seleziona **Configura variabili MIB SNMP**.

   La finestra di dialogo Configura variabili MIB SNMP si apre.

4. Inserisci uno o più dei seguenti valori, quindi fai clic su **Save**.
   - **Nome** — Il valore per la variabile MIB `sysName`. Ad esempio, immettere un nome per l'array di archiviazione.
   - **Posizione** — Il valore per la variabile MIB `sysLocation`. Ad esempio, immettere una posizione dell'array di archiviazione.
   - **Contatto** — Il valore per la variabile MIB `sysContact`. Ad esempio, immettere un amministratore responsabile dell'array di storage.

Risultati

Questi valori compaiono nei messaggi trap SNMP per gli avvisi degli array di storage.

Modifica le community per le trap SNMPv2c in SANtricity System Manager

È possibile modificare i nomi delle community per le trap SNMPv2c.

Prima di iniziare

È necessario creare un nome community.

Passaggi

1. Seleziona menu: Impostazioni[Avvisi].
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole e i nomi delle comunità appaiono nella tabella.

3. Seleziona **Configure Communities**.
4. Inserisci il nuovo nome della community, quindi fai clic su **Salva**. I nomi delle community possono essere composti solo da caratteri ASCII stampabili.

Risultati

La scheda SNMP della pagina Avvisi visualizza il nome della community aggiornato.

Modifica le impostazioni utente per le trap SNMPv3 in SANtricity System Manager

È possibile modificare le definizioni utente per le trap SNMPv3.

Prima di iniziare

È necessario creare un utente per la trap SNMPv3.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole e i nomi utente vengono visualizzati nella tabella.

3. Per modificare la definizione di un utente, selezionare l'utente nella tabella e quindi fare clic su **Configure Users**.

4. Nella finestra di dialogo, fai clic su **Visualizza/Modifica impostazioni**.
5. Modifica le seguenti informazioni:
   - **Nome utente** — Cambia il nome che identifica l'utente, che può essere lungo fino a 31 caratteri.
   - **ID motore** — Selezionare l'ID motore, utilizzato per generare le chiavi di autenticazione e crittografia per i messaggi, e che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, si dovrebbe selezionare **Locale**. Se si dispone di una configurazione non standard, selezionare **Personalizzata**; verrà visualizzato un altro campo in cui è necessario immettere l'ID motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32.
   - **Credenziali di autenticazione** — Seleziona un protocollo di autenticazione, che garantisce l'identità degli utenti. Successivamente, inserisci una password di autenticazione, necessaria quando il protocollo di autenticazione viene impostato o modificato. La password deve essere lunga tra 8 e 128 caratteri.
   - **Credenziali di privacy** — Seleziona un protocollo di privacy, che viene utilizzato per crittografare il contenuto dei messaggi. Successivamente, inserisci una password di privacy, richiesta quando il protocollo di privacy viene impostato o modificato. La password deve essere compresa tra 8 e 128 caratteri.

Risultati

La scheda SNMP della pagina Alerts visualizza le impostazioni aggiornate.

Aggiungi community per trap SNMPv2c in SANtricity System Manager

È possibile aggiungere fino a 256 nomi di community per le trap SNMPv2c.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole e i nomi delle comunità appaiono nella tabella.

3. Seleziona **Configure Communities**.

   Si apre la finestra di dialogo Configure Communities.

4. Seleziona **Aggiungi un'altra community**.
5. Inserisci il nuovo nome della community, quindi fai clic su **Salva**.

Risultati

Il nuovo nome della community viene visualizzato nella scheda SNMP della pagina Alerts.

Aggiungi utenti per le trap SNMPv3 in SANtricity System Manager

È possibile aggiungere fino a 256 utenti per le trap SNMPv3.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole e i nomi utente vengono visualizzati nella tabella.

3. Seleziona **Configure Users**.

   Si apre la finestra di dialogo Configura SNMPv3 Users.

4. Seleziona **Aggiungi**.
5. Inserisci le seguenti informazioni, quindi fai clic su **Aggiungi**.
   - **Nome utente** — Inserire un nome per identificare l'utente, che può essere lungo fino a 31 caratteri.
   - **ID motore** — Selezionare l'ID motore, utilizzato per generare le chiavi di autenticazione e crittografia per i messaggi, e che deve essere univoco nel dominio amministrativo. Nella maggior parte dei casi, si dovrebbe selezionare **Locale**. Se si dispone di una configurazione non standard, selezionare **Personalizzata**; verrà visualizzato un altro campo in cui è necessario immettere l'ID motore autorevole come stringa esadecimale, con un numero pari di caratteri compreso tra 10 e 32.
   - **Credenziali di autenticazione** — Seleziona un protocollo di autenticazione, che garantisce l'identità degli utenti. Successivamente, inserisci una password di autenticazione, necessaria quando il protocollo di autenticazione viene impostato o modificato. La password deve essere lunga tra 8 e 128 caratteri.
   - **Credenziali di privacy** — Seleziona un protocollo di privacy, che viene utilizzato per crittografare il contenuto dei messaggi. Successivamente, inserisci una password di privacy, richiesta quando il protocollo di privacy viene impostato o modificato. La password deve essere compresa tra 8 e 128 caratteri.

Rimuovere le community per le trap SNMPv2c in SANtricity System Manager

È possibile rimuovere un nome della community per le trap SNMPv2c.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trap e i nomi delle community appaiono nella pagina **Avvisi**.

3. Seleziona **Configure Communities**.

   Si apre la finestra di dialogo Configure Communities.

4. Seleziona il nome della community che desideri eliminare, quindi fai clic sull'icona **Remove** (X) all'estrema destra.

   Se a questo nome di comunità sono associate destinazioni di trap, la finestra di dialogo Conferma rimozione comunità mostra gli indirizzi delle destinazioni di trap interessate.

5. Conferma l'operazione, quindi fai clic su **Remove**.

Risultati

Il nome della comunità e la relativa destinazione trap vengono rimossi dalla pagina degli avvisi.

Rimuovere gli utenti per le trap SNMPv3 in SANtricity System Manager

È possibile rimuovere un utente per le trap SNMPv3.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Le destinazioni delle trappole e i nomi utente vengono visualizzati nella pagina Alerts.

3. Seleziona **Configure Users**.

   Si apre la finestra di dialogo Configura SNMPv3 Users.

4. Seleziona il nome utente che desideri eliminare, quindi fai clic su **Delete**.
5. Conferma l'operazione, quindi fai clic su **Delete**.

Risultati

Il nome utente e la relativa destinazione trap vengono rimossi dalla pagina degli avvisi.

Elimina le destinazioni trap in SANtricity System Manager

È possibile eliminare un indirizzo di destinazione delle trap in modo che il monitor degli eventi dell'array di storage non invii più trap SNMP a tale indirizzo.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **SNMP**.

   Gli indirizzi di destinazione delle trappole sono riportati nella tabella.

3. Seleziona una destinazione trap, quindi fai clic su **Elimina** nell'angolo in alto a destra della pagina.
4. Conferma l'operazione, quindi fai clic su **Delete**.

   L'indirizzo di destinazione non viene più visualizzato nella pagina degli avvisi.

Risultati

La destinazione trap eliminata non riceve più trap SNMP dal monitor eventi dell'array di storage.

Gestire gli avvisi syslog

Configurare il server syslog per gli avvisi in SANtricity System Manager

Per configurare gli avvisi syslog, è necessario inserire un indirizzo del server syslog e una porta UDP. Sono consentiti fino a cinque server syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero di porta UDP del syslog server deve essere disponibile. Questa porta è tipicamente 514.

Informazioni su questa attività

Questa procedura descrive come inserire l'indirizzo e la porta del server syslog e quindi testare l'indirizzo inserito.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Syslog**.

   Se un server syslog non è ancora stato definito, la pagina Avvisi visualizza "Aggiungi server syslog".

3. Fai clic su **Aggiungi Syslog Servers**.

   Si apre la finestra di dialogo Aggiungi Syslog Server.

4. Inserisci le informazioni relative a uno o più syslog server (massimo cinque), quindi fai clic su **Aggiungi**.
   - **Indirizzo del server** — Inserire un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
   - **Porta UDP** — In genere, la porta UDP per syslog è 514. La tabella mostra i syslog server configurati.
5. Per inviare un avviso di prova agli indirizzi del server, selezionare **Test All Syslog Servers**.

Risultati

Il monitor degli eventi invia avvisi al server syslog ogni volta che si verifica un evento che richiede un avviso. Per configurare ulteriormente le impostazioni syslog per i log di controllo, vedere "Configura il server syslog per i log di controllo".

> Se sono configurati più server syslog, tutti i server syslog configurati riceveranno un registro di controllo.

Modifica i server syslog per gli avvisi in SANtricity System Manager

È possibile modificare l'indirizzo del server utilizzato per ricevere gli avvisi syslog.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Syslog**.
3. Dalla tabella, seleziona un indirizzo del server syslog e poi fai clic sull'icona **Modifica** (matita) all'estrema destra.

   La riga diventa un campo modificabile.

4. Modifica l'indirizzo del server e il numero di porta UDP, quindi fai clic sull'icona **Save** (segno di spunta).

Risultati

L'indirizzo del server aggiornato compare nella tabella.

Aggiungere server syslog per gli avvisi in SANtricity System Manager

È possibile aggiungere un massimo di cinque server per gli avvisi syslog.

Prima di iniziare

- L'indirizzo del server syslog deve essere disponibile. Questo indirizzo può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
- Il numero di porta UDP del syslog server deve essere disponibile. Questa porta è tipicamente la 514.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Syslog**.
3. Seleziona **Aggiungi server Syslog**.

   Si apre la finestra di dialogo Aggiungi Syslog Server.

4. Seleziona **Aggiungi un altro syslog server**.
5. Inserisci le informazioni per il syslog server, quindi fai clic su **Aggiungi**.
   - **Indirizzo del server Syslog** — Inserire un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
   - **Porta UDP** — In genere, la porta UDP per syslog è 514.

   È possibile configurare fino a cinque syslog server.

Risultati

Gli indirizzi dei server syslog vengono visualizzati nella tabella.

Eliminare i server syslog per gli avvisi in SANtricity System Manager

È possibile eliminare un syslog server in modo che non riceva più avvisi.

Passaggi

1. Seleziona **Impostazioni › Avvisi**.
2. Seleziona la scheda **Syslog**.
3. Seleziona un indirizzo del server syslog, quindi fai clic su **Rimuovi** in alto a destra.

   Si apre la finestra di dialogo Conferma eliminazione Syslog server.

4. Conferma l'operazione, quindi fai clic su **Delete**.

Risultati

Il server che hai rimosso non riceve più avvisi dal monitor degli eventi.

Domande frequenti sugli avvisi del sistema di storage per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa succede se gli avvisi sono disattivati?

Se si desidera che gli amministratori ricevano notifiche relative a eventi importanti che si verificano nell'array di storage, è necessario configurare un metodo di avviso.

Per gli array di storage gestiti con SANtricity System Manager, configuri gli avvisi dalla pagina Avvisi. Le notifiche di avviso possono essere inviate tramite email, trap SNMP o messaggi syslog. Inoltre, gli avvisi email possono essere configurati dalla procedura guidata di configurazione iniziale.

Come configuro gli avvisi SNMP o syslog?

Oltre agli avvisi via e-mail, è possibile configurare gli avvisi da inviare tramite trap Simple Network Management Protocol (SNMP) o tramite messaggi syslog.

Per configurare gli avvisi SNMP o syslog, vai al **Impostazioni › Avvisi**.

Perché i timestamp non sono coerenti tra l'array e gli avvisi?

Quando l'array di storage invia avvisi, non corregge il fuso orario del server o host di destinazione che riceve gli avvisi. Al contrario, l'array di storage utilizza l'ora locale (GMT) per creare il timestamp utilizzato per il record di avviso. Di conseguenza, potresti vedere delle incongruenze tra i timestamp dell'array di storage e quelli del server o host che riceve un avviso.

Poiché l'array di storage non corregge il fuso orario durante l'invio degli avvisi, il timestamp degli avvisi è relativo al GMT, che ha un offset di fuso orario pari a zero. Per calcolare un timestamp appropriato al proprio fuso orario locale, è necessario determinare l'offset orario rispetto al GMT e quindi aggiungere o sottrarre tale valore dai timestamp.

Impostazioni array

Scopri la panoramica delle impostazioni in SANtricity System Manager

È possibile configurare SANtricity System Manager per alcune impostazioni generali dell'array e funzionalità aggiuntive.

Quali impostazioni posso configurare?

Le impostazioni dell'array includono:

- "Impostazioni cache e prestazioni"
- "Bilanciamento del carico automatico"
- "Funzionalità aggiuntive"
- "Sicurezza del disco"

Attività correlate

Scopri di più sulle attività relative alle System Settings:

- "Scarica l'interfaccia a riga di comando (CLI)"
- "Crea chiave di sicurezza interna"
- "Crea chiave di sicurezza esterna"
- "Configurare le porte iSCSI"
- "Configurare le porte NVME over IB"
- "Configura le porte NVMe over RoCE"

Concetti

Scopri le impostazioni della cache e le prestazioni nel software SANtricity

La memoria cache è un'area di memoria volatile temporanea sul controller che ha un tempo di accesso più rapido rispetto ai supporti di memorizzazione.

Grazie alla cache, le prestazioni complessive di I/O possono essere aumentate come segue:

- I dati richiesti all'host per una lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando così la necessità di accedere all'unità.
- I dati vengono inizialmente scritti nella cache, il che consente all'applicazione di continuare invece di attendere che i dati vengano scritti sull'unità.

Le impostazioni predefinite della cache soddisfano i requisiti della maggior parte degli ambienti, ma puoi modificarle se lo desideri.

Impostazioni della cache dell'array di storage

Per tutti i volumi nell'array di storage, puoi specificare i seguenti valori dalla pagina System:

- **Valore iniziale per lo svuotamento** — la percentuale di dati non scritti nella cache che attiva lo svuotamento della cache (scrittura su disco). Quando la cache contiene la percentuale iniziale specificata di dati non scritti, viene attivato lo svuotamento. Per impostazione predefinita, il controller avvia lo svuotamento della cache quando la cache raggiunge l'80 percento di riempimento.
- **Dimensione del blocco cache** — la dimensione massima di ciascun blocco cache, che rappresenta un'unità organizzativa per la gestione della cache. La dimensione del blocco cache è per impostazione predefinita 8 KiB, ma può essere impostata su 4, 8, 16 o 32 KiB. Idealmente, la dimensione del blocco cache dovrebbe essere impostata sulla dimensione I/O predominante delle tue applicazioni. I file system o le applicazioni di database generalmente utilizzano dimensioni inferiori, mentre una dimensione maggiore è adatta per applicazioni che richiedono grandi trasferimenti di dati o I/O sequenziale.

Impostazioni della cache di volume

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

- **Cache di lettura** — La cache di lettura è un buffer che memorizza i dati che sono stati letti dalle unità. I dati per un'operazione di lettura potrebbero essere già presenti nella cache da un'operazione precedente, eliminando la necessità di accedere alle unità. I dati rimangono nella cache di lettura finché non vengono svuotati.
  - **Precaricamento dinamico della cache di lettura** — Il precaricamento dinamico della cache di lettura consente al controller di copiare ulteriori blocchi di dati sequenziali nella cache mentre legge i blocchi di dati da un'unità alla cache. Questa memorizzazione nella cache aumenta la probabilità che le future richieste di dati possano essere soddisfatte dalla cache. Il precaricamento dinamico della cache di lettura è importante per le applicazioni multimediali che utilizzano I/O sequenziali. La velocità e la quantità di dati precaricati nella cache si regolano automaticamente in base alla velocità e alla dimensione delle richieste di lettura dell'host. L'accesso casuale non causa il precaricamento dei dati nella cache. Questa funzione non si applica quando la memorizzazione nella cache di lettura è disabilitata.
- **Cache di scrittura** — La cache di scrittura è un buffer che memorizza i dati provenienti dall'host che non sono ancora stati scritti sulle unità. I dati rimangono nella cache di scrittura finché non vengono scritti sulle

unità. La cache di scrittura può migliorare le prestazioni di I/O.

> **Possibile perdita di dati** — Se si abilita l'opzione **Write caching without batteries** e non si dispone di un alimentatore universale di protezione, si potrebbero perdere dati. Inoltre, si potrebbero perdere dati se non si dispone di batterie per il controller e si abilita l'opzione **Write caching without batteries**.

- **Cache di scrittura senza batterie** — L'impostazione cache di scrittura senza batterie consente di continuare la cache di scrittura anche quando le batterie sono mancanti, guaste, completamente scariche o non completamente cariche. La scelta della cache di scrittura senza batterie non è generalmente consigliata, perché i dati potrebbero andare persi se si verifica un'interruzione di corrente. In genere, la cache di scrittura viene temporaneamente disattivata dal controller fino a quando le batterie non sono cariche o una batteria guasta viene sostituita.
- **Cache di scrittura con mirroring** — La cache di 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 la cache di scrittura è abilitata e sono presenti due controller. La cache di scrittura con mirroring è l'impostazione predefinita alla creazione del volume.

Scopri il bilanciamento automatico del carico nel software SANtricity

Il bilanciamento automatico del carico fornisce una gestione delle risorse I/O migliorata reagendo dinamicamente alle variazioni di carico nel tempo e regolando automaticamente l'assegnazione dei controller di volume per correggere eventuali problemi di squilibrio del carico quando i carichi di lavoro si spostano tra i controller.

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

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

- Monitora e bilancia automaticamente l'utilizzo delle risorse del controller.
- Regola automaticamente la proprietà del controller di volume quando necessario, ottimizzando così la larghezza di banda tra gli host e l'array di storage.

Attivazione e disattivazione del bilanciamento automatico del carico

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

Potresti voler disabilitare il bilanciamento automatico del carico sul tuo array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un particolare volume per bilanciare il carico di lavoro.
- State operando in un ambiente altamente ottimizzato, dove la distribuzione del carico è configurata appositamente per ottenere una specifica distribuzione tra i controller.

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

Anche se il bilanciamento automatico del carico è abilitato a livello di array di storage, il tipo di host che selezioni per un host o un cluster influisce direttamente su come funziona questa funzionalità.

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

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

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

Tipo di host che supporta il bilanciamento automatico del carico	Con questo driver multipath
Windows o Windows Clustered	MPIO con NetApp E-Series DSM
Linux DM-MP (Kernel 3.10 o successivo)	DM-MP con `scsi_dh_alua` device handler
VMware	Native Multipathing Plugin (NMP) con `VMW_SATP_ALUA Storage Array Type` plug-in

> Salvo rare eccezioni, i tipi di host che non supportano il bilanciamento automatico del carico continuano a funzionare normalmente, indipendentemente dal fatto che la funzionalità sia abilitata. Un'eccezione è che, se un sistema ha un failover, gli array di storage spostano i volumi non mappati o non assegnati sul controller proprietario quando il percorso dei dati viene ripristinato. Qualsiasi volume mappato o assegnato a host non Automatic Load Balancing non viene spostato.

Consultare la "Strumento Interoperability Matrix Tool" per informazioni sulla compatibilità relative a driver multipath specifici, livelli di sistema operativo e supporto per i vassoi delle unità del controller.

Verifica della compatibilità del sistema operativo con la funzionalità Automatic Load Balancing

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

1. Vai su "Strumento Interoperability Matrix Tool" per trovare la tua soluzione e verificare il supporto.

   Se il tuo sistema utilizza Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, contatta il supporto tecnico.

2. Aggiorna e configura il `/etc/multipath.conf file`.
3. Assicurarsi che sia `retain_attached_device_handler` che `detect_prio` siano impostati su `yes` per il fornitore e il prodotto applicabili, oppure utilizzare le impostazioni predefinite.

Configura le impostazioni dell’array

Modifica il nome dell’array di storage in SANtricity System Manager

È possibile modificare il nome dell’array di storage visualizzato nella barra del titolo di SANtricity System Manager.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Generale**, cerca il campo **Name:**.

   Se non è stato definito un nome per l’array di archiviazione, questo campo visualizza "Unknown".

3. Fai clic sull’icona **Edit** (matita) accanto al nome dell’array di archiviazione.

   Il campo diventa modificabile.

4. Inserisci un nuovo nome.

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

5. Fai clic sull’icona **Salva** (segno di spunta).

   Se desideri chiudere il campo modificabile senza apportare modifiche, fai clic sull’icona **Cancel** (X).

Risultati

Il nuovo nome viene visualizzato nella barra del titolo di SANtricity System Manager.

Attiva le spie di localizzazione dell’array di storage in SANtricity System Manager

Per individuare la posizione fisica di un array di storage in un armadio, è possibile accendere le luci di localizzazione (LED).

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Generale**, fare clic su **Attiva le spie di localizzazione dell’array di storage**.

   La finestra di dialogo Attiva le spie di localizzazione dell’array di storage si apre e le spie di localizzazione dell’array di storage corrispondente si accendono.

3. Quando hai individuato fisicamente lo storage array, torna alla finestra di dialogo e seleziona **Turn Off**.

Risultati

Le spie di localizzazione si spengono e la finestra di dialogo si chiude.

Sincronizza gli orologi degli array di storage in SANtricity System Manager

Se il Network Time Protocol (NTP) non è abilitato, puoi impostare manualmente gli

orologi sui controller in modo che siano sincronizzati con il client di gestione (il sistema utilizzato per eseguire il browser che accede a SANtricity System Manager).

Informazioni su questa attività

La sincronizzazione garantisce che i time stamp degli eventi nel registro eventi corrispondano ai time stamp scritti nei file di registro dell'host. Durante il processo di sincronizzazione, i controller rimangono disponibili e operativi.

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

> Dopo la sincronizzazione, potresti notare che le statistiche sulle prestazioni sono perse o distorte, le pianificazioni (ASUP, snapshot, ecc.) sono influenzate e i time stamp nei dati di log sono distorti. L'utilizzo di NTP evita questo problema.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Generale**, fare clic su **Sincronizza gli orologi dell'array di storage**.

   Si apre la finestra di dialogo Sincronizza orologi array di storage. Mostra la data e l'ora correnti per il/i controller e il computer utilizzato come client di gestione.

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

3. Se gli orari visualizzati nella finestra di dialogo non corrispondono, fai clic su **Sincronizza**.

Risultati

Dopo che la sincronizzazione è stata completata con successo, i timestamp degli eventi sono gli stessi sia per il registro eventi che per i registri host.

Salva la configurazione dell'array di storage in SANtricity System Manager

È possibile salvare le informazioni di configurazione di un array di storage in un file di script per risparmiare tempo nell'impostazione di ulteriori array di storage con la stessa configurazione.

Prima di iniziare

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

Informazioni su questa attività

Il salvataggio della configurazione dell'array di storage genera uno script dell'interfaccia a riga di comando (CLI) che contiene le impostazioni dell'array di storage, la configurazione del volume, la configurazione dell'host o le assegnazioni host-volume per un array di storage. È possibile utilizzare questo script CLI generato per replicare una configurazione su un altro array di storage con la stessa identica configurazione hardware.

Tuttavia, non dovresti utilizzare questo script CLI generato per il disaster recovery. Invece, per eseguire un ripristino del sistema, utilizza il file di backup del database di configurazione che crei manualmente oppure contatta il supporto tecnico per ottenere questi dati dagli ultimi dati Auto-Support.

Questa operazione *non* salva queste impostazioni:

- La durata della batteria
- L'orario del controller
- Le impostazioni della memoria ad accesso casuale statica nonvolatile (NVSRAM)
- Qualsiasi funzionalità premium
- La password dell'array di storage
- Lo stato operativo e gli stati dei componenti hardware
- Lo stato operativo (ad eccezione di Optimal) e gli stati dei gruppi di volume
- Servizi di copia, come il mirroring e la copia di volumi

Rischio di errori applicativi — Non utilizzare questa opzione se l'array di storage è sottoposto a un'operazione che modificherà qualsiasi impostazione di configurazione logica. Esempi di queste operazioni includono la creazione o l'eliminazione di volumi, il download del firmware, l'assegnazione o la modifica di hot spare, o l'aggiunta di capacità (unità) a un gruppo di volumi.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Seleziona **Salva configurazione array di archiviazione**.
3. Seleziona gli elementi della configurazione che desideri salvare:
   - Impostazioni dell'array di storage
   - Configurazione del volume
   - Configurazione host
   - Assegnazioni host-volume

   Se selezioni la voce **Assegnazioni host-volume**, vengono selezionate automaticamente anche le voci **Configurazione volume** e **Configurazione host**. Non è possibile salvare "Assegnazioni host-volume" senza salvare anche "Configurazione volume" e "Configurazione host".
4. Fare clic su **Save**.

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

Dopo aver finito

Per caricare la configurazione salvata dell'array di storage su un altro array di storage, utilizzare l'interfaccia a riga di comando SANtricity (SMcli) con l'opzione `-f` per applicare il file `.cfg`.

È inoltre possibile caricare la configurazione di un array di storage su altri array di storage utilizzando l'interfaccia di Unified Manager (selezionare menu: Manage [Import Settings]).

Cancella la configurazione dell'array di storage in SANtricity System Manager

Utilizzare l'operazione Clear Configuration quando si desidera eliminare tutti i pool, i gruppi di volumi, i volumi, le definizioni host e le assegnazioni host dall'array di storage.

Prima di iniziare

Prima di cancellare la configurazione dell'array di archiviazione, eseguire il backup dei dati.

Informazioni su questa attività

Sono disponibili due opzioni Clear Storage Array Configuration:

- **Volume** — In genere, potresti utilizzare l'opzione Volume per riconfigurare un array di storage di test come array di storage di produzione. Ad esempio, potresti configurare un array di storage per il test e poi, al termine del test, rimuovere la configurazione di test e configurare l'array di storage per un ambiente di produzione.
- **Array di storage** — In genere, potresti utilizzare l'opzione Array di storage per spostare un array di storage in un altro reparto o gruppo. Ad esempio, potresti utilizzare un array di storage in Engineering e ora Engineering sta ricevendo un nuovo array di storage, quindi vuoi spostare l'array di storage attuale in Administration dove verrà riconfigurato.

  L'opzione Storage Array elimina alcune impostazioni aggiuntive.

	Volume	Array di archiviazione
Disattiva ARVM	X	X
Elimina pool e gruppi di volumi	X	X
Elimina volumi	X	X
Elimina host e cluster di host	X	X
Elimina le assegnazioni host	X	X
Elimina il nome dell'array di archiviazione		X
Reimposta le impostazioni della cache dell'array di archiviazione ai valori predefiniti		X

Rischio di perdita di dati — Questa operazione elimina tutti i dati dall'array di archiviazione. (Non esegue una cancellazione sicura.) Non è possibile annullare questa operazione dopo l'avvio. Eseguire questa operazione solo su indicazione del supporto tecnico.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Seleziona **Cancella configurazione array di archiviazione**.

3. Nell'elenco a discesa, seleziona **Volume** o **Storage Array**.
4. **Facoltativo:** Se si desidera salvare la configurazione (non i dati), utilizzare i link nella finestra di dialogo.
5. Conferma che desideri eseguire l'operazione.

Risultati

- La configurazione corrente viene eliminata, distruggendo tutti i dati esistenti sull'array di archiviazione.
- Tutte le unità sono non assegnate.

> L'array di storage si avvierà in modalità di ripristino. È necessario disattivare la modalità di ripristino prima di utilizzare l'array di storage. Vedere "Cancella modalità di ripristino" per ulteriori informazioni.

Modificare le impostazioni della cache dell'array di storage in SANtricity System Manager

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

Informazioni su questa attività

La memoria cache è un'area di archiviazione volatile temporanea sul controller, che offre tempi di accesso più rapidi rispetto ai supporti di memorizzazione. Per ottimizzare le prestazioni della cache, è possibile regolare le seguenti impostazioni:

Impostazione della cache	Descrizione
Avvia lo svuotamento della cache su richiesta	L'avvio dello svuotamento della cache su richiesta specifica la percentuale di dati non scritti nella cache che attiva uno svuotamento della cache (scrittura su disco). Per impostazione predefinita, lo svuotamento della cache inizia quando i dati non scritti raggiungono l'80% della capacità. Una percentuale più alta è una buona scelta per ambienti con operazioni prevalentemente di scrittura, così le nuove richieste di scrittura possono essere elaborate dalla cache senza dover accedere al disco. Impostazioni inferiori sono migliori in ambienti in cui l'I/O è irregolare (con picchi di dati), così il sistema svuota la cache frequentemente tra i picchi di dati. Tuttavia, una percentuale di avvio inferiore all'80% può causare una diminuzione delle prestazioni.
Dimensione del blocco cache	La dimensione del blocco della cache determina la dimensione massima di ciascun blocco della cache, che rappresenta un'unità organizzativa per la gestione della cache. Per impostazione predefinita, la dimensione del blocco è 32 KiB. Il sistema consente che la dimensione del blocco della cache sia 4, 8, 16 o 32 KiBs. Le applicazioni utilizzano dimensioni di blocco diverse, che hanno un impatto sulle performance dello storage. Una dimensione inferiore è una buona scelta per file system o applicazioni di database. Una dimensione maggiore è ideale per applicazioni che generano I/O sequenziali, come quelle multimediali.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive** e poi fai clic su **Modifica impostazioni cache**.

Si apre la finestra di dialogo Change Cache Settings.

3. Regola i seguenti valori:
   - **Avvia lo svuotamento della cache su richiesta** — Scegli una percentuale appropriata per l'I/O utilizzato nel tuo ambiente. Se scegli un valore inferiore all'80%, potresti notare un calo delle prestazioni.
   - **Cache block size —** Scegli una dimensione appropriata per le tue applicazioni.
4. Fare clic su **Save**.

Imposta il bilanciamento automatico del carico in SANtricity System Manager

La funzione di bilanciamento automatico del carico garantisce che il traffico I/O in entrata dagli host venga gestito e bilanciato dinamicamente tra entrambi i controller. Questa funzione è abilitata per impostazione predefinita, ma puoi disabilitarla da SANtricity System Manager.

Informazioni su questa attività

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

- Monitora e bilancia automaticamente l'utilizzo delle risorse del controller.
- Regola automaticamente la proprietà del controller di volume quando necessario, ottimizzando così la larghezza di banda tra gli host e l'array di storage.

Potresti voler disabilitare il bilanciamento automatico del carico sul tuo array di storage per i seguenti motivi:

- Non si desidera modificare automaticamente la proprietà del controller di un particolare volume per bilanciare il carico di lavoro.
- State operando in un ambiente altamente ottimizzato, dove la distribuzione del carico è configurata appositamente per ottenere una specifica distribuzione tra i controller.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive**, quindi fai clic su **Attiva/Disattiva bilanciamento automatico del carico**.

   Il testo sotto questa opzione indica se la funzione è attualmente abilitata o disabilitata.

   Si apre una finestra di dialogo di conferma.

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

   Selezionando questa opzione, si alterna la funzione tra abilitata/disabilitata.

   > Se questa funzione passa dallo stato disabilitato a quello abilitato, anche la funzione Host Connectivity Reporting viene abilitata automaticamente.

Abilitare o disabilitare l'interfaccia di gestione legacy in SANtricity System Manager

È possibile abilitare o disabilitare l'interfaccia di gestione legacy (SYMbol), che è un

metodo di comunicazione tra il sistema storage e il client di gestione.

Informazioni su questa attività

Per impostazione predefinita, l'interfaccia di gestione legacy è attiva. Se la disabiliti, l'array di storage e il client di gestione utilizzeranno un metodo di comunicazione più sicuro (REST API su https); tuttavia, alcuni strumenti e attività potrebbero essere influenzati se viene disabilitata.

Per il sistema storage EF600, questa funzione è disabilitata per impostazione predefinita.

L'impostazione influisce sulle operazioni come segue:

- **On** (impostazione predefinita) — Impostazione necessaria per configurare il mirroring tramite CLI e alcuni altri strumenti, come l'adattatore OCI.
- **Disattivato** — Impostazione necessaria per garantire la riservatezza delle comunicazioni tra l'array di storage e il client di gestione e per accedere a strumenti esterni. Impostazione consigliata durante la configurazione di un Directory Server (LDAP).

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. Scorri verso il basso fino a **Impostazioni aggiuntive** e poi fai clic su **Modifica interfaccia di gestione**.
3. Nella finestra di dialogo, fai clic su **Yes** per continuare.

Configura le funzionalità aggiuntive

Come funzionano le funzionalità aggiuntive in SANtricity System Manager

I componenti aggiuntivi sono funzionalità non incluse nella configurazione standard di SANtricity System Manager e potrebbero richiedere una chiave per essere abilitate. Un componente aggiuntivo può essere una singola funzionalità premium o un pacchetto di funzionalità.

I seguenti passaggi forniscono una panoramica per abilitare una funzionalità premium o un pacchetto di funzionalità:

1. Ottenere le seguenti informazioni:
   - Il numero di serie dello chassis e il Feature Enable Identifier, che identificano l'array di storage per il quale la funzionalità deve essere installata. Questi elementi sono disponibili in System Manager.
   - Codice di attivazione della funzionalità, disponibile sul sito di Support quando si acquista la funzionalità.
2. Ottieni la chiave della funzionalità contattando il tuo provider di storage o accedendo al sito di attivazione delle funzionalità Premium. Fornisci il numero di serie dello chassis, l'identificativo di abilitazione e il codice della funzionalità per l'attivazione.
3. Tramite System Manager, abilita la funzionalità premium o il pacchetto di funzionalità utilizzando il file della chiave delle funzionalità.

Scopri la terminologia relativa alle funzionalità aggiuntive nel software SANtricity

Scopri come si applicano i termini delle funzionalità aggiuntive al tuo storage array.

Termine	Descrizione
Identificatore di abilitazione della funzionalità	L'identificativo di abilitazione delle funzionalità è una stringa univoca che identifica uno specifico array di storage. Questo identificativo garantisce che quando si ottiene la funzionalità premium, essa sia associata solo a quello specifico array di storage. Questa stringa viene visualizzata nella sezione Add-Ons della pagina System.
File chiave funzionalità	Un file chiave funzionalità è un file che si riceve per sbloccare e abilitare una funzionalità premium o un feature pack.
Pacchetto funzionalità	Un feature pack è un pacchetto che modifica gli attributi di un array di storage (ad esempio, cambiando il protocollo da Fibre Channel a iSCSI). I feature pack richiedono una chiave speciale per essere abilitati.
Funzionalità premium	Una funzionalità premium è un'opzione aggiuntiva che richiede una chiave per essere attivata. Non è inclusa nella configurazione standard di System Manager.

Ottieni un file della chiave delle funzionalità in SANtricity System Manager

Per abilitare una funzionalità premium o un pacchetto di funzionalità sul tuo storage array, devi prima ottenere un file chiave della funzionalità. Una chiave è associata a un solo storage array.

Informazioni su questa attività

Questa attività descrive come raccogliere le informazioni necessarie per la funzionalità e quindi inviare una richiesta per un file chiave della funzionalità. Le informazioni richieste includono:

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

Passaggi

1. In System Manager, individua e annota il numero di serie dello chassis. Puoi visualizzare questo numero di serie posizionando il puntatore del mouse sul riquadro del Support Center.
2. In System Manager, individua il Feature Enable Identifier. Vai al **Settings › System**, quindi scorri verso il basso fino a **Add-ons**. Cerca il **Feature Enable Identifier**. Annota il numero del Feature Enable Identifier.
3. Individua e annota il codice per l'attivazione delle funzionalità. Per i feature pack, questo codice è fornito nelle istruzioni appropriate per eseguire la conversione.

   Per le funzionalità premium, puoi accedere al codice di attivazione dal sito di supporto, come segue:

   a. Accedi a "NetApp Supporto".
   b. Vai a **Licenze software** per il tuo prodotto.
   c. Inserisci il numero di serie dello chassis dello storage array, quindi fai clic su **Vai**.
   d. Cerca i codici di attivazione delle funzionalità nella colonna **License Key**.
   e. Annota il Feature Activation Code per la funzione che desideri.

4. Richiedete un file di attivazione della funzionalità inviando un'email o un documento di testo al vostro fornitore di storage con le seguenti informazioni: numero di serie dello chassis, identificativo di abilitazione e codice di attivazione della funzionalità.

   Puoi anche accedere a "NetApp License Activation: Attivazione della funzionalità Premium di Storage Array" e inserire le informazioni richieste per ottenere la funzionalità o il pacchetto di funzionalità. (Le istruzioni su questo sito si riferiscono alle funzionalità premium, non ai pacchetti di funzionalità.)

Dopo aver finito

Quando si dispone di un file di chiave delle funzionalità, è possibile abilitare la funzionalità premium o il pacchetto di funzionalità.

Abilita una funzionalità premium in SANtricity System Manager

Una funzionalità premium è un'opzione extra che richiede una chiave per essere abilitata.

Prima di iniziare

- Hai ottenuto una feature key. Se necessario, contatta il supporto tecnico per una chiave.
- Hai caricato il file chiave sul client di gestione (il sistema con un browser per accedere a System Manager).

Informazioni su questa attività

Questa procedura descrive come utilizzare System Manager per abilitare una funzionalità premium.

> Se si desidera disabilitare una funzionalità premium, è necessario utilizzare il comando Disable Storage Array Feature (`disable storageArray) (featurePack | feature=featureAttributeList`) nell'interfaccia a riga di comando (CLI).

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Componenti aggiuntivi**, seleziona **Abilita funzionalità Premium**.

   Si apre la finestra di dialogo Enable a Premium Feature.

3. Fai clic su **Sfoglia**, quindi seleziona il file chiave.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Fai clic su **Enable**.

Abilita il pacchetto di funzionalità in SANtricity System Manager

Un feature pack è un pacchetto che modifica gli attributi di un array di storage (ad esempio, cambiando il protocollo da Fibre Channel a iSCSI). I feature pack richiedono una chiave speciale per l'abilitazione.

Prima di iniziare

- Hai seguito le istruzioni appropriate relative alla conversione e alla preparazione per i nuovi attributi dell'array di storage. Per le istruzioni sulla conversione del protocollo host, consulta la guida alla manutenzione hardware del tuo modello di controller.
- L'array di storage è offline, quindi nessun host o applicazione vi sta accedendo.

- Tutti i dati sono sottoposti a backup.
- Hai ottenuto un file feature pack.

  Il file del pacchetto di funzionalità viene caricato sul client di gestione (il sistema dotato di un browser per accedere a System Manager).

> È necessario pianificare una finestra di manutenzione di downtime e interrompere tutte le operazioni di I/O tra l'host e i controller. Inoltre, si tenga presente che non sarà possibile accedere ai dati sull'array di storage fino al completamento con successo della conversione.

Informazioni su questa attività

Questa procedura descrive come utilizzare System Manager per abilitare un pacchetto di funzionalità. Al termine, è necessario riavviare il storage array.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Componenti aggiuntivi**, selezionare **Cambia Feature Pack**.
3. Fai clic su **Sfoglia**, quindi seleziona il file chiave.

   Il nome del file viene visualizzato nella finestra di dialogo.

4. Digita `change` nel campo.
5. Fai clic su **Change**.

   La migrazione del pacchetto di funzionalità ha inizio e i controller vengono riavviati. I dati della cache non ancora scritti vengono eliminati, il che garantisce l'assenza di attività di I/O. Entrambi i controller si riavviano automaticamente affinché il nuovo pacchetto di funzionalità abbia effetto. L'array di storage torna a uno stato reattivo al termine del riavvio.

Scarica l'interfaccia a riga di comando (CLI) SANtricity

Da SANtricity System Manager, puoi scaricare il pacchetto della command line interface (CLI).

La CLI fornisce un metodo testuale per configurare e monitorare gli array di storage. Comunica tramite https e utilizza la stessa sintassi della CLI disponibile nel pacchetto software di gestione installato esternamente. Non è necessaria alcuna chiave per scaricare la CLI.

Prima di iniziare

Sul sistema di gestione in cui si intende eseguire i comandi CLI deve essere disponibile un Java Runtime Environment (JRE), versione 8 o superiore.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Componenti aggiuntivi**, selezionare **Interfaccia a riga di comando**.

   Il pacchetto ZIP viene scaricato nel browser.

3. Salva il file ZIP nel sistema di gestione in cui intendi eseguire i comandi CLI per lo storage array, quindi

estrai il file.

Ora è possibile eseguire comandi CLI da un prompt del sistema operativo, come il prompt C: di DOS. Un riferimento ai comandi CLI è disponibile dal menu Guida in alto a destra dell'interfaccia utente di System Manager.

Domande frequenti sulle impostazioni degli array di storage per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Che cos'è il bilanciamento automatico del carico?

La funzione Automatic Load Balancing fornisce un bilanciamento I/O automatizzato e garantisce che il traffico I/O in entrata dagli host venga gestito e bilanciato dinamicamente tra entrambi i controller.

La funzione di bilanciamento automatico del carico fornisce una migliore gestione delle risorse I/O reagendo dinamicamente alle variazioni di carico nel tempo e regolando automaticamente l'assegnazione dei controller di volume per correggere eventuali problemi di squilibrio del carico quando i carichi di lavoro si spostano tra i controller.

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

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

- Monitora e bilancia automaticamente l'utilizzo delle risorse del controller.
- Regola automaticamente la proprietà del controller di volume quando necessario, ottimizzando così la larghezza di banda tra gli host e l'array di storage.

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

Che cos'è la cache del controller?

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

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

Quando la cache del controller riceve dati, il controller comunica alle applicazioni host che ora sta mantenendo i dati. In questo modo, le applicazioni host non devono attendere che l'I/O venga scritto su disco. Al contrario, le applicazioni possono continuare le operazioni. I dati memorizzati nella cache sono inoltre facilmente accessibili dalle applicazioni server, eliminando la necessità di ulteriori letture dal disco per accedere ai dati.

La cache del controller influisce sulle prestazioni complessive dell'array di storage in diversi modi:

- La cache funge da buffer, così i trasferimenti di dati tra host e disco non devono essere sincronizzati.

- I dati per un'operazione di lettura o scrittura dall'host potrebbero essere nella cache da un'operazione precedente, il che elimina la necessità di accedere al disco.
- Se si utilizza la cache di scrittura, l'host può inviare comandi di scrittura successivi prima che i dati di un'operazione di scrittura precedente vengano scritti su disco.
- Se il prefetch della cache è abilitato, l'accesso in lettura sequenziale viene ottimizzato. Il prefetch della cache rende più probabile che un'operazione di lettura trovi i suoi dati nella cache, invece di leggerli dal disco.

Possibile perdita di dati — Se si abilita l'opzione **Write caching without batteries** e non si dispone di un alimentatore universale di protezione, si potrebbero perdere dati. Inoltre, si potrebbero perdere dati se non si dispone di batterie per il controller e si abilita l'opzione **Write caching without batteries**.

Che cos'è lo svuotamento della cache?

Quando la quantità di dati non ancora scritti nella cache raggiunge un certo livello, il controller scrive periodicamente i dati memorizzati nella cache su un'unità. Questo processo di scrittura è chiamato "flushing".

Il controller utilizza due algoritmi per lo svuotamento della cache: uno basato sulla domanda e uno basato sull'età. Il controller utilizza un algoritmo basato sulla domanda finché la quantità di dati memorizzati nella cache non scende al di sotto della soglia di svuotamento della cache. Per impostazione predefinita, uno svuotamento inizia quando l'80 percento della cache è in uso.

In System Manager, è possibile impostare la soglia "Start demand cache flushing" per supportare al meglio il tipo di I/O utilizzato nel proprio ambiente. In un ambiente costituito principalmente da operazioni di scrittura, è necessario impostare la percentuale "Start demand cache flushing" su un valore alto per aumentare la probabilità che eventuali nuove richieste di scrittura possano essere elaborate dalla cache senza dover accedere al disco. Un'impostazione di percentuale alta limita il numero di svuotamenti della cache in modo che più dati rimangano nella cache, il che aumenta la possibilità di più riscontri nella cache.

In un ambiente in cui l'I/O è irregolare (con burst di dati), puoi utilizzare un basso svuotamento della cache in modo che il sistema svuoti la cache frequentemente tra i burst di dati. In un ambiente I/O eterogeneo che elabora una varietà di carichi, o quando il tipo di carichi è sconosciuto, imposta la soglia al 50 percento come buon compromesso. Tieni presente che se scegli una percentuale iniziale inferiore all'80 percento, potresti riscontrare una diminuzione delle performance perché i dati necessari per una lettura host potrebbero non essere disponibili. Scegliere una percentuale inferiore aumenta anche il numero di scritture su disco necessarie per mantenere il livello della cache, il che aumenta il sovraccarico del sistema.

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

Possibile perdita di dati — Se si abilita l'opzione **Write caching without batteries** e non si dispone di un alimentatore universale di protezione, si potrebbero perdere dati. Inoltre, si potrebbero perdere dati se non si dispone di batterie per il controller e si abilita l'opzione **Write caching without batteries**.

Che cos'è la dimensione del blocco della cache?

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

Le applicazioni utilizzano diverse dimensioni di blocco, che possono avere un impatto sulle performance dello storage. Per impostazione predefinita, la dimensione del blocco in System Manager è di 32 KiB, ma è possibile impostare il valore su 8, 16, 32 KiBs. Una dimensione più piccola è una buona scelta per file system o applicazioni database. Una dimensione più grande è una buona scelta per applicazioni che richiedono trasferimenti di dati di grandi dimensioni, I/O sequenziale o larghezza di banda elevata, come i multimedia.

Quando devo sincronizzare gli orologi degli array di storage?

È necessario sincronizzare manualmente gli orologi del controller nell'array di storage se si nota che i time stamp visualizzati in SANtricity System Manager non sono allineati con i time stamp visualizzati nel client di gestione (il computer che accede a SANtricity System Manager tramite browser). Questa operazione è necessaria solo se NTP (Network Time Protocol) non è abilitato in SANtricity System Manager.

> Consigliamo vivamente di utilizzare un server NTP anziché sincronizzare manualmente gli orologi. NTP sincronizza automaticamente gli orologi con un server esterno tramite SNTP (Simple Network Time Protocol).

È possibile verificare lo stato di sincronizzazione dalla finestra di dialogo Sincronizza orologi array di storage, disponibile nella pagina Sistema. Se gli orari visualizzati nella finestra di dialogo non corrispondono, eseguire una sincronizzazione. È possibile visualizzare periodicamente questa finestra di dialogo, che indica se le visualizzazioni degli orologi del controller si sono discostate e non sono più sincronizzate.

Sicurezza del disco

Scopri la sicurezza delle unità disco in SANtricity System Manager

È possibile configurare Drive Security e la gestione delle chiavi dalla pagina Security Key Management.

Che cos'è Drive Security?

La funzione *Drive Security* impedisce l'accesso non autorizzato ai dati sulle unità con sicurezza abilitata quando vengono rimosse dall'array di storage. Queste unità possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Quando le unità FDE o FIPS vengono rimosse fisicamente dall'array, non possono funzionare finché non vengono installate in un altro array; a quel punto, le unità saranno in uno stato di Security Locked finché non viene fornita la corretta security key. Una *security key* è una stringa di caratteri condivisa tra questi tipi di unità e i controller in un array di storage.

Per saperne di più:

- "Come funziona la funzione Drive Security"
- "Come funziona la gestione delle chiavi di sicurezza"
- "Terminologia della sicurezza delle unità"

Come si configura la gestione delle chiavi?

Per implementare Drive Security, è necessario che siano installate nell'array unità FDE o FIPS. Per configurare la gestione delle chiavi per queste unità, vai su **Settings › System › Security key management** dove puoi creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Infine, abiliti Drive Security per pool e gruppi di volumi selezionando "secure-capable" nelle impostazioni del volume.

Per saperne di più:

- "Crea chiave di sicurezza interna"
- "Crea chiave di sicurezza esterna"
- "Crea pool manualmente"
- "Crea gruppi di volume"

Come si sbloccano le unità?

Se hai configurato la gestione delle chiavi e successivamente sposti le unità secure-enabled da un array di storage a un altro, devi riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sulle unità.

Per saperne di più:

- "Sblocca le unità quando utilizzi la gestione interna delle chiavi"
- "Sblocca le unità quando utilizzi la gestione delle chiavi esterna"

Informazioni correlate

Scopri di più sulle attività relative alla gestione delle chiavi:

- "Utilizzare certificati firmati da CA per l'autenticazione con un server di gestione delle chiavi"
- "Esegui il backup della chiave di sicurezza"

Concetti

Come funziona la funzione Drive Security in SANtricity System Manager

Drive Security è una funzionalità degli array di storage che fornisce un ulteriore livello di sicurezza con unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS).

Quando queste unità vengono utilizzate con la funzione Drive Security, richiedono una chiave di sicurezza per accedere ai loro dati. Quando le unità vengono rimosse fisicamente dall'array, non possono funzionare finché non vengono installate in un altro array, a quel punto saranno in uno stato di Security Locked finché non verrà fornita la chiave di sicurezza corretta.

Come implementare Drive Security

Per implementare Drive Security, eseguire i seguenti passaggi.

1. Dotate il vostro storage array di unità compatibili con la sicurezza, ovvero unità FDE o unità FIPS. (Per i volumi che richiedono il supporto FIPS, utilizzate solo unità FIPS. La combinazione di unità FIPS e FDE in

un gruppo o pool di volumi comporterà il trattamento di tutte le unità come unità FDE. Inoltre, un'unità FDE non può essere aggiunta o utilizzata come unità di riserva in un gruppo o pool di volumi interamente composto da unità FIPS.)

2. Crea una chiave di sicurezza, ovvero una stringa di caratteri condivisa tra il controller e le unità per l'accesso in lettura/scrittura. Puoi creare una chiave interna dalla memoria persistente del controller oppure una chiave esterna da un key management server. Per la gestione delle chiavi esterne, è necessario stabilire l'autenticazione con il key management server.
3. Abilita la sicurezza delle unità per pool e gruppi di volumi:
   - Crea un pool o un gruppo di volumi (cerca **Yes** nella colonna **Secure-capable** nella tabella Candidates).
   - Selezionate un pool o un gruppo di volumi quando create un nuovo volume (cercate **Sì** accanto a **Compatibile con Secure** nella tabella dei candidati per pool e gruppi di volumi).

Come funziona Drive Security a livello di drive

Un'unità con funzionalità di sicurezza, FDE o FIPS, crittografa i dati durante la scrittura e li decrittografa durante la lettura. Questa crittografia e decrittografia non influisce sulle prestazioni o sul flusso di lavoro dell'utente. Ogni unità ha la propria chiave di crittografia univoca, che non può mai essere trasferita dall'unità.

La funzionalità Drive Security offre un ulteriore livello di protezione con unità compatibili con la protezione. Quando i gruppi di volumi o i pool su queste unità vengono selezionati per Drive Security, le unità cercano una chiave di sicurezza prima di consentire l'accesso ai dati. È possibile abilitare Drive Security per pool e gruppi di volumi in qualsiasi momento, senza influire sui dati esistenti sull'unità. Tuttavia, non è possibile disabilitare Drive Security senza cancellare tutti i dati presenti sull'unità.

Come funziona Drive Security a livello di storage array

Con la funzione Drive Security, si crea una chiave di sicurezza che viene condivisa tra le unità abilitate alla sicurezza e i controller in un array di storage. Ogni volta che l'alimentazione delle unità viene interrotta e riattivata, le unità abilitate alla sicurezza passano a uno stato Security Locked finché il controller non applica la chiave di sicurezza.

Se un'unità con protezione abilitata viene rimossa dall'array di storage e reinstallata in un array di storage diverso, l'unità sarà in uno stato di Security Locked. L'unità ricollocata cerca la security key prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, si applica la security key dall'array di storage di origine. Dopo un processo di sblocco riuscito, l'unità ricollocata utilizzerà la security key già memorizzata nell'array di storage di destinazione e il file della security key importato non sarà più necessario.

> Per la gestione interna delle chiavi, la chiave di sicurezza effettiva è memorizzata sul controller in una posizione non accessibile. Non è in un formato leggibile dall'uomo, né è accessibile agli utenti.

Come funziona Drive Security a livello di volume

Quando si crea un pool o un gruppo di volumi da unità compatibili con la sicurezza, è possibile abilitare la sicurezza dell'unità anche per tali pool o gruppi di volumi. L'opzione Sicurezza unità rende le unità e i gruppi di volumi e pool associati secure-*enabled*.

Tenete presenti le seguenti linee guida prima di creare gruppi di volumi e pool con funzionalità di sicurezza:

- I gruppi e i pool di volumi devono essere costituiti interamente da unità compatibili con la sicurezza. (Per i volumi che richiedono il supporto FIPS, utilizzare solo unità FIPS. La combinazione di unità FIPS e FDE in un gruppo o pool di volumi comporterà che tutte le unità vengano trattate come unità FDE. Inoltre, un'unità

FDE non può essere aggiunta o utilizzata come unità di riserva in un gruppo o pool di volumi composto esclusivamente da unità FIPS.)

- I gruppi di volume e i pool devono trovarsi in uno stato ottimale.

Come funziona la gestione delle chiavi di sicurezza in SANtricity System Manager

Quando si implementa la funzionalità Drive Security, le unità abilitate per la sicurezza (FIPS o FDE) richiedono una chiave di sicurezza per l'accesso ai dati. Una chiave di sicurezza è una stringa di caratteri condivisa tra questi tipi di unità e i controller in un array di storage.

Ogni volta che l'alimentazione delle unità viene interrotta e riattivata, le unità con funzionalità di sicurezza attiva passano allo stato Security Locked finché il controller non applica la chiave di sicurezza. Se un'unità con funzionalità di sicurezza attiva viene rimossa dall'array di storage, i dati dell'unità vengono bloccati. Quando l'unità viene reinstallata in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale.

È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi:

- Gestione interna delle chiavi sulla memoria persistente del controller.
- Gestione delle chiavi esterne su un server di gestione delle chiavi esterno.

Gestione interna delle chiavi

Le chiavi interne vengono gestite e "nasconste" in una posizione non accessibile nella memoria persistente del controller. Per implementare la gestione delle chiavi interne, eseguire i seguenti passaggi:

1. Installare unità con funzionalità di sicurezza nell'array di storage. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).
2. Assicurati che la funzione Drive Security sia abilitata. Se necessario, contatta il fornitore del tuo sistema di archiviazione per istruzioni su come abilitare la funzione Drive Security.
3. Creare una chiave di sicurezza interna, che prevede la definizione di un identificatore e di una pass phrase. L'identificatore è una stringa associata alla chiave di sicurezza, ed è memorizzato sul controller e su tutte le unità associate alla chiave. La pass phrase viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Per creare una chiave interna, andare su **Settings › System › Security key management › Create Internal Key**.

La chiave di sicurezza viene memorizzata sul controller in una posizione nascosta e non accessibile. È quindi possibile creare gruppi o pool di volumi con sicurezza abilitata, oppure abilitare la sicurezza su gruppi e pool di volumi esistenti.

Gestione delle chiavi esterne

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un Key Management Interoperability Protocol (KMIP). Per implementare la gestione delle chiavi esterne, eseguire i seguenti passaggi:

1. Installare unità con funzionalità di sicurezza nell'array di storage. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).
2. Assicurati che la funzione Drive Security sia abilitata. Se necessario, contatta il fornitore del tuo sistema di archiviazione per istruzioni su come abilitare la funzione Drive Security.

3. Ottieni un file di certificato client firmato. Un certificato client convalida i controller dell'array di storage, così il server di gestione delle chiavi può considerare attendibili le loro richieste KMIP.
   a. Innanzitutto, è necessario completare e scaricare una client Certificate Signing Request (CSR). Andare al **Settings › Certificates › Key Management › Complete CSR**.
   b. Successivamente, è necessario richiedere un certificato client firmato a una CA considerata attendibile dal key management server. (È anche possibile creare e scaricare un certificato client dal key management server utilizzando il file CSR.)
   c. Una volta ottenuto il file del certificato client, copia quel file sull'host da cui accedi a System Manager.
   d. In alternativa, è possibile generare esternamente una richiesta di firma del certificato utilizzando una coppia di chiavi privata e pubblica.
4. Recupera un file di certificato dal server di gestione delle chiavi e poi copia quel file sull'host da cui stai accedendo a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, così l'array di storage può considerare attendibile il suo indirizzo IP. Puoi utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.
5. Crea una chiave esterna, che comporta la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, carichi anche i file del certificato. Per creare una chiave esterna, vai su **Settings › System › Security key management › Create External Key**.

Il sistema si connette al server di gestione delle chiavi con le credenziali inserite. È quindi possibile creare gruppi o pool di volumi con sicurezza abilitata, oppure abilitare la sicurezza su gruppi e pool di volumi esistenti.

Scopri la terminologia relativa alla sicurezza delle unità nel software SANtricity

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

Termine	Descrizione
Funzione di sicurezza dell'unità	Drive Security è una funzionalità dell'array di storage che fornisce un ulteriore livello di sicurezza con unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS). Quando queste unità vengono utilizzate con la funzionalità Drive Security, richiedono una chiave di sicurezza per accedere ai loro dati. Quando le unità vengono rimosse fisicamente dall'array, non possono funzionare finché non vengono installate in un altro array; a quel punto, saranno in uno stato Security Locked finché non viene fornita la chiave di sicurezza corretta.
Unità FDE	Le unità Full Disk Encryption (FDE) eseguono la crittografia sul disco a livello hardware. Il disco rigido contiene un chip ASIC che crittografa i dati durante la scrittura e li decrittografa durante la lettura.
Unità FIPS	Le unità FIPS utilizzano i Federal Information Processing Standards (FIPS) 140-2 livello 2. Sono essenzialmente unità FDE che rispettano gli standard del governo degli Stati Uniti per garantire algoritmi e metodi di crittografia robusti. Le unità FIPS hanno standard di sicurezza più elevati rispetto alle unità FDE.
Client di gestione	Un sistema locale (computer, tablet, ecc.) che include un browser per accedere a System Manager.

Termine	Descrizione
Passphrase	La pass phrase viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. La stessa pass phrase utilizzata per crittografare la chiave di sicurezza deve essere fornita quando la chiave di sicurezza di cui è stato eseguito il backup viene importata a seguito di una migrazione del disco o di una sostituzione della testina. Una pass phrase può avere tra 8 e 32 caratteri. La passphrase per Drive Security è indipendente dalla password dell'Administrator dell'array di storage.
unità compatibili con la sicurezza	Le unità secure-capable possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS), che crittografano i dati durante la scrittura e li decrittografano durante la lettura. Queste unità sono considerate secure-*capable* perché possono essere utilizzate per una sicurezza aggiuntiva tramite la funzionalità Drive Security. Se la funzionalità Drive Security è abilitata per i gruppi di volumi e i pool utilizzati con queste unità, le unità diventano secure-*enabled*.
Unità con protezione abilitata	Le unità secure-enabled vengono utilizzate con la funzionalità Drive Security. Quando si abilita la funzionalità Drive Security e la si applica a un pool o a un gruppo di volumi su unità secure-capable, le unità diventano secure-enabled. L'accesso in lettura e scrittura è disponibile solo tramite un controller configurato con la chiave di sicurezza corretta. Questa maggiore sicurezza impedisce l'accesso non autorizzato ai dati su un'unità fisicamente rimossa dall'array di storage.
Chiave di sicurezza	Una chiave di sicurezza è una stringa di caratteri condivisa tra le unità abilitate alla sicurezza e i controller in un array di storage. Ogni volta che l'alimentazione delle unità viene interrotta e riattivata, le unità abilitate alla sicurezza passano allo stato Security Locked finché il controller non applica la chiave di sicurezza. Se un'unità abilitata alla sicurezza viene rimossa dall'array di storage, i dati dell'unità vengono bloccati. Quando l'unità viene reinstallata in un array di storage diverso, cerca la chiave di sicurezza prima di rendere nuovamente accessibili i dati. Per sbloccare i dati, è necessario applicare la chiave di sicurezza originale. È possibile creare e gestire le chiavi di sicurezza utilizzando uno dei seguenti metodi: • Gestione delle chiavi interne: crea e mantieni le chiavi di sicurezza nella memoria persistente del controller. • Gestione delle chiavi esterne: crea e mantieni le chiavi di sicurezza su un server di gestione delle chiavi esterno.
Identificatore della chiave di sicurezza	L'identificativo della chiave di sicurezza è una stringa associata alla chiave di sicurezza durante la creazione della chiave. L'identificativo viene memorizzato sul controller e su tutte le unità associate alla chiave di sicurezza.

Configura le chiavi di sicurezza

Creare una chiave di sicurezza interna in SANtricity System Manager

Per utilizzare la funzionalità Drive Security, è possibile creare una chiave di sicurezza interna che viene condivisa dai controller e dalle unità compatibili con la sicurezza presenti nell'array di storage. Le chiavi interne vengono mantenute nella memoria persistente del controller.

Prima di iniziare

- Nell'array di storage devono essere installate unità con funzionalità di sicurezza. Queste unità possono essere unità Full Disk Encryption (FDE) o unità Federal Information Processing Standard (FIPS).
- La funzionalità Drive Security deve essere abilitata. In caso contrario, durante questa operazione verrà visualizzata la finestra di dialogo Cannot Create Security Key. Se necessario, contattare il proprio storage vendor per istruzioni su come abilitare la funzionalità Drive Security.

> Se nell'array di storage sono installate sia unità FDE che FIPS, tutte condividono la stessa chiave di sicurezza.

Informazioni su questa attività

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

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

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiavi di sicurezza**, selezionare **Crea chiave interna**.

   Se non hai ancora generato una chiave di sicurezza, si apre la finestra di dialogo Crea chiave di sicurezza.

3. Inserisci le informazioni nei seguenti campi:

   - **Definisci un identificatore per la chiave di sicurezza** — Puoi accettare il valore predefinito (nome dell'array di storage e timestamp, generato dal firmware del controller) oppure inserire un valore personalizzato. Puoi inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

     > Vengono generati automaticamente dei caratteri aggiuntivi, aggiunti a entrambe le estremità della stringa inserita. I caratteri generati garantiscono che l'identificativo sia univoco.

   - **Definisci una pass phrase/Reinserisci la pass phrase** — Inserisci e conferma una pass phrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti:
     - Una o più lettere maiuscole. Ricorda che la pass phrase distingue tra maiuscole e minuscole.
     - Un numero (uno o più).
     - Un carattere non alfanumerico, come !, *, @ (uno o più).

     > **Assicurati di annotare le tue voci per un utilizzo successivo**. Se devi spostare un'unità protetta dall'array di storage, devi conoscere l'identificativo e la pass phrase per sbloccare i dati dell'unità.

4. Fai clic su **Create**.

   La chiave di sicurezza è memorizzata sul controller in una posizione non accessibile. Insieme alla chiave effettiva, viene scaricato dal browser un file chiave crittografato.

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

5. Annota il tuo identificatore chiave, la pass phrase e la posizione del file chiave scaricato, quindi fai clic su **Chiudi**.

Risultati

Ora puoi creare gruppi o pool di volumi con sicurezza abilitata, oppure puoi abilitare la sicurezza su gruppi e pool di volumi esistenti.

> Ogni volta che l'alimentazione delle unità viene interrotta e poi riattivata, tutte le unità con sicurezza abilitata passano allo stato Security Locked. In questo stato, i dati sono inaccessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione dell'unità. Se qualcuno rimuove fisicamente un'unità bloccata e la installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai suoi dati.

Dopo aver finito

Dovresti convalidare la chiave di sicurezza per assicurarti che il file della chiave non sia danneggiato.

Crea una chiave di sicurezza esterna in SANtricity System Manager

Per utilizzare la funzionalità Drive Security con un key management server, è necessario creare una chiave esterna condivisa dal key management server e dalle unità secure-capable nell'array di storage.

Prima di iniziare

- Nell'array devono essere installate unità secure-capable. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).

  > Se nell'array di storage sono installate sia unità FDE che FIPS, tutte condividono la stessa chiave di sicurezza.

- La funzionalità Drive Security deve essere abilitata. In caso contrario, durante questa operazione verrà visualizzata la finestra di dialogo Cannot Create Security Key. Se necessario, contattare il proprio storage vendor per istruzioni su come abilitare la funzionalità Drive Security.
- Hai un file di certificato client firmato per i controller dell'array di storage e lo hai copiato sull'host da cui accedi a System Manager. Un certificato client convalida i controller dell'array di storage, quindi il server di gestione delle chiavi può considerare attendibili le loro richieste Key Management Interoperability Protocol (KMIP).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi e quindi copiarlo sull'host da cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, quindi l'array di storage può considerare attendibile il suo indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

Per ulteriori informazioni sul certificato del server, consultare la documentazione per il proprio key management server.

Informazioni su questa attività

In questa attività, si definisce l'indirizzo IP del server di gestione delle chiavi e il numero di porta che utilizza, quindi si caricano i certificati per la gestione delle chiavi esterne.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiavi di sicurezza**, selezionare **Crea chiave esterna**.

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

   Si apre la finestra di dialogo Create External Security Key.

3. In **Connetti al server delle chiavi**, inserisci le informazioni nei seguenti campi.

   - **Indirizzo del server di gestione delle chiavi** — Inserire il fully qualified domain name o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - **Numero di porta per la gestione delle chiavi** — Inserire il numero di porta utilizzato per le comunicazioni KMIP. Il numero di porta più comune utilizzato per le comunicazioni con il key management server è 5696.

     Facoltativo: Se si desidera configurare un server di chiavi di backup, fare clic su **Aggiungi server di chiavi** e quindi immettere le informazioni relative a tale server. Il secondo server di chiavi verrà utilizzato se il server di chiavi primario non può essere raggiunto. Assicurarsi che ciascun server di chiavi abbia accesso allo stesso database di chiavi; in caso contrario, l'array genererà errori e non potrà utilizzare il server di backup.

     Viene utilizzato un solo server di chiavi alla volta. Se l'array di storage non riesce a raggiungere il server di chiavi primario, l'array contatterà il server di chiavi di backup. Tieni presente che è necessario mantenere la parità tra entrambi i server; in caso contrario potrebbero verificarsi errori.

   - **Seleziona il certificato client** — Fai clic sul primo pulsante **Browse** per selezionare il file del certificato per i controller dell'array di storage.
   - **Seleziona il file della chiave privata** — Se necessario, fai clic sul secondo pulsante **Sfoglia** per selezionare un file della chiave privata per i controller dell'array di storage.
   - **Seleziona il certificato del server di gestione delle chiavi** — Fai clic sul terzo pulsante **Sfoglia** per selezionare il file del certificato per il server di gestione delle chiavi. Puoi scegliere un certificato root, intermedio o server per il server di gestione delle chiavi.
4. Fai clic su **Avanti**.
5. In **Crea/Backup Key**, puoi creare una chiave di backup per motivi di sicurezza.

   - (Consigliato) Per creare una chiave di backup, mantieni la casella di controllo selezionata, quindi inserisci e conferma una pass phrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti:
     - Una o più lettere maiuscole. Ricorda che la pass phrase distingue tra maiuscole e minuscole.

- Un numero (uno o più).
- Un carattere non alfanumerico, come !, *, @ (uno o più).

Assicurati di annotare le tue voci per un utilizzo successivo. Se devi spostare un'unità protetta dall'array di archiviazione, devi conoscere la pass phrase per sbloccare i dati dell'unità.

+

- Se non si desidera creare una chiave di backup, deselezionare la casella di controllo.

Tieni presente che se perdi l'accesso al server delle chiavi esterno e non disponi di una chiave di backup, perderai l'accesso ai dati presenti sulle unità se queste vengono migrate su un altro storage array. Questa opzione è l'unico metodo per creare una chiave di backup in System Manager.

6. Fare clic su **Fine**.

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

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

7. Annota la tua pass phrase e la posizione del file chiave scaricato, quindi fai clic su **Chiudi**.

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

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

8. Verifica la connessione tra l'array di storage e il key management server selezionando **Test Communication**.

   I risultati del test vengono visualizzati nella finestra di dialogo.

Risultati

Quando la gestione delle chiavi esterne è abilitata, è possibile creare gruppi o pool di volumi con protezione abilitata, oppure abilitare la sicurezza su gruppi e pool di volumi esistenti.

Ogni volta che l'alimentazione delle unità viene interrotta e poi riattivata, tutte le unità con sicurezza abilitata passano allo stato Security Locked. In questo stato, i dati sono inaccessibili finché il controller non applica la chiave di sicurezza corretta durante l'inizializzazione dell'unità. Se qualcuno rimuove fisicamente un'unità bloccata e la installa in un altro sistema, lo stato Security Locked impedisce l'accesso non autorizzato ai suoi dati.

Dopo aver finito

Dovresti convalidare la chiave di sicurezza per assicurarti che il file della chiave non sia danneggiato.

Gestisci le chiavi di sicurezza

Modificare una chiave di sicurezza in SANtricity System Manager

È possibile sostituire una chiave di sicurezza con una nuova in qualsiasi momento. Potrebbe essere necessario modificare una chiave di sicurezza in caso di potenziale violazione della sicurezza nella propria azienda e voler assicurarsi che il personale non autorizzato non possa accedere ai dati delle unità.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Security key management**, selezionare **Change Key**.

   Si apre la finestra di dialogo Change Security Key.

3. Inserisci le informazioni nei seguenti campi.
   - **Definisci un identificatore per la chiave di sicurezza** — (Solo per chiavi di sicurezza interne.) Accetta il valore predefinito (nome dell'array di storage e timestamp, generato dal firmware del controller) oppure inserisci un valore personalizzato. Puoi inserire fino a 189 caratteri alfanumerici senza spazi, punteggiatura o simboli.

     Vengono generati automaticamente dei caratteri aggiuntivi che vengono aggiunti a entrambe le estremità della stringa inserita. I caratteri generati contribuiscono a garantire che l'identificativo sia univoco.

   - **Definisci una pass phrase/Reinserisci la pass phrase** — In ciascuno di questi campi, inserisci la tua pass phrase. Il valore può contenere da 8 a 32 caratteri e deve includere ciascuno dei seguenti:
     - Una o più lettere maiuscole. Ricorda che la pass phrase distingue tra maiuscole e minuscole.
     - Un numero (uno o più).
     - Un carattere non alfanumerico, come !, *, @ (uno o più).
4. Per le chiavi di sicurezza esterne, se si desidera eliminare la vecchia chiave di sicurezza quando viene creata quella nuova, selezionare la casella di controllo "Elimina la chiave di sicurezza corrente…" in fondo alla finestra di dialogo.

   Assicurati di annotare le tue voci per un utilizzo successivo — Se devi spostare un'unità secure-enabled dall'array di archiviazione, devi conoscere l'identificatore e la pass phrase per sbloccare i dati dell'unità.

5. Fai clic su **Change**.

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

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

6. Annota il tuo identificatore chiave, la pass phrase e la posizione del file chiave scaricato, quindi fai clic su **Chiudi**.

Dopo aver finito

Dovresti convalidare la chiave di sicurezza per assicurarti che il file della chiave non sia danneggiato.

Passare dalla gestione delle chiavi esterna a quella interna in SANtricity System Manager

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

Informazioni su questa attività

In questa operazione, si disabilita la gestione esterna delle chiavi e si scarica una nuova copia di backup sul computer locale. La chiave esistente viene comunque utilizzata per Drive Security, ma sarà gestita internamente nell'array di storage.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione delle chiavi di sicurezza**, selezionare **Disabilita gestione chiavi esterne**.

   Si apre la finestra di dialogo Disable External Key Management.

3. In **Definisci una pass phrase/Reinserisci pass phrase**, inserisci e conferma una pass phrase per la copia di backup della chiave. Il valore può avere tra 8 e 32 caratteri e deve includere ciascuno dei seguenti:

   - Una o più lettere maiuscole. Ricorda che la pass phrase distingue tra maiuscole e minuscole.
   - Un numero (uno o più).
   - Un carattere non alfanumerico, come !, *, @ (uno o più).

   > Assicurati di annotare le tue voci per un utilizzo successivo. Se devi spostare un'unità abilitata alla sicurezza dall'array di storage, devi conoscere l'identificativo e la pass phrase per sbloccare i dati dell'unità.

4. Fai clic su **Disable**.

   La chiave di backup viene scaricata sul tuo host locale.

5. Annota il tuo identificatore chiave, la pass phrase e la posizione del file chiave scaricato, quindi fai clic su **Chiudi**.

Risultati

La sicurezza delle unità è ora gestita internamente tramite l'array di storage.

Dopo aver finito

Dovresti convalidare la chiave di sicurezza per assicurarti che il file della chiave non sia danneggiato.

Modifica le impostazioni del key management server in SANtricity System Manager

Se hai configurato la gestione delle chiavi esterna, puoi visualizzare e modificare le impostazioni del key management server in qualsiasi momento.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione delle chiavi di sicurezza**, selezionare **Visualizza/Modifica Key Management Server Settings**.
3. Modifica le informazioni nei seguenti campi:
   - **Indirizzo del server di gestione delle chiavi** — Inserire il fully qualified domain name o l'indirizzo IP (IPv4 o IPv6) del server utilizzato per la gestione delle chiavi.
   - **Numero di porta per la gestione delle chiavi** — Inserire il numero di porta utilizzato per le comunicazioni del Key Management Interoperability Protocol (KMIP).

     Opzionale: puoi includere un altro key server facendo clic su **Add Key Server**.
4. Fare clic su **Save**.

Eseguire il backup delle chiavi di sicurezza in SANtricity System Manager

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

Informazioni su questa attività

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

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiave di sicurezza**, selezionare **Back Up Key**.

   Si apre la finestra di dialogo Back Up Security Key.
3. Nei campi **Definisci una pass phrase/Reinserisci la pass phrase**, inserisci e conferma una pass phrase per questo backup.

   Il valore può avere tra 8 e 32 caratteri e deve includere ciascuno dei seguenti:
   - Una o più lettere maiuscole
   - Un numero (uno o più)
   - Un carattere non alfanumerico, come !, *, @ (uno o più)

   Assicurati di annotare la tua voce per un utilizzo futuro. Ti serve la passphrase per accedere al backup di questa chiave di sicurezza.
4. Fai clic su **Back Up**.

   Una copia di backup della chiave di sicurezza viene scaricata sull'host locale, e quindi si apre la finestra di dialogo **Conferma/Registra backup chiave di sicurezza**.

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

5. Annota la tua pass phrase in un luogo sicuro, quindi fai clic su **Chiudi**.

Dopo aver finito

Dovresti convalidare la chiave di sicurezza di backup.

Convalida la chiave di sicurezza in SANtricity System Manager

È possibile convalidare la chiave di sicurezza per assicurarsi che non sia stata danneggiata e per verificare di avere una pass phrase corretta.

Informazioni su questa attività

Questa procedura descrive come convalidare la chiave di sicurezza creata in precedenza. Si tratta di un passaggio importante per assicurarsi che il file della chiave non sia danneggiato e che la pass phrase sia corretta, il che garantisce che sia possibile accedere ai dati dell'unità se si sposta un'unità abilitata alla sicurezza da un array di storage a un altro.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiavi di sicurezza**, seleziona **Convalida chiave**.

   Si apre la finestra di dialogo Validate Security Key.

3. Fai clic su **Sfoglia**, quindi seleziona il file chiave (ad esempio, `drivesecurity.slk`).
4. Inserisci la pass phrase associata alla chiave che hai selezionato.

   Quando selezioni un file chiave valido e una passphrase valida, il pulsante **Convalida** diventa disponibile.

5. Fai clic su **Validate**.

   I risultati della convalida vengono visualizzati nella finestra di dialogo.

6. Se il risultato mostra "La chiave di sicurezza è stata convalidata correttamente", fai clic su **Chiudi**. Se viene visualizzato un messaggio di errore, segui le istruzioni suggerite nella finestra di dialogo.

Sblocca le unità quando utilizzi la gestione delle chiavi interne in SANtricity System Manager

Se hai configurato la gestione interna delle chiavi e successivamente sposti le unità abilitate alla sicurezza da un array di storage a un altro, devi riassegnare la chiave di sicurezza al nuovo array di storage per accedere ai dati crittografati sulle unità.

Prima di iniziare

- Sull'array di origine (l'array da cui si stanno rimuovendo le unità), sono stati esportati i gruppi di volumi e sono state rimosse le unità. Sull'array di destinazione, hai reinstallato le unità.

  > La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia a riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nel "NetApp Knowledge Base". Assicurarsi di seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- La funzionalità Drive Security deve essere abilitata. In caso contrario, durante questa operazione verrà visualizzata la finestra di dialogo Cannot Create Security Key. Se necessario, contattare il proprio storage vendor per istruzioni su come abilitare la funzionalità Drive Security.
- È necessario conoscere la chiave di sicurezza associata alle unità che si desidera sbloccare.
- Il file della chiave di sicurezza è disponibile sul client di gestione (il sistema dotato di browser utilizzato per accedere a System Manager). Se si spostano le unità in un array di storage gestito da un sistema diverso, è necessario spostare il file della chiave di sicurezza su tale client di gestione.

Informazioni su questa attività

Quando si utilizza la gestione interna delle chiavi, la chiave di sicurezza viene memorizzata localmente sull'array di storage. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dalle unità per l'accesso in lettura/scrittura. Quando le unità vengono fisicamente rimosse dall'array e installate in un altro, non possono funzionare finché non viene fornita la chiave di sicurezza corretta.

> È possibile creare una chiave interna dalla memoria persistente del controller o una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando si utilizza la gestione delle chiavi *interna*. Se si utilizza la gestione delle chiavi *esterna*, vedere "Sblocca le unità quando utilizzi la gestione delle chiavi esterna". Se si sta eseguendo un aggiornamento del controller e si stanno sostituendo tutti i controller con l'hardware più recente, è necessario seguire procedure diverse come descritto nel centro di documentazione E-Series e SANtricity, in "Sblocca le unità".

Una volta reinstallate le unità protette in un altro array, quell'array rileva le unità e visualizza una condizione "Richiede attenzione" insieme allo stato "Chiave di sicurezza necessaria". Per sbloccare i dati dell'unità, selezionare il file della chiave di sicurezza e inserire la passphrase della chiave. (Questa passphrase non è la stessa della password di amministratore dell'array di storage.)

Se nel nuovo array di storage sono installate altre unità con funzionalità di sicurezza, queste potrebbero utilizzare una chiave di sicurezza diversa da quella che si sta importando. Durante il processo di importazione, la vecchia chiave di sicurezza viene utilizzata solo per sbloccare i dati delle unità che si stanno installando. Quando il processo di sblocco viene completato con successo, alle unità appena installate viene assegnata la chiave di sicurezza dell'array di storage di destinazione.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiavi di sicurezza**, selezionare **Sblocca unità protette**.

   Si apre la finestra di dialogo Sblocca unità protette. Le unità che richiedono una chiave di sicurezza vengono visualizzate nella tabella.

3. **Opzionale:** passa il mouse sopra il numero di un'unità per visualizzare la posizione dell'unità (numero di shelf e numero di bay).
4. Fai clic su **Sfoglia**, quindi seleziona il file della chiave di sicurezza che corrisponde all'unità che desideri sbloccare.

   Il file chiave selezionato appare nella finestra di dialogo.

5. Inserisci la pass phrase associata a questo file chiave.

   I caratteri che inserisci sono mascherati.

6. Fai clic su **Unlock**.

Se l'operazione di sblocco ha esito positivo, la finestra di dialogo visualizza: "Le unità protette associate sono state sbloccate."

Risultati

Quando tutte le unità vengono bloccate e poi sbloccate, ogni controller nell'array di storage si riavvia. Tuttavia, se sono già presenti alcune unità sbloccate nell'array di storage di destinazione, i controller non si riavviano.

Dopo aver finito

Sull'array di destinazione (l'array con le unità appena installate), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia a riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nel "NetApp Knowledge Base".

Sblocca le unità quando utilizzi la gestione delle chiavi esterne in SANtricity System Manager

Se hai configurato la gestione delle chiavi esterne e successivamente sposti le unità abilitate alla sicurezza da un array di storage a un altro, devi riassegnare la chiave di sicurezza al nuovo array di storage per poter accedere ai dati crittografati sulle unità.

Prima di iniziare

- Sull'array di origine (l'array da cui si stanno rimuovendo le unità), sono stati esportati i gruppi di volumi e sono state rimosse le unità. Sull'array di destinazione, hai reinstallato le unità.

  > La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia a riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

  Le istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nel "NetApp Knowledge Base". Assicurarsi di seguire le istruzioni appropriate per gli array più recenti gestiti da System Manager o per i sistemi legacy.

- La funzionalità Drive Security deve essere abilitata. In caso contrario, durante questa operazione verrà visualizzata la finestra di dialogo Cannot Create Security Key. Se necessario, contattare il proprio storage vendor per istruzioni su come abilitare la funzionalità Drive Security.
- È necessario conoscere l'indirizzo IP e il numero di porta del key management server.
- Hai un file di certificato client firmato per i controller dell'array di storage e lo hai copiato sull'host da cui accedi a System Manager. Un certificato client convalida i controller dell'array di storage, quindi il server di gestione delle chiavi può considerare attendibili le loro richieste Key Management Interoperability Protocol (KMIP).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi e quindi copiarlo sull'host da cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, quindi l'array di storage può considerare attendibile il suo indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione per il proprio key management server.

Informazioni su questa attività

Quando si utilizza la gestione delle chiavi esterna, la chiave di sicurezza viene memorizzata esternamente su un server progettato per proteggere le chiavi di sicurezza. Una chiave di sicurezza è una stringa di caratteri condivisa dal controller e dalle unità per l'accesso in lettura/scrittura. Quando le unità vengono fisicamente rimosse dall'array e installate in un altro, non possono funzionare finché non viene fornita la chiave di sicurezza corretta.

> È possibile creare una chiave interna dalla memoria persistente del controller oppure una chiave esterna da un server di gestione delle chiavi. Questo argomento descrive lo sblocco dei dati quando si utilizza la gestione delle chiavi *esterna*. Se si utilizza la gestione delle chiavi *interna*, consultare "Sblocca le unità quando utilizzi la gestione interna delle chiavi". Se si sta eseguendo un aggiornamento del controller e si stanno sostituendo tutti i controller con l'hardware più recente, è necessario seguire procedure diverse come descritto nel centro di documentazione E-Series e SANtricity, in "Sblocca le unità".

Una volta reinstallate le unità con funzionalità di sicurezza in un altro array, quell'array rileva le unità e visualizza una condizione "Richiede attenzione" insieme a uno stato "Chiave di sicurezza necessaria". Per sbloccare i dati dell'unità, si importa il file della chiave di sicurezza e si inserisce la passphrase della chiave. (Questa passphrase non è la stessa della password di amministratore dell'array di storage.) Durante questo processo, si configura l'array di storage per utilizzare un server di gestione delle chiavi esterno e quindi la chiave di sicurezza sarà accessibile. È necessario fornire le informazioni di contatto del server affinché l'array di storage possa connettersi e recuperare la chiave di sicurezza.

Se nel nuovo array di storage sono installate altre unità con funzionalità di sicurezza, queste potrebbero utilizzare una chiave di sicurezza diversa da quella che si sta importando. Durante il processo di importazione, la vecchia chiave di sicurezza viene utilizzata solo per sbloccare i dati delle unità che si stanno installando. Quando il processo di sblocco viene completato con successo, alle unità appena installate viene assegnata la chiave di sicurezza dell'array di storage di destinazione.

Passaggi

1. Selezionare **Impostazioni › Sistema**.
2. In **Gestione chiavi di sicurezza**, selezionare **Crea chiave esterna**.
3. Completa la procedura guidata con le informazioni di connessione prerequisito e i certificati.
4. Fai clic su **Test Communication** per assicurarti l'accesso al server esterno di gestione delle chiavi.
5. Seleziona **Sblocca unità protette**.

   Si apre la finestra di dialogo Sblocca unità protette. Le unità che richiedono una chiave di sicurezza vengono visualizzate nella tabella.

6. **Opzionale:** passa il mouse sopra il numero di un'unità per visualizzare la posizione dell'unità (numero di shelf e numero di bay).
7. Fai clic su **Sfoglia**, quindi seleziona il file della chiave di sicurezza che corrisponde all'unità che desideri sbloccare.

   Il file chiave selezionato appare nella finestra di dialogo.

8. Inserisci la pass phrase associata a questo file chiave.

   I caratteri che inserisci sono mascherati.

9. Fai clic su **Unlock**.

Se l'operazione di sblocco ha esito positivo, la finestra di dialogo visualizza: "Le unità protette associate sono state sbloccate."

Risultati

Quando tutte le unità vengono bloccate e poi sbloccate, ogni controller nell'array di storage si riavvia. Tuttavia, se sono già presenti alcune unità sbloccate nell'array di storage di destinazione, i controller non si riavviano.

Dopo aver finito

Sull'array di destinazione (l'array con le unità appena installate), è ora possibile importare gruppi di volumi.

> La funzione di esportazione/importazione non è supportata nell'interfaccia utente di System Manager; è necessario utilizzare l'interfaccia a riga di comando (CLI) per esportare/importare un gruppo di volumi in un array di storage diverso.

Istruzioni dettagliate per la migrazione di un gruppo di volumi sono fornite nel "NetApp Knowledge Base".

Domande frequenti sulla sicurezza delle unità di archiviazione per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa devo sapere prima di creare una chiave di sicurezza?

Una chiave di sicurezza è condivisa dai controller e dalle unità abilitate alla sicurezza all'interno di un array di storage. Se un'unità abilitata alla sicurezza viene rimossa 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 sulla memoria persistente del controller.
- Gestione delle chiavi esterne su un server di gestione delle chiavi esterno.

Gestione interna delle chiavi

Le chiavi interne vengono gestite e "nasconste" in una posizione non accessibile nella memoria persistente del controller. Prima di creare una chiave di sicurezza interna, è necessario eseguire le seguenti operazioni:

1. Installare unità con funzionalità di sicurezza nell'array di storage. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).
2. Assicurati che la funzione Drive Security sia abilitata. Se necessario, contatta il fornitore del tuo sistema di archiviazione per istruzioni su come abilitare la funzione Drive Security.

È quindi possibile creare una chiave di sicurezza interna, che prevede la definizione di un identificatore e di una pass phrase. L'identificatore è una stringa associata alla chiave di sicurezza e viene memorizzato sul controller e su tutte le unità associate alla chiave. La pass phrase viene utilizzata per crittografare la chiave di sicurezza a scopo di backup. Al termine della procedura, la chiave di sicurezza viene memorizzata sul controller in una posizione non accessibile. È quindi possibile creare gruppi o pool di volumi con funzionalità di sicurezza abilitate, oppure abilitare la sicurezza su gruppi e pool di volumi esistenti.

Gestione delle chiavi esterne

Le chiavi esterne vengono gestite su un server di gestione delle chiavi separato, utilizzando un Key

Management Interoperability Protocol (KMIP). Prima di creare una chiave di sicurezza esterna, è necessario eseguire le seguenti operazioni:

1. Installare unità con funzionalità di sicurezza nell'array di storage. Queste unità possono essere Full Disk Encryption (FDE) o Federal Information Processing Standard (FIPS).
2. Assicurati che la funzione Drive Security sia abilitata. Se necessario, contatta il fornitore del tuo sistema di archiviazione per istruzioni su come abilitare la funzione Drive Security.
3. Ottieni un file di certificato client firmato. Un certificato client convalida i controller dell'array di storage, così il server di gestione delle chiavi può considerare attendibili le loro richieste KMIP.
   a. Innanzitutto, è necessario completare e scaricare una client Certificate Signing Request (CSR). Andare al **Settings › Certificates › Key Management › Complete CSR**.
   b. Successivamente, è necessario richiedere un certificato client firmato a una CA considerata attendibile dal server di gestione delle chiavi. (È anche possibile creare e scaricare un certificato client dal server di gestione delle chiavi utilizzando il file CSR scaricato.)
   c. Una volta ottenuto il file del certificato client, copia quel file sull'host da cui accedi a System Manager.
4. Recupera un file di certificato dal server di gestione delle chiavi e poi copia quel file sull'host da cui stai accedendo a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, così l'array di storage può considerare attendibile il suo indirizzo IP. Puoi utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

È quindi possibile creare una chiave esterna, che comporta la definizione dell'indirizzo IP del server di gestione delle chiavi e del numero di porta utilizzato per le comunicazioni KMIP. Durante questo processo, si caricano anche i file del certificato. Quando hai finito, il sistema si connette al server di gestione delle chiavi con le credenziali inserite. È quindi possibile creare gruppi o pool di volumi con sicurezza abilitata, oppure abilitare la sicurezza su gruppi e pool di volumi esistenti.

Perché devo definire una pass phrase?

La pass phrase viene utilizzata per crittografare e decrittografare il file della chiave di sicurezza memorizzato sul client di gestione locale. Senza la pass phrase, la chiave di sicurezza non può essere decrittografata e utilizzata per sbloccare i dati da un'unità con protezione abilitata se questa viene reinstallata in un altro storage array.

Perché è importante registrare le informazioni sulla chiave di sicurezza?

Se si perdono le informazioni relative alla chiave di sicurezza e non si dispone di un backup, si potrebbero perdere dati durante lo spostamento di unità con protezione abilitata o l'aggiornamento di un controller. È necessaria la chiave di sicurezza per sbloccare i dati sulle unità.

Assicurati di annotare l'identificatore della chiave di sicurezza, la frase di accesso associata e il percorso sul computer locale in cui è stato salvato il file della chiave di sicurezza.

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

Se la chiave di sicurezza originale si corrompe e non si dispone di un backup, si perderà l'accesso ai dati sulle unità se vengono migrate da un array di storage a un altro.

Prima di eseguire il backup di una chiave di sicurezza, tieni presenti queste linee guida:

- Assicurati di conoscere l'identificativo della chiave di sicurezza e la pass phrase del file chiave originale.

Solo le chiavi interne utilizzano identificatori. Quando hai creato l'identificatore, sono stati generati automaticamente dei caratteri aggiuntivi che sono stati aggiunti a entrambe le estremità della stringa dell'identificatore. I caratteri generati garantiscono che l'identificatore sia univoco.

- Si crea una nuova pass phrase per il backup. Questa pass phrase non deve corrispondere alla pass phrase utilizzata quando è stata creata o modificata l'ultima volta la chiave originale. La pass phrase viene applicata solo al backup che si sta creando.

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

- Il file di backup della chiave di sicurezza viene scaricato sul client di gestione. Il percorso del file scaricato potrebbe dipendere dalla posizione di download predefinita del browser. Assicurati di annotare dove sono memorizzate le informazioni della chiave di sicurezza.

Cosa devo sapere prima di sbloccare le unità secure?

Per sbloccare i dati da un'unità con protezione attivata, è necessario importare la sua chiave di sicurezza.

Prima di sbloccare le unità secure-enabled, tieni presente le seguenti linee guida:

- L'array di storage deve già disporre di una chiave di sicurezza. Le unità migrate verranno riassociate alla chiave dell'array di storage di destinazione.
- Per le unità che si stanno migrando, è necessario conoscere l'identificativo della chiave di sicurezza e la pass phrase corrispondente al file della chiave di sicurezza.
- Il file della chiave di sicurezza deve essere disponibile sul client di gestione (il sistema con un browser utilizzato per accedere a System Manager).
- Se stai ripristinando un'unità NVMe bloccata, devi immettere l'ID di sicurezza dell'unità. Per individuare l'ID di sicurezza, devi rimuovere fisicamente l'unità e trovare la stringa PSID (massimo 32 caratteri) sull'etichetta dell'unità. Assicurati che l'unità sia reinstallata prima di iniziare l'operazione.

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

La finestra Impostazioni unità include informazioni sugli attributi di sicurezza dell'unità. "Accesso in lettura/scrittura" è uno degli attributi che viene visualizzato se i dati di un'unità sono stati bloccati.

Per visualizzare gli attributi di sicurezza dell'unità, vai alla pagina Hardware. Seleziona un'unità, fai clic su **Visualizza impostazioni** e poi su **Mostra altre impostazioni**. Nella parte inferiore della pagina, il valore dell'attributo Read/Write Accessible è **Sì** quando l'unità è sbloccata. Il valore dell'attributo Read/Write Accessible è **No, invalid security key** quando l'unità è bloccata. Puoi sbloccare un'unità protetta importando una security key (vai al **Settings › System › Unlock Secure Drives**).

Cosa devo sapere sulla convalida della security key?

Dopo aver creato una chiave di sicurezza, dovresti convalidare il file della chiave per assicurarti che non sia corrotto.

Se la convalida non riesce, procedi come segue:

- Se l'identificatore della chiave di sicurezza non corrisponde all'identificatore sul controller, individua il file della chiave di sicurezza corretto e quindi riprova la convalida.
- Se il controller non riesce a decrittare la chiave di sicurezza per la convalida, potresti aver inserito la pass phrase in modo errato. Ricontrolla la pass phrase, reinseriscila se necessario e poi prova di nuovo la convalida. Se il messaggio di errore appare di nuovo, seleziona un backup del file della chiave (se disponibile) e riprova la convalida.
- Se non riesci ancora a convalidare la chiave di sicurezza, il file originale potrebbe essere danneggiato. Crea un nuovo backup della chiave e convalida quella copia.

Qual è la differenza tra chiave di sicurezza interna e gestione della chiave di sicurezza esterna?

Quando si implementa la funzionalità Drive Security, è possibile utilizzare una chiave di sicurezza interna o una chiave di sicurezza esterna per bloccare i dati quando un'unità con sicurezza abilitata viene rimossa dall'array di archiviazione.

Una chiave di sicurezza è una stringa di caratteri, che è condivisa tra le unità abilitate alla sicurezza e i controller in un array di storage. Le chiavi interne sono mantenute nella memoria persistente del controller. Le chiavi esterne sono mantenute su un server di gestione delle chiavi separato, utilizzando un Key Management Interoperability Protocol (KMIP).

Gestione degli accessi

Scopri la gestione degli accessi in SANtricity System Manager

Access Management è un metodo per stabilire l'autenticazione degli utenti in SANtricity System Manager.

Quali metodi di autenticazione sono disponibili?

I metodi di autenticazione includono RBAC (in base al ruolo), Directory Services e Security Assertion Markup Language (SAML):

- **RBAC/Ruoli utente locali** — L'autenticazione viene gestita tramite le funzionalità RBAC implementate nell'array di storage. I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **Servizi di directory** — L'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e Directory Services, come Microsoft's Active Directory.
- **SAML** — L'autenticazione viene gestita tramite un Identity Provider (IdP) utilizzando SAML 2.0.

Per saperne di più:

- "Come funziona la gestione degli accessi"
- "Terminologia relativa alla gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "Ruoli utente locali"
- "Servizi di directory"
- "SAML"

Come si configura l'autenticazione?

L'array di storage è preconfigurato per utilizzare i ruoli utente locali, che rappresentano un'implementazione delle funzionalità RBAC. Se si desidera configurare un metodo diverso, andare su **Settings › Access Management**.

Per saperne di più:

- "Aggiungere un server di directory LDAP"
- "Configura SAML"

Informazioni correlate

Scopri di più sulle attività relative alla gestione degli accessi:

- "Modifica password"
- "Visualizza l'attività del registro di controllo"
- "Configura il server syslog per i log di controllo"

Concetti

Come funziona Access Management in SANtricity System Manager

Access Management è un metodo per stabilire l'autenticazione degli utenti in SANtricity System Manager.

La configurazione e l'autenticazione dell'utente funzionano come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni Security Admin.

   > Al primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. L'utente `admin` ha pieno accesso a tutte le funzioni del sistema.

2. L'amministratore accede alla sezione Access Management nell'interfaccia utente. L'array di storage è preconfigurato per utilizzare i ruoli utente locali, che sono un'implementazione delle funzionalità RBAC (role-based access control).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
   - **Ruoli utente locali** — L'autenticazione viene gestita tramite le funzionalità RBAC applicate nell'array di storage. I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come unico metodo di autenticazione o usarli in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, tranne l'impostazione delle password per gli utenti.
   - **Servizi di directory** — L'autenticazione viene gestita tramite un LDAP server (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft's Active Directory. Un amministratore si connette al LDAP server e quindi associa gli utenti LDAP ai ruoli utente locali incorporati nell'array di storage.
   - **SAML** — L'autenticazione viene gestita tramite un Identity Provider (IdP) utilizzando il Security Assertion Markup Language (SAML) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi associa gli utenti IdP ai ruoli utente locali incorporati nell'array di

storage.

4. L’amministratore fornisce agli utenti le credenziali di accesso per System Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali.

> Se l’autenticazione viene gestita con SAML e un SSO (single sign-on), il sistema potrebbe bypassare la finestra di dialogo di accesso di System Manager.

Durante l’accesso, il sistema esegue le seguenti attività in background:

- Autentica il nome utente e la password rispetto all’account utente.
- Determina le autorizzazioni dell’utente in base ai ruoli assegnati.
- Fornisce all’utente l’accesso alle attività nell’interfaccia utente.
- Visualizza il nome utente nell’angolo in alto a destra dell’interfaccia.

Attività disponibili in System Manager

L’accesso alle attività dipende dai ruoli assegnati all’utente, che includono i seguenti:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l’interfaccia di gestione legacy (SYMbol).
- **Support admin** — Accesso a tutte le risorse hardware sull’array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Un’attività non disponibile viene visualizzata in grigio o non è presente nell’interfaccia utente. Ad esempio, un utente con il ruolo di Monitor può visualizzare tutte le informazioni sui volumi, ma non può accedere alle funzioni per modificare quel volume. Le schede relative a funzionalità come **Copy Services** e **Add to Workload** saranno disattivate; sarà disponibile solo **View/Edit Settings**.

Limitazioni in Unified Manager e Storage Manager

Se SAML è configurato per un array di storage, gli utenti non possono individuare o gestire lo storage per tale array da Unified Manager o dalle interfacce legacy Storage Manager.

Quando vengono configurati i ruoli utente locali e i servizi di directory, gli utenti devono immettere le credenziali prima di eseguire una delle seguenti funzioni:

- Rinominare lo storage array
- Aggiornamento firmware del controller
- Caricamento di una configurazione di storage array
- Esecuzione di uno script
- Tentativo di eseguire un’operazione attiva quando una sessione non utilizzata è scaduta

Scopri la terminologia relativa alla gestione degli accessi nel software SANtricity

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

Termine	Descrizione
Token di accesso	I token di accesso vengono utilizzati per l'autenticazione con l'API REST o l'interfaccia a riga di comando (CLI) al posto di nome utente e password. I token sono associati a un utente specifico (inclusi gli utenti LDAP) e includono un insieme di autorizzazioni e una scadenza.
Active Directory	Active Directory (AD) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Legame	Le operazioni di bind vengono utilizzate per autenticare i client al directory server. Il bind richiede in genere credenziali di account e password, ma alcuni server consentono operazioni di bind anonime.
CA	Un'autorità di certificazione (CA) è un'entità fidata che rilascia documenti elettronici, chiamati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti web, il che consente connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli aggressori di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e sull'identità dell'entità di fiducia che certifica (firma) queste informazioni.
IdP	Un Identity Provider (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se quell'utente è stato autenticato con successo. L'IdP può essere configurato per fornire l'autenticazione a più fattori e per utilizzare qualsiasi database utente, come Active Directory. Il team di sicurezza è responsabile della manutenzione dell'IdP.
LDAP	Il Lightweight Directory Access Protocol (LDAP) è un protocollo applicativo per l'accesso e la gestione di servizi di informazioni di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi di connettersi al LDAP server per validare gli utenti.
RBAC	Il controllo degli accessi in base al ruolo (RBAC) è un metodo per regolare l'accesso alle risorse di rete o del computer in base ai ruoli dei singoli utenti. I controlli RBAC vengono applicati all'array di storage e includono ruoli predefiniti.
SAML	Security Assertion Markup Language (SAML) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata nell'array di storage è conforme a SAML2.0 per l'asserzione dell'identità, l'autenticazione e l'autorizzazione.

Termine	Descrizione
SP	Un Service Provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, l'array di storage agisce come Service Provider per richiedere l'autenticazione dall'Identity Provider.
SSO	Il single sign-on (SSO) è un servizio di autenticazione che consente di utilizzare un unico set di credenziali di accesso per accedere a più applicazioni.

Scopri le autorizzazioni per i ruoli mappati in SANtricity System Manager

Le funzionalità RBAC (controllo degli accessi in base al ruolo) applicate sull'array di storage includono profili utente predefiniti con uno o più ruoli associati. Ciascun ruolo include le autorizzazioni per accedere alle attività in SANtricity System Manager.

I profili utente e i ruoli mappati sono accessibili dal **Impostazioni › Gestione accessi › Ruoli utente locali** nell'interfaccia utente di entrambi i System Manager.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol).
- **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata attività, tale attività viene visualizzata in grigio oppure non viene mostrata nell'interfaccia utente.

Configura la gestione degli accessi con ruoli utente locali in SANtricity System Manager

Per Access Management, gli amministratori possono utilizzare le funzionalità RBAC (in base al ruolo) applicate nell'array di storage. Queste funzionalità sono denominate "local user roles".

Flusso di lavoro di configurazione

I ruoli utente locali sono preconfigurati per l'array di storage. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono fare quanto segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni Security Admin.

   L' `admin`utente ha pieno accesso a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente, che sono predefiniti e non possono essere modificati.
3. Facoltativamente, l'amministratore assegna nuove password per ciascun profilo utente.
4. Gli utenti accedono al sistema con le credenziali loro assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Cambia password.
- Imposta una lunghezza minima per le password.
- Consenti agli utenti di accedere senza password.

Configura la gestione degli accessi con i servizi di directory in SANtricity System Manager

Per Access Management, gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft Active Directory.

Flusso di lavoro di configurazione

Se nella rete vengono utilizzati un LDAP server e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni Security Admin.

   L' `admin`utente ha pieno accesso a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il LDAP server. Le impostazioni includono il domain name, l'URL e le informazioni sull'account Bind.
3. Se il LDAP server utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati di una Certificate Authority (CA) per l'autenticazione tra il LDAP server e lo storage array.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli dell'array di storage. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il LDAP server e lo storage array.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services loro assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungi un server di directory.
- Modifica le impostazioni del server di directory.
- Associa gli utenti LDAP ai ruoli utente locali.
- Rimuovi un server di directory.

Configura la gestione degli accessi con SAML in SANtricity System Manager

Per Access Management, gli amministratori possono utilizzare le funzionalità Security Assertion Markup Language (SAML) 2.0 integrate nell'array.

Flusso di lavoro di configurazione

La configurazione SAML funziona come segue:

1. Un amministratore accede a System Manager con un profilo utente che include le autorizzazioni Security Admin.

   L `admin`utente ha pieno accesso a tutte le funzioni in System Manager.

2. L'amministratore va alla scheda **SAML** sotto Gestione accessi.
3. Un amministratore configura le comunicazioni con l'Identity Provider (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è stato autenticato con successo. Per configurare le comunicazioni con l'array di storage, l'amministratore scarica il file dei metadati dell'IdP dal sistema IdP e quindi utilizza System Manager per caricare il file sull'array di storage.
4. Un amministratore stabilisce una relazione di fiducia tra il Service Provider e l'IdP. Un Service Provider controlla l'autorizzazione degli utenti; in questo caso, il controller nell'array di storage funge da Service Provider. Per configurare le comunicazioni, l'amministratore utilizza System Manager per esportare un file di metadati del Service Provider per ciascun controller. Dal sistema IdP, l'amministratore importa quindi quei file di metadati nell'IdP.

   Gli amministratori devono inoltre assicurarsi che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi utente definiti nell'IdP. Per fare ciò, l'amministratore utilizza System Manager per creare le associazioni.
6. L'amministratore verifica l'accesso SSO all'URL dell'IdP. Questo test garantisce che l'array di storage e l'IdP possano comunicare.

   Una volta abilitato SAML, *non è possibile* disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

7. Da System Manager, l'amministratore abilita SAML per l'array di storage.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modifica o crea nuove mappature dei ruoli
- Esporta file del Service Provider

Restrizioni di accesso

Quando SAML è abilitato, gli utenti non possono individuare o gestire lo storage per quell'array da Unified Manager o dall'interfaccia legacy Storage Manager.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse dell'array di storage:

- Enterprise Management Window (EMW)
- Client dei Software Developer Kits (SDK)
- Clienti in banda
- Accedi utilizzando l'endpoint REST API standard

Connettività limitata con SAML abilitato

Le seguenti funzionalità degli array di storage presentano una connettività limitata con l'autenticazione JSON Web Token ogni volta che SAML è abilitato.

- Interfaccia a riga di comando (CLI)
- Client REST API con autenticazione HTTP Basic

Scopri i token di accesso e il software SANtricity

I token di accesso forniscono un metodo di autenticazione con l'API REST o l'interfaccia a riga di comando (CLI), senza esporre nomi utente e password. Un token è associato a uno specifico utente (inclusi gli utenti LDAP) e include un insieme di autorizzazioni e una scadenza.

Accesso SAML e JSON web token

Per impostazione predefinita, un sistema con SAML abilitato non consente l'accesso agli strumenti da riga di comando tradizionali. L'API REST e la CLI diventano di fatto inutilizzabili perché il flusso di lavoro MFA richiede un reindirizzamento a un Identity Provider server per l'autenticazione. Pertanto, è necessario generare token in System Manager, il che impone che un utente sia autenticato tramite MFA.

> Non è necessario abilitare SAML per utilizzare i token web, ma SAML è consigliato per il massimo livello di sicurezza.

Flusso di lavoro per la creazione e l'utilizzo dei token

1. Crea un token in System Manager e determina la sua scadenza.
2. Copia il testo del token negli appunti o scaricalo in un file, quindi salva il testo del token in un luogo sicuro.
3. Utilizzare il token come segue:
   - **REST API**: Per utilizzare un token in una richiesta REST API, aggiungi un'intestazione HTTP alle tue richieste. Ad esempio:
     `Authorization: Bearer <access-token-value>`
   - **Secure CLI**: Per utilizzare un token nella CLI, aggiungi il valore del token sulla riga di comando oppure usa il percorso di un file contenente il valore del token. Ad esempio:
     - Valore del token sulla riga di comando: `-t access-token-value`

- Percorso di un file contenente il valore del token: `-T access-token-file`

Per saperne di più:

- "Crea token di accesso"
- "Modifica i token di accesso"
- "Revoca i token di accesso"

Utilizzare i ruoli utente locali

Visualizza i ruoli utente locali in SANtricity System Manager

Nella scheda Ruoli utente locali, è possibile visualizzare le mappature dei profili utente ai ruoli predefiniti. Queste mappature fanno parte dei controlli di accesso in base al ruolo (role-based access controls, RBAC) applicati nell'array di storage.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Informazioni su questa attività

I profili utente e le mappature non possono essere modificati. Solo le password possono essere modificate.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.

   I profili utente sono mostrati nella tabella:

   - **Amministratore root** (admin) — Super amministratore con accesso a tutte le funzioni del sistema. Questo profilo utente include tutti i ruoli.
   - **Amministratore dello storage** (storage) — L'amministratore responsabile di tutto il provisioning dello storage. Questo profilo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **Amministratore della sicurezza** (security) — L'utente responsabile della configurazione della sicurezza, inclusa la gestione degli accessi, la gestione dei certificati e le funzioni delle unità secure-enabled. Questo profilo utente include i seguenti ruoli: Security Admin e Monitor.
   - **Support admin** (support) — L'utente responsabile delle risorse hardware, dei dati relativi ai guasti e degli aggiornamenti del firmware. Questo profilo utente include i seguenti ruoli: Support Admin e Monitor.
   - **Monitor** (monitor) — Un utente con accesso di sola lettura al sistema. Questo profilo utente include solo il ruolo Monitor.

Modifica le password in SANtricity System Manager

È possibile modificare le password utente per ciascun profilo utente in Access Management.

Prima di iniziare

- È necessario aver effettuato l'accesso come amministratore locale, il che include i permessi di Root admin.

- È necessario conoscere la password dell'amministratore locale.

Informazioni su questa attività

Tieni a mente queste linee guida quando scegli una password:

- Le nuove password degli utenti locali devono soddisfare o superare l'impostazione corrente per la password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostate. Fai attenzione a includere gli spazi se erano inclusi nella password.
- Per una maggiore sicurezza, usa almeno 15 caratteri alfanumerici e cambia la password frequentemente.

> La modifica della password in System Manager comporta anche la modifica della stessa nell'interfaccia a riga di comando (CLI). Inoltre, la modifica della password causa la terminazione della sessione attiva dell'utente.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.
3. Seleziona un utente dalla tabella.

   Il pulsante Change Password diventa disponibile.

4. Seleziona **Change Password**.

   Si apre la finestra di dialogo Change Password.

5. Se non è impostata alcuna lunghezza minima per le password degli utenti locali, è possibile selezionare la casella per richiedere all'utente selezionato di immettere una password per accedere all'array di archiviazione, quindi è possibile digitare la nuova password per l'utente selezionato.
6. Inserisci la password dell'amministratore locale, quindi fai clic su **Change**.

Risultati

Se l'utente è attualmente connesso, la modifica della password causa la terminazione della sessione attiva dell'utente.

Modificare le impostazioni della password dell'utente locale in SANtricity System Manager

È possibile impostare la lunghezza minima richiesta per tutte le nuove password degli utenti locali o per quelle aggiornate sull'array di storage. È inoltre possibile consentire agli utenti locali di accedere all'array di storage senza immettere una password.

Prima di iniziare

È necessario aver effettuato l'accesso come amministratore locale, il che include i permessi di Root admin.

Informazioni su questa attività

Tenete a mente queste linee guida quando impostate la lunghezza minima per le password degli utenti locali:

- Le modifiche alle impostazioni non influiranno sulle password degli utenti locali esistenti.

- La lunghezza minima richiesta per le password degli utenti locali deve essere compresa tra 0 e 30 caratteri.
- Qualsiasi nuova password utente locale deve soddisfare o superare l'impostazione attuale della lunghezza minima.
- Non impostare una lunghezza minima per la password se desideri che gli utenti locali accedano all'array di storage senza inserire una password.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.
3. Seleziona il pulsante **Visualizza/Modifica impostazioni**.

   Si apre la finestra di dialogo Impostazioni password utente locale.

4. Eseguire una delle seguenti operazioni:
   - Per consentire agli utenti locali di accedere all'array di archiviazione *senza* inserire una password, deselezionare la casella di controllo "Richiedi che tutte le password degli utenti locali siano almeno".
   - Per impostare una lunghezza minima per tutte le password degli utenti locali, seleziona la casella di controllo "Richiedi che tutte le password degli utenti locali siano almeno di" e poi utilizza la casella di selezione numerica per impostare la lunghezza minima richiesta per tutte le password degli utenti locali.

     Le nuove password degli utenti locali devono soddisfare o superare l'impostazione attuale.

5. Fare clic su **Save**.

Utilizzare i servizi di directory

Aggiungi un LDAP directory server in SANtricity System Manager

Per configurare l'autenticazione per Access Management, è possibile stabilire comunicazioni tra l'array di storage e un LDAP server, e quindi mappare i gruppi di utenti LDAP ai ruoli predefiniti dell'array.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali dell'LDAP server devono essere disponibili, inclusi il domain name, l'URL del server e, facoltativamente, il nome utente e la password dell'account di bind.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del LDAP server deve essere installata sul computer locale.

Informazioni su questa attività

L'aggiunta di un server di directory è un processo in due fasi. Innanzitutto, si immettono il domain name e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per l'autenticazione se è firmato da un'autorità di firma non standard. Se si dispone delle credenziali per un bind account, è possibile inserire anche il nome utente e la password. Successivamente, si associano i gruppi di utenti del LDAP server ai ruoli predefiniti dell'array di storage.

Durante la procedura di aggiunta di un LDAP server, l'interfaccia di gestione legacy verrà disabilitata. L'interfaccia di gestione legacy (SYMbol) è un metodo di comunicazione tra l'array di storage e il client di gestione. Quando disabilitata, l'array di storage e il client di gestione utilizzano un metodo di comunicazione più sicuro (REST API su https).

Passaggi

1. Selezionare **Settings › Access Management**.
2. Dalla scheda Directory Services, selezionare **Add Directory Server**.

   Si apre la finestra di dialogo Add Directory Server.

3. Nella scheda Impostazioni server, inserire le credenziali per il LDAP server.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio(i)
Inserisci il domain name del LDAP server. Per più domain name, inseriscili in un elenco separato da virgole. Il domain name viene utilizzato nel login (*username@domain*) per specificare quale directory server utilizzare per l'autenticazione.	URL del server
Inserire l'URL per accedere al LDAP server nel formato `ldap[s]://**host**:*port*`.	Carica certificato (facoltativo)
Questo campo viene visualizzato solo se nel campo Server URL sopra è specificato un protocollo LDAPS. Fai clic su **Sfoglia** e seleziona un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati attendibili utilizzati per autenticare il LDAP server.	Account di bind (facoltativo)

Impostazione	Descrizione
Inserire un account utente di sola lettura per le query di ricerca sul LDAP server e per le ricerche all'interno dei gruppi. Inserire il nome dell'account in un formato di tipo LDAP. Ad esempio, se il bind user si chiama "bindacct", è possibile inserire un valore come "CN=bindacct,CN=Users,DC=cpoc,DC=local".	Password di bind (facoltativa)
Questo campo viene visualizzato quando si inserisce un bind account sopra. Inserisci la password per l'account bind.	Verifica la connessione al server prima di aggiungere

Impostazione	Descrizione
Seleziona questa casella di controllo se vuoi assicurarti che l'array di storage possa comunicare con la configurazione del LDAP server che hai inserito. Il test viene eseguito dopo che fai clic su **Aggiungi** nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test fallisce, la configurazione non viene aggiunta. Devi risolvere l'errore oppure deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.	**Impostazioni dei privilegi**
DN di base di ricerca	Inserire il contesto LDAP per cercare gli utenti, in genere nella forma `CN=Users, DC=cpoc, DC=local`.
Attributo username	Inserisci l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i di gruppo	Inserisci un elenco di attributi di gruppo sull'utente, che viene utilizzato per la mappatura gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

4. Fai clic sulla scheda **Role Mapping**.
5. Assegna i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mappature	DN gruppo
Specificare il group distinguished name (DN) per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	Fai clic nel campo e seleziona uno dei ruoli dell'array di storage da mappare al Group DN. Devi selezionare singolarmente ogni ruolo che desideri includere per questo gruppo. Il ruolo Monitor è necessario in combinazione con gli altri ruoli per accedere a SANtricity System Manager. I ruoli mappati includono le seguenti autorizzazioni: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol). • **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

6. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
7. Quando hai terminato con le mappature, fai clic su **Aggiungi**.

Il sistema esegue una convalida, assicurandosi che l'array di storage e LDAP server possano comunicare. Se viene visualizzato un messaggio di errore, controlla le credenziali inserite nella finestra di dialogo e reinserisci le informazioni se necessario.

Modifica le impostazioni del server di directory e le mappature dei ruoli in SANtricity System Manager

Se in precedenza hai configurato un server di directory in Access Management, puoi modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e le associazioni tra gruppi e ruoli.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- È necessario definire un server di directory.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Directory Services**.
3. Se sono definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Seleziona **Visualizza/Modifica impostazioni**.

   Si apre la finestra di dialogo Directory Server Settings.

5. Nella scheda Server Settings, modificare le impostazioni desiderate.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio(i)
Il domain name dei LDAP server. Per più domain name, inserirli in un elenco separato da virgole. Il domain name viene utilizzato nel login (*username* @*domain*) per specificare quale directory server utilizzare per l'autenticazione.	URL del server
L'URL per accedere al LDAP server nel formato `ldap[s]://host:port`.	Account di bind (facoltativo)
Account utente di sola lettura per le query di ricerca contro il LDAP server e per la ricerca all'interno dei gruppi.	Password di bind (facoltativa)
La password per l'account di bind. (Questo campo viene visualizzato quando si inserisce un account di bind.)	Verifica la connessione al server prima di salvare

Impostazione	Descrizione
Verifica che l'array di storage possa comunicare con la configurazione del LDAP server. Il test viene eseguito dopo aver fatto clic su **Salva** nella parte inferiore della finestra di dialogo. Se questa casella di controllo è selezionata e il test fallisce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
DN di base di ricerca	Il contesto LDAP per la ricerca degli utenti, in genere nella forma di `CN=Users, DC=cpoc, DC=local`.
Attributo username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i del gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per la mappatura gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

6. Nella scheda Role Mapping, modificare la mappatura desiderata.

Dettagli del campo

Impostazione	Descrizione
Mappature	DN gruppo
Il domain name per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	I ruoli dell'array di storage da mappare al Group DN. È necessario selezionare singolarmente ogni ruolo che si desidera includere per questo gruppo. Il ruolo Monitor è richiesto in combinazione con gli altri ruoli per accedere a SANtricity System Manager. I ruoli dell'array di storage includono i seguenti: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol). • **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

7. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
8. Fare clic su **Save**.

Risultati

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione

utente corrente verrà mantenuta.

Rimuovere il server directory in SANtricity System Manager

Per interrompere la connessione tra un server di directory e l'array di storage, è possibile rimuovere le informazioni del server dalla pagina Access Management. Potresti voler eseguire questa operazione se hai configurato un nuovo server e poi vuoi rimuovere quello vecchio.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Informazioni su questa attività

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione utente corrente verrà mantenuta.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Directory Services**.
3. Dall'elenco, seleziona il server di directory che vuoi eliminare.
4. Fai clic su **Remove**.

   Si apre la finestra di dialogo Remove Directory Server.

5. Digita `remove` nel campo e poi fai clic su **Rimuovi**.

   Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e le mappature dei ruoli vengono rimosse. Gli utenti non possono più accedere con le credenziali di questo server.

Usa SAML

Configura SAML in SANtricity System Manager

Per configurare l'autenticazione per Access Management, puoi utilizzare le funzionalità di Security Assertion Markup Language (SAML) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un Identity Provider e lo Storage Provider.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o il domain name di ciascun controller nell'array di storage.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore dell'IdP ha verificato che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.
- Un amministratore ha verificato che gli orologi del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni dell'orologio del controller).

- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a System Manager.

Informazioni su questa attività

Un Identity Provider (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se quell'utente è stato autenticato con successo. L'IdP può essere configurato per fornire l'autenticazione a più fattori e per utilizzare qualsiasi database utente, come Active Directory. Il team di sicurezza è responsabile della manutenzione dell'IdP. Un Service Provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, l'array di storage agisce come Service Provider per richiedere l'autenticazione all'Identity Provider. Per stabilire una connessione tra l'IdP e l'array di storage, si condividono i file di metadati tra queste due entità. Successivamente, si mappano le entità utente dell'IdP ai ruoli dell'array di storage. E infine, si testa la connessione e gli accessi SSO prima di abilitare SAML.

SAML e Directory Services. Se si abilita SAML quando Directory Services è configurato come metodo di autenticazione, SAML ha la precedenza su Directory Services in System Manager. Se si disabilita SAML in seguito, la configurazione di Directory Services torna alla configurazione precedente.

Modifica e disabilitazione. Una volta abilitato SAML, *non* è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

La configurazione dell'autenticazione SAML è una procedura in più fasi.

Passaggio 1: Carica il file dei metadati IdP

Per fornire all'array di storage le informazioni di connessione all'IdP, è necessario importare i metadati IdP in System Manager. Il sistema IdP necessita di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per convalidare le risposte ricevute. È sufficiente caricare un solo file di metadati per l'array di storage, anche se sono presenti due controller.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.

   La pagina mostra una panoramica dei passaggi di configurazione.

3. Fai clic sul collegamento **Import Identity Provider (IdP) file**.

   Si apre la finestra di dialogo Import Identity Provider File.

4. Fai clic su **Sfoglia** per selezionare e caricare il file di metadati dell'IdP che hai copiato sul tuo sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'IdP Entity ID.

5. Fai clic su **Import**.

Passaggio 2: Esporta i file del Service Provider

Per stabilire una relazione di fiducia tra l'IdP e l'array di storage, è necessario importare i metadati del Service Provider nell'IdP. L'IdP necessita di questi metadati per stabilire una relazione di fiducia con i controller e per

elaborare le richieste di autorizzazione. Il file include informazioni quali il domain name del controller o l'indirizzo IP, in modo che l'IdP possa comunicare con i Service Provider.

Passaggi

1. Fai clic sul collegamento **Export Service Provider files**.

   Si apre la finestra di dialogo Export Service Provider Files.

2. Inserisci l'indirizzo IP del controller o il nome DNS nel campo **Controller A**, quindi fai clic su **Esporta** per salvare il file di metadati sul tuo sistema locale. Se l'array di storage include due controller, ripeti questo passaggio per il secondo controller nel campo **Controller B**.

   Dopo aver fatto clic su **Esporta**, i metadati del Service Provider vengono scaricati sul sistema locale. Prendi nota della posizione in cui viene salvato il file.

3. Dal sistema locale, individua il file o i file di metadati del Service Provider che hai esportato.

   Esiste un file in formato XML per ciascun controller.

4. Dal server IdP, importa il file o i file di metadati del Service Provider per stabilire la relazione di fiducia. Puoi importare i file direttamente oppure inserire manualmente le informazioni del controller dai file.

Passaggio 3: Mappa i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a System Manager, è necessario mappare gli attributi utente dell'IdP e le appartenenze ai gruppi ai ruoli predefiniti dell'array di storage.

Prima di iniziare

- Un amministratore dell'IdP ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- Il file dei metadati dell'IdP viene importato in System Manager.
- Un file di metadati del Service Provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

Passaggi

1. Fai clic sul collegamento per **mappare i ruoli di System Manager**.

   Si apre la finestra di dialogo Role Mapping.

2. Assegna attributi e gruppi utente dell'IdP ai ruoli predefiniti. A un gruppo possono essere assegnati più ruoli.

Dettagli del campo

Impostazione	Descrizione
Mappature	Attributo utente
Specificare l'attributo (ad esempio, "member of") per il gruppo SAML da mappare.	Valore attributo
Specificare il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\ ) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	Fai clic nel campo e seleziona uno dei ruoli dell'array di storage da associare all'Attribute. Devi selezionare singolarmente ogni ruolo che desideri includere. Il ruolo Monitor è necessario in combinazione con gli altri ruoli per accedere a System Manager. Il ruolo Security Admin è inoltre necessario per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol). • **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

3. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.

Le mappature dei ruoli possono essere modificate dopo che SAML è stato abilitato.

4. Quando hai terminato con le mappature, fai clic su **Salva**.

Passaggio 4: Test SSO login

Per garantire che il sistema IdP e l'array di storage possano comunicare, è possibile testare facoltativamente un accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file dei metadati dell'IdP viene importato in System Manager.
- Un file di metadati del Service Provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.

Passaggi

1. Seleziona il link **Test SSO Login**.

   Si apre una finestra di dialogo per l'inserimento delle credenziali SSO.

2. Inserisci le credenziali di accesso per un utente con autorizzazioni sia di Security Admin sia di Monitor.

   Si apre una finestra di dialogo mentre il sistema verifica l'accesso.

3. Cerca un messaggio Test Successful. Se il test viene completato con successo, passa al passaggio successivo per abilitare SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

   - L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
   - I metadati che hai caricato per il server IdP sono corretti.
   - Gli indirizzi del controller nei file di metadati SP sono corretti.

Passaggio 5: Abilita SAML

L'ultimo passaggio consiste nel completare la configurazione SAML per l'autenticazione degli utenti. Durante questo processo, il sistema richiede anche di testare un accesso SSO. La procedura di test dell'accesso SSO è descritta nel passaggio precedente.

Prima di iniziare

- Il file dei metadati dell'IdP viene importato in System Manager.
- Un file di metadati del Service Provider per ciascun controller viene importato nel sistema IdP per la relazione di trust.
- È configurata almeno una mappatura dei ruoli di Monitor e di Security Admin.

Modifica e disabilitazione. Una volta abilitato SAML, *non* è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

Passaggi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML**.

   Si apre la finestra di dialogo Conferma abilitazione SAML.

2. Digita `enable`, quindi fai clic su **Enable**.
3. Inserisci le credenziali utente per un test di login SSO.

Risultati

Dopo che il sistema abilita SAML, termina tutte le sessioni attive e inizia ad autenticare gli utenti tramite SAML.

Modificare le mappature dei ruoli SAML in SANtricity System Manager

Se in precedenza hai configurato SAML per Access Management, puoi modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- Un amministratore dell'IdP ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- SAML è configurato e abilitato.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.
3. Seleziona **Mappatura dei ruoli**.

   Si apre la finestra di dialogo Role Mapping.

4. Assegna attributi e gruppi utente dell'IdP ai ruoli predefiniti. A un gruppo possono essere assegnati più ruoli.

   Fai attenzione a non rimuovere le tue autorizzazioni mentre SAML è abilitato, o perderai l'accesso a System Manager.

Dettagli del campo

Impostazione	Descrizione
Mappature	Attributo utente
Specificare l'attributo (ad esempio, "member of") per il gruppo SAML da mappare.	Valore attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

5. Facoltativamente, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
6. Fare clic su **Save**.

Risultati

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione utente corrente verrà mantenuta.

Esporta i file del Service Provider SAML in SANtricity System Manager

Se necessario, è possibile esportare i metadati del Service Provider per l'array di storage e reimportare il file o i file nel sistema Identity Provider (IdP).

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- SAML è configurato e abilitato.

Informazioni su questa attività

In questa attività, si esportano metadati dai controller (un file per ciascun controller). L'IdP necessita di questi metadati per stabilire una relazione di fiducia con i controller e per elaborare le richieste di autenticazione. Il file include informazioni quali il domain name o l'indirizzo IP del controller che l'IdP può utilizzare per inviare le richieste.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.
3. Seleziona **Export**.

   Si apre la finestra di dialogo Export Service Provider Files.

4. Per ogni controller, fai clic su **Esporta** per salvare il file di metadati sul tuo sistema locale.

   I campi domain name per ciascun controller sono di sola lettura.

   Prendi nota di dove è memorizzato il file.

5. Dal sistema locale, individua il file o i file di metadati del Service Provider che hai esportato.

   Esiste un file in formato XML per ciascun controller.

6. Dal server IdP, importa il/i file di metadati del Service Provider. Puoi importare i file direttamente oppure inserire manualmente le informazioni del controller da essi.
7. Fare clic su **Close**.

Usa i token di accesso

Crea token di accesso in SANtricity System Manager

È possibile creare un access token per autenticarsi con la REST API o l'interfaccia a riga di comando (CLI) al posto di username e password.

I token non hanno password, quindi devi gestirli con attenzione.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Access Tokens**.
3. Seleziona **Visualizza/Modifica impostazioni token di accesso**. Nella finestra di dialogo, assicurati che la casella di controllo **Abilita token di accesso** sia selezionata. Fai clic su **Salva** per chiudere la finestra di dialogo.
4. Seleziona **Create Access Token**.
5. Nella finestra di dialogo, seleziona la durata per cui il token sarà valido.

   Dopo la scadenza del token, i tentativi di autenticazione dell'utente falliranno.

6. Fai clic su **Create**.
7. Nella finestra di dialogo, selezionare una delle seguenti:
   - **Copia** per salvare il testo del token negli appunti.
   - **Download** per salvare il testo del token in un file.

     Assicurati di salvare il testo del token. Questa è l'unica opportunità per visualizzare il testo prima di chiudere la finestra di dialogo.

8. Fare clic su **Close**.
9. Utilizzare il token come segue:
   - **REST API**: Per utilizzare un token in una richiesta REST API, aggiungi un'intestazione HTTP alle tue richieste. Ad esempio:
     `Authorization: Bearer <access-token-value>`

- **Secure CLI**: Per utilizzare un token nella CLI, aggiungi il valore del token sulla riga di comando oppure usa il percorso di un file contenente il valore del token. Ad esempio:
  - Valore del token sulla riga di comando: `-t access-token-value`
  - Percorso di un file contenente il valore del token: `-T access-token-file`

> L'CLI richiede all'utente un valore del token di accesso sulla riga di comando se non viene specificato alcun nome utente, password o token.

Modifica le impostazioni del token di accesso in SANtricity System Manager

È possibile modificare le impostazioni dei token di accesso, che includono i tempi di scadenza e la possibilità di creare nuovi token.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Access Tokens**.
3. Seleziona **View/Edit Access Token Settings**.
4. Nella finestra di dialogo, è possibile eseguire una o entrambe queste attività:
   - Abilita o disabilita la creazione di token.
   - Modifica la scadenza dei token esistenti.

> Quando si deseleziona l'impostazione **Enable access tokens**, si impedisce sia la creazione dei token che l'autenticazione tramite token. Se in seguito si riattiva questa impostazione, i token non scaduti possono essere riutilizzati. Se si desidera revocare definitivamente tutti i token esistenti, vedere "Revoca i token di accesso".

5. Fare clic su **Save**.

Revoca i token di accesso in SANtricity System Manager

È possibile revocare tutti i token di accesso se si determina che un token è stato compromesso o se si desidera eseguire una rotazione manuale delle chiavi utilizzate per firmare e convalidare i token di accesso.

Questa operazione rigenera le chiavi utilizzate per firmare i token. Una volta reimpostate le chiavi, *tutti* i token emessi vengono immediatamente invalidati. Poiché l'array di archiviazione non tiene traccia dei token, i singoli token non possono essere revocati.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Access Tokens**.
3. Seleziona **Revoke All Access Tokens**.
4. Nella finestra di dialogo, fai clic su **Yes**.

Dopo aver revocato tutti i token, puoi crearne di nuovi e usarli immediatamente.

Gestisci syslog

Visualizza l'attività del registro di controllo in SANtricity System Manager

Visualizzando i registri di controllo, gli utenti con autorizzazioni di Security Admin possono monitorare le azioni degli utenti, i tentativi di autenticazione non riusciti, i tentativi di accesso non validi e la durata delle sessioni utente.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Audit Log**.

   Le attività del registro di controllo vengono visualizzate in formato tabellare, che include le seguenti colonne di informazioni:

   - **Data/Ora** — Timestamp di quando l'array di storage ha rilevato l'evento (in GMT).
   - **Nome utente** — Il nome utente associato all'evento. Per qualsiasi azione non autenticata sull'array di storage, "N/A" viene visualizzato come nome utente. Le azioni non autenticate potrebbero essere attivate dal proxy interno o da qualche altro meccanismo.
   - **Codice di stato** — Codice di stato HTTP dell'operazione (200, 400, ecc.) e testo descrittivo associato all'evento.
   - **URL consultato** — URL completo (incluso host) e stringa di query.
   - **Indirizzo IP del client** — Indirizzo IP del client associato all'evento.
   - **Source** — Origine del registro associata all'evento, che può essere System Manager, CLI, Web Services o Support Shell.
   - **Descrizione** — Informazioni aggiuntive sull'evento, se applicabile.
3. Utilizza le selezioni nella pagina Audit Log per visualizzare e gestire gli eventi.

Dettagli della selezione

Selezione	Descrizione
Mostra eventi da…	Limita gli eventi visualizzati per intervallo di date (ultime 24 ore, ultimi 7 giorni, ultimi 30 giorni o un intervallo di date personalizzato).
Filtro	Limita gli eventi visualizzati in base ai caratteri inseriti nel campo. Usa le virgolette ("") per una corrispondenza esatta della parola, inserisci `OR` per restituire una o più parole oppure inserisci un trattino (—) per omettere parole.
Aggiorna	Seleziona **Aggiorna** per aggiornare la pagina agli eventi più recenti.
Visualizza/Modifica impostazioni	Seleziona **Visualizza/Modifica impostazioni** per aprire una finestra di dialogo che consente di specificare una policy di log completa e il livello di azioni da registrare.
Elimina eventi	Seleziona **Delete** per aprire una finestra di dialogo che consente di rimuovere eventi vecchi dalla pagina.
Mostra/nascondi colonne	Fai clic sull'icona della colonna **Mostra/Nascondi** per selezionare colonne aggiuntive da visualizzare nella tabella. Le colonne aggiuntive includono: • **Metodo** — Il metodo HTTP (per esempio, POST, GET, DELETE, ecc.). • **Comando CLI eseguito** — Il comando CLI (grammatica) eseguito per le richieste Secure CLI. • **Stato di ritorno CLI** — Un codice di stato CLI o una richiesta di file di input dal client. • **Procedura SYMbol** — La procedura SYMbol è stata eseguita. • **Tipo di evento SSH** — Tipo di evento Secure Shell (SSH), come login, logout e login_fail. • **SSH Session PID** — Numero identificativo del processo della sessione SSH. • **Durata della sessione SSH (s)** — Il numero di secondi in cui l'utente è rimasto connesso. • **Tipo di autenticazione** — I tipi possono includere utente locale, LDAP, SAML e Access token. • **ID di autenticazione** — ID della sessione autenticata.
Attiva/disattiva i filtri di colonna	Fai clic sull'icona **Toggle** per aprire i campi di filtro per ciascuna colonna. Inserisci caratteri in un campo di colonna per limitare gli eventi visualizzati da quei caratteri. Fai nuovamente clic sull'icona per chiudere i campi di filtro.

Selezione	Descrizione
Annulla modifiche	Fai clic sull'icona **Annulla** per ripristinare la tabella alla configurazione predefinita.
Esporta	Fai clic su **Esporta** per salvare i dati della tabella in un file CSV (comma separated value).

Definire le policy dei log di audit in SANtricity System Manager

È possibile modificare la policy di sovrascrittura e i tipi di eventi registrati nel registro di audit.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Informazioni su questa attività

Questa procedura descrive come modificare le impostazioni del registro di controllo, che includono la policy per la sovrascrittura degli eventi vecchi e la policy per la registrazione dei tipi di evento.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Audit Log**.
3. Seleziona **Visualizza/Modifica impostazioni**.

   Si apre la finestra di dialogo Audit Log Settings.

4. Modifica la policy di sovrascrittura o i tipi di eventi registrati.

Dettagli del campo

Impostazione	Descrizione
Criterio di sovrascrittura	Determina la politica per la sovrascrittura degli eventi precedenti quando viene raggiunta la capacità massima: • **Consente la sovrascrittura degli eventi più vecchi nel registro di controllo quando il registro di controllo è pieno** — Sovrascrive gli eventi più vecchi quando il registro di controllo raggiunge 50.000 record. • **Richiedi l'eliminazione manuale degli eventi del registro di controllo** — Specifica che gli eventi non verranno eliminati automaticamente; invece, al raggiungimento della percentuale impostata, verrà visualizzato un avviso di soglia. Gli eventi devono essere eliminati manualmente. Se la politica di sovrascrittura è disabilitata e le voci del registro di controllo raggiungono il limite massimo, l'accesso a System Manager viene negato agli utenti privi di autorizzazioni Security Admin. Per ripristinare l'accesso al sistema agli utenti privi di autorizzazioni Security Admin, un utente a cui è assegnato il ruolo Security Admin deve eliminare i vecchi record degli eventi. Le policy di sovrascrittura non si applicano se un syslog server è configurato per l'archiviazione dei log di controllo.
Livello delle azioni da registrare	Determina i tipi di eventi da registrare: • **Registra solo gli eventi di modifica** — Mostra solo gli eventi in cui un'azione dell'utente comporta una modifica nel sistema. • **Registra tutti gli eventi di modifica e di sola lettura** — Mostra tutti gli eventi, inclusa un'azione dell'utente che comporta la lettura o il download di informazioni.

5. Fare clic su **Save**.

Eliminare gli eventi dal registro di audit in SANtricity System Manager

È possibile cancellare gli eventi meno recenti dal registro di controllo, semplificando la ricerca tra gli eventi. È possibile salvare gli eventi meno recenti in un file CSV (comma-separated values) al momento dell'eliminazione.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Audit Log**.
3. Seleziona **Delete**.

   Si apre la finestra di dialogo Delete Audit Log.

4. Seleziona o inserisci il numero di eventi meno recenti che desideri eliminare.
5. Se desideri esportare gli eventi eliminati in un file CSV (consigliato), mantieni selezionata la casella di controllo. Ti verrà richiesto di inserire un nome file e una posizione quando fai clic su **Elimina** nel passaggio successivo. Altrimenti, se non desideri salvare gli eventi in un file CSV, fai clic sulla casella di controllo per deselezionarla.
6. Fai clic su **Delete**.

   Si apre una finestra di dialogo di conferma.

7. Digita `delete` nel campo e poi fai clic su **Cancella**.

   Gli eventi più vecchi vengono rimossi dalla pagina Audit Log.

Configurare il server syslog per i log di controllo in SANtricity System Manager

Se si desidera archiviare i log di controllo su un server syslog esterno, è possibile configurare la comunicazione tra tale server e l'array di storage. Una volta stabilita la connessione, i log di controllo vengono salvati automaticamente sul server syslog.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio, TLS), un certificato di Certificate Authority (CA) deve essere disponibile sul sistema locale. I certificati CA identificano i proprietari dei siti web per connessioni sicure tra server e client.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Dalla scheda Audit Log, selezionare **Configure Syslog Servers**.

   Si apre la finestra di dialogo Configura Syslog Servers.

3. Fai clic su **Add**.

   Si apre la finestra di dialogo Aggiungi Syslog Server.

4. Inserisci le informazioni per il server, quindi fai clic su **Aggiungi**.
   - **Indirizzo del server** — Inserire un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
   - **Protocollo** — Seleziona un protocollo dall'elenco a discesa (ad esempio, TLS, UDP o TCP).

- **Carica il certificato (facoltativo)** — Se hai selezionato il protocollo TLS e non hai ancora caricato un certificato CA firmato, fai clic su **Sfoglia** per caricare un file di certificato. I log di controllo non vengono archiviati su un syslog server senza un certificato attendibile.

  > Se in seguito il certificato diventa non valido, la stretta di mano TLS fallirà. Di conseguenza, viene registrato un messaggio di errore nel registro di controllo e i messaggi non vengono più inviati al syslog server. Per risolvere questo problema, è necessario correggere il certificato sul syslog server e quindi andare su **Settings › Audit Log › Configure Syslog Servers › Test All**.

- **Porta** — Inserire il numero di porta per il syslog receiver. Dopo aver fatto clic su **Aggiungi**, si apre la finestra di dialogo Configura Syslog Servers e viene visualizzato il syslog server configurato nella pagina.

5. Per testare la connessione del server con l'array di storage, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi log di controllo vengono inviati al server syslog. I log precedenti non vengono trasferiti. Per configurare ulteriormente le impostazioni syslog per gli avvisi, vedere "Configura il server syslog per gli avvisi".

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

Modifica le impostazioni del server syslog per i record del registro di controllo in SANtricity System Manager

È possibile modificare le impostazioni del syslog server utilizzato per l'archiviazione dei log di controllo e caricare anche un nuovo certificato di autorità di certificazione (CA) per il server.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
- Se si sta caricando un nuovo certificato CA, il certificato deve essere disponibile sul sistema locale.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Dalla scheda Audit Log, selezionare **Configure Syslog Servers**.

   I server syslog configurati vengono visualizzati nella pagina.

3. Per modificare le informazioni del server, seleziona l'icona **Edit** (matita) a destra del nome del server, quindi apporta le modifiche desiderate nei seguenti campi:
   - **Indirizzo del server** — Inserire un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
   - **Protocollo** — Seleziona un protocollo dall'elenco a discesa (ad esempio, TLS, UDP o TCP).

◦ **Porta** — Inserire il numero di porta per il syslog receiver.

4. Se hai modificato il protocollo passando al protocollo sicuro TLS (da UDP o TCP), fai clic su **Import Trusted Certificate** per caricare un certificato CA.
5. Per testare la nuova connessione con l'array di archiviazione, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi log di controllo vengono inviati al syslog server. I log precedenti non vengono trasferiti.

Domande frequenti sulla gestione degli accessi utente per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Perché non posso accedere?

Se ricevi un errore quando tenti di accedere a SANtricity System Manager, esamina queste possibili cause.

Gli errori di accesso a System Manager possono verificarsi per uno dei seguenti motivi:

- Hai inserito un nome utente o una password non corretti.
- Non disponi di privilegi sufficienti.
- Il server di directory (se configurato) potrebbe non essere disponibile. Se questo è il caso, prova ad accedere con un ruolo utente locale.
- Hai tentato di accedere senza successo più volte, il che ha attivato la modalità di blocco. Attendi 10 minuti per accedere nuovamente.
- Si è verificata una condizione di blocco e il registro di controllo potrebbe essere pieno. Vai a Access Management ed elimina gli eventi obsoleti dal registro di controllo.
- L'autenticazione SAML è abilitata. Aggiorna il browser per accedere.

Gli errori di accesso a un array di archiviazione remoto per le attività di mirroring possono verificarsi per uno dei seguenti motivi:

- Hai inserito una password non corretta.
- Hai tentato di accedere senza successo più volte, il che ha attivato la modalità di blocco. Attendi 10 minuti per accedere di nuovo.
- È stato raggiunto il numero massimo di connessioni client utilizzate sul controller. Verificare la presenza di più utenti o client.

Cosa devo sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, assicurarsi di soddisfare i seguenti requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali dell'LDAP server devono essere disponibili, inclusi il domain name, l'URL del server e, facoltativamente, il nome utente e la password dell'account di bind.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del LDAP server deve essere installata sul computer locale.

Cosa devo sapere sulla mappatura ai ruoli degli array di storage?

Prima di associare i gruppi ai ruoli, consultare le seguenti linee guida.

Le funzionalità RBAC (in base al ruolo, role-based access control) integrate nell'array di storage includono i seguenti ruoli:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol).
- **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Servizi di directory

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e Directory Services, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Conosci i domain name dei gruppi per i gruppi di utenti LDAP. Le espressioni regolari sono supportate. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\ se non fanno parte di un pattern di espressione regolare:

```
\.[]{}()<>*+-=!?^$|
```

- Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

SAML

Se si utilizzano le funzionalità Security Assertion Markup Language (SAML) incorporate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- Conosci i nomi dei gruppi di appartenenza.
- Conosci il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\ se non fanno parte di un modello di espressione regolare:

```
\.[]{}()<>*+-=!?^$|
```

- Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. System Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

Quali strumenti di gestione esterni potrebbero essere interessati da questa modifica?

Quando si apportano determinate modifiche in SANtricity System Manager, come il cambio dell'interfaccia di gestione o l'utilizzo di SAML come metodo di autenticazione, alcuni strumenti e funzionalità esterni potrebbero essere limitati dall'uso.

Interfaccia di gestione

Gli strumenti che comunicano direttamente con l'interfaccia di gestione legacy (SYMbol), come il SANtricity SMI-S Provider o OnCommand Insight (OCI), non funzionano a meno che l'impostazione Legacy Management Interface non sia abilitata. Inoltre, non è possibile utilizzare i comandi CLI legacy o eseguire operazioni di mirroring se questa impostazione è disabilitata.

Contatta il supporto tecnico per ulteriori informazioni.

Autenticazione SAML

Quando SAML è abilitato, i seguenti client non possono accedere ai servizi e alle risorse dell'array di storage:

- Enterprise Management Window (EMW)
- Interfaccia a riga di comando (CLI)
- Client dei Software Developer Kits (SDK)
- Clienti in banda
- Client REST API con autenticazione HTTP Basic
- Accedi utilizzando l'endpoint REST API standard

Contatta il supporto tecnico per ulteriori informazioni.

Cosa devo sapere prima di configurare e abilitare SAML?

Prima di configurare e abilitare le funzionalità Security Assertion Markup Language (SAML) per l'autenticazione, assicurati di soddisfare i seguenti requisiti e di comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurati che:

- Un Identity Provider (IdP) è configurato nella tua rete. Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è stato autenticato con successo. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi utente e i gruppi nel sistema IdP.
- Un amministratore dell'IdP ha verificato che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.
- Un amministratore ha verificato che gli orologi del server IdP e del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni dell'orologio del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e reso disponibile sul sistema locale utilizzato per accedere a System Manager.
- Conosci l'indirizzo IP o domain name di ciascun controller nell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza. Si consiglia di testare gli accessi SSO prima di abilitare SAML nella fase finale della configurazione. (Il sistema esegue anche un test di accesso SSO prima di abilitare SAML.)
- Se in futuro si disabilita SAML, il sistema ripristina automaticamente la configurazione precedente (Local User Roles e/o Directory Services).
- Se Directory Services sono attualmente configurati per l'autenticazione degli utenti, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse dello storage array:
  - Enterprise Management Window (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client dei Software Developer Kits (SDK)
  - Clienti in banda
  - Client REST API con autenticazione HTTP Basic
  - Accedi utilizzando l'endpoint REST API standard

Quali tipi di eventi vengono registrati nel registro di controllo?

Il registro di controllo può registrare eventi di modifica o sia eventi di modifica che eventi di sola lettura.

A seconda delle impostazioni dei criteri, vengono visualizzati i seguenti tipi di eventi:

- **Eventi di modifica** — Azioni dell'utente da System Manager che comportano modifiche al sistema, come il provisioning dello storage.
- **Eventi di modifica e di sola lettura** — Azioni dell'utente che comportano modifiche al sistema, nonché eventi che comportano la visualizzazione o il download di informazioni, come la visualizzazione delle assegnazioni dei volumi.

Cosa devo sapere prima di configurare un syslog server?

È possibile archiviare i log di controllo su un syslog server esterno.

Prima di configurare un syslog server, tenete a mente le seguenti linee guida.

- Assicurati di conoscere l'indirizzo del server, il protocollo e il numero di porta. L'indirizzo del server può essere un fully qualified domain name, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio, TLS), un certificato di Certificate Authority (CA) deve essere disponibile sul sistema locale. I certificati CA identificano i proprietari dei siti web per connessioni sicure tra server e client.
- Dopo la configurazione, tutti i nuovi log di controllo vengono inviati al syslog server. I log precedenti non vengono trasferiti.
- Le impostazioni dei criteri di sovrascrittura (disponibili in **Visualizza/Modifica impostazioni**) non influiscono sulla gestione dei log con una configurazione del server syslog.
- I registri di audit seguono il formato di messaggistica RFC 5424.

Il syslog server non riceve più i log di controllo. Cosa devo fare?

Se hai configurato un syslog server con il protocollo TLS, il server non può ricevere messaggi se il certificato diventa non valido per qualsiasi motivo. Un messaggio di errore relativo al certificato non valido viene registrato nel registro di controllo.

Per risolvere questo problema, è necessario innanzitutto correggere il certificato del syslog server. Una volta stabilita una catena di certificati valida, vai su **Settings › Audit Log › Configure Syslog Servers › Test All**.

Certificati

Scopri i certificati in SANtricity System Manager

È possibile utilizzare SANtricity System Manager per creare Certificate Signing Requests (CSR), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti web e server, per comunicazioni sicure su internet. Esistono due tipi di certificati: un *certificato firmato* è convalidato da un'autorità di certificazione (CA) e un *certificato autofirmato* è convalidato dal proprietario dell'entità invece che da una terza parte.

Per saperne di più:

- "Come funzionano i certificati"
- "Terminologia dei certificati"

Come si configurano i certificati firmati?

È possibile generare una richiesta di firma da System Manager o esternamente utilizzando una coppia di chiavi privata e pubblica. La richiesta di firma viene inviata a una CA per generare i file del certificato. Una volta che la CA restituisce i file del certificato, li importi utilizzando System Manager.

Per saperne di più:

- "Utilizza certificati firmati da CA per i controller"
- "Utilizzare certificati firmati da CA per l'autenticazione con un server di gestione delle chiavi"

Informazioni correlate

Scopri di più sulle attività relative ai certificati:

- "Visualizza le informazioni sul certificato importato"
- "Abilita la verifica della revoca dei certificati"

Concetti

Come funzionano i certificati in SANtricity System Manager

I certificati sono file digitali che identificano entità online, come siti web e server, per comunicazioni sicure su internet.

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, privata e inalterata, esclusivamente tra il server e il client specificati. Utilizzando System Manager, puoi gestire i certificati tra il browser su un sistema di gestione host (che funge da client) e i controller in un sistema storage (che fungono da server).

Un certificato può essere firmato da un'autorità fidata, oppure può essere autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e ha stabilito che i suoi dispositivi possono essere considerati affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. Puoi continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati da una CA per una connessione più sicura tra i controller e i sistemi host.

> Sebbene i certificati firmati da una CA offrano una maggiore protezione della sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), comportano anche costi che possono essere elevati 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), ovvero un'organizzazione terza fidata. I certificati firmati includono dettagli sul proprietario dell'entità (in genere un server o un sito web), la data di emissione e di scadenza del certificato, i domini validi per l'entità e una firma digitale composta da lettere e numeri.

Quando apri un browser e inserisci un indirizzo web, il tuo sistema esegue in background un processo di verifica del certificato per determinare se ti stai connettendo a un sito web che include un certificato valido, CA-signed. In genere, un sito protetto da un certificato firmato presenta un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se tenti di connetterti a un sito web che non contiene un certificato CA-signed, il browser visualizza un avviso che il sito non è sicuro.

L'autorità di certificazione (CA) adotta delle misure per verificare la tua identità durante il processo di richiesta. Potrebbe inviare un'e-mail alla tua azienda registrata, verificare l'indirizzo della tua azienda ed eseguire una verifica HTTP o DNS. Una volta completata la procedura di richiesta, la CA ti invia dei file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di fiducia, come segue:

- **Root** — Al vertice della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. Il root identifica una specifica organizzazione CA. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedi** — Dalla radice si diramano i certificati intermedi. La CA emette uno o più certificati intermedi che fungono da intermediari tra una radice protetta e i certificati del server.
- **Server** — Alla base della catena si trova il certificato del server, che identifica la tua entità specifica, come un sito web o un altro dispositivo. Ogni controller in un storage array richiede un certificato server separato.

Certificati autofirmati

Ogni controller nell'array di storage include un certificato autofirmato preinstallato. Un certificato autofirmato è simile a un certificato firmato da una CA, con la differenza che viene convalidato dal proprietario dell'entità invece che da una terza parte. Come un certificato firmato da una CA, un certificato autofirmato contiene la propria chiave privata e garantisce anche che i dati siano crittografati e inviati tramite una connessione HTTPS tra un server e un client. Tuttavia, un certificato autofirmato non utilizza la stessa catena di fiducia di un certificato firmato da una CA.

I certificati autofirmati non sono "trusted" dai browser. Ogni volta che si tenta di connettersi a un sito web che

contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di procedere al sito web; così facendo, si accetta il certificato autofirmato.

Certificati utilizzati per il key management server

Se si utilizza un server di gestione delle chiavi esterno con la funzionalità Drive Security, è possibile gestire anche i certificati per l'autenticazione tra tale server e i controller.

Scopri la terminologia relativa ai certificati nel software SANtricity

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CA	Un'autorità di certificazione (CA) è un'entità fidata che rilascia documenti elettronici, chiamati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti web, il che consente connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per rilasciare un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli aggressori di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e sull'identità dell'entità di fiducia che certifica (firma) queste informazioni.
Catena di certificati	Una gerarchia di file che aggiunge un livello di sicurezza ai certificati. In genere, la catena include un certificato radice al vertice della gerarchia, uno o più certificati intermedi e i certificati del server che identificano le entità.
Certificato client	Per la gestione delle chiavi di sicurezza, un certificato client convalida i controller dell'array di storage, così il server di gestione delle chiavi può fidarsi dei loro indirizzi IP.
Certificato intermedio	Uno o più certificati intermedi si diramano dal certificato radice nella catena di certificati. La CA emette uno o più certificati intermedi che fungono da intermediari tra un certificato radice protetto e i certificati del server.
Certificato del server di gestione delle chiavi	Per la gestione delle chiavi di sicurezza, un certificato del server di gestione delle chiavi convalida il server, così il sistema storage può considerare attendibile il suo indirizzo IP.
Keystore	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle corrispondenti chiavi pubbliche e certificati. Queste chiavi e certificati identificano le proprie entità, come i controller.

Termine	Descrizione
Server OCSP	Il server Online Certificate Status Protocol (OCSP) determina se l'autorità di certificazione (CA) ha revocato dei certificati prima della loro data di scadenza prevista e quindi blocca l'utente dall'accedere a un server se il certificato è stato revocato.
Certificato radice	Il certificato radice si trova al vertice della gerarchia nella catena di certificati e contiene una chiave privata utilizzata per firmare altri certificati. Il root identifica una particolare organizzazione CA. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato radice.
Certificato firmato	Un certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include dettagli relativi al proprietario dell'entità (in genere, un server o un sito web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di fiducia e pertanto viene utilizzato più spesso in ambienti di produzione. È anche noto come "CA-signed certificate" o "management certificate".
Certificato autofirmato	Un certificato autofirmato viene convalidato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di fiducia di un certificato firmato da una CA e pertanto viene spesso utilizzato in ambienti di test. Viene anche definito come certificato "preinstallato".
Certificato del server	Il certificato del server si trova alla base della catena di certificati. Identifica la tua entità specifica, come un sito web o un altro dispositivo. Ogni controller in un sistema storage richiede un certificato server separato.

Usa i certificati

Utilizza certificati firmati da CA per i controller in SANtricity System Manager

È possibile ottenere certificati firmati da CA per comunicazioni sicure tra i controller e il browser utilizzato per accedere a SANtricity System Manager.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o i nomi DNS di ciascun controller.

Informazioni su questa attività

L'utilizzo di certificati firmati da una CA è una procedura in tre fasi.

Passaggio 1: Completare i CSR per i controller

Per prima cosa, è necessario generare un file di richiesta di firma del certificato (CSR) per ciascun controller nell'array di archiviazione.

Informazioni su questa attività

Questa procedura descrive come generare un file CSR da System Manager. Il CSR fornisce informazioni sulla tua organizzazione e sull'indirizzo IP o sul nome DNS del controller. Durante questa procedura, viene generato un file CSR se l'array di storage ha un controller e due file CSR se ne ha due.

In alternativa, puoi generare un file CSR utilizzando uno strumento come OpenSSL e puoi passare a Passaggio 2: invia i file CSR.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Dalla scheda Array Management, selezionare **Complete CSR**.

   Se viene visualizzata una finestra di dialogo che richiede di accettare un certificato autofirmato per il secondo controller, fare clic su **Accept Self-Signed Certificate** per procedere.

3. Inserisci le seguenti informazioni, quindi fai clic su **Avanti**:
   - **Organizzazione** — Il nome legale completo della tua azienda o organizzazione. Includi i suffissi, come Inc. o Corp.
   - **Unità organizzativa (facoltativa)** — La divisione della tua organizzazione che si occupa del certificato.
   - **Città/Località** — La città in cui si trova il tuo storage array o la tua attività.
   - **Stato/Regione (facoltativo)** — Lo stato o la regione in cui si trova il tuo storage array o la tua business.
   - **Codice ISO del Paese** — Il codice ISO (International Organization for Standardization) a due cifre del tuo Paese, ad esempio US.

   Alcuni campi potrebbero essere precompilati con le informazioni appropriate, come l'indirizzo IP del controller. Non modificare i valori precompilati a meno che non si sia certi che siano errati. Ad esempio, se non si è ancora completato un CSR, l'indirizzo IP del controller è impostato su "localhost." In questo caso, è necessario modificare "localhost" con il nome DNS o l'indirizzo IP del controller.

4. Verificare o immettere le seguenti informazioni sul controller A nell'array di storage:
   - **Nome comune del controller A** — L'indirizzo IP o il nome DNS del controller A viene visualizzato per impostazione predefinita. Assicurarsi che questo indirizzo sia corretto; deve corrispondere esattamente a quello inserito per accedere a System Manager nel browser. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi del controller A** — Se il nome comune è un indirizzo IP, è possibile inserire facoltativamente ulteriori indirizzi IP o alias per controller A. Per più voci, utilizzare il formato separato da virgole.
   - **Nomi DNS alternativi del controller A** — Se il nome comune è un nome DNS, inserire eventuali nomi DNS aggiuntivi per il controller A. Per più voci, utilizzare il formato separato da virgole. Se non sono presenti nomi DNS alternativi, ma è stato inserito un nome DNS nel primo campo, copiare quel nome

qui. Il nome DNS non può iniziare con un carattere jolly. Se l'array di storage ha un solo controller, il pulsante **Finish** è disponibile.

Se l'array di storage dispone di due controller, il pulsante **Next** è disponibile.

> Non fare clic sul collegamento **Salta questo passaggio** durante la creazione iniziale di una richiesta CSR. Questo collegamento viene fornito in situazioni di recupero dagli errori. In rari casi, una richiesta CSR potrebbe non riuscire su un controller, ma non sull'altro. Questo collegamento consente di saltare il passaggio per la creazione di una richiesta CSR sul controller A se è già definita, e di continuare al passaggio successivo per ricreare una richiesta CSR sul controller B.

5. Se è presente un solo controller, fare clic su **Fine**. Se sono presenti due controller, fare clic su **Avanti** per inserire le informazioni per il controller B (come sopra), quindi fare clic su **Fine**.

   Per un singolo controller, un file CSR viene scaricato sul sistema locale. Per due controller, vengono scaricati due file CSR. La posizione della cartella di download dipende dal browser.

6. Vai a Passaggio 2: invia i file CSR.

Passaggio 2: invia i file CSR

Dopo aver creato i file di richiesta di firma del certificato (CSR), invia i file a un'autorità di certificazione (CA). I sistemi E-Series richiedono il formato PEM (codifica Base64 ASCII) per i certificati firmati, che include i seguenti tipi di file: .pem, .crt, .cer o .key.

Passaggi

1. Individua i file CSR scaricati.
2. Invia i file CSR a una CA (ad esempio, Verisign o DigiCert) e richiedi certificati firmati in formato PEM.

> **Dopo aver inviato un file CSR alla CA, NON generare un altro file CSR.** Ogni volta che generi un CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte del CSR, mentre la chiave privata viene conservata nel keystore del sistema. Quando ricevi i certificati firmati e li importi, il sistema garantisce che sia la chiave privata che quella pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno e devi richiedere nuovi certificati alla CA.

3. Quando la CA restituisce i certificati firmati, vai su Passaggio 3: Importa i certificati firmati per i controller.

Passaggio 3: Importa i certificati firmati per i controller

Dopo aver ricevuto i certificati firmati dall'Certificate Authority (CA), importa i file per i controller.

Prima di iniziare

- L'autorità di certificazione (CA) ha restituito i file dei certificati firmati. Questi file includono il certificato radice, uno o più certificati intermedi e i certificati del server.
- Se la CA ha fornito un file di certificati concatenati (ad esempio, un file .p7b), è necessario estrarre il file concatenato in file individuali: il certificato root, uno o più certificati intermedi e i certificati server che identificano i controller. È possibile utilizzare l'utilità Windows `certmgr` per estrarre i file (fare clic con il pulsante destro del mouse e selezionare **Tutte le attività › Esporta**). Si consiglia la codifica Base-64. Al termine dell'esportazione, viene visualizzato un file CER per ciascun file di certificato nella catena.
- Hai copiato i file del certificato sul sistema host da cui accedi a System Manager.

Passaggi

1. Selezionare **Impostazioni › Certificati**
2. Dalla scheda Array Management, selezionare **Import**.

   Si apre una finestra di dialogo per l'importazione del/dei file del certificato.

3. Fai clic sui pulsanti **Sfoglia** per selezionare prima i file del certificato radice e intermedio, quindi seleziona ciascun certificato server per i controller. I file radice e intermedio sono gli stessi per entrambi i controller. Solo i certificati server sono univoci per ciascun controller. Se hai generato la CSR da uno strumento esterno, devi anche importare il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fai clic su **Import**.

   I file sono stati caricati e convalidati.

Risultato

La sessione viene terminata automaticamente. Devi effettuare nuovamente l'accesso affinché i certificati abbiano effetto. Quando effettui nuovamente l'accesso, per la tua sessione vengono utilizzati i nuovi certificati firmati dalla CA.

Reimposta i certificati di gestione in SANtricity System Manager

È possibile ripristinare i certificati sui controller passando dai certificati firmati da CA a quelli autofirmati predefiniti di fabbrica.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- I certificati firmati da una CA devono essere importati preventivamente.

Informazioni su questa attività

La funzione Reset elimina i file dei certificati firmati dalla CA attualmente presenti su ciascun controller. I controller torneranno quindi a utilizzare certificati autofirmati.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Dalla scheda Array Management, selezionare **Reset**.

   Si apre una finestra di dialogo Confirm Reset Management Certificates.

3. Digita `reset` nel campo, quindi fai clic su **Ripristina**.

   Dopo l'aggiornamento della pagina, 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 a utilizzare certificati autofirmati. Per eliminare la condizione che blocca l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultati

I controller tornano a utilizzare certificati autofirmati. Di conseguenza, il sistema richiede agli utenti di accettare

manualmente il certificato autofirmato per le proprie sessioni.

Visualizza le informazioni sul certificato importato in SANtricity System Manager

Dalla pagina Certificati, è possibile visualizzare il tipo di certificato, l'autorità emittente e l'intervallo di date di validità dei certificati per l'array di storage.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Seleziona una delle schede per visualizzare le informazioni sui certificati.

Scheda	Descrizione
Gestione array	Visualizza le informazioni sui certificati firmati da CA importati per ciascun controller, inclusi il file root, i file intermedi e i file server.
Attendibile	Visualizza le informazioni relative a tutti gli altri tipi di certificati importati per i controller. Utilizza il campo filtro sotto **Mostra i certificati che sono…** per visualizzare i certificati installati dall'utente o quelli preinstallati. • **Installati dall'utente** — Certificati che un utente ha caricato nell'array di archiviazione, che possono includere certificati attendibili quando il controller agisce come client (anziché come server), certificati LDAPS e certificati di federazione delle identità. • **Pre-installati** — Certificati autofirmati inclusi con l'array di storage.
Gestione delle chiavi	Visualizza informazioni sui certificati firmati da CA importati per un server di gestione delle chiavi esterno.

Importa certificati per i controller quando agiscono come client in SANtricity System Manager

Se il controller rifiuta una connessione perché non riesce a convalidare la catena di fiducia per un server di rete, puoi importare un certificato dalla scheda Trusted che consente al controller (agendo come client) di accettare comunicazioni da quel server.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- I file del certificato sono installati sul sistema locale.

Informazioni su questa attività

L'importazione dei certificati dalla scheda Attendibili potrebbe essere necessaria se si desidera consentire a un altro server di contattare i controller (ad esempio, un LDAP server o un syslog server che utilizza TLS).

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Dalla scheda Trusted, selezionare **Import**.

   Si apre una finestra di dialogo per l'importazione dei file del certificato attendibile.

3. Fai clic su **Sfoglia** per selezionare i file del certificato per i controller.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fai clic su **Import**.

Risultati

I file sono stati caricati e convalidati.

Abilitare la verifica della revoca dei certificati in SANtricity System Manager

È possibile abilitare i controlli automatici per i certificati revocati, in modo che un server Online Certificate Status Protocol (OCSP) impedisca agli utenti di effettuare connessioni non sicure.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- Un DNS server è configurato su entrambi i controller, il che consente l'utilizzo di un fully qualified domain name per il server OCSP. Questa operazione è disponibile nella pagina Hardware.
- Se si desidera specificare il proprio server OCSP, è necessario conoscere l'URL di quel server.

Informazioni su questa attività

Il controllo automatico della revoca è utile nei casi in cui la CA abbia emesso un certificato in modo improprio o una chiave privata sia stata compromessa.

Durante questa operazione, puoi configurare un server OCSP o utilizzare il server specificato nel file del certificato. Il server OCSP determina se la CA ha revocato dei certificati prima della loro data di scadenza programmata e quindi blocca l'utente dall'accedere a un sito se il certificato è stato revocato.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Seleziona la scheda **Trusted**.

   È inoltre possibile abilitare il controllo di revoca dalla scheda **Key Management**.

3. Fai clic su **Uncommon Tasks** e poi seleziona **Enable Revocation Checking** dal menu a discesa.
4. Seleziona **I want to enable revocation checking**, in modo che nella casella di controllo compaia un segno di spunta e nella finestra di dialogo vengano visualizzati campi aggiuntivi.
5. Nel campo **Indirizzo del risponditore OCSP**, è possibile inserire facoltativamente un URL per un server risponditore OCSP. Se non si inserisce un indirizzo, il sistema utilizza l'URL del server OCSP dal file del certificato.
6. Fai clic su **Test Address** per assicurarti che il sistema sia in grado di stabilire una connessione all'URL specificato.

7. Fare clic su **Save**.

Risultati

Se l'array di storage tenta di connettersi a un server con un certificato revocato, la connessione viene negata e un evento viene registrato.

Eliminare i certificati attendibili in SANtricity System Manager

È possibile eliminare i certificati installati dall'utente precedentemente importati dalla scheda Trusted.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- Se si aggiorna un certificato attendibile con una nuova versione, il certificato aggiornato deve essere importato prima di eliminare il vecchio certificato.

> Potresti perdere l'accesso a un sistema se elimini un certificato utilizzato per autenticare i controller e un altro server, come un LDAP server, prima di importare un certificato sostitutivo.

Informazioni su questa attività

Questa procedura descrive come eliminare i certificati installati dall'utente. I certificati autofirmati preinstallati non possono essere eliminati.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Seleziona la scheda **Trusted**.

   La tabella mostra i certificati attendibili dell'array di storage.

3. Dalla tabella, seleziona il certificato che vuoi rimuovere.
4. Fare clic su **Uncommon Tasks › Elimina**.

   Si apre una finestra di dialogo Conferma eliminazione certificato attendibile.

5. Digita `delete` nel campo e poi fai clic su **Cancella**.

Utilizzare certificati firmati da CA per l'autenticazione con un key management server in SANtricity System Manager

Per comunicazioni sicure tra un key management server e i controller dell'array di storage, è necessario configurare i set di certificati appropriati.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.

Informazioni su questa attività

L'autenticazione tra i controller e un key management server è una procedura in due fasi.

Passaggio 1: Completare e inviare la CSR per l'autenticazione con un key management server

È necessario innanzitutto generare un file di richiesta di firma del certificato (CSR) e quindi utilizzare il CSR per richiedere un certificato client firmato a un'autorità di certificazione (CA) considerata attendibile dal key management server. È anche possibile creare e scaricare un certificato client dal key management server utilizzando il file CSR scaricato. Un certificato client convalida i controller dell'array di storage, così il key management server può considerare attendibili le loro richieste Key Management Interoperability Protocol (KMIP).

> I file CSR generati esternamente tramite coppie di chiavi private e pubbliche possono essere importati tramite la finestra di dialogo Crea chiave di sicurezza esterna. Per ulteriori informazioni sull'importazione di un file CSR generato esternamente, vedere "Passaggio 2: Importa i certificati per il key management server".

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Dalla scheda Key Management, selezionare **Complete CSR**.
3. Inserisci le seguenti informazioni:
   - **Nome comune** — Un nome che identifica il client. È prassi comune far sì che il nome comune corrisponda ai requisiti del server KMS per le convenzioni di denominazione dei certificati client. Il nome comune in genere aiuta il KMS a identificare il certificato del client quando viene presentato durante una stretta di mano.
   - **Organizzazione** — Il nome legale completo della tua azienda o organizzazione. Includi i suffissi, come Inc. o Corp.
   - **Unità organizzativa (facoltativa)** — La divisione della tua organizzazione che si occupa del certificato.
   - **Città/Località** — La città o località in cui ha sede la tua organizzazione.
   - **Stato/Regione (facoltativo)** — Lo stato o la regione in cui si trova la tua organizzazione.
   - **Codice ISO del Paese** — Il codice ISO (International Organization for Standardization) a due cifre, ad esempio US, dove si trova la tua organizzazione.
4. Fai clic su **Download**.

   Un file CSR viene salvato sul sistema locale.

5. Richiedi un certificato client firmato dalla CA considerata attendibile dal server di gestione delle chiavi.

   > È comune che il server di gestione delle chiavi disponga di una funzionalità che genera direttamente certificati firmati, poiché funge da propria CA.

6. Quando disponi di un certificato client, vai a Passaggio 2: Importa i certificati per il key management server.

Passaggio 2: Importa i certificati per il key management server

Come passaggio successivo, si importano i certificati per l'autenticazione tra l'array di storage e il key management server. Esistono due tipi di certificati: il certificato client convalida i controller dell'array di storage, mentre il certificato del key management server convalida il server. È necessario caricare sia il file del certificato client per i controller sia il file del certificato del server per il key management server.

Prima di iniziare

- Hai un file di certificato client firmato (vedi Passaggio 1: Completare e inviare la CSR per l'autenticazione con un key management server) e lo hai copiato sull'host da cui accedi a System Manager. Un certificato client convalida i controller dell'array di storage, così il server di gestione delle chiavi può considerare attendibili le loro richieste Key Management Interoperability Protocol (KMIP).
- È necessario recuperare un file di certificato dal server di gestione delle chiavi e quindi copiarlo sull'host da cui si accede a System Manager. Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, quindi l'array di storage può considerare attendibile il suo indirizzo IP. È possibile utilizzare un certificato root, intermedio o server per il server di gestione delle chiavi.

> Per ulteriori informazioni sul certificato del server, consultare la documentazione per il proprio key management server.

Passaggi

1. Selezionare **Impostazioni › Certificati**.
2. Dalla scheda Key Management, selezionare **Import**.

   Si apre una finestra di dialogo per l'importazione dei file del certificato.
3. Accanto a **Seleziona certificato client**, fai clic sul pulsante **Sfoglia** per selezionare il file del certificato client per i controller dell'array di storage.

   Il nome del file viene visualizzato nella finestra di dialogo.
4. Se hai generato un file di certificato esternamente utilizzando una coppia di chiavi privata e pubblica, fai clic sul pulsante **Sfoglia** accanto a **Seleziona file chiave privata** per selezionare il file di certificato per i controller dell'array di storage.

   Il nome del file viene visualizzato nella finestra di dialogo.
5. Accanto a **Select key management server's server certificate**, fai clic sul pulsante **Sfoglia** per selezionare il file del certificato del server per il tuo key management server. Puoi scegliere un certificato root, intermedio o server per il key management server.

   Il nome del file viene visualizzato nella finestra di dialogo.
6. Fai clic su **Import**.

   I file sono stati caricati e convalidati.

Esportare i certificati del server di gestione delle chiavi in SANtricity System Manager

È possibile salvare un certificato per un key management server sul computer locale.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- I certificati devono essere stati importati in precedenza.

Passaggi

1. Selezionare **Impostazioni › Certificati**.

2. Selezionare la scheda **Key Management**.
3. Dalla tabella, seleziona il certificato che desideri esportare e quindi fai clic su **Export**.

   Si apre una finestra di dialogo Salva.

4. Inserisci un nome file e fai clic su **Save**.

Domande frequenti sui certificati firmati da CA e autofirmati per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Perché viene visualizzata la finestra di dialogo Cannot Access Other Controller?

Quando si eseguono determinate operazioni relative ai certificati CA (ad esempio, importare un certificato), potrebbe apparire una finestra di dialogo che richiede di accettare un certificato self-signed per il secondo controller.

Negli array di storage con due controller (configurazioni duplex), questa finestra di dialogo viene talvolta visualizzata se SANtricity System Manager non riesce a comunicare con il secondo controller o se il browser non può accettare il certificato durante un determinato punto di un'operazione.

Se viene visualizzata questa finestra di dialogo, fare clic su **Accetta certificato autofirmato** per procedere. Se viene visualizzata un'altra finestra di dialogo che richiede una password, immettere la password di Administrator utilizzata per accedere a System Manager.

Se questa finestra di dialogo viene visualizzata di nuovo e non è possibile completare un'attività relativa al certificato, prova una delle seguenti procedure:

- Utilizza un tipo di browser diverso per accedere a questo controller, accetta il certificato e continua.
- Accedere al secondo controller withSystem Manager, accettare il certificato autofirmato, quindi tornare al primo controller e continuare.

Come faccio a sapere quali certificati devono essere caricati su SANtricity System Manager per l'external key management?

Per la gestione delle chiavi esterne, importi due tipi di certificati per l'autenticazione tra l'array di storage e il key management server, così che le due entità possano fidarsi l'una dell'altra.

Un certificato client convalida i controller dell'array di storage, così il server di gestione delle chiavi può considerare attendibili le loro richieste Key Management Interoperability Protocol (KMIP).

Per ottenere un certificato client, si utilizza System Manager per completare una CSR per lo storage array. È anche possibile generare una CSR esternamente utilizzando una coppia di chiavi privata e pubblica.

A questo punto, è possibile caricare la CSR su un server di gestione delle chiavi e generare un certificato client da lì. Una volta ottenuto un certificato client, copiare quel file sull'host da cui si accede a System Manager.

Un certificato del server di gestione delle chiavi convalida il server di gestione delle chiavi, quindi il sistema storage può considerare attendibile il suo indirizzo IP. Recupera il file del certificato del server dal server di gestione delle chiavi e poi copia quel file sull'host da cui accedi a System Manager.

Cosa devo sapere sulla verifica della revoca dei certificati?

SANtricity System Manager consente di verificare la presenza di certificati revocati utilizzando un server Online Certificate Status Protocol (OCSP), invece di caricare Certificate Revocation Lists (CRL).

I certificati revocati non dovrebbero più essere considerati affidabili. Un certificato può essere revocato per diversi motivi; ad esempio, se l'Autorità di Certificazione (CA) ha emesso il certificato in modo improprio, se una chiave privata è stata compromessa o se l'entità identificata non ha rispettato i requisiti delle policy.

Dopo aver stabilito una connessione a un server OCSP in System Manager, l'array di storage esegue un controllo di revoca ogni volta che si connette a un AutoSupport server, a un server External Key Management Server (EKMS), a un server Lightweight Directory Access Protocol over SSL (LDAPS) o a un server Syslog. L'array di storage tenta di convalidare i certificati di questi server per assicurarsi che non siano stati revocati. Il server restituisce quindi un valore tra "good", "revoked" o "unknown" per quel certificato. Se il certificato è revocato o l'array non riesce a contattare il server OCSP, la connessione viene rifiutata.

> Specificando un indirizzo di responder OCSP in System Manager o nella command line interface (CLI), si sovrascrive l'indirizzo OCSP presente nel file del certificato.

Per quali tipi di server sarà abilitato il controllo della revoca?

L'array di storage esegue un controllo di revoca ogni volta che si connette a un AutoSupport server, a un External Key Management Server (EKMS), a un server Lightweight Directory Access Protocol over SSL (LDAPS) o a un server Syslog.

Supporto

Ottieni supporto in SANtricity System Manager

La pagina di supporto fornisce l'accesso alle risorse di supporto tecnico.

Quali attività di Support sono disponibili?

In Supporto, puoi visualizzare i contatti del supporto tecnico, eseguire la diagnostica, configurare AutoSupport, visualizzare il registro eventi ed eseguire gli aggiornamenti del software.

Per saperne di più:

- "Panoramica della funzione AutoSupport"
- "Panoramica del registro eventi"
- "Panoramica di Upgrade Center"

Come posso contattare il supporto tecnico?

Dalla pagina principale, fare clic su **Support › Support Center › Support Resources tab**. Le informazioni di contatto del supporto tecnico sono elencate in alto a destra dell'interfaccia.

Visualizza informazioni e diagnostica

Visualizza il profilo di un array di storage in SANtricity System Manager

Il profilo dell’array di storage fornisce una descrizione di tutti i componenti e le proprietà dell’array di storage.

Informazioni su questa attività

È possibile utilizzare il profilo dell’array di storage come ausilio durante il ripristino o come panoramica della configurazione corrente dell’array di storage. Potresti voler salvare una copia del profilo dell’array di storage sul client di gestione e conservare una copia cartacea del profilo dell’array di storage insieme all’array di storage. Crea una nuova copia del profilo dell’array di storage se la configurazione cambia.

Passaggi

1. Selezionare **Support › Support Center › Support Resources** scheda.
2. Scorri verso il basso fino a **Avvia informazioni dettagliate sull’array di storage**, quindi seleziona **Storage Array Profile**.

   Il report appare sullo schermo.

Dettagli del campo

Sezione	Descrizione
Array di archiviazione	Mostra tutte le opzioni che puoi configurare e le opzioni statiche di sistema per il tuo array di storage. Queste opzioni includono il numero di controller, drive shelves, drives, disk pools, gruppi di volumi, volumi e hot spare drives; il numero massimo di drive shelves, drives, Solid State Disks (SSD) e volumi consentiti; il numero di gruppi di snapshot, immagini snapshot, volumi snapshot e gruppi di coerenza; informazioni sulle funzionalità; informazioni sulle versioni del firmware; informazioni sul numero di serie dello chassis; stato di AutoSupport e informazioni sulla pianificazione di AutoSupport; le impostazioni per la raccolta automatica di dati di supporto e la raccolta di dati di supporto pianificata; il World-Wide Identifier (WWID) dell'array di storage; e le impostazioni di scansione dei supporti e cache.
Storage	Mostra un elenco di tutti i dispositivi di storage nell'array di storage. A seconda della configurazione dell'array di storage, la sezione Storage potrebbe mostrare queste sottosezioni. • **Disk Pools** — Mostra un elenco di tutti i disk pools nell'array di storage. • **Gruppi di volumi** — Mostra un elenco di tutti i gruppi di volumi nell'array di storage. I volumi e la capacità libera sono elencati nell'ordine in cui sono stati creati. • **Volumi** — Mostra un elenco di tutti i volumi nell'array di storage. Le informazioni visualizzate includono il nome del volume, lo stato del volume, la capacità, il livello RAID, il gruppo di volumi o il pool di dischi, il tipo di unità e ulteriori dettagli. • **Volumi mancanti** — Mostra un elenco di tutti i volumi nell'array di storage che attualmente hanno uno stato mancante. Le informazioni elencate includono il World Wide Identifier (WWID) per ciascun volume mancante.

Sezione	Descrizione
Servizi di copia	Mostra un elenco di tutti i servizi di copia utilizzati per l'array di storage. A seconda della configurazione dell'array di storage, la sezione Copy Services potrebbe mostrare queste sottosezioni: • **Copie del volume** — Mostra un elenco di tutte le coppie di copie presenti nell'array di storage. Le informazioni visualizzate includono il numero di copie, i nomi delle coppie di copie, lo stato, il timestamp di inizio e ulteriori dettagli. • **Snapshot Groups** — Mostra un elenco di tutti i gruppi di snapshot nell'array di storage. • **Snapshot Images** — Mostra un elenco di tutte le snapshot presenti nell'array di archiviazione. • **Snapshot Volumes** — Mostra un elenco di tutti i volumi snapshot nell'array di archiviazione. • **Gruppi di coerenza** — Mostra un elenco di tutti i gruppi di coerenza nell'array di archiviazione. • **Volumi membri** — Mostra un elenco di tutti i volumi membri del gruppo di coerenza nell'array di storage. • **Mirror Groups** — Mostra un elenco di tutti i volumi mirrorati. • **Capacità riservata** — Mostra un elenco di tutti i volumi di capacità riservata nell'array di storage.
Assegnazioni host	Mostra un elenco delle assegnazioni host nell'array di storage. Le informazioni elencate includono il nome del volume, il numero di unità logica (LUN), l'ID del controller, host name o il nome del cluster host e lo stato del volume. Ulteriori informazioni elencate includono le definizioni della topologia e le definizioni del tipo di host.

Sezione	Descrizione
Hardware	Mostra un elenco di tutto l'hardware nell'array di storage. A seconda della configurazione dell'array di storage, la sezione Hardware potrebbe mostrare queste sottosezioni. • **Controller** — Mostra un elenco di tutti i controller presenti nell'array di storage e include la posizione, lo stato e la configurazione del controller. Inoltre, include informazioni sul canale dell'unità, sul canale host e sulle porte Ethernet. • **Unità** — Mostra un elenco di tutte le unità nell'array di storage. Le unità sono elencate in ordine di shelf ID, drawer ID, slot ID. Le informazioni visualizzate includono lo shelf ID, il drawer ID, lo slot ID, lo stato, la raw capacity, il media type, l'interface type, la current data rate, il product ID e la firmware version per ciascuna unità. La sezione Unità include anche informazioni sul drive channel, informazioni sulla copertura hot spare e informazioni sulla wear life (solo per le unità SSD). Le informazioni sulla wear life includono la percentuale di endurance utilizzata, ovvero la quantità di dati scritti sulle unità SSD fino ad oggi, divisa per il limite teorico totale di scrittura per le unità. • **Canali unità** — Mostra le informazioni relative a tutti i canali unità nell'array di storage. Le informazioni elencate includono lo stato del canale, lo stato del collegamento (se applicabile), il conteggio delle unità e il conteggio cumulativo degli errori. • **Shelves** — Mostra le informazioni relative a tutti gli shelf nell'array di storage. Le informazioni elencate includono i tipi di drive e le informazioni di stato per ciascun componente dello shelf. I componenti dello shelf possono includere pacchi batteria, ricetrasmettitori Small Form-factor Pluggable (SFP), contenitori power-fan o contenitori per moduli di input/output (IOM). La sezione Hardware mostra anche l'identificativo della chiave di sicurezza se una chiave di sicurezza viene utilizzata dall'array di storage.
Caratteristiche	Mostra un elenco dei pacchetti di funzionalità installati e il numero massimo consentito di gruppi di snapshot, snapshot (legacy) e volumi per host o host cluster. Le informazioni nella sezione Funzionalità includono anche Drive Security; ovvero se l'array di storage è security enabled o security disabled.

3. Per cercare nel profilo dell'array di storage, digita un termine di ricerca nella casella di testo **Find** e quindi fai clic su **Find**.

   Tutti i termini corrispondenti sono evidenziati. Per scorrere tutti i risultati uno alla volta, continua a cliccare **Cerca**.

4. Per salvare il profilo dell'array di storage, fai clic su **Save**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome `storage-array-profile.txt`.

Visualizza l'inventario del software e del firmware in SANtricity System Manager

L'inventario del software e del firmware elenca le versioni del firmware per ciascun componente del tuo array di storage.

Informazioni su questa attività

Un array di storage è composto da numerosi componenti, che possono includere controller, unità, cassetti e moduli di input/output (IOM). Ciascuno di questi componenti contiene firmware. Alcune versioni di firmware dipendono da altre versioni di firmware. Per acquisire informazioni su tutte le versioni di firmware presenti nell'array di storage, visualizza l'inventario del software e del firmware. Il supporto tecnico può analizzare l'inventario del software e del firmware per rilevare eventuali incongruenze del firmware.

Passaggi

1. Selezionare **Support › Support Center › Support Resources** scheda.
2. Scorri verso il basso fino a **Launch detailed storage array information**, quindi seleziona **Software and Firmware Inventory**.

   Il report dell'inventario del software e del firmware viene visualizzato sullo schermo.

3. Per salvare l'inventario del software e del firmware, fare clic su **Salva**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome file `firmware-inventory.txt`.

4. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Raccogli dati diagnostici

Raccogli manualmente i dati di supporto in SANtricity System Manager

È possibile raccogliere in un unico file diversi tipi di dati relativi a inventario, stato e prestazioni del proprio array di storage. Il supporto tecnico può utilizzare il file per la risoluzione dei problemi e ulteriori analisi.

Informazioni su questa attività

Se la funzione AutoSupport è abilitata, puoi anche raccogliere questi dati andando alla scheda **AutoSupport** e selezionando **Invia AutoSupport Dispatch**.

È possibile eseguire una sola operazione di raccolta alla volta. Se si tenta di avviare un'altra operazione, viene visualizzato un messaggio di errore.

Eseguire questa operazione solo quando richiesto dal supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Collect Support Data**.
3. Fai clic su **Collect**.

   Il file viene salvato nella cartella Downloads del browser con il nome `support-data.7z`. Se il shelf

contiene cassetti, i dati diagnostici per quel shelf vengono archiviati in un file zip separato denominato `tray-component-state-capture.7z`.

4. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Raccogli i dati di configurazione in SANtricity System Manager

È possibile salvare i dati di configurazione RAID dal controller, inclusi tutti i dati relativi ai gruppi di volumi e ai pool di dischi. Successivamente, è possibile contattare il supporto tecnico per assistenza con il ripristino dei dati.

Informazioni su questa attività

Questa procedura descrive come salvare lo stato corrente del database di configurazione RAID. Questi dati vengono recuperati dalla posizione di memoria RPA del controller.

> La funzione Collect Configuration Data salva le stesse informazioni del comando CLI per `save storageArray dbmDatabase`.

Devi eseguire questa operazione solo quando richiesto da un'operazione Recovery Guru o dal supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Collect Configuration Data**.
3. Nella finestra di dialogo, fai clic su **Collect**.

   Il file, `configurationData-<arrayName>-<dateTime>.7z`, viene salvato nella cartella Download del tuo browser.

4. Contatta il supporto tecnico per ulteriori informazioni sull'invio del file a loro e sul caricamento dei dati nel sistema.

Recupera i file di supporto al ripristino in SANtricity System Manager

Il supporto tecnico può utilizzare i file di supporto per il ripristino per risolvere i problemi. SANtricity System Manager salva automaticamente questi file.

Prima di iniziare

Il supporto tecnico ha richiesto che tu invii loro file aggiuntivi per la risoluzione dei problemi.

Informazioni su questa attività

I file di supporto per il ripristino includono questi tipi di file:

- File di dati di supporto
- Cronologia AutoSupport
- Log AutoSupport
- File di diagnostica SAS/RLS
- Dati del profilo di recupero

- file di acquisizione del database

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Retrieve Recovery Support Files**.

   Viene visualizzata una finestra di dialogo che elenca tutti i file di supporto al ripristino raccolti dall'array di storage. Per trovare file specifici, è possibile ordinare una qualsiasi delle colonne o digitare caratteri nella casella **Filter**.

3. Seleziona un file, quindi fai clic su **Download**.

   Il file viene salvato nella cartella Downloads del tuo browser.

4. Se devi salvare altri file, ripeti il passaggio precedente.
5. Fare clic su **Close**.
6. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Recupera i buffer di traccia in SANtricity System Manager

È possibile recuperare i buffer di traccia dai controller e inviare il file al supporto tecnico per l'analisi.

Informazioni su questa attività

Il firmware utilizza i buffer di traccia per registrare l'elaborazione, in particolare le condizioni di eccezione, che possono essere utili per il debug. È possibile recuperare i buffer di traccia senza interrompere il funzionamento dell'array di storage e con un impatto minimo sulle prestazioni.

Eseguire questa operazione solo quando richiesto dal supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Recupera buffer di traccia**.
3. Seleziona la check box accanto a ciascun controller per cui desideri recuperare i buffer di traccia.

   È possibile selezionare uno o entrambi i controller. Se il messaggio di stato del controller a destra di una check box è Failed o Disabled, la check box è disabilitata.

4. Fai clic su **Yes**.

   Il file viene salvato nella cartella Downloads del tuo browser con il filename `trace-buffers.7z`.

5. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Raccogli statistiche del percorso I/O in SANtricity System Manager

È possibile salvare il file delle statistiche del percorso I/O e inviarlo al supporto tecnico per l'analisi.

Informazioni su questa attività

Il supporto tecnico utilizza le statistiche del percorso I/O per aiutare a diagnosticare i problemi di prestazioni. I problemi di prestazioni dell'applicazione possono essere causati dall'utilizzo della memoria, dall'utilizzo della CPU, dalla latenza di rete, dalla latenza I/O o da altri problemi. Le statistiche del percorso I/O vengono raccolte automaticamente durante la raccolta di dati di supporto oppure è possibile raccoglierle manualmente. Inoltre, se hai AutoSupport attivo, le statistiche del percorso I/O vengono raccolte automaticamente e inviate al supporto tecnico.

I contatori delle statistiche del percorso I/O vengono azzerati dopo aver confermato che si desidera raccogliere le statistiche del percorso I/O. I contatori vengono azzerati anche se si annulla successivamente l'operazione. I contatori vengono inoltre azzerati quando il controller si resetta (riavvia).

Eseguire questa operazione solo quando richiesto dal supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Selezionare **Raccogli statistiche del percorso I/O**.
3. Conferma di voler eseguire l'operazione digitando `collect`, quindi fai clic su **Collect**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome file `io-path-statistics.7z`.

4. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Recuperare l'immagine di stato in SANtricity System Manager

È possibile esaminare un'immagine di stato del controller. Un'immagine di stato è un dump di dati raw della memoria del processore del controller che il supporto tecnico può utilizzare per diagnosticare un problema con un controller.

Informazioni su questa attività

Il firmware genera automaticamente un'immagine di stato quando rileva determinati errori. Dopo che è stata generata un'immagine di stato, il controller che ha presentato l'errore si riavvia e un evento viene registrato nel registro eventi.

Se hai AutoSupport attivato, l'immagine dello stato di salute viene inviata automaticamente al supporto tecnico. Se non hai AutoSupport attivato, devi contattare il supporto tecnico per istruzioni su come recuperare l'immagine dello stato di salute e inviarla per l'analisi.

Eseguire questa operazione solo quando richiesto dal supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Retrieve Health Image**.

   È possibile visualizzare la sezione dettagli per vedere le dimensioni dell'immagine di integrità prima di scaricare il file.

3. Fai clic su **Collect**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome `health-image.7z`.

4. Segui le istruzioni fornite dal supporto tecnico per inviare loro il file.

Intraprendere azioni di recupero

Visualizza il registro dei settori illeggibili in SANtricity System Manager

È possibile salvare il registro dei settori illeggibili e inviare il file al supporto tecnico per l'analisi.

Informazioni su questa attività

Il registro dei settori illeggibili contiene informazioni dettagliate sui settori illeggibili causati da unità che segnalano errori irreversibili del supporto di memorizzazione. I settori illeggibili vengono rilevati durante le normali operazioni di I/O e durante le operazioni di modifica, come le ricostruzioni. Quando vengono rilevati settori illeggibili su un array di storage, viene visualizzato un avviso Needs Attention per l'array di storage. Il Recovery Guru distingue quale condizione di settore illeggibile richiede attenzione. Tutti i dati contenuti in un settore illeggibile non possono essere recuperati e devono essere considerati persi.

Il registro dei settori illeggibili può memorizzare fino a 1.000 settori illeggibili. Quando il registro dei settori illeggibili raggiunge 1.000 voci, si applicano le seguenti condizioni:

- Se durante la ricostruzione vengono rilevati nuovi settori illeggibili, la ricostruzione fallisce e non viene registrata alcuna voce.
- Per i nuovi settori illeggibili rilevati durante l'I/O, l'I/O fallisce e non viene registrata alcuna voce.

> Queste azioni includono scritture RAID 5 e scritture RAID 6 che sarebbero andate a buon fine prima dell'overflow.

> **Possibile perdita di dati** — Il recupero da settori illeggibili è una procedura complessa che può prevedere diversi metodi. Eseguire questa operazione solo su indicazione del supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Visualizza/Cancella settori illeggibili**.
3. Per salvare il registro dei settori illeggibili:

   a. Nella prima colonna della tabella, puoi selezionare i singoli volumi per cui desideri salvare il registro dei settori illeggibili (fai clic sulla check box accanto a ciascun volume) oppure selezionare tutti i volumi (seleziona la check box nell'intestazione della tabella).

      Per trovare volumi specifici, puoi ordinare una qualsiasi delle colonne o digitare caratteri nella casella **Filter**.

   b. Fare clic su **Save**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome `unreadable-sectors.txt`.

4. Se il supporto tecnico ti istruisce a cancellare il registro dei settori illeggibili, esegui i seguenti passaggi:

   a. Nella prima colonna della tabella, puoi selezionare i singoli volumi per cui desideri cancellare il registro dei settori illeggibili (fai clic sulla check box accanto a ciascun volume) oppure selezionare tutti i volumi (seleziona la check box nell'intestazione della tabella).

b. Fai clic su **Clear** e conferma di voler eseguire l'operazione.

Riattiva le porte delle unità in SANtricity System Manager

È possibile indicare al controller che è stata intrapresa un'azione correttiva per recuperare da una condizione di cablaggio errato.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Riattiva porte unità** e conferma che vuoi eseguire l'operazione.

   Questa opzione viene visualizzata solo quando l'array di storage ha porte delle unità disabilitate.

   Il controller riattiva tutte le porte SAS che erano state disabilitate quando è stato rilevato un cablaggio errato.

Cancella la modalità di ripristino nel software SANtricity

Dopo aver ripristinato la configurazione di un array di storage, utilizzare l'operazione Cancella modalità di ripristino per riprendere l'I/O sull'array di storage e riportarlo alle normali operazioni.

Prima di iniziare

- Se si desidera riportare l'array di storage a una configurazione precedente, è necessario ripristinare la configurazione dal backup prima di disattivare la modalità di ripristino.
- È necessario eseguire dei controlli di convalida o contattare il supporto tecnico per accertarsi che il ripristino sia andato a buon fine. Dopo aver determinato che il ripristino è stato completato con successo, è possibile disattivare la modalità di ripristino.

Informazioni su questa attività

L'array di storage contiene un database di configurazione che include una registrazione della sua configurazione logica (pool, gruppi di volumi, volumi e così via). Se si cancella intenzionalmente la configurazione dell'array di storage o se il database di configurazione viene danneggiato, l'array di storage entra in modalità di ripristino. La modalità di ripristino interrompe le operazioni di I/O e blocca il database di configurazione, dandoti il tempo di eseguire una delle seguenti operazioni:

- Ripristina la configurazione dal backup automatico memorizzato nelle memorie flash del controller. È necessario contattare il supporto tecnico per eseguire questa operazione.
- Ripristina la configurazione da una precedente operazione di Save Configuration Database. Le operazioni di Save Configuration Database vengono eseguite tramite l'interfaccia a riga di comando (CLI).
- Riconfigurare l'array di storage da zero.

Dopo che la configurazione dell'array di storage è stata ripristinata o ridefinita e hai verificato che tutto sia a posto, devi cancellare manualmente la modalità di ripristino.

> Non è possibile annullare l'operazione Clear Recovery Mode dopo che è stata avviata. La cancellazione della modalità di ripristino può richiedere molto tempo. Eseguire questa operazione solo su indicazione del supporto tecnico.

Passaggi

1. Selezionare **Support › Support Center › Diagnostics** scheda.
2. Seleziona **Clear Recovery Mode** e conferma di voler eseguire questa operazione.

   Questa opzione viene visualizzata solo se l'array di storage è in modalità di ripristino.

Gestisci AutoSupport

Scopri AutoSupport per E-Series

La funzionalità AutoSupport monitora lo stato di salute di un array di storage e invia automaticamente segnalazioni al supporto tecnico.

Il supporto tecnico utilizza i dati AutoSupport in modo reattivo per accelerare la diagnosi e la risoluzione dei problemi dei clienti e in modo proattivo per individuare ed evitare potenziali problemi.

AutoSupport data include informazioni sulla configurazione, lo stato, le prestazioni e gli eventi di sistema di un array di storage. I dati AutoSupport non contengono alcun dato utente. Le richieste possono essere inviate immediatamente o secondo una pianificazione (giornaliera e settimanale).

Principali vantaggi

Alcuni dei principali vantaggi della funzionalità AutoSupport includono:

- Tempi di risoluzione dei casi accelerati
- Monitoraggio sofisticato per una gestione più rapida degli incidenti
- Generazione automatica di report in base a una pianificazione, nonché generazione automatica di report relativi a eventi critici
- Richieste automatizzate di sostituzione hardware per componenti selezionati come drive
- Avvisi non invasivi per notificarti un problema e fornire informazioni al supporto tecnico per intraprendere azioni correttive
- AutoSupport analysis tools che monitorano le spedizioni per problemi di configurazione noti

Caratteristiche individuali di AutoSupport

La funzionalità AutoSupport è composta da tre funzionalità individuali che si abilitano separatamente.

- **Base AutoSupport** — Consente al tuo array di storage di raccogliere e inviare automaticamente i dati al supporto tecnico.
- **AutoSupport OnDemand** — Consente al supporto tecnico di richiedere la ritrasmissione di una precedente spedizione AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
- **Diagnostica remota** — Consente al supporto tecnico di richiedere una nuova, aggiornata AutoSupport dispatch quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se ci sono nuove richieste in sospeso e risponde di conseguenza.

Differenza tra AutoSupport e Collect Support Data

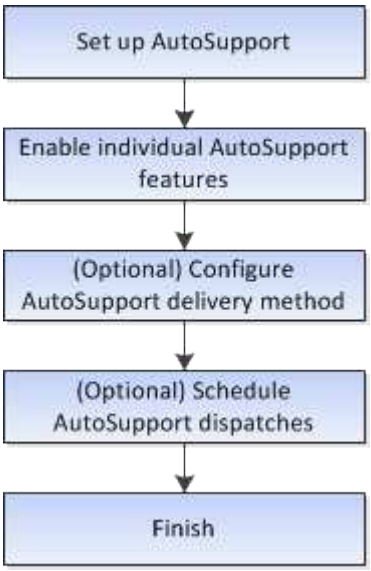
Esistono due metodi per la raccolta dei dati di supporto nell'array di archiviazione:

- **AutoSupport feature** — I dati vengono raccolti automaticamente.
- **Opzione Collect Support Data** — I dati devono essere raccolti e inviati manualmente.

La funzionalità AutoSupport è più facile da usare perché i dati vengono raccolti e inviati automaticamente. I dati AutoSupport possono essere utilizzati in modo proattivo per prevenire i problemi prima che si verifichino. La funzionalità AutoSupport velocizza la risoluzione dei problemi perché il supporto tecnico ha già accesso ai dati. Per questi motivi, la funzionalità AutoSupport è il metodo di raccolta di dati preferito da utilizzare.

Configura AutoSupport in SANtricity System Manager

In SANtricity System Manager, configuri la funzionalità AutoSupport seguendo questi passaggi.



Attivare o disattivare le funzionalità AutoSupport in SANtricity System Manager

È possibile abilitare la funzione AutoSupport e le singole funzioni AutoSupport durante la configurazione iniziale oppure abilitarle o disattivarle in un secondo momento.

Prima di iniziare

Se si desidera abilitare AutoSupport OnDemand o la Diagnostica remota, il metodo di consegna di AutoSupport deve essere impostato su HTTPS.

Informazioni su questa attività

È possibile disabilitare la funzione AutoSupport in qualsiasi momento, ma si consiglia vivamente di lasciarla abilitata. L'abilitazione della funzione AutoSupport può accelerare significativamente la determinazione e la risoluzione dei problemi qualora si verificasse un problema sullo storage array.

La funzionalità AutoSupport è composta da tre funzionalità individuali che si abilitano separatamente.

- **Base AutoSupport** — Consente al tuo array di storage di raccogliere e inviare automaticamente i dati al supporto tecnico.

- **AutoSupport OnDemand** — Consente al supporto tecnico di richiedere la ritrasmissione di una precedente spedizione AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
- **Diagnostica remota** — Consente al supporto tecnico di richiedere una nuova, aggiornata AutoSupport dispatch quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se ci sono nuove richieste in sospeso e risponde di conseguenza.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Seleziona **Abilita/Disabilita AutoSupport Features**.
3. Seleziona le caselle di controllo accanto alle funzionalità AutoSupport che desideri abilitare.

   Le funzionalità dipendono l'una dall'altra, come indicato dalla rientranza degli elementi nella finestra di dialogo. Ad esempio, è necessario abilitare AutoSupport OnDemand prima di poter abilitare Remote Diagnostics.

4. Fare clic su **Save**.

   Se disattivi AutoSupport, viene visualizzata una notifica nella pagina Home. Puoi ignorare la notifica facendo clic su **Ignore**.

Configurare il metodo di consegna AutoSupport in SANtricity System Manager

La funzionalità AutoSupport supporta i protocolli HTTPS e SMTP per l'invio di comunicazioni al supporto tecnico.

Prima di iniziare

- La funzione AutoSupport deve essere abilitata. Puoi verificare se è abilitata nella pagina AutoSupport.
- È necessario installare e configurare un DNS server nella rete. L'indirizzo del DNS server deve essere configurato in System Manager (questa operazione è disponibile nella pagina Hardware).

Informazioni su questa attività

Esamina i diversi protocolli:

- **HTTPS** — Consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTPS. Se si desidera abilitare AutoSupport OnDemand o la diagnostica remota, il metodo di consegna AutoSupport deve essere impostato su HTTPS.
- **Email** — Consente di utilizzare un server di posta elettronica come metodo di consegna per l'invio di AutoSupport dispatches.

> **Differenze tra i metodi HTTPS ed Email**. Il metodo di consegna Email, che utilizza SMTP, presenta alcune importanti differenze rispetto al metodo di consegna HTTPS. In primo luogo, la dimensione degli invii per il metodo Email è limitata a 5MB, il che significa che alcune raccolte di dati ASUP non verranno inviate. In secondo luogo, la funzionalità AutoSupport OnDemand è disponibile solo con il metodo di consegna HTTPS.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Seleziona **Configura AutoSupport Delivery Method**.

   Viene visualizzata una finestra di dialogo che elenca i metodi di consegna della spedizione.

3. Seleziona il metodo di consegna desiderato, quindi seleziona i parametri per tale metodo. Esegui una delle seguenti operazioni:
   - Se hai selezionato HTTPS, seleziona uno dei seguenti parametri di consegna:
     - **Direttamente** — Questo parametro di consegna è la selezione predefinita. Scegliendo questa opzione è possibile connettersi direttamente al sistema di supporto tecnico di destinazione utilizzando il protocollo HTTPS.
     - **Tramite proxy server** — Scegliendo questa opzione è possibile specificare i dettagli del proxy server HTTP necessari per stabilire la connessione con il sistema di supporto tecnico di destinazione. È necessario specificare l'indirizzo host e il numero di porta. Tuttavia, è necessario inserire i dettagli di autenticazione dell'host (nome utente e password) solo se richiesto.
     - **Tramite script di autoconfigurazione proxy (PAC)** — Specificare il percorso di un file di script di autoconfigurazione proxy (PAC). Un file PAC consente al sistema di scegliere automaticamente il proxy server appropriato per stabilire una connessione con il sistema di supporto tecnico di destinazione.
   - Se hai selezionato Email, inserisci le seguenti informazioni:
     - L'indirizzo del server di posta come fully qualified domain name, indirizzo IPv4 o indirizzo IPv6.
     - L'indirizzo email che compare nel campo Da dell'email di invio AutoSupport.
     - **Facoltativo; se si desidera eseguire un test di configurazione**: L'indirizzo e-mail a cui viene inviata una conferma quando il AutoSupport system riceve la richiesta di test.
     - Se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. In caso contrario, selezionare **None**.
     - Se necessario, inserire un nome utente e una password per l'autenticazione con il mittente in uscita e il server di posta.
4. Se hai un firewall che blocca la consegna di questi ASUP dispatches, aggiungi il seguente URL alla tua whitelist: `https://support.netapp.com/put/AsupPut/`
5. Fai clic su **Verifica configurazione** per testare la connessione al server di supporto tecnico utilizzando i parametri di consegna specificati. Se hai abilitato la funzione AutoSupport On-Demand, il sistema testerà anche la connessione per la consegna di AutoSupport OnDemand.

   Se il test di configurazione non riesce, verifica le impostazioni di configurazione ed esegui nuovamente il test. Se il test continua a non riuscire, contatta il supporto tecnico.

6. Fare clic su **Save**.

Pianifica le spedizioni AutoSupport in SANtricity System Manager

SANtricity System Manager crea automaticamente una pianificazione predefinita per le spedizioni di AutoSupport. Se preferisci, puoi specificare la tua pianificazione.

Prima di iniziare

La funzione AutoSupport deve essere abilitata. Puoi verificare se è abilitata nella pagina AutoSupport.

Informazioni su questa attività

- **Orario giornaliero** — I messaggi giornalieri vengono raccolti e inviati ogni giorno nell'intervallo di tempo specificato. System Manager seleziona un orario casuale all'interno di tale intervallo. Tutti gli orari sono espressi in Coordinated Universal Time (UTC), che potrebbe essere diverso dall'ora locale dell'array di storage. È necessario convertire l'ora locale dell'array di storage in UTC.
- **Giorno settimanale** — Le spedizioni settimanali vengono raccolte e inviate una volta a settimana. System Manager seleziona un giorno casuale tra quelli che specifichi. Deseleziona i giorni in cui non desideri consentire una spedizione settimanale. System Manager seleziona un giorno casuale tra quelli che consenti.
- **Orario settimanale** — Le spedizioni settimanali vengono raccolte e inviate una volta a settimana nell'intervallo di tempo che si specifica. System Manager seleziona un orario casuale all'interno dell'intervallo. Tutti gli orari sono in Coordinated Universal Time (UTC), che potrebbe essere diverso dall'ora locale dell'array di storage. È necessario convertire l'ora locale dell'array di storage in UTC.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Selezionare **Schedule AutoSupport Dispatches**.

   Viene visualizzata la procedura guidata di pianificazione delle spedizioni AutoSupport.

3. Segui i passaggi della procedura guidata.

Invia i dispacci AutoSupport in SANtricity System Manager

SANtricity System Manager consente di inviare le segnalazioni AutoSupport al supporto tecnico, senza dover attendere una segnalazione programmata.

Prima di iniziare

La funzione AutoSupport deve essere abilitata. Puoi verificare se è abilitata nella pagina AutoSupport.

Informazioni su questa attività

Questa operazione raccoglie i dati di supporto e li invia automaticamente al supporto tecnico, così che possano risolvere i problemi.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Seleziona **Invia AutoSupport Dispatch**.

   Viene visualizzata la finestra di dialogo Invia AutoSupport Dispatch.

3. Confermare l'operazione selezionando **Invia**.

Visualizza lo stato di AutoSupport in SANtricity System Manager

La pagina AutoSupport mostra se la funzionalità AutoSupport e le singole funzionalità AutoSupport sono attualmente abilitate.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Guardate il lato destro della pagina, appena sotto le schede, per verificare se la funzione base

AutoSupport è abilitata.

3. Passa il cursore del mouse sul punto interrogativo per verificare se le singole funzionalità AutoSupport sono abilitate.

Visualizza il file di log AutoSupport in SANtricity System Manager

Il registro AutoSupport fornisce informazioni sullo stato, la cronologia delle spedizioni e gli errori riscontrati durante la consegna delle spedizioni AutoSupport.

Informazioni su questa attività

Possono esistere più file di log. Quando il file di log corrente raggiunge i 200 KB, viene archiviato e viene creato un nuovo file di log. Il nome del file di log archiviato è `ASUPMessages.n`, dove *n* è un numero intero da 1 a 9. Se esistono più file di log, è possibile scegliere di visualizzare il log più recente o uno precedente.

- **Registro corrente** — Mostra un elenco degli ultimi eventi acquisiti.
- **Registro archiviato** — Mostra un elenco di eventi precedenti.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Seleziona **Visualizza AutoSupport Log**.

   Viene visualizzata una finestra di dialogo che elenca il registro AutoSupport corrente.

3. Se desideri visualizzare i registri AutoSupport precedenti, seleziona il pulsante di opzione **Archiviati** e poi seleziona un registro dall'elenco a discesa **Seleziona registro AutoSupport**.

   L'opzione Archiviati viene visualizzata solo se esistono log archiviati sull'array di storage.

   Il registro AutoSupport selezionato viene visualizzato nella finestra di dialogo.

4. **Facoltativo:** Per cercare nel registro AutoSupport, digita un termine nella casella **Trova** e fai clic su **Trova**.

   Fai clic su **Trova** di nuovo per cercare altre occorrenze del termine.

Abilitare la finestra di manutenzione AutoSupport in SANtricity System Manager

Abilitare la finestra di manutenzione AutoSupport per sopprimere la creazione automatica di ticket in caso di eventi di errore. In modalità operativa normale, l'array di storage utilizza AutoSupport per aprire un caso con il Supporto in caso di problemi.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Selezionare **Abilita AutoSupport finestra di manutenzione**.
3. Inserisci l'indirizzo email per ricevere una conferma che la richiesta della finestra di manutenzione è stata elaborata.

   A seconda della configurazione, potresti essere in grado di inserire fino a cinque indirizzi email. Se desideri aggiungere più di un indirizzo, seleziona **Aggiungi un altro indirizzo email** per aprire un altro campo.

4. Specificare la durata (in ore) per abilitare la finestra di manutenzione.

La durata massima supportata è 72 ore.

5. Fai clic su **Yes**.

   AutoSupport la creazione automatica di ticket in caso di eventi di errore è temporaneamente soppressa per la finestra di durata specificata.

Dopo aver finito

La finestra di manutenzione non inizia finché la richiesta dell'array di storage non viene elaborata dai server AutoSupport. Attendi di aver ricevuto un'e-mail di conferma prima di eseguire qualsiasi attività di manutenzione sull'array di storage.

Disabilita la finestra di manutenzione AutoSupport in SANtricity System Manager

Disabilita la finestra di manutenzione AutoSupport per consentire la creazione automatica di ticket in caso di eventi di errore. Quando la finestra di manutenzione AutoSupport è disabilitata, l'array di storage utilizzerà AutoSupport per aprire un caso con il Supporto in caso di problemi.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Selezionare **Disabilita AutoSupport Maintenance window**.
3. Inserisci l'indirizzo email per ricevere una conferma che la richiesta di disattivazione della finestra di manutenzione è stata elaborata.

   A seconda della configurazione, potresti essere in grado di inserire fino a cinque indirizzi email. Se desideri aggiungere più di un indirizzo, seleziona **Aggiungi un altro indirizzo email** per aprire un altro campo.

4. Fai clic su **Yes**.

   AutoSupport la creazione automatica dei ticket in caso di eventi di errore è abilitata.

Dopo aver finito

La finestra di manutenzione non terminerà finché la richiesta dell'array di storage non sarà stata elaborata dai server AutoSupport. Attendi di aver ricevuto un'email di conferma prima di procedere.

Visualizza eventi

Scopri il registro eventi nel software SANtricity

Il registro eventi fornisce una cronologia degli eventi verificatisi sull'array di storage, il che aiuta il supporto tecnico nella risoluzione dei problemi che hanno portato ai guasti.

È possibile utilizzare il registro eventi come strumento diagnostico supplementare a Recovery Guru per tracciare gli eventi dell'array di storage. Consultare sempre Recovery Guru come prima opzione quando si tenta di ripristinare da guasti dei componenti dell'array di storage.

Categorie di eventi

Gli eventi nel registro eventi sono classificati in base a diversi stati. Gli eventi che richiedono un intervento hanno i seguenti stati:

- Critico
- Avvertimento

Gli eventi di natura informativa che non richiedono alcuna azione immediata sono i seguenti:

- Informativo

Eventi critici

Gli eventi critici indicano un problema con l'array di storage. Se si risolve immediatamente l'evento critico, si potrebbe evitare la perdita di accesso ai dati.

Quando si verifica un evento critico, questo viene registrato nel registro eventi. Tutti gli eventi critici vengono inviati alla console di gestione SNMP o al destinatario e-mail che hai configurato per ricevere le notifiche di avviso. Se l'ID dello shelf non è noto al momento dell'evento, l'ID dello shelf viene visualizzato come "Shelf unknown."

Quando ricevi un evento critico, consulta la procedura di Recovery Guru per una descrizione dettagliata dell'evento critico. Completa la procedura di Recovery Guru per correggere l'evento critico. Per correggere alcuni eventi critici, potrebbe essere necessario contattare il supporto tecnico.

Visualizza gli eventi utilizzando il log eventi in SANtricity System Manager

È possibile visualizzare il registro eventi, che fornisce una cronologia degli eventi che si sono verificati sull'array di storage.

Passaggi

1. Selezionare il **Support › Event Log**.

   Viene visualizzata la pagina del registro eventi.

Dettagli della pagina

Articolo	Descrizione
Visualizza tutti i campi	Consente di passare tra tutti gli eventi e solo gli eventi critici e di avviso.
Campo filtro	Filtra gli eventi. Utile per visualizzare solo gli eventi relativi a un componente specifico, a un evento specifico, ecc.
Seleziona l'icona delle colonne.	Consente di selezionare altre colonne da visualizzare. Le altre colonne forniscono informazioni aggiuntive sull'evento.
Caselle di controllo	Consente di selezionare gli eventi da salvare. La check box nell'intestazione della tabella seleziona tutti gli eventi.
Colonna Data/Ora	La data e l'ora dell'evento, secondo l'orologio del controller. Il registro eventi inizialmente ordina gli eventi in base al numero di sequenza. Solitamente, questa sequenza corrisponde alla data e all'ora. Tuttavia, i due orologi del controller nell'array di storage potrebbero non essere sincronizzati. In questo caso, potrebbero apparire delle incongruenze nel registro eventi relative agli eventi e alla data e all'ora mostrate.
Colonna priorità	Questi valori di priorità esistono: • **Critico** — Esiste un problema con l'array di storage. Tuttavia, se si interviene immediatamente, si potrebbe evitare di perdere l'accesso ai dati. Gli eventi critici vengono utilizzati per le notifiche di avviso. Tutti gli eventi critici vengono inviati a qualsiasi client di gestione della rete (tramite trap SNMP) o al destinatario email che hai configurato. • **Avviso** — Si è verificato un errore che ha degradato le prestazioni e la capacità dell'array di archiviazione di riprendersi da un altro errore. • **Informativo** — Informazioni non critiche relative allo storage array.
Colonna Tipo di componente	Il componente interessato dall'evento. Il componente potrebbe essere hardware, come un'unità o un controller, oppure software, come il firmware del controller.
Colonna posizione componente	La posizione fisica del componente nell'array di archiviazione.
Colonna descrizione	Una descrizione dell'evento. **Esempio** — `Drive write failure - retries exhausted`

Articolo	Descrizione
Colonna Sequence Number	Un numero a 64 bit che identifica in modo univoco una specifica voce di registro per un array di storage. Questo numero viene incrementato di uno a ogni nuova voce di registro eventi. Per visualizzare queste informazioni, fare clic sull'icona **Seleziona colonne**.
Colonna Tipo evento	Un numero di 4 cifre che identifica ogni tipo di evento registrato. Per visualizzare queste informazioni, fare clic sull'icona **Seleziona colonne**.
Colonna Codici specifici dell'evento	Queste informazioni vengono utilizzate dal supporto tecnico. Per visualizzare queste informazioni, fai clic sull'icona **Seleziona colonne**.
Colonna Categoria evento	• **Guasto** – Un componente nell'array di archiviazione ha avuto un guasto; ad esempio, guasto dell'unità o guasto della batteria. • **Cambio di stato** – Un elemento dell'array di storage che ha cambiato stato; ad esempio, un volume è passato allo stato Optimal o un controller è passato allo stato Offline. • **Interno** – Operazioni interne del controller che non richiedono azione da parte dell'utente; ad esempio, il controller ha completato start-of-day. • **Comando** – Un comando che è stato impartito all'array di storage; ad esempio, è stato assegnato un hot spare. • **Errore** – È stata rilevata una condizione di errore sull'array di storage; ad esempio, un controller non è in grado di sincronizzare e svuotare la cache, oppure è stato rilevato un errore di ridondanza sull'array di storage. • **Generale** – Qualsiasi evento che non rientra bene in nessun'altra categoria. Per visualizzare queste informazioni, fai clic sull'icona **Seleziona colonne**.
Colonna Logged By	Il nome del controller che ha registrato l'evento. Per visualizzare queste informazioni, fare clic sull'icona **Select columns**.

2. Per recuperare nuovi eventi dall'array di archiviazione, fare clic su **Refresh**.

   Possono essere necessari diversi minuti prima che un evento venga registrato e diventi visibile nella pagina Event Log.

3. Per salvare il registro eventi in un file:
   a. Seleziona la check box accanto a ciascun evento che vuoi salvare.
   b. Fare clic su **Save**.

      Il file viene salvato nella cartella Downloads del tuo browser con il nome `major-event-log-timestamp.log`.

4. Per cancellare gli eventi dal registro eventi:

Il registro eventi memorizza circa 8.000 eventi prima di sostituire un evento con uno nuovo. Se si desidera conservare gli eventi, è possibile salvarli e cancellarli dal registro eventi.

a. Innanzitutto, salva il registro eventi.

b. Fai clic su **Clear All** e conferma di voler eseguire l'operazione.

Gestisci gli aggiornamenti

Scopri come aggiornare il software SANtricity

Utilizza l'Upgrade Center per scaricare il software e il firmware più recenti e per aggiornare i controller e i drive.

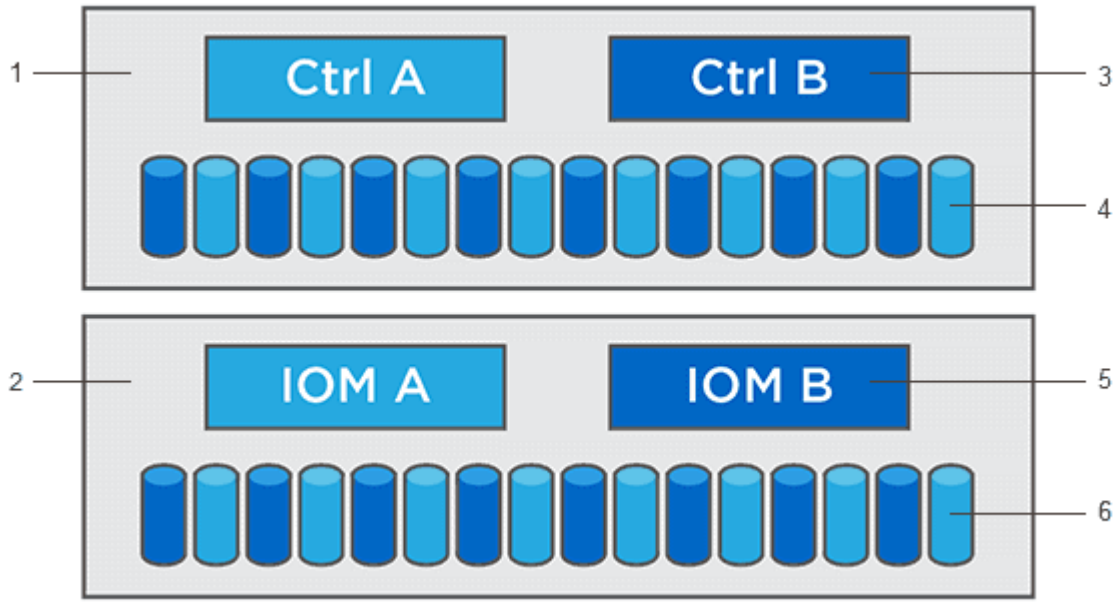
Panoramica sull'aggiornamento del controller

È possibile aggiornare il software e il firmware dell'array di storage per usufruire di tutte le funzionalità più recenti e delle correzioni di bug.

Componenti inclusi nell'aggiornamento del controller del sistema operativo

Diversi componenti degli array di storage contengono software o hardware che potresti voler aggiornare occasionalmente.

- **Software di gestione** — System Manager è il software che gestisce l'array di storage.
- **Controller firmware** — Il firmware del controller gestisce l'I/O tra host e volumi.
- **Controller NVSRAM** — Controller NVSRAM è un file che specifica le impostazioni predefinite per i controller.
- **IOM firmware** — Il firmware del modulo I/O (IOM) gestisce la connessione tra un controller e uno shelf di dischi. Monitora inoltre lo stato dei componenti.
- **Software di supervisione** — Il software di supervisione è la macchina virtuale su un controller in cui viene eseguito il software.



[1] Alloggiamento del controller; [2] Alloggiamento dell'unità; [3] Software, firmware del controller, NVSRAM del controller, software di supervisione; [4] Drive firmware; [5] IOM firmware; [6] Drive firmware

È possibile visualizzare le versioni correnti del software e del firmware nella finestra di dialogo Inventario software e firmware. Accedere al **Support › Upgrade Center**, e quindi fare clic sul collegamento **Software and Firmware Inventory**.

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover e/o il driver HBA dell'host affinché quest'ultimo possa interagire correttamente con i controller. Per determinare se questo è il caso, vedere la "Netapp Interoperability Matrix Tool".

Quando interrompere l'I/O

Se l'array di storage contiene due controller ed è installato un driver multipath, l'array di storage può continuare a elaborare le operazioni di I/O durante l'aggiornamento. Durante l'aggiornamento, il controller A esegue il failover di tutti i suoi volumi sul controller B, esegue l'aggiornamento, riprende i propri volumi e tutti i volumi del controller B, quindi aggiorna il controller B.

Controllo di integrità pre-aggiornamento

Un controllo dello stato di salute pre-aggiornamento viene eseguito come parte del processo di aggiornamento. Il controllo dello stato di salute pre-aggiornamento valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa procedere. Le seguenti condizioni potrebbero impedire l'aggiornamento:

- Unità assegnate non riuscite
- Hot spare in uso
- Gruppi di volumi incompleti
- Operazioni esclusive in corso
- Volumi mancanti
- Controllore in stato non ottimale
- Numero eccessivo di eventi del registro eventi
- Errore di convalida del database di configurazione
- Dischi con vecchie versioni di DACstore

È anche possibile eseguire il controllo di integrità pre-aggiornamento separatamente senza eseguire un aggiornamento.

Panoramica sull'aggiornamento del disco

Il firmware del disco controlla le caratteristiche operative di basso livello di un disco. Periodicamente, i produttori di unità rilasciano aggiornamenti del firmware per aggiungere nuove funzionalità, migliorare le prestazioni e correggere i difetti.

Aggiornamenti del firmware dell'unità online e offline

Esistono due tipi di aggiornamento del firmware del disco: online e offline.

Online

Durante un aggiornamento online, le unità vengono aggiornate in sequenza, una alla volta. L'array di storage

continua a elaborare I/O durante l'aggiornamento. Non è necessario interrompere I/O. Se un'unità può eseguire un aggiornamento online, il metodo online viene utilizzato automaticamente.

Le unità che possono eseguire un aggiornamento online includono le seguenti:

- Dischi in un pool ottimale
- Unità disco in un gruppo di volumi ridondante ottimale (RAID 1, RAID 5 e RAID 6)
- Unità non assegnate
- Unità hot spare di standby

L'aggiornamento online del firmware del disco può richiedere diverse ore, esponendo l'array di storage a potenziali guasti del volume. Il guasto del volume potrebbe verificarsi in questi casi:

- In un gruppo di volumi RAID 1 o RAID 5, un'unità si guasta mentre un'altra unità del gruppo di volumi viene aggiornata.
- In un pool RAID 6 o gruppo di volumi, due unità si guastano mentre un'altra unità nel pool o gruppo di volumi viene aggiornata.

Offline (parallelo)

Durante un aggiornamento offline, tutte le unità dello stesso tipo vengono aggiornate contemporaneamente. Questo metodo richiede l'interruzione dell'attività di I/O sui volumi associati alle unità selezionate. Poiché è possibile aggiornare più unità contemporaneamente (in parallelo), il tempo di inattività complessivo si riduce significativamente. Se un'unità può eseguire solo un aggiornamento offline, il metodo offline viene utilizzato automaticamente.

Le seguenti unità DEVONO utilizzare il metodo offline:

- Unità in un gruppo di volumi non ridondante (RAID 0)
- Unità in un pool o gruppo di volumi non ottimale
- Unità nella cache SSD

Compatibilità

Ogni file del firmware dell'unità contiene informazioni sul tipo di unità su cui il firmware viene eseguito. È possibile scaricare il file del firmware specificato solo su un'unità compatibile. System Manager verifica automaticamente la compatibilità durante il processo di aggiornamento.

Aggiornare il software e il firmware in SANtricity System Manager

È possibile aggiornare il software dell'array di storage e, facoltativamente, il firmware IOM e la memoria non volatile statica ad accesso casuale (NVSRAM) per assicurarsi di disporre di tutte le funzionalità e le correzioni di bug più recenti.

Prima di iniziare

- Sai già se vuoi aggiornare il firmware IOM.

  Normalmente, è consigliabile aggiornare tutti i componenti contemporaneamente. Tuttavia, si può decidere di non aggiornare il firmware IOM se non si desidera aggiornarlo come parte dell'aggiornamento del software SANtricity OS o se il supporto tecnico ha richiesto di effettuare il downgrade del firmware IOM (è possibile eseguire il downgrade del firmware solo utilizzando l'interfaccia a riga di comando).

- Sai se vuoi aggiornare il file NVSRAM del controller.

  Normalmente, dovresti aggiornare tutti i componenti contemporaneamente. Tuttavia, potresti decidere di non aggiornare il file NVSRAM del controller se il tuo file è stato patchato o è una versione personalizzata e non vuoi sovrascriverlo.

- Sai se desideri attivare l'aggiornamento del sistema operativo ora o più tardi.

  I motivi per attivare in un secondo momento potrebbero includere:

  - **Orario della giornata** — L'attivazione del software e del firmware può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. I controller effettuano un failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — Potresti voler testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri storage array.
- Sai se vuoi passare da unità non protette o da unità protette internamente all'utilizzo di un server di gestione delle chiavi esterno (KMS) per la sicurezza delle unità.
- Sai se desideri utilizzare il controllo degli accessi in base al ruolo nel tuo array di storage.

Informazioni su questa attività

È possibile scegliere di aggiornare solo il file del software del sistema operativo, solo il file Controller NVSRAM oppure entrambi i file.

Eseguire questa operazione solo quando richiesto dal supporto tecnico.

> **Rischio di perdita di dati o rischio di danneggiamento dell'array di storage** — Non apportare modifiche all'array di storage durante l'aggiornamento. Mantenere l'alimentazione dell'array di storage.

Passaggi

1. Se l'array di storage contiene un solo controller o non hai installato un driver multipath, interrompi l'attività di I/O verso l'array di storage per evitare errori dell'applicazione. Se l'array di storage ha due controller e hai installato un driver multipath, non è necessario interrompere l'attività di I/O.
2. Selezionare **Support › Upgrade Center**.
3. Scarica il nuovo file dal sito Support sul tuo client di gestione.

   a. Fai clic su **NetApp Support** per avviare il sito Web di supporto.
   b. Sul sito web di supporto, fai clic sulla scheda **Downloads** e quindi seleziona **Downloads**.
   c. Selezionare **E-Series SANtricity OS Controller Software**.
   d. Segui le istruzioni rimanenti.

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

4. Se NON si desidera aggiornare il firmware IOM in questo momento, fare clic su **Sospendi sincronizzazione automatica dell'IOM**.

   Se si dispone di un array di storage con un singolo controller, il firmware IOM non viene aggiornato.

5. In Aggiornamento software SANtricity OS, fare clic su **Avvia aggiornamento**.

   Viene visualizzata la finestra di dialogo Aggiorna il software SANtricity OS.

6. Seleziona uno o più file per iniziare il processo di aggiornamento:
   a. Seleziona il file del software SANtricity OS facendo clic su **Sfoglia** e navigando fino al file del software che hai scaricato dal sito web di Support.
   b. Seleziona il file NVSRAM del controller facendo clic su **Sfoglia** e navigando fino al file NVSRAM che hai 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 dello storage array.
      - Quando si seleziona un file per l'aggiornamento, vengono visualizzati il nome e le dimensioni del file.
7. **Facoltativo:** Se hai selezionato un file SANtricity OS Software da aggiornare, puoi trasferire i file al controller senza attivarli selezionando la check box **Trasferisci ora i file, ma non aggiornare (attiva l'aggiornamento in seguito)**.
8. Fai clic su **Start** e conferma di voler eseguire l'operazione.

   È possibile annullare l'operazione durante il controllo di integrità pre-aggiornamento, ma non durante il trasferimento o l'attivazione.

9. **Facoltativo:** Per vedere un elenco di ciò che è stato aggiornato, fare clic su **Salva registro**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome `drive_upgrade_log-timestamp.txt`.

Dopo aver finito

- Verifica che tutti i componenti siano visualizzati nella pagina Hardware.
- Verifica le nuove versioni del software e del firmware controllando la finestra di dialogo Inventario software e firmware (vai al **Supporto › Upgrade Center**, e quindi fai clic sul collegamento **Inventario software e firmware**).
- Se hai aggiornato la NVSRAM del controller, tutte le impostazioni personalizzate applicate alla NVSRAM esistente vengono perse durante il processo di attivazione. Devi applicare nuovamente le impostazioni personalizzate alla NVSRAM dopo che il processo di attivazione è stato completato.

Attivare il software del controller e il firmware in SANtricity System Manager

È possibile scegliere di attivare immediatamente i file di upgrade oppure attendere un momento più opportuno.

Informazioni su questa attività

È possibile scaricare e trasferire i file senza attivarli. Potresti scegliere di attivare in seguito per questi motivi:

- **Orario della giornata** — L'attivazione del software e del firmware può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. I controller effettuano un failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento

dell'aggiornamento.

- **Tipo di pacchetto** — Potresti voler testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri storage array.

Quando si dispone di software o firmware trasferiti ma non attivati, viene visualizzata una notifica nell'area Notifiche della pagina iniziale di System Manager e anche nella pagina del Centro aggiornamenti.

Non è possibile interrompere il processo di attivazione dopo che è iniziato.

Passaggi

1. Selezionare **Support › Upgrade Center**.
2. Nell'area denominata SANtricity OS Controller Software upgrade, fare clic su **Attiva** e confermare di voler eseguire l'operazione.

   È possibile annullare l'operazione durante il controllo di integrità pre-aggiornamento, ma non durante l'attivazione.

   Viene avviato il controllo di integrità preliminare all'aggiornamento. Se il controllo di integrità preliminare all'aggiornamento ha esito positivo, il processo di aggiornamento procede con l'attivazione dei file. Se il controllo di integrità preliminare all'aggiornamento non ha esito positivo, utilizzare Recovery Guru o contattare il supporto tecnico per risolvere il problema. Per alcuni tipi di condizioni, il supporto tecnico potrebbe consigliare di continuare con l'aggiornamento nonostante gli errori selezionando la casella di controllo **Allow Upgrade**.

   Una volta completato con successo il controllo di integrità preliminare all'aggiornamento, si procede all'attivazione. Il tempo necessario per l'attivazione dipende dalla configurazione dell'array di storage e dai componenti che si stanno attivando.

3. **Facoltativo:** Per vedere un elenco di ciò che è stato aggiornato, fare clic su **Salva registro**.

   Il file viene salvato nella cartella Downloads del tuo browser con il nome `drive_upgrade_log-timestamp.txt`.

Dopo aver finito

- Verifica che tutti i componenti siano visualizzati nella pagina Hardware.
- Verifica le nuove versioni del software e del firmware controllando la finestra di dialogo Inventario software e firmware (vai al **Supporto › Upgrade Center**, e quindi fai clic sul collegamento **Inventario software e firmware**).
- Se hai aggiornato la NVSRAM del controller, tutte le impostazioni personalizzate applicate alla NVSRAM esistente vengono perse durante il processo di attivazione. Devi applicare nuovamente le impostazioni personalizzate alla NVSRAM dopo che il processo di attivazione è stato completato.

Aggiorna il firmware del disco in SANtricity System Manager

È possibile aggiornare il firmware dei dischi per assicurarsi di disporre di tutte le funzionalità più recenti e delle correzioni di bug.

Prima di iniziare

- Hai eseguito il backup dei tuoi dati utilizzando un backup da disco a disco, una copia del volume (su un gruppo di volumi non interessato dall'aggiornamento del firmware pianificato) o un mirror remoto.

- L’array di archiviazione ha uno stato ottimale.
- Tutti i dischi hanno uno stato Optimal.
- Non sono in corso modifiche di configurazione sull’array di storage.
- Se le unità sono in grado di eseguire solo un aggiornamento offline, l’attività di I/O su tutti i volumi associati alle unità viene interrotta.

Passaggi

1. Selezionare **Support › Upgrade Center**.
2. Scarica i nuovi file dal sito di Support sul tuo client di gestione.
3. In Aggiornamento del firmware del disco, fare clic su **Begin Upgrade**.

   Viene visualizzata una finestra di dialogo che elenca i file del firmware dell’unità attualmente in uso.

4. Estrai (decomprimi) i file che hai scaricato dal sito Support.
5. Fai clic su **Sfoglia** e seleziona i nuovi file del firmware dell’unità che hai scaricato dal sito di Support.

   I file del firmware dell’unità hanno un nome file simile a `D_HUC101212CSS600_30602291_MS01_2800_0002` con l’estensione di `.dlp`.

   È possibile selezionare fino a quattro file di firmware del disco, uno alla volta. Se più di un file di firmware del disco è compatibile con la stessa unità, viene visualizzato un errore di conflitto di file. Decidere quale file di firmware del disco utilizzare per l’aggiornamento e rimuovere l’altro.

6. Fai clic su **Avanti**.

   Viene visualizzata la finestra di dialogo **Select Drives**, 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 Informazioni sul firmware proposto. Se è necessario modificare il firmware, fare clic su **Back** per tornare alla finestra di dialogo precedente.

7. Seleziona il tipo di aggiornamento che desideri eseguire:
   - **Online (predefinito)** — Mostra le unità che possono supportare un download del firmware *mentre l’array di storage sta elaborando I/O*. Non è necessario interrompere l’I/O sui volumi associati che utilizzano queste unità quando si seleziona questo metodo di aggiornamento. Queste unità vengono aggiornate una alla volta mentre l’array di storage sta elaborando I/O su tali unità.
   - **Offline (parallelo)** — Mostra le unità che possono supportare un download del firmware *solo mentre tutte le attività di I/O sono interrotte* su qualsiasi volume che utilizza tali unità. È necessario interrompere tutte le attività di I/O su qualsiasi volume che utilizza le unità che si stanno aggiornando quando si seleziona questo metodo di aggiornamento. Le unità che non dispongono di ridondanza devono essere elaborate come un’operazione offline. Questo requisito include qualsiasi unità associata a cache SSD, a un gruppo di volumi RAID 0 o a qualsiasi pool o gruppo di volumi degradato. L’aggiornamento offline (parallelo) è in genere più veloce del metodo online (predefinito).
8. Nella prima colonna della tabella, seleziona il disco o i dischi che desideri aggiornare.
9. Fai clic su **Start** e conferma di voler eseguire l’operazione.

   Se devi interrompere l’aggiornamento, fai clic su **Interrompi**. Tutti i download del firmware attualmente in corso vengono completati. Tutti i download del firmware non ancora avviati vengono annullati.

L’interruzione dell’aggiornamento del firmware del disco potrebbe comportare la perdita di dati o rendere le unità non disponibili.

10. **Facoltativo:** Per vedere un elenco di ciò che è stato aggiornato, fare clic su **Salva registro**.

    Il file viene salvato nella cartella Downloads del tuo browser con il nome `drive_upgrade_log-timestamp.txt`.

11. Se si verifica uno dei seguenti errori durante la procedura di aggiornamento, adottare la relativa azione consigliata.

Errori e azioni consigliate

Se riscontri questo errore durante il download del firmware…	Quindi procedi come segue…
Unità assegnate non riuscite	Una delle cause del problema potrebbe essere che l'unità non ha la firma appropriata. Assicurati che l'unità interessata sia un'unità autorizzata. Contatta il supporto tecnico per ulteriori informazioni. Quando si sostituisce un drive, assicurarsi che il drive sostitutivo abbia una capacità pari o superiore a quella del drive guasto che si sta sostituendo. È possibile sostituire l'unità guasta mentre l'array di storage riceve I/O.
Verifica l'array di archiviazione	• Assicurarsi che a ciascun controller sia stato assegnato un indirizzo IP. • Assicurarsi che tutti i cavi collegati al controller non siano danneggiati. • Assicurati che tutti i cavi siano collegati saldamente.
Unità hot spare integrate	Questa condizione di errore deve essere corretta prima di poter aggiornare il firmware. Avvia System Manager e utilizza il Recovery Guru per risolvere il problema.
Gruppi di volumi incompleti	Se uno o più gruppi di volumi o pool di dischi risultano incompleti, è necessario correggere questo errore prima di poter aggiornare il firmware. Avviare System Manager e utilizzare il Recovery Guru per risolvere il problema.
Operazioni esclusive (diverse dalla scansione di supporto/parità in background) attualmente in esecuzione su qualsiasi gruppo di volumi	Se sono in corso una o più operazioni esclusive, le operazioni devono essere completate prima che il firmware possa essere aggiornato. Utilizzare System Manager per monitorare l'avanzamento delle operazioni.
Volumi mancanti	È necessario correggere il problema del volume mancante prima che il firmware possa essere aggiornato. Avviare System Manager e utilizzare il Recovery Guru per risolvere il problema.
Uno dei due controller si trova in uno stato diverso da Ottimale	Uno dei controller dell'array di storage necessita di attenzione. Questo problema deve essere risolto prima che il firmware possa essere aggiornato. Avvia System Manager e utilizza Recovery Guru per risolvere il problema.
Informazioni sulle partizioni di archiviazione non corrispondenti tra i grafici degli oggetti del controller	Si è verificato un errore durante la convalida dei dati sui controller. Contattare il supporto tecnico per risolvere questo problema.

Se riscontri questo errore durante il download del firmware…	Quindi procedi come segue…
SPM Verify Database Controller check non riesce	Si è verificato un errore nel database di mappatura delle partizioni di archiviazione su un controller. Contattare il supporto tecnico per risolvere questo problema.
Convalida del database di configurazione \(se supportata dalla versione del controller dell'array di storage\)	Si è verificato un errore nel database di configurazione di un controller. Contattare il supporto tecnico per risolvere il problema.
Verifiche relative al MEL	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 10 eventi DDE Informational o Critical MEL.	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici di livello 2C	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici di canale di unità degradato	Contatta il supporto tecnico per risolvere questo problema.
Più di 4 voci critiche MEL negli ultimi 7 giorni	Contatta il supporto tecnico per risolvere questo problema.

Dopo aver finito

L'aggiornamento del firmware del disco è stato completato. È possibile riprendere le normali operazioni.

Scopri gli errori di aggiornamento del software e del firmware di SANtricity

Possono verificarsi errori durante l'aggiornamento del software del controller o durante l'aggiornamento del firmware del disco.

Errore download firmware	Descrizione	Azione consigliata
Unità assegnate non riuscite	Impossibile aggiornare un drive assegnato nello storage array.	Una delle cause del problema potrebbe essere che l'unità non ha la firma appropriata. Assicurati che l'unità interessata sia un'unità autorizzata. Contatta il supporto tecnico per ulteriori informazioni. Quando si sostituisce un drive, assicurarsi che il drive sostitutivo abbia una capacità pari o superiore a quella del drive guasto che si sta sostituendo. È possibile sostituire l'unità guasta mentre l'array di storage riceve I/O.
Unità hot spare integrate	Se l'unità è contrassegnata come hot spare ed è in uso per un gruppo di volumi, il processo di aggiornamento del firmware non riesce.	Questa condizione di errore deve essere corretta prima di poter aggiornare il firmware. Avvia System Manager e utilizza il Recovery Guru per risolvere il problema.
Gruppi di volumi incompleti	Se un'unità che fa parte di un gruppo di volumi viene bypassata, rimossa o non risponde, viene considerata un gruppo di volumi incompleto. Un gruppo di volumi incompleto impedisce l'aggiornamento del firmware.	Se uno o più gruppi di volumi o pool di dischi risultano incompleti, è necessario correggere questo errore prima di poter aggiornare il firmware. Avviare System Manager e utilizzare il Recovery Guru per risolvere il problema.
Operazioni esclusive (diverse dalla scansione di supporto/parità in background) attualmente in esecuzione su qualsiasi gruppo di volumi	Impossibile aggiornare il firmware se sono in corso operazioni esclusive su un volume.	Se sono in corso una o più operazioni esclusive, le operazioni devono essere completate prima che il firmware possa essere aggiornato. Utilizzare System Manager per monitorare l'avanzamento delle operazioni.
Volumi mancanti	Impossibile aggiornare il firmware se manca un volume.	È necessario correggere il problema del volume mancante prima che il firmware possa essere aggiornato. Avviare System Manager e utilizzare il Recovery Guru per risolvere il problema.
Uno dei due controller si trova in uno stato diverso da Ottimale	Impossibile aggiornare il firmware se uno dei controller si trova in uno stato diverso da ottimale.	Uno dei controller dell'array di storage necessita di attenzione. Questo problema deve essere risolto prima che il firmware possa essere aggiornato. Avvia System Manager e utilizza Recovery Guru per risolvere il problema.

Errore download firmware	Descrizione	Azione consigliata
SPM Verify Database Controller check non riesce	Impossibile aggiornare il firmware perché il database delle mappature delle partizioni di storage è danneggiato.	Si è verificato un errore nel database di mappatura delle partizioni di archiviazione su un controller. Contattare il supporto tecnico per risolvere questo problema.
Convalida del database di configurazione (se supportato dalla versione del controller dell'array di storage)	Impossibile aggiornare il firmware perché il database di configurazione è danneggiato.	Si è verificato un errore nel database di configurazione di un controller. Contattare il supporto tecnico per risolvere il problema.
Verifiche relative al MEL	Impossibile aggiornare il firmware perché il registro eventi contiene errori.	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 10 eventi DDE Informational o Critical MEL.	Impossibile aggiornare il firmware perché sono stati segnalati più di 10 eventi MEL informativi o critici di DDE negli ultimi sette giorni.	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici di livello 2C	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono stati segnalati più di due eventi critici MEL di pagina 2C.	Contatta il supporto tecnico per risolvere questo problema.
Negli ultimi 7 giorni sono stati segnalati più di 2 eventi MEL critici di canale di unità degradato	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono stati segnalati più di due eventi MEL critici relativi al canale del disco degradato.	Contatta il supporto tecnico per risolvere questo problema.
Più di 4 voci critiche MEL negli ultimi 7 giorni	Impossibile aggiornare il firmware perché negli ultimi sette giorni sono state segnalate più di quattro voci critiche nel registro degli eventi.	Contatta il supporto tecnico per risolvere questo problema.
È necessario un indirizzo IP di gestione valido.	Per eseguire questa operazione è necessario un indirizzo IP del controller valido.	Contatta il supporto tecnico per risolvere questo problema.
Il comando richiede che venga fornito un indirizzo IP di gestione attivo per ciascun controller.	Per questa operazione è necessario un indirizzo IP del controller per ciascun controller associato all'array di storage.	Contatta il supporto tecnico per risolvere questo problema.
È stato restituito un tipo di file di download non gestito.	Il file di download specificato non è supportato.	Contatta il supporto tecnico per risolvere questo problema.

Errore download firmware	Descrizione	Azione consigliata
Si è verificato un errore durante la procedura di download e caricamento del firmware.	Il download del firmware non è riuscito perché il controller non è in grado di elaborare la richiesta. Verificare che l'array di storage sia ottimale e riprovare l'operazione.	Se questo errore si ripresenta dopo aver verificato che l'array di storage sia ottimale, contattare il supporto tecnico per risolvere questo problema.
Si è verificato un errore durante la procedura di attivazione del firmware.	L'attivazione del firmware non è riuscita perché il controller non è in grado di elaborare la richiesta. Verificare che l'array di storage sia ottimale e riprovare l'operazione.	Se questo errore si ripresenta dopo aver verificato che l'array di storage sia ottimale, contattare il supporto tecnico per risolvere questo problema.
Timeout raggiunto durante l'attesa che il controller {0} si riavvii.	Il software di gestione non riesce a riconnettersi al controller {0} dopo un riavvio. Verificare che esista un percorso di connessione funzionante all'array di storage e riprovare l'operazione se non è stata completata correttamente.	Se questo errore si ripresenta dopo aver verificato che l'array di storage sia ottimale, contattare il supporto tecnico per risolvere questo problema.

È possibile correggere alcune di queste condizioni utilizzando Recovery Guru in System Manager. Tuttavia, per alcune di queste condizioni potrebbe essere necessario contattare il supporto tecnico. Le informazioni sul download del firmware del controller più recente sono disponibili dall'array di storage. Queste informazioni aiutano il supporto tecnico a comprendere le condizioni di errore che hanno impedito l'aggiornamento e il download del firmware.

AutoSupport FAQ per SANtricity System Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Quali dati sto raccogliendo?

La funzionalità AutoSupport e la funzionalità manuale di raccolta dati di supporto forniscono modi per raccogliere dati in un pacchetto di supporto clienti per la risoluzione remota dei problemi e l'analisi dei problemi da parte del supporto tecnico.

Il pacchetto di assistenza clienti raccoglie tutti i tipi di informazioni relative all'array di storage in un unico file compresso. Le informazioni raccolte includono la configurazione fisica, la configurazione logica, le informazioni sulla versione, gli eventi, i file di log e i dati sulle prestazioni. Le informazioni vengono utilizzate solo dal supporto tecnico per risolvere i problemi relativi all'array di storage.

Cosa mostrano i dati dei settori illeggibili?

È possibile visualizzare dati dettagliati sui settori illeggibili rilevati sulle unità nel proprio storage array.

Il registro dei settori illeggibili mostra per primo il settore illeggibile più recente. Il registro contiene le seguenti informazioni sui volumi che contengono i settori illeggibili. I campi sono ordinabili.

Campo	Descrizione
Volume interessato	Mostra l'etichetta del volume. Se un volume mancante contiene settori illeggibili, viene visualizzato il World Wide Identifier per il volume mancante.
Logical Unit Number (LUN)	Mostra il LUN del volume. Se il volume non ha un LUN, la finestra di dialogo mostra NA.
Assegnato a	Mostra gli host o i cluster di host che hanno accesso al volume. Se il volume non è accessibile da un host, cluster di host o anche da un Default Cluster, la finestra di dialogo mostra NA.

Per visualizzare ulteriori informazioni sui settori illeggibili, fare clic sul segno più (+) accanto a un volume.

Campo	Descrizione
Data/Ora	Mostra la data e l'ora in cui è stato rilevato il settore illeggibile.
Indirizzo del blocco logico del volume	Mostra l'indirizzo del blocco logico (LBA) del volume.
Posizione dell'unità	Mostra il drive shelf, il drawer (se il drive shelf è dotato di drawer) e la posizione del bay.
Indirizzo del blocco logico dell'unità	Mostra l'LBA dell'unità.
Tipo di guasto	Mostra uno dei seguenti tipi di errore: • **Fisico** — Un errore del supporto fisico. • **Logico** — Un errore di lettura in un altro punto della striscia che causa dati illeggibili. Ad esempio, un settore illeggibile a causa di errori del supporto in un altro punto del volume. • **Incoerente** — dati di ridondanza incoerenti. • **Data Assurance** — Errore di Data Assurance.

Che cos'è una health image?

Un health image è un dump di dati raw della memoria del processore del controller che il supporto tecnico può utilizzare per diagnosticare un problema con un controller.

Il firmware genera automaticamente un'immagine di stato quando rileva determinati errori. In alcune situazioni di risoluzione dei problemi, il supporto tecnico potrebbe richiedere di recuperare il file dell'immagine di stato e di inviarlo.

A cosa servono le funzionalità di AutoSupport?

La funzionalità AutoSupport è composta da tre funzionalità individuali che si abilitano separatamente.

- **Base AutoSupport** — Consente al tuo array di storage di raccogliere e inviare automaticamente i dati al supporto tecnico.
- **AutoSupport OnDemand** — Consente al supporto tecnico di richiedere la ritrasmissione di una precedente spedizione AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
- **Diagnostica remota** — Consente al supporto tecnico di richiedere una nuova, aggiornata AutoSupport dispatch quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se ci sono nuove richieste in sospeso e risponde di conseguenza.

Che tipo di dati vengono raccolti tramite la funzionalità AutoSupport?

La funzionalità AutoSupport contiene tre tipologie standard di invio: invii per eventi, invii programmati e invii di diagnostica su richiesta e da remoto.

I dati AutoSupport non contengono alcun dato utente.

- **Invio degli eventi**

  Quando si verificano eventi sul sistema che richiedono una notifica proattiva al supporto tecnico, la funzionalità AutoSupport invia automaticamente una segnalazione attivata dall'evento.

  - Inviato quando si verifica un evento di supporto sull'array di storage gestito.
  - Include un'istantanea completa di ciò che stava accadendo con l'array di storage al momento in cui si è verificato l'evento.
- **Spedizioni programmate**

  La funzione AutoSupport invia automaticamente diversi messaggi a intervalli regolari.

  - **Rapporti giornalieri** — Inviati una volta al giorno durante un intervallo di tempo configurabile dall'utente. Includono i registri eventi di sistema e i dati sulle prestazioni correnti.
  - **Comunicazioni settimanali** — Inviate una volta a settimana durante un intervallo di tempo e un giorno configurabili dall'utente. Include informazioni sulla configurazione e sullo stato del sistema.
- **AutoSupport OnDemand e interventi di diagnostica a distanza**
  - **AutoSupport OnDemand** — Consente al supporto tecnico di richiedere la ritrasmissione di una precedente spedizione AutoSupport quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se sono presenti richieste di ritrasmissione in sospeso e risponde di conseguenza.
  - **Diagnostica remota** — Consente al supporto tecnico di richiedere una nuova, aggiornata AutoSupport dispatch quando necessario per la risoluzione di un problema. Tutte le trasmissioni vengono avviate dall'array di storage, non dal server AutoSupport. L'array di storage si connette periodicamente al server AutoSupport per determinare se ci sono nuove richieste in sospeso e risponde di conseguenza.

Come configuro il metodo di consegna per la funzionalità AutoSupport?

La funzionalità AutoSupport supporta i protocolli HTTPS e SMTP per la consegna delle comunicazioni AutoSupport al supporto tecnico.

Prima di iniziare

- La funzione AutoSupport deve essere abilitata. Puoi verificare se è abilitata nella pagina AutoSupport.
- È necessario installare e configurare un DNS server nella rete. L'indirizzo del DNS server deve essere configurato in System Manager (questa operazione è disponibile nella pagina Hardware).

Informazioni su questa attività

Esamina i diversi protocolli:

- **HTTPS** — Consente di connettersi direttamente al server di supporto tecnico di destinazione utilizzando HTTPS. Se si desidera abilitare AutoSupport OnDemand o la diagnostica remota, il metodo di consegna AutoSupport deve essere impostato su HTTPS.
- **Email** — Consente di utilizzare un server di posta elettronica come metodo di consegna per l'invio di AutoSupport dispatches.

> **Differenze tra i metodi HTTPS ed Email**. Il metodo di consegna Email, che utilizza SMTP, presenta alcune importanti differenze rispetto al metodo di consegna HTTPS. In primo luogo, la dimensione degli invii per il metodo Email è limitata a 5MB, il che significa che alcune raccolte di dati ASUP non verranno inviate. In secondo luogo, la funzionalità AutoSupport OnDemand è disponibile solo con il metodo di consegna HTTPS.

Passaggi

1. Selezionare **Supporto › Support Center › AutoSupport** scheda.
2. Seleziona **Configura AutoSupport Delivery Method**.

   Viene visualizzata una finestra di dialogo che elenca i metodi di consegna della spedizione.

3. Seleziona il metodo di consegna desiderato, quindi seleziona i parametri per tale metodo. Esegui una delle seguenti operazioni:
   - Se hai selezionato HTTPS, seleziona uno dei seguenti parametri di consegna:
     - **Direttamente** — Questo parametro di consegna è la selezione predefinita. Scegliendo questa opzione è possibile connettersi direttamente al sistema di supporto tecnico di destinazione utilizzando il protocollo HTTPS.
     - **Tramite proxy server** — Scegliendo questa opzione è possibile specificare i dettagli del proxy server HTTP necessari per stabilire la connessione con il sistema di supporto tecnico di destinazione. È necessario specificare l'indirizzo host e il numero di porta. Tuttavia, è necessario inserire i dettagli di autenticazione dell'host (nome utente e password) solo se richiesto.
     - **Tramite script di autoconfigurazione proxy (PAC)** — Specificare il percorso di un file di script di autoconfigurazione proxy (PAC). Un file PAC consente al sistema di scegliere automaticamente il proxy server appropriato per stabilire una connessione con il sistema di supporto tecnico di destinazione.
   - Se hai selezionato Email, inserisci le seguenti informazioni:
     - L'indirizzo del server di posta come fully qualified domain name, indirizzo IPv4 o indirizzo IPv6.
     - L'indirizzo email che compare nel campo Da dell'email di invio AutoSupport.
     - **Facoltativo; se si desidera eseguire un test di configurazione.** L'indirizzo e-mail a cui viene inviata una conferma quando il AutoSupport system riceve la richiesta di test.
     - Se si desidera crittografare i messaggi, selezionare **SMTPS** o **STARTTLS** come tipo di crittografia, quindi selezionare il numero di porta per i messaggi crittografati. In caso contrario, selezionare **None**.

        - Se necessario, inserire un nome utente e una password per l'autenticazione con il mittente in uscita e il server di posta.

4. Fai clic su **Verifica configurazione** per testare la connessione al server di supporto tecnico utilizzando i parametri di consegna specificati. Se hai abilitato la funzione AutoSupport On-Demand, il sistema testerà anche la connessione per la consegna di AutoSupport OnDemand.

   Se il test di configurazione non riesce, verifica le impostazioni di configurazione ed esegui nuovamente il test. Se il test continua a non riuscire, contatta il supporto tecnico.

5. Fare clic su **Save**.

Che cosa sono i dati di configurazione?

Quando si seleziona Collect Configuration Data, il sistema salva lo stato corrente del database di configurazione RAID.

Il database di configurazione RAID include tutti i dati relativi ai gruppi di volumi e ai pool di dischi sul controller. La funzione Raccogli dati di configurazione salva le stesse informazioni del comando CLI per `save storageArray dbmDatabase`.

Cosa devo sapere prima di aggiornare il software SANtricity OS?

Prima di aggiornare il software e il firmware del controller, tieni presente questi elementi.

- Hai letto il documento e il `readme.txt` file e hai deciso di procedere con l'aggiornamento.
- Sai già se vuoi aggiornare il firmware IOM.

  Normalmente, dovresti aggiornare tutti i componenti contemporaneamente. Tuttavia, potresti decidere di non aggiornare il firmware IOM se non vuoi aggiornarlo come parte dell'aggiornamento del software del controller SANtricity OS o se il supporto tecnico ti ha istruito a eseguire il downgrade del firmware IOM (puoi eseguire il downgrade del firmware solo utilizzando l'interfaccia a riga di comando).

- Sai se vuoi aggiornare il file NVSRAM del controller.

  Normalmente, dovresti aggiornare tutti i componenti contemporaneamente. Tuttavia, potresti decidere di non aggiornare il file NVSRAM del controller se il tuo file è stato patchato o è una versione personalizzata e non vuoi sovrascriverlo.

- Sai se vuoi attivare ora o più tardi.

  I motivi per attivare in un secondo momento potrebbero includere:

  - **Orario della giornata** — L'attivazione del software e del firmware può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. I controller effettuano un failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — Potresti voler testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri storage array.

Questi componenti fanno parte dell'aggiornamento del software del controller SANtricity OS:

- **Software di gestione** — System Manager è il software che gestisce l'array di storage.
- **Controller firmware** — Il firmware del controller gestisce l'I/O tra host e volumi.

- **Controller NVSRAM** — Controller NVSRAM è un file che specifica le impostazioni predefinite per i controller.
- **IOM firmware** — Il firmware del modulo I/O (IOM) gestisce la connessione tra un controller e uno shelf di dischi. Monitora inoltre lo stato dei componenti.
- **Software di supervisione** — Il software di supervisione è la macchina virtuale su un controller in cui viene eseguito il software.

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover e/o il driver HBA dell'host, affinché quest'ultimo possa interagire correttamente con i controller.

Per determinare se questo è il caso, vedere il "Tool NetApp Interoperability Matrix".

Se l'array di storage contiene un solo controller o non hai installato un driver multipath, interrompi l'attività di I/O verso l'array di storage per evitare errori dell'applicazione. Se l'array di storage ha due controller e hai installato un driver multipath, non è necessario interrompere l'attività di I/O.

Non apportare modifiche all'array di archiviazione durante l'aggiornamento.

Cosa devo sapere prima di sospendere la sincronizzazione automatica dell'IOM?

La sospensione della sincronizzazione automatica dell'IOM impedisce l'aggiornamento del firmware dell'IOM al successivo aggiornamento del software del controller SANtricity OS.

Normalmente, il software del controller e il firmware IOM vengono aggiornati come un pacchetto. È possibile sospendere la sincronizzazione automatica dell'IOM se si dispone di una build speciale del firmware IOM che si desidera conservare sull'enclosure. Altrimenti, verrà ripristinato il firmware IOM incluso nel software del controller la prossima volta che si esegue un aggiornamento del software del controller.

Perché l'aggiornamento del firmware procede così lentamente?

L'avanzamento dell'aggiornamento del firmware dipende dal carico complessivo del sistema.

Durante un aggiornamento online del firmware del disco, se si verifica un trasferimento di volume durante il processo di ricostruzione rapida, il sistema avvia una ricostruzione completa sul volume che è stato trasferito. Questa operazione potrebbe richiedere un tempo considerevole. Il tempo effettivo di ricostruzione completa dipende da diversi fattori, tra cui la quantità di attività di I/O che si verifica durante l'operazione di ricostruzione, il numero di dischi nel gruppo di volumi, l'impostazione della priorità di ricostruzione e le prestazioni del disco.

Cosa devo sapere prima di aggiornare il firmware del disco?

Prima di aggiornare il firmware del disco, tieni presente questi elementi.

- A titolo precauzionale, esegui il backup dei dati utilizzando un backup da disco a disco, una copia del volume (su un gruppo di volumi non interessato dall'aggiornamento del firmware pianificato) o un mirror remoto.
- Potresti voler aggiornare solo alcune unità per testare il comportamento del nuovo firmware per assicurarti che funzioni correttamente. Se il nuovo firmware funziona correttamente, aggiorna le unità rimanenti.
- Se hai delle unità disco guaste, riparale prima di iniziare l'aggiornamento del firmware.
- Se le unità possono eseguire un aggiornamento offline, interrompere l'attività di I/O su tutti i volumi associati alle unità. Quando l'attività di I/O è interrotta, non è possibile eseguire operazioni di

configurazione associate a tali volumi.

- Non rimuovere alcuna unità durante l'aggiornamento del firmware del disco.
- Non apportare alcuna modifica alla configurazione dell'array di storage durante l'aggiornamento del firmware del disco.

Come faccio a scegliere quale tipo di aggiornamento eseguire?

Si sceglie il tipo di aggiornamento da eseguire sul disco a seconda dello stato del pool o del gruppo di volumi.

- **Online**

  Se il pool o il gruppo di volumi supporta la ridondanza ed è Ottimale, puoi utilizzare il metodo Online per aggiornare il firmware del disco. Il metodo Online scarica il firmware *mentre l'array di storage sta elaborando I/O* sui volumi associati che utilizzano questi dischi. Non è necessario interrompere l'I/O sui volumi associati che utilizzano questi dischi. Questi dischi vengono aggiornati uno alla volta sui volumi associati ai dischi. Se il disco non è assegnato a un pool o a un gruppo di volumi, il suo firmware può essere aggiornato tramite il metodo Online o Offline. Le prestazioni del sistema potrebbero essere influenzate quando utilizzi il metodo Online per aggiornare il firmware del disco.

- **Offline**

  Se il pool o il gruppo di volumi non supporta la ridondanza (RAID 0), o è degradato, è necessario utilizzare il metodo Offline per l'aggiornamento del firmware del disco. Il metodo Offline aggiornerà il firmware sui volumi associati che utilizzano questi dischi. È necessario interrompere tutta l'attività di I/O su qualsiasi volume associato che utilizza questi dischi. Se il disco non è assegnato a un pool o a un gruppo di volumi, il suo firmware può essere aggiornato tramite il metodo Online o Offline.

Gestione di array multipli con SANtricity Unified Manager 7

Interfaccia principale

Scopri SANtricity Unified Manager

SANtricity Unified Manager è un'interfaccia basata su web che consente di gestire più array di storage in un'unica visualizzazione.

Pagina principale

Quando accedi a Unified Manager, la pagina principale si apre su **Manage - All**. Da questa pagina, puoi scorrere un elenco di array di storage rilevati nella tua rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Barra laterale di navigazione

È possibile accedere alle funzionalità e alle funzioni di Unified Manager dalla barra laterale di navigazione.

Area	Descrizione
Gestire	Scopri gli array di storage nella tua rete, avvia SANtricity System Manager per un array, importa le impostazioni da un array a più array e gestisci i gruppi di array. Seleziona le caselle di controllo accanto ai nomi degli array per eseguire operazioni su di essi, come importare le impostazioni e creare gruppi di array. I puntini di sospensione alla fine di ogni riga forniscono un menu inline per le operazioni su un singolo array, come la ridenominazione.
Operazioni	Visualizza l'avanzamento delle operazioni batch, come l'importazione delle impostazioni da un array a un altro. Alcune operazioni non sono disponibili quando un array di storage ha uno stato non ottimale.
Gestione dei certificati	Gestisci i certificati per autenticare tra browser e client.
Gestione degli accessi	Stabilire l'autenticazione utente per l'interfaccia Unified Manager.
Supporto	Visualizza le opzioni di supporto tecnico, le risorse e i contatti.

Impostazioni dell'interfaccia e guida

In alto a destra dell'interfaccia, puoi accedere alla Guida e ad altra documentazione. Puoi anche accedere alle opzioni di amministrazione, disponibili dal menu a tendina accanto al tuo nome di accesso.

Accessi utente e password

L'utente attualmente connesso al sistema viene visualizzato in alto a destra dell'interfaccia.

Per ulteriori informazioni su utenti e password, consultare:

- "Imposta la protezione con password di amministratore"
- "Cambia la password dell'amministratore"
- "Modifica le password per i profili utente locali"

Browser supportati per SANtricity Unified Manager

SANtricity Unified Manager può essere accessibile da diversi tipi di browser.

Sono supportati i seguenti browser e versioni.

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

Il Web Services Proxy deve essere installato e disponibile per il browser.

Scopri la protezione della password di amministratore in SANtricity Unified Manager

È necessario configurare SANtricity Unified Manager con una password di amministratore per proteggerlo da accessi non autorizzati.

Password di amministratore e profili utente

Quando si avvia Unified Manager per la prima volta, viene richiesto di impostare una password di amministratore. Qualsiasi utente che dispone della password di amministratore può apportare modifiche alla configurazione degli storage arrays.

Oltre alla password di amministratore, l'interfaccia di Unified Manager include profili utente preconfigurati con uno o più ruoli associati. Per ulteriori informazioni, vedere "Come funziona la gestione degli accessi".

Non è possibile modificare gli utenti e le mappature. È possibile modificare solo le password. Per modificare le password, consultare:

- "Cambia la password dell'amministratore"
- "Modifica le password per i profili utente locali"

Timeout di sessione

Il software richiede la password una sola volta durante una singola sessione di gestione. Una sessione scade dopo 30 minuti di inattività per impostazione predefinita, momento in cui è necessario inserire nuovamente la password. Se un altro utente accede al software da un altro client di gestione e modifica la password mentre la tua sessione è in corso, ti verrà richiesta la password la prossima volta che tenterai un'operazione di configurazione o di visualizzazione.

Per motivi di sicurezza, è possibile tentare di inserire una password solo cinque volte prima che il software entri in stato di "lockout". In questo stato, il software rifiuta i successivi tentativi di inserimento della password. È necessario attendere 10 minuti affinché il sistema torni in stato "normale" prima di poter provare a inserire nuovamente la password.

È possibile regolare i timeout di sessione oppure disabilitare completamente i timeout di sessione. Per ulteriori informazioni, vedere "Gestisci i timeout di sessione".

Modifica la password di admin in SANtricity Unified Manager

È possibile modificare la password di amministratore utilizzata per accedere a SANtricity Unified Manager.

Prima di iniziare

- È necessario aver effettuato l'accesso come amministratore locale, il che include i permessi di Root admin.
- È necessario conoscere la password admin corrente.

Informazioni su questa attività

Tieni a mente queste linee guida quando scegli una password:

- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostate. Fai attenzione a includere gli spazi se erano inclusi nella password.
- Per una maggiore sicurezza, usa almeno 15 caratteri alfanumerici e cambia la password frequentemente.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.
3. Seleziona l'utente **admin** dalla tabella.

   Il pulsante Change Password diventa disponibile.

4. Seleziona **Change Password**.

   Si apre la finestra di dialogo Change Password.

5. Se non è stata impostata una lunghezza minima per le password degli utenti locali, selezionare la casella di controllo per richiedere all'utente di immettere una password per accedere al sistema.
6. Inserisci la nuova password nei due campi.
7. Inserisci la password dell'amministratore locale per confermare questa operazione, quindi fai clic su **Cambia**.

Gestire i timeout di sessione in SANtricity Unified Manager

È possibile configurare i timeout per SANtricity Unified Manager, in modo che le sessioni inattive degli utenti vengano disconnesse dopo un tempo specificato.

Informazioni su questa attività

Per impostazione predefinita, il timeout della sessione per Unified Manager è di 30 minuti. Puoi regolare tale tempo oppure puoi disabilitare completamente i timeout di sessione.

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

Passaggi

1. Dalla barra dei menu, seleziona la freccia a discesa accanto al tuo user login name.
2. Seleziona **Abilita/Disabilita timeout sessione**.

   Si apre la finestra di dialogo Enable/Disable Session Timeout.

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

   Il timeout minimo che puoi impostare è di 15 minuti.

   > Per disabilitare i timeout di sessione, deselezionare la casella di controllo **Imposta la durata di tempo…**.

4. Fare clic su **Save**.

Array di archiviazione

Scopri la scoperta in SANtricity Unified Manager

Per gestire le risorse di storage, è necessario innanzitutto individuare gli array di storage presenti nella rete.

Come faccio a scoprire gli array?

Utilizza la pagina Aggiungi/Individua per trovare e aggiungere gli array di storage che desideri gestire nella rete della tua organizzazione. Puoi individuare più array o puoi individuare un singolo array. Per fare ciò, inserisci gli indirizzi IP di rete e quindi Unified Manager tenta connessioni individuali con ciascun indirizzo IP in quell'intervallo.

Per saperne di più:

- "Considerazioni per la scoperta di array"
- "Scopri più array di storage"
- "Scopri single array"

Come si gestiscono gli array?

Dopo aver individuato gli array, vai alla pagina **Manage - All**. Da questa pagina, puoi scorrere un elenco degli array di storage rilevati nella rete, visualizzarne lo stato ed eseguire operazioni su un singolo array o su un gruppo di array.

Se desideri gestire un singolo array, puoi selezionarlo e aprire System Manager.

Per saperne di più:

- "Considerazioni per l'accesso a System Manager"
- "Gestire un singolo array di storage"
- "Visualizza lo stato dell'array di storage"

Concetti

Scopri come individuare gli array di storage in SANtricity Unified Manager

Prima che SANtricity Unified Manager possa visualizzare e gestire le risorse di storage, deve individuare gli array di storage che si desidera gestire nella rete dell'organizzazione. È possibile individuare più array oppure un singolo array.

Individuazione di più array di storage

Se si sceglie di rilevare più array, è necessario immettere un intervallo di indirizzi IP di rete e quindi Unified Manager tenterà connessioni individuali a ciascun indirizzo IP in tale intervallo. Qualsiasi array di storage raggiunto con successo viene visualizzato nella pagina Discover e può essere aggiunto al dominio di gestione.

Individuazione di un singolo storage array

Se si sceglie di rilevare un singolo array, si inserisce l'indirizzo IP di uno dei controller nell'array di storage e quindi il singolo array di storage viene aggiunto.

> Unified Manager rileva e visualizza solo il singolo indirizzo IP o l'indirizzo IP compreso in 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, allora Unified Manager non li rileverà né li visualizzerà. Tuttavia, una volta aggiunto l'array di storage, tutti gli indirizzi IP associati verranno rilevati e visualizzati nella vista Manage.

Credenziali utente

Nell'ambito del processo di rilevamento, è necessario fornire la password di amministratore per ogni storage array che si desidera aggiungere.

Certificati dei servizi web

Nell'ambito del processo di rilevamento, Unified Manager verifica che gli array di storage rilevati utilizzino certificati rilasciati da una fonte attendibile. Unified Manager utilizza due tipi di autenticazione basata su certificati per tutte le connessioni che stabilisce con il browser:

- **Certificati attendibili**

  Per gli array rilevati da Unified Manager, potrebbe essere necessario installare certificati attendibili

aggiuntivi forniti dalla Certificate Authority.

Utilizza il pulsante **Importa** per importare questi certificati. Se ti sei già connesso a questo array in precedenza, uno o entrambi i certificati del controller sono scaduti, revocati o manca un certificato radice o intermedio nella catena di certificati. Devi sostituire il certificato scaduto o revocato oppure aggiungere il certificato radice o intermedio mancante prima di gestire l'array di storage.

- **Certificati autofirmati**

  È possibile utilizzare anche certificati autofirmati. Se l'amministratore tenta di rilevare gli array senza importare certificati firmati, Unified Manager visualizza una finestra di dialogo di errore che consente all'amministratore di accettare il certificato autofirmato. Il certificato autofirmato dell'array di storage verrà contrassegnato come attendibile e l'array di storage verrà aggiunto a Unified Manager.

  Se non ti fidi delle connessioni all'array di storage, seleziona **Annulla** e convalida la strategia del certificato di sicurezza dell'array di storage prima di aggiungere l'array di storage a Unified Manager.

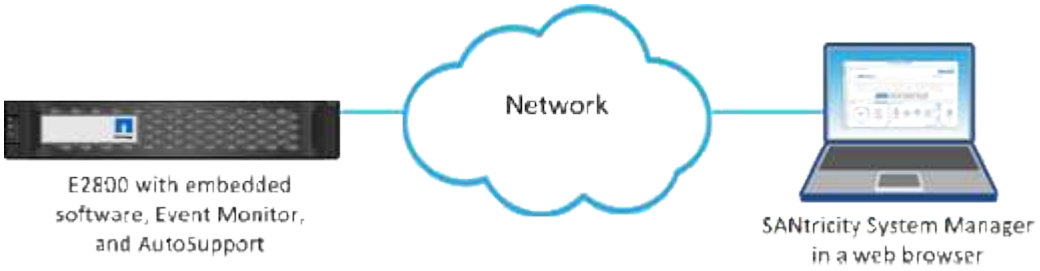
Scopri come accedere a SANtricity System Manager da Unified Manager

Selezionare uno o più array di storage e utilizzare l'opzione Avvia per aprire SANtricity System Manager quando si desidera configurare e gestire gli array di storage.

System Manager è un'applicazione integrata nei controller, connessa alla rete tramite una porta di gestione Ethernet. Include tutte le funzioni basate sull'array.

Per accedere a System Manager, è necessario disporre di:

- Uno dei modelli di array elencati qui: "Panoramica hardware E-Series"
- Una connessione fuori banda a un client di gestione di rete con un browser web.



Scopri gli array

Scopri più array di storage in SANtricity Unified Manager

Si scoprono più array per rilevare tutti gli array di storage nella sottorete in cui risiede il server di gestione e per aggiungere automaticamente gli array scoperti al dominio di gestione.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni Security Admin.
- L'array di storage deve essere impostato e configurato correttamente.
- Le password per gli array di storage devono essere configurate utilizzando il riquadro Gestione accessi di System Manager.

- Per risolvere i problemi relativi ai certificati non attendibili, è necessario disporre di file di certificato attendibili da una Certificate Authority (CA), e che i file di certificato siano disponibili sul sistema locale.

La scoperta degli array è una procedura in più fasi.

Passaggio 1: Inserire l'indirizzo di rete

Immettere un intervallo di indirizzi di rete per eseguire la ricerca nella sottorete locale. Qualsiasi array di storage raggiunto con successo viene visualizzato nella pagina Discover e può essere aggiunto al dominio di gestione.

Se per qualsiasi motivo è necessario interrompere l'operazione di discovery, fare clic su **Stop Discovery**.

Passaggi

1. Dalla pagina Manage, seleziona **Add/Discover**.

   Viene visualizzata la finestra di dialogo Add/Discover.

2. Seleziona il pulsante di opzione **Individua tutti gli array di storage all'interno di un intervallo di rete**.
3. Inserisci l'indirizzo di rete iniziale e l'indirizzo di rete finale per cercare nella tua sottorete locale, quindi fai clic su **Start Discovery**.

   Il processo di rilevamento ha inizio. Questo processo di rilevamento può richiedere diversi minuti per essere completato. La tabella nella pagina Discover viene popolata man mano che vengono rilevati gli array di storage.

   > Se non vengono rilevati array gestibili, verificare che gli array di storage siano correttamente connessi alla rete e che gli indirizzi assegnati siano compresi nell'intervallo. Fare clic su **New Discovery Parameters** per tornare alla pagina Add/Discover.

4. Esamina l'elenco degli array di archiviazione rilevati.
5. Seleziona la check box accanto a qualsiasi storage array che desideri aggiungere al tuo management domain, quindi fai clic su **Next**.

   Unified Manager esegue un controllo delle credenziali su ogni array che si aggiunge al dominio di gestione. Potrebbe essere necessario risolvere eventuali certificati autofirmati e certificati non attendibili associati a tale array.

6. Fai clic su **Avanti** per procedere al passaggio successivo nella procedura guidata.

Passaggio 2: Risolvere i certificati autofirmati durante la fase di rilevamento

Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage utilizzino certificati rilasciati da una fonte attendibile.

Passaggi

1. Eseguire una delle seguenti operazioni:
   - Se ti fidi delle connessioni agli array di storage rilevati, procedi alla scheda successiva della procedura guidata. I certificati autofirmati verranno contrassegnati come attendibili e gli array di storage verranno aggiunti a Unified Manager.
   - Se non ti fidi delle connessioni agli array di storage, seleziona **Annulla** e convalida la strategia del certificato di sicurezza di ciascun array di storage prima di aggiungerne uno a Unified Manager.

2. Fai clic su **Avanti** per procedere al passaggio successivo nella procedura guidata.

Passaggio 3: Risolvere i certificati non attendibili durante il rilevamento

I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Durante il processo di rilevamento dell'array, puoi risolvere i certificati non attendibili importando un certificato di un'autorità di certificazione (CA) (o un certificato firmato da una CA) rilasciato da una terza parte attendibile.

Potrebbe essere necessario installare certificati CA attendibili aggiuntivi se si verifica una delle seguenti condizioni:

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

Passaggi

1. Seleziona la check box accanto a qualsiasi storage array per cui desideri risolvere i certificati non attendibili, quindi seleziona il pulsante **Import**.

   Si apre una finestra di dialogo per l'importazione dei file del certificato attendibile.

2. Fai clic su **Sfoglia** per selezionare i file del certificato per gli array di storage.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

3. Fai clic su **Import**.

   I file sono stati caricati e convalidati.

   > Qualsiasi array di storage con problemi di certificati non attendibili non risolti non verrà aggiunto a Unified Manager.

4. Fai clic su **Avanti** per procedere al passaggio successivo nella procedura guidata.

Passaggio 4: Fornire le password

È necessario immettere le password per gli array di storage che si desidera aggiungere al proprio dominio di gestione.

Passaggi

1. Inserisci la password per ogni array di storage che desideri aggiungere a Unified Manager.
2. **Facoltativo:** Associa gli array di storage a un gruppo: dall'elenco a discesa, seleziona il gruppo desiderato da associare agli array di storage selezionati.
3. Fare clic su **Fine**.

Dopo aver finito

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

La connessione di Unified Manager agli array di storage specificati può richiedere diversi minuti.

Scopri un singolo array in SANtricity Unified Manager

Utilizza l'opzione Aggiungi/Individua singolo storage array per individuare e aggiungere manualmente un singolo storage array alla rete della tua organizzazione.

Prima di iniziare

- L'array di storage deve essere impostato e configurato correttamente.
- Le password per gli array di storage devono essere configurate utilizzando il riquadro Gestione accessi di System Manager.

Passaggi

1. Dalla pagina Manage, seleziona **Add/Discover**.

   Viene visualizzata la finestra di dialogo Add/Discover.

2. Seleziona il pulsante di opzione **Discover a single storage array**.
3. Inserisci l'indirizzo IP di uno dei controller nell'array di storage, quindi fai clic su **Start Discovery**.

   La connessione di Unified Manager all'array di storage specificato può richiedere diversi minuti.

   Il messaggio Storage Array Not Accessible viene visualizzato quando la connessione all'indirizzo IP del controller specificato non riesce.

4. Se richiesto, risolvi eventuali certificati autofirmati.

   Nell'ambito del processo di rilevamento, il sistema verifica che gli array di storage rilevati utilizzino certificati rilasciati da una fonte attendibile. Se non riesce a trovare un certificato digitale per un array di storage, ti invita a risolvere il certificato non firmato da un'autorità di certificazione (CA) riconosciuta aggiungendo un'eccezione di sicurezza.

5. Se richiesto, risolvi eventuali certificati non attendibili.

   I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura a Unified Manager, ma la connessione non viene confermata come sicura. Risolvere i certificati non attendibili importando un certificato di autorità di certificazione (CA) emesso da una terza parte attendibile.

6. Fai clic su **Avanti**.
7. **Facoltativo:** Associa l'array di storage rilevato a un gruppo: dall'elenco a discesa, seleziona il gruppo desiderato da associare all'array di storage.

   Il gruppo "All" è selezionato per impostazione predefinita.

8. Inserisci la password di amministratore per l'array di storage che desideri aggiungere al tuo domain name di gestione, quindi fai clic su **OK**.

Dopo aver finito

L'array di storage viene aggiunto a Unified Manager e, se specificato, viene aggiunto anche al gruppo che hai selezionato.

Se la raccolta di dati di supporto automatica è abilitata, i dati di supporto vengono raccolti automaticamente per

un array di storage che aggiungi.

Gestisci array

Visualizza lo stato dell'array di storage in SANtricity Unified Manager

SANtricity Unified Manager visualizza lo stato di ciascun storage array che è stato rilevato.

Vai alla pagina **Gestisci - Tutto**. Da questa pagina, puoi visualizzare lo stato della connessione tra il Web Services Proxy e quell'array di storage.

Gli indicatori di stato sono descritti nella tabella seguente.

Stato	Indica
Ottimale	L'array di storage è in condizioni ottimali. Non ci sono problemi con i certificati e la password è valida.
Password non valida	È stata fornita una password non valida per lo storage array.
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 da una CA e i certificati CA root e intermedi non sono stati importati.
Necessita attenzione	Si è verificato un problema con lo storage array che richiede il tuo intervento per essere risolto.
Lockdown	L'array di storage è in stato di blocco.
Sconosciuto	L'array di storage non è mai stato contattato. Questo può accadere quando il Web Services Proxy si sta avviando e non ha ancora stabilito un contatto con l'array di storage, oppure quando l'array di storage è offline e non è mai stato contattato dall'avvio del Web Services Proxy.
Offline	Il Web Services Proxy si era precedentemente connesso all'array di storage, ma ora ha perso ogni connessione con esso.

Gestisci un singolo array di storage in SANtricity Unified Manager

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

Passaggi

1. Dalla pagina Manage, seleziona uno o più storage array che desideri gestire.
2. Fai clic su **Launch**.

   Il sistema apre una nuova finestra e visualizza la pagina di accesso di System Manager.

3. Inserisci il tuo nome utente e la tua password, quindi fai clic su **Log in**.

Modificare le password degli array di storage in SANtricity Unified Manager

È possibile aggiornare le password utilizzate per visualizzare e accedere agli array di storage in SANtricity Unified Manager.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni Storage admin.
- È necessario conoscere la password corrente per l'array di storage, che è impostata in System Manager.

Informazioni su questa attività

In questa attività, si immette la password corrente per un array di storage in modo da potervi accedere in Unified Manager. Ciò potrebbe essere necessario se la password dell'array è stata modificata in System Manager e ora deve essere modificata anche in Unified Manager.

Passaggi

1. Dalla pagina Manage, seleziona uno o più storage array.
2. Selezionare **Uncommon Tasks › Provide Storage Array Passwords**.
3. Inserisci la password o le password per ciascun array di archiviazione, quindi fai clic su **Save**.

Rimuovere gli array di storage da SANtricity Unified Manager

È possibile rimuovere uno o più storage array se non si desidera più gestirli da SANtricity Unified Manager.

Informazioni su questa attività

Non è possibile accedere a nessuno degli array di storage che si rimuovono. È comunque possibile stabilire una connessione a uno qualsiasi degli array di storage rimossi puntando un browser direttamente al relativo indirizzo IP o host name.

La rimozione di un array di storage non influisce in alcun modo sull'array di storage o sui suoi dati. Se un array di storage viene rimosso accidentalmente, può essere aggiunto di nuovo.

Passaggi

1. Seleziona la pagina **Manage**.
2. Seleziona uno o più storage array che desideri rimuovere.
3. Selezionare **Uncommon Tasks › Rimuovi storage array**.

   L'array di storage viene rimosso da tutte le viste in SANtricity Unified Manager.

Importazione delle impostazioni

Scopri come importare le impostazioni dell'array di storage in SANtricity Unified Manager

La funzione Import Settings consente di eseguire un'operazione batch per importare le impostazioni da un array a più array. Questa funzione consente di risparmiare tempo

quando è necessario configurare più array nella rete.

Quali impostazioni possono essere importate?

È possibile importare metodi di avviso, AutoSupport configurazioni, configurazioni di Directory Services, configurazioni dello storage (come gruppi di volumi e pool) e impostazioni di sistema (come bilanciamento del carico automatico).

Per saperne di più:

- "Come funzionano le impostazioni di importazione"
- "Requisiti per la replica delle configurazioni dello storage"

Come si esegue un'importazione in batch?

Su un array di storage da utilizzare come origine, apri System Manager e configura le impostazioni desiderate. Quindi, da Unified Manager, vai alla pagina Manage e importa le impostazioni in uno o più array.

Per saperne di più:

- "Importa impostazioni di avviso"
- "Importa impostazioni AutoSupport"
- "Importa le impostazioni dei servizi di directory"
- "Importa le impostazioni di configurazione dello storage"
- "Importa le impostazioni di sistema"

Concetti

Scopri come configurare più array di storage in SANtricity Unified Manager

È possibile utilizzare SANtricity Unified Manager per importare le impostazioni da un array di storage a più array di storage. La funzione Import Settings è un'operazione batch che consente di risparmiare tempo quando è necessario configurare più array nella rete.

Impostazioni disponibili per l'importazione

Le seguenti configurazioni possono essere importate in più array:

- **Avvisi** — Metodi di avviso per inviare eventi importanti agli amministratori, tramite e-mail, un syslog server o un server SNMP.
- **AutoSupport** — Una funzionalità che monitora lo stato di salute di un array di storage e invia notifiche automatiche al supporto tecnico.
- **Servizi di directory** — Un metodo di autenticazione utente gestito tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft Active Directory.
- **Configurazione dello storage** — Configurazioni relative a quanto segue:
  - Volumi (solo volumi thick e non-repository)
  - Gruppi di volumi e pool
  - Assegnazione delle unità hot spare

- **Impostazioni di sistema** — Configurazioni relative a quanto segue:
  - Impostazioni di scansione dei supporti per un volume
  - Impostazioni SSD
  - Bilanciamento del carico automatico (non include la segnalazione della connettività host)

Flusso di lavoro di configurazione

Per importare le impostazioni, segui questo workflow:

1. Su un array di storage da utilizzare come origine, configurare le impostazioni utilizzando System Manager.
2. Sugli array di storage da utilizzare come target, eseguire il backup della loro configurazione utilizzando System Manager.
3. Da Unified Manager, vai alla pagina **Manage** e importa le impostazioni.
4. Dalla pagina **Operazioni**, esamina i risultati dell'operazione Import Settings.

Requisiti per la replica delle configurazioni degli array di storage in SANtricity Unified Manager

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

Shelf di espansione

- Gli alloggiamenti in cui risiedono i controller devono essere identici nell'array di origine e in quello di destinazione.
- Gli ID degli shelf devono essere identici sugli array di origine e di destinazione.
- Gli alloggiamenti di espansione devono essere popolati negli stessi slot con gli stessi tipi di unità (se l'unità viene utilizzata nella configurazione, la posizione delle unità non utilizzate non è rilevante).

Controllori

- Il tipo di controller può essere diverso tra gli array di origine e di destinazione (ad esempio, importando da un E2800 a un E5700), ma il tipo di enclosure RBOD deve essere identico.
- Gli HIC, comprese le funzionalità DA dell'host, devono essere identici tra gli array di origine e di destinazione.
- L'importazione da una configurazione duplex a una simplex non è supportata; tuttavia, l'importazione da simplex a duplex è consentita.
- Le impostazioni FDE non sono incluse nel processo di importazione.

Stato

- Gli array di destinazione devono trovarsi in stato Optimal.
- L'array di origine non deve essere nello stato Ottimale.

Storage

- La capacità delle unità può variare tra gli array di origine e di destinazione, purché la capacità dei volumi sulla destinazione sia maggiore di quella dell'origine. (Un array di destinazione potrebbe avere unità più recenti e con maggiore capacità che non verrebbero configurate completamente in volumi dall'operazione di replica.)

- I volumi del pool di dischi da 64 TB o superiori sull'array di origine impediranno il processo di importazione sui target.
- I volumi sottili non sono inclusi nel processo di importazione.

Utilizzare le importazioni batch

Importa le impostazioni degli avvisi in SANtricity Unified Manager

È possibile importare le configurazioni degli avvisi da un array di storage ad altri array di storage. Questa operazione in batch consente di risparmiare tempo quando è necessario configurare più array nella rete.

Prima di iniziare

- Gli avvisi vengono configurati in System Manager per l'array di storage che si desidera utilizzare come origine (**Settings › Alerts**).
- La configurazione esistente per gli array di storage di destinazione viene salvata in System Manager (menu: Impostazioni [Sistema > Salva configurazione array di storage]).

Informazioni su questa attività

È possibile selezionare avvisi email, SNMP o syslog per l'operazione di importazione. Le impostazioni importate includono:

- **Avvisi email** — Un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Avvisi syslog** — Un indirizzo del server syslog e una porta UDP.
- **Avvisi SNMP** — Un nome della community e un indirizzo IP per il server SNMP.

Passaggi

1. Dalla pagina Manage, fai clic su **Import Settings**.

   Si apre la procedura guidata Import Settings.

2. Nella finestra di dialogo Seleziona impostazioni, seleziona **Email alerts**, **SNMP alerts** o **Syslog alerts**, quindi fai clic su **Avanti**.

   Si apre una finestra di dialogo per selezionare l'array di origine.

3. Nella finestra di dialogo Seleziona origine, seleziona l'array con le impostazioni che desideri importare, quindi fai clic su **Next**.
4. Nella finestra di dialogo Seleziona destinazioni, seleziona una o più matrici per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non può comunicare con quell'array (ad esempio, se è offline o se presenta problemi di certificato, password o di rete).

5. Fare clic su **Fine**.

   La pagina Operazioni mostra i risultati dell'operazione di importazione. Se l'operazione non riesce, puoi fare clic sulla sua riga per vedere ulteriori informazioni.

Risultati

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

Importa le impostazioni AutoSupport in SANtricity Unified Manager

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

Prima di iniziare

- AutoSupport è configurato in System Manager per l'array di storage che si desidera utilizzare come origine (**Support › Support Center**).
- La configurazione esistente per gli array di storage di destinazione viene salvata in System Manager (menu: Impostazioni [Sistema > Salva configurazione array di storage]).

Informazioni su questa attività

Le impostazioni importate includono le singole funzionalità (Basic AutoSupport, AutoSupport OnDemand e Remote Diagnostics), la finestra di manutenzione, il metodo di consegna e il programma di spedizione.

Passaggi

1. Dalla pagina Manage, fai clic su **Import Settings**.

   Si apre la procedura guidata Import Settings.

2. Nella finestra di dialogo Seleziona impostazioni, seleziona **AutoSupport** e poi fai clic su **Next**.

   Si apre una finestra di dialogo per selezionare l'array di origine.

3. Nella finestra di dialogo Seleziona origine, seleziona l'array con le impostazioni che desideri importare, quindi fai clic su **Next**.
4. Nella finestra di dialogo Seleziona destinazioni, seleziona una o più matrici per ricevere le nuove impostazioni.

   > Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non può comunicare con quell'array (ad esempio, se è offline o se presenta problemi di certificato, password o di rete).

5. Fare clic su **Fine**.

   La pagina Operazioni mostra i risultati dell'operazione di importazione. Se l'operazione non riesce, puoi fare clic sulla sua riga per vedere ulteriori informazioni.

Risultati

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

Importa le impostazioni dei servizi di directory in SANtricity Unified Manager

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

Prima di iniziare

- I servizi di directory vengono configurati in System Manager per l'array di storage che si desidera utilizzare come origine (**Settings › Access Management**).
- La configurazione esistente per gli array di storage di destinazione viene salvata in System Manager (menu: Impostazioni [Sistema > Salva configurazione array di storage]).

Informazioni su questa attività

Le impostazioni importate includono il domain name e l'URL di un server LDAP (Lightweight Directory Access Protocol), insieme alle mappature dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.

Passaggi

1. Dalla pagina Manage, fai clic su **Import Settings**.

   Si apre la procedura guidata Import Settings.

2. Nella finestra di dialogo Select Settings, seleziona **Directory services** e quindi fai clic su **Next**.

   Si apre una finestra di dialogo per selezionare l'array di origine.

3. Nella finestra di dialogo Seleziona origine, seleziona l'array con le impostazioni che desideri importare, quindi fai clic su **Next**.
4. Nella finestra di dialogo Seleziona destinazioni, seleziona una o più matrici per ricevere le nuove impostazioni.

   Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non può comunicare con quell'array (ad esempio, se è offline o se presenta problemi di certificato, password o di rete).

5. Fare clic su **Fine**.

   La pagina Operazioni mostra i risultati dell'operazione di importazione. Se l'operazione non riesce, puoi fare clic sulla sua riga per vedere ulteriori informazioni.

Risultati

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

Importa le impostazioni di sistema in SANtricity Unified Manager

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

Prima di iniziare

- Le impostazioni di sistema vengono configurate in System Manager per l'array di storage che si desidera utilizzare come origine.
- La configurazione esistente per gli array di storage di destinazione viene salvata in System Manager (menu: Impostazioni [Sistema > Salva configurazione array di storage]).

Informazioni su questa attività

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

Passaggi

1. Dalla pagina Manage, fai clic su **Import Settings**.

   Si apre la procedura guidata Import Settings.

2. Nella finestra di dialogo Seleziona impostazioni, seleziona **System** e quindi fai clic su **Next**.

   Si apre una finestra di dialogo per selezionare l'array di origine.

3. Nella finestra di dialogo Seleziona origine, seleziona l'array con le impostazioni che desideri importare, quindi fai clic su **Next**.
4. Nella finestra di dialogo Seleziona destinazioni, seleziona una o più matrici per ricevere le nuove impostazioni.

   Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non può comunicare con quell'array (ad esempio, se è offline o se presenta problemi di certificato, password o di rete).

5. Fare clic su **Fine**.

   La pagina Operazioni mostra i risultati dell'operazione di importazione. Se l'operazione non riesce, puoi fare clic sulla sua riga per vedere ulteriori informazioni.

Risultati

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

Importa le impostazioni di configurazione dello storage in SANtricity Unified Manager

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

Prima di iniziare

- Lo storage è configurato in SANtricity System Manager per l'array di storage che si desidera utilizzare come origine.
- La configurazione esistente per gli array di storage di destinazione viene salvata in System Manager (menu: Impostazioni [Sistema > Salva configurazione array di storage]).
- Gli array di origine e di destinazione devono soddisfare questi requisiti:
  - Gli scaffali su cui sono alloggiati i controller devono essere identici.

- I codici identificativi degli shelf devono essere identici.
- Gli alloggiamenti di espansione devono essere popolati negli stessi slot con gli stessi tipi di unità disco.
- Il tipo di enclosure RBOD deve essere identico.
- Gli HIC, comprese le funzionalità di Data Assurance dell'host, devono essere identici.
- Gli array di destinazione devono trovarsi in stato Optimal.
- La capacità del volume sull'array di destinazione è maggiore della capacità dell'array di origine.

- Comprendi le seguenti restrizioni:
  - L'importazione da una configurazione duplex a una simplex non è supportata; tuttavia, l'importazione da simplex a duplex è consentita.
  - I volumi del pool di dischi da 64 TB o superiori sull'array di origine impediranno il processo di importazione sui target.
  - I volumi sottili non sono inclusi nel processo di importazione.

Informazioni su questa attività

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

Passaggi

1. Dalla pagina Manage, fai clic su **Import Settings**.

   Si apre la procedura guidata Import Settings.

2. Nella finestra di dialogo Seleziona impostazioni, seleziona **configurazione dello storage** e quindi fai clic su **Avanti**.

   Si apre una finestra di dialogo per selezionare l'array di origine.

3. Nella finestra di dialogo Seleziona origine, seleziona l'array con le impostazioni che desideri importare, quindi fai clic su **Next**.
4. Nella finestra di dialogo Seleziona destinazioni, seleziona una o più matrici per ricevere le nuove impostazioni.

   Gli array di storage con firmware inferiore a 8.50 non sono disponibili per la selezione. Inoltre, un array non viene visualizzato in questa finestra di dialogo se Unified Manager non può comunicare con quell'array (ad esempio, se è offline o se presenta problemi di certificato, password o di rete).

5. Fare clic su **Fine**.

   La pagina Operazioni mostra i risultati dell'operazione di importazione. Se l'operazione non riesce, puoi fare clic sulla sua riga per vedere ulteriori informazioni.

Risultati

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

Domande frequenti sulle impostazioni di importazione per SANtricity Unified Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Quali impostazioni verranno importate?

La funzione Import Settings è un'operazione batch che carica le configurazioni da un array di storage a più array di storage. Le impostazioni che vengono importate durante questa operazione dipendono da come è configurato l'array di storage di origine in SANtricity System Manager.

Le seguenti impostazioni possono essere importate in più storage array:

- **Avvisi email** — Le impostazioni includono un indirizzo del server di posta e gli indirizzi email dei destinatari degli avvisi.
- **Avvisi syslog** — Le impostazioni includono un indirizzo del server syslog e una porta UDP.
- **Avvisi SNMP** — Le impostazioni includono un nome di community e un indirizzo IP per il server SNMP.
- **AutoSupport** — Le impostazioni includono le singole funzionalità (Basic AutoSupport, AutoSupport OnDemand e Remote Diagnostics), la finestra di manutenzione, il metodo di consegna e il programma di spedizione.
- **Servizi di directory** — La configurazione include il domain name e l'URL di un server LDAP (Lightweight Directory Access Protocol), insieme alle mappature dei gruppi di utenti del server LDAP ai ruoli predefiniti dell'array di storage.
- **Configurazione dello storage** — Le configurazioni includono volumi (solo thick e solo non-repository volumi), gruppi di volumi, pool e assegnazioni di hot spare drive.
- **Impostazioni di sistema** — Le configurazioni includono le impostazioni di scansione dei supporti per un volume, SSD cache per i controller e bilanciamento del carico automatico (non include la segnalazione della connettività host).

Perché non vedo tutti i miei storage array?

Durante l'operazione Import Settings, alcuni dei tuoi 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 a 8.50.
- L'array di archiviazione è offline.
- Il sistema non può comunicare con quell'array (ad esempio, l'array presenta problemi di certificato, password o di rete).

Gruppi di array

Scopri la panoramica dei gruppi in SANtricity Unified Manager

Dalla pagina Manage Groups, è possibile creare un set di gruppi di array di storage per una gestione più semplice.

Che cosa sono i gruppi di array?

È possibile gestire l'infrastruttura fisica e virtualizzata raggruppando un insieme di array di storage. Potresti voler raggruppare gli array di storage per semplificare l'esecuzione di attività di monitoraggio o di reporting.

Esistono due tipi di gruppi:

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

Come si configurano i gruppi?

Dalla pagina Manage Groups, è possibile creare un gruppo e quindi aggiungere array a tale gruppo.

Per saperne di più:

- "Configura il gruppo di array di storage"

Configurare un gruppo di array di storage in SANtricity Unified Manager

Si creano gruppi di storage e poi si aggiungono storage array ai gruppi.

La configurazione dei gruppi è una procedura in due fasi.

Passaggio 1: Crea gruppo

Per prima cosa, si crea un gruppo. Il gruppo di archiviazione definisce quali unità forniscono lo storage che costituisce il volume.

Passaggi

1. Dalla pagina Manage, selezionare **Manage Groups › Crea storage array group**.
2. Nel campo **Name**, digita un nome per il nuovo gruppo.
3. Seleziona gli array di storage che desideri aggiungere al nuovo gruppo.
4. Fai clic su **Create**.

Passaggio 2: Aggiungi l'array di storage al gruppo

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

Passaggi

1. Dalla schermata principale, seleziona **Manage** e poi seleziona il gruppo a cui desideri aggiungere gli array di archiviazione.
2. Selezionare menu:Manage Groups [Add storage arrays to group].
3. Seleziona gli array di storage che desideri aggiungere al gruppo.
4. Fai clic su **Aggiungi.**

Rimuovi gli array di storage da un gruppo in SANtricity Unified Manager

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

Informazioni su questa attività

La rimozione di storage array da un gruppo non influisce in alcun modo sullo storage array o sui suoi dati. Se il tuo storage array è gestito da System Manager, puoi comunque gestirlo utilizzando il browser. Se uno storage array viene rimosso accidentalmente da un gruppo, può essere aggiunto di nuovo.

Passaggi

1. Dalla pagina Manage, selezionare **Manage Groups › Remove storage arrays from group**.
2. Dal menu a tendina, seleziona il gruppo che contiene gli array di storage che desideri rimuovere, e poi fai clic sulla check box accanto a ciascun array di storage che desideri rimuovere dal gruppo.
3. Fai clic su **Remove**.

Eliminare un gruppo di array di storage in SANtricity Unified Manager

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

Informazioni su questa attività

Questa operazione elimina solo il gruppo di array di storage. Gli array di storage associati al gruppo eliminato rimangono accessibili tramite la vista Manage All o qualsiasi altro gruppo a cui sono associati.

Passaggi

1. Dalla pagina Manage, selezionare **Manage Groups › Delete storage array group**.
2. Seleziona uno o più gruppi di storage array che desideri eliminare.
3. Fai clic su **Delete**.

Rinominare un gruppo di array di storage in SANtricity Unified Manager

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

Informazioni su questa attività

Tenete presenti queste linee guida.

- Un nome può essere composto da lettere, numeri e dai caratteri speciali underscore (_), trattino (-) e cancelletto (#). Se si scelgono altri caratteri, viene visualizzato un messaggio di errore. Viene richiesto di scegliere un altro nome.
- Limitare il nome a 30 caratteri. Eventuali spazi iniziali e finali nel nome vengono eliminati.
- Utilizza un nome unico, significativo, facile da capire e da ricordare.
- Evitate nomi arbitrari o nomi che perderebbero rapidamente il loro significato in futuro.

Passaggi

1. Dalla schermata principale, seleziona **Manage** e quindi seleziona il gruppo di storage array che desideri rinominare.

2. Selezionare **Manage Groups › Rinomina storage array group**.
3. Nel campo **Group Name**, digita un nuovo nome per il gruppo.
4. Fai clic su **Rinomina**.

Aggiornamenti

Scopri il Centro aggiornamenti in SANtricity Unified Manager

Dall'Upgrade Center, è possibile gestire gli aggiornamenti del software SANtricity OS e della NVSRAM per più array di storage.

Come funzionano gli aggiornamenti?

Si scarica il software OS più recente e si aggiorna uno o più array.

Aggiornamento del workflow

I seguenti passaggi forniscono un high-level workflow per l'esecuzione degli aggiornamenti software.

1. Scaricate il file software SANtricity OS più recente dal sito di supporto (un link è disponibile da Unified Manager nella pagina di Supporto). Salvate il file sul sistema host di gestione (l'host da cui accedete a Unified Manager tramite browser), e quindi decomprimete il file.
2. In Unified Manager, si caricano il file del software SANtricity OS e il file NVSRAM nel repository (un'area del server Web Services Proxy in cui vengono archiviati i file). È possibile aggiungere i file dal menu: Upgrade Center [Upgrade SANtricity OS Software] oppure da Upgrade Center > Manage Software Repository.
3. Dopo aver caricato i file nel repository, puoi quindi selezionare il file da utilizzare per l'aggiornamento. Dalla pagina Upgrade SANtricity OS software (menu: Upgrade Center [Upgrade SANtricity OS software]), selezioni il file SANtricity OS software e il file NVSRAM. Dopo aver selezionato un file software, in questa pagina viene visualizzato un elenco di array di storage compatibili. Quindi selezioni gli array di storage che desideri aggiornare con il nuovo software. (Non puoi selezionare array incompatibili.)
4. A questo punto è possibile avviare immediatamente il trasferimento e l'attivazione del software, oppure scegliere di preparare i file per l'attivazione in un secondo momento. Durante il processo di aggiornamento, Unified Manager esegue le seguenti operazioni:
   a. Esegue un controllo di integrità sugli array di storage per determinare se esistono condizioni che potrebbero impedire il completamento dell'aggiornamento. Se uno o più array non superano il controllo di integrità, puoi saltare tale array e continuare l'aggiornamento per gli altri, oppure interrompere l'intero processo e risolvere i problemi relativi agli array che non hanno superato il controllo.
   b. Trasferisce i file di aggiornamento a ciascun controller.
   c. Riavvia i controller e attiva il nuovo software SANtricity OS, un controller alla volta. Durante l'attivazione, il file SANtricity OS esistente viene sostituito con il nuovo file.

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

Aggiornamento immediato o graduale

È possibile attivare l'aggiornamento immediatamente oppure programmarlo per un secondo momento. Potresti scegliere di attivarlo in un secondo momento per questi motivi:

- **Orario del giorno** — L'attivazione del software può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. A seconda del carico di I/O e delle dimensioni della cache, un aggiornamento del controller può generalmente richiedere tra 15 e 25 minuti per essere completato. I controller si riavviano e passano in modalità failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — Potresti voler testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri storage array.

Per attivare il software in fase di staging, vai su **Support › Upgrade Center** e fai clic su **Attiva** nell'area denominata SANtricity OS Controller Software upgrade.

Controllo dello stato

Un controllo dello stato di salute viene eseguito come parte del processo di aggiornamento, ma è anche possibile eseguire un controllo dello stato di salute separatamente prima di iniziare (andare su **Upgrade Center › Pre-Upgrade Health Check**).

Il controllo di integrità valuta tutti i componenti del sistema storage per assicurarsi che l'aggiornamento possa procedere. Le seguenti condizioni potrebbero impedire l'aggiornamento:

- Unità assegnate non riuscite
- Hot spare in uso
- Gruppi di volumi incompleti
- Operazioni esclusive in corso
- Volumi mancanti
- Controllore in stato non ottimale
- Numero eccessivo di eventi del registro eventi
- Errore di convalida del database di configurazione
- Dischi con vecchie versioni di DACstore

Cosa devo sapere prima di effettuare l'aggiornamento?

Prima di aggiornare più array di storage, esaminare le considerazioni chiave come parte della pianificazione.

Versioni attuali

È possibile visualizzare le versioni correnti del software SANtricity OS dalla pagina Gestisci di Unified Manager per ogni array di storage rilevato. La versione è visualizzata nella colonna Software SANtricity OS. Le informazioni sul firmware del controller e sulla NVSRAM sono disponibili in una finestra di dialogo a comparsa quando si fa clic sulla versione di SANtricity OS in ciascuna riga.

Altri componenti che richiedono l'aggiornamento

Nell'ambito del processo di aggiornamento, potrebbe essere necessario aggiornare anche il driver multipath/failover dell'host o il driver HBA affinché l'host possa interagire correttamente con i controller.

Per informazioni sulla compatibilità, fare riferimento a "Matrice di interoperabilità NetApp". Consultare anche le procedure nelle Guide rapide per il proprio sistema operativo. Le Guide rapide sono disponibili su "Documentazione E-Series e SANtricity".

Doppio controller

Se un array di storage contiene due controller ed è installato un driver multipath, l'array di storage può continuare a elaborare le operazioni di I/O durante l'upgrade. Durante l'upgrade, si verifica il seguente processo:

1. Il controller A esegue il failover di tutte le sue LUN sul controller B.
2. L'aggiornamento avviene sul controller A.
3. Il controller A riprende possesso delle proprie LUN e di tutte le 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 vengano restituiti al controller proprietario corretto.

Aggiorna software e firmware

Eseguire un controllo di integrità pre-aggiornamento in SANtricity Unified Manager

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

Passaggi

1. Dalla schermata principale, selezionare **Gestisci** e quindi selezionare **Upgrade Center › Pre-Upgrade Health Check**.

   Si apre la finestra di dialogo Controllo integrità pre-aggiornamento, che elenca tutti i sistemi storage rilevati.

2. Se necessario, filtra o ordina i sistemi storage nell'elenco, così puoi visualizzare tutti i sistemi che non sono attualmente nello stato Optimal.
3. Seleziona le caselle di controllo per i sistemi storage che desideri sottoporre al controllo di integrità.
4. Fai clic su **Start**.

   L'avanzamento viene visualizzato nella finestra di dialogo mentre viene eseguito il controllo di integrità.

5. Al termine del controllo dello stato di salute, puoi fare clic sui puntini di sospensione (…) a destra di ciascuna riga per visualizzare ulteriori informazioni ed eseguire altre operazioni.

> Se uno o più array non superano il controllo di integrità, puoi saltare quell'array specifico e continuare l'aggiornamento per gli altri, oppure puoi interrompere l'intero processo e risolvere i problemi degli array che non hanno superato il controllo.

Aggiorna il sistema operativo SANtricity

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

Prima di iniziare

- I file più recenti di SANtricity OS sono disponibili sul sistema host in cui sono in esecuzione SANtricity Web Services Proxy e Unified Manager.
- Sai se desideri attivare l'aggiornamento del software ora o in un secondo momento.

  Potresti scegliere di attivare in un secondo momento per i seguenti motivi:

  - **Orario della giornata** — L'attivazione del software può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. I controller effettuano un failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
  - **Tipo di pacchetto** — Potresti voler testare il nuovo software OS su un array di storage prima di aggiornare i file su altri array di storage.

> I sistemi devono eseguire SANtricity OS 11.70.5 per eseguire l'aggiornamento alla versione 11.80.x o successiva.

Informazioni su questa attività

> Rischio di perdita di dati o rischio di danneggiamento dell'array di storage - non apportare modifiche all'array di storage durante l'aggiornamento. Mantenere l'alimentazione all'array di storage.

Passaggi

1. Se il tuo array di storage contiene solo un controller o non è in uso un driver multipath, interrompi l'attività di I/O verso l'array di storage per evitare errori dell'applicazione. Se il tuo array di storage ha due controller e hai installato un driver multipath, non è necessario interrompere l'attività di I/O.
2. Dalla schermata principale, seleziona **Manage** e quindi seleziona uno o più storage array che desideri aggiornare.
3. Selezionare menu: Upgrade Center [Upgrade SANtricity OS Software].

   Viene visualizzata la pagina di aggiornamento del software SANtricity OS.

4. Scarica il pacchetto software SANtricity OS più recente dal sito di supporto NetApp sul tuo computer locale.

   a. Fare clic su **Aggiungi nuovo file al repository software**.
   b. Fai clic sul link per trovare gli ultimi **SANtricity OS Downloads**.
   c. Fai clic sul link **Download Latest Release**.
   d. Segui le istruzioni rimanenti per scaricare il file SANtricity OS e il file NVSRAM sul tuo computer locale.

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

5. Seleziona il file del software OS e il file NVSRAM che desideri utilizzare per aggiornare i controller:

   a. Dal menu a tendina **Seleziona un file software SANtricity OS**, seleziona il file OS che hai scaricato sulla tua macchina locale.

      Se sono disponibili più file, i file vengono ordinati dal più recente al più vecchio.

Il repository software elenca tutti i file software associati al Web Services Proxy. Se non vedi il file che desideri utilizzare, puoi fare clic sul collegamento **Aggiungi nuovo file al repository software** per individuare la posizione in cui si trova il file OS che desideri aggiungere.

a. Dal menu a tendina **Select an NVSRAM file**, seleziona il file del controller che desideri utilizzare.

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

6. Nella tabella Compatible Storage Array, esamina gli storage array compatibili con il file software OS che hai selezionato, quindi seleziona gli array che desideri aggiornare.
   - Gli array di storage che hai selezionato nella vista Gestione e che sono compatibili con il file firmware selezionato sono selezionati per impostazione predefinita nella tabella Array di storage compatibili.
   - Gli array di storage che non possono essere aggiornati con il file firmware selezionato non sono selezionabili nella tabella Compatible Storage Array, come indicato dallo stato **Incompatible**.
7. **Facoltativo:** Per trasferire il file del software sugli array di storage senza attivarli, selezionare la check box **Trasferisci il software del sistema operativo sugli array di storage, contrassegnalo come preparato e attivalo in un secondo momento**.
8. Fai clic su **Start**.
9. A seconda che tu abbia scelto di attivare ora o in un secondo momento, procedi in uno dei seguenti modi:
   - Digita **TRANSFER** per confermare che desideri trasferire le versioni del software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fai clic su **Transfer**.

     Per attivare il software trasferito, selezionare **Upgrade Center › Attiva software del sistema operativo preinstallato**.

   - Digita **UPGRADE** per confermare che desideri trasferire e attivare le versioni del software del sistema operativo proposte sugli array selezionati per l'aggiornamento, quindi fai clic su **Upgrade**.

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

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

   - Un controllo preliminare dello stato di salute viene eseguito come parte del processo di aggiornamento. Il controllo preliminare dello stato di salute valuta tutti i componenti dell'array di storage per assicurarsi che l'aggiornamento possa procedere.
   - Se un controllo di integrità di un array di storage non riesce, l'aggiornamento si interrompe. Puoi fare clic sui puntini di sospensione (…) e selezionare **Salva registro** per esaminare gli errori. Puoi anche scegliere di ignorare l'errore del controllo di integrità e quindi fare clic su **Continua** per procedere con l'aggiornamento.
   - È possibile annullare l'operazione di upgrade dopo il controllo dello stato di salute pre-upgrade.
10. **Facoltativo:** Una volta completato l'aggiornamento, puoi vedere un elenco di ciò che è stato aggiornato per uno specifico storage array facendo clic sui puntini di sospensione (…) e quindi selezionando **Save Log**.

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

Attivare il software del sistema operativo in staging in SANtricity Unified Manager

È possibile scegliere di attivare il file del software immediatamente oppure attendere un momento più opportuno. Questa procedura presuppone che si scelga di attivare il file del software in un secondo momento.

Informazioni su questa attività

È possibile trasferire i file del firmware senza attivarli. Potresti scegliere di attivare in seguito per questi motivi:

- **Orario della giornata** — L'attivazione del software può richiedere molto tempo, quindi potresti voler attendere che i carichi di I/O siano più leggeri. I controller si riavviano e passano in modalità failover durante l'attivazione, quindi le prestazioni potrebbero essere inferiori al solito fino al completamento dell'aggiornamento.
- **Tipo di pacchetto** — Potresti voler testare il nuovo software e firmware su un array di storage prima di aggiornare i file su altri storage array.

> Non è possibile interrompere il processo di attivazione dopo che è iniziato.

Passaggi

1. Dalla schermata principale, selezionare **Gestisci**. Se necessario, fare clic sulla colonna Stato per ordinare, nella parte superiore della pagina, tutti gli array di storage con stato "Aggiornamento del sistema operativo (in attesa di attivazione)".
2. Seleziona uno o più array di storage per i quali desideri attivare il software, quindi seleziona **Upgrade Center › Activate Staged OS Software**.

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

   - Un controllo preliminare dello stato di salute viene eseguito come parte del processo di attivazione. Il controllo preliminare dello stato di salute valuta tutti i componenti dell'array di storage per assicurarsi che l'attivazione possa procedere.
   - Se un controllo di integrità per un array di storage non riesce, l'attivazione si interrompe. Puoi fare clic sui puntini di sospensione (…) e selezionare **Salva registro** per esaminare gli errori. Puoi anche scegliere di ignorare l'errore del controllo di integrità e quindi fare clic su **Continua** per procedere con l'attivazione.
   - È possibile annullare l'operazione di attivazione dopo il controllo di integrità pre-aggiornamento. Al completamento con successo del controllo di integrità pre-aggiornamento, l'attivazione avviene. Il tempo necessario per l'attivazione dipende dalla configurazione dell'array di storage e dai componenti che si stanno attivando.
3. **Facoltativo:** Dopo il completamento dell'attivazione, puoi vedere un elenco di ciò che è stato attivato per uno specifico storage array facendo clic sui puntini di sospensione (…) e poi selezionando **Salva registro**.

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

Gestire il repository SANtricity in Unified Manager

Il repository software elenca tutti i file software associati al Web Services Proxy.

Se non visualizzi il file che desideri utilizzare, puoi usare l'opzione Gestisci repository software per importare uno o più file SANtricity OS nel sistema host in cui Web Services Proxy e Unified Manager sono in esecuzione. Puoi anche scegliere di eliminare uno o più file SANtricity OS disponibili nel repository software.

Prima di iniziare

Se stai aggiungendo file di SANtricity OS, assicurati che i file OS siano disponibili sul tuo sistema locale.

Passaggi

1. Dalla schermata principale, selezionare **Gestisci** e quindi selezionare **Upgrade Center › Manage Software Repository**.

   Viene visualizzata la finestra di dialogo Manage Software Repository.

2. Eseguire una delle seguenti azioni:

Opzione	Fai così….
Importare	a. Fai clic su **Import**. b. Fai clic su **Sfoglia** e quindi naviga fino alla posizione in cui si trovano i file del sistema operativo che desideri aggiungere. I file del sistema operativo hanno un nome file simile a `N2800-830000-000.dlp`. c. Seleziona uno o più file del sistema operativo che desideri aggiungere, quindi fai clic su **Import**.
Elimina	a. Seleziona uno o più file del sistema operativo che desideri rimuovere dal repository software. b. Fai clic su **Delete**.

Risultati

Se hai selezionato import, i file vengono caricati e convalidati. Se hai selezionato delete, i file vengono rimossi dal repository del software.

Cancella il software del sistema operativo in fase in SANtricity Unified Manager

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

Passaggi

1. Dalla schermata principale, selezionare **Gestisci** e quindi selezionare **Upgrade Center › Clear Staged OS Software**.

   Si apre la finestra di dialogo Cancella software del sistema operativo in fase di installazione e vengono elencati tutti i sistemi di storage rilevati con software o NVSRAM in sospeso.

2. Se necessario, filtra o ordina i sistemi di archiviazione nell'elenco, così puoi visualizzare tutti i sistemi che hanno software in staging.
3. Seleziona le caselle di controllo per i sistemi di storage con software in sospeso che desideri cancellare.
4. Fai clic su **Clear**.

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

Mirroring

Scopri il mirroring in SANtricity Unified Manager

Utilizza le funzionalità di mirroring per replicare i dati tra un array di storage locale e un array di storage remoto, in modo asincrono o sincrono.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Che cos'è il mirroring?

Le applicazioni SANtricity includono due tipi di mirroring: asincrono e sincrono. Il mirroring asincrono copia i volumi di dati su richiesta o secondo una pianificazione, riducendo al minimo o evitando i tempi di inattività che potrebbero derivare da corruzione o perdita di dati. Il mirroring sincrono replica i volumi di dati in tempo reale per garantire disponibilità continua.

Per saperne di più:

- "Come funziona il mirroring"
- "Terminologia del mirroring"

Come si configura il mirroring?

È possibile configurare il mirroring asincrono o sincrono in Unified Manager, quindi utilizzare System Manager per gestire le sincronizzazioni.

Per saperne di più:

- "Flusso di lavoro di configurazione del mirroring"
- "Requisiti per l'utilizzo del mirroring"
- "Crea una coppia speculare asincrona"
- "Crea una coppia speculare sincrona"

Concetti

Scopri il mirroring di SANtricity

SANtricity Unified Manager include opzioni di configurazione per le funzionalità di mirroring di SANtricity, che consentono agli amministratori di replicare i dati tra due array di storage per la protezione dei dati.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Tipi di mirroring

Le applicazioni SANtricity includono due tipi di mirroring: asincrono e sincrono.

Il mirroring asincrono copia i volumi di dati su richiesta o secondo una pianificazione, riducendo al minimo o evitando i tempi di inattività che potrebbero derivare da danneggiamento o perdita di dati. Il mirroring asincrono acquisisce lo stato del volume primario in un determinato momento e copia solo i dati che sono cambiati dall'ultima acquisizione dell'immagine. Il sito primario può essere aggiornato immediatamente e il sito secondario può essere aggiornato man mano che la larghezza di banda lo consente. Le informazioni vengono memorizzate nella cache e inviate in un secondo momento, quando le risorse di rete diventano disponibili. Questo tipo di mirroring è ideale per processi periodici come backup e archiviazione.

Il mirroring sincrono replica i volumi di dati in tempo reale per garantire disponibilità continua. Lo scopo è raggiungere un recovery point objective (RPO) di zero dati persi, avendo una copia dei dati importanti disponibile se si verifica un disastro su uno dei due storage array. La copia è identica ai dati di produzione in ogni momento perché ogni volta che viene eseguita una scrittura sul volume primario, viene eseguita una scrittura anche sul volume secondario. L'host non riceve una conferma che la scrittura è stata eseguita con successo finché il volume secondario non viene aggiornato con le modifiche apportate al volume primario. Questo tipo di mirroring è ideale per scopi di business continuity come il disaster recovery.

Differenze tra i tipi di mirroring

La tabella seguente descrive le principali differenze tra i due tipi di mirroring.

Attributo	Asincrono	Sincrono
Metodo di replicazione	Point-in-time — il mirroring viene eseguito su richiesta o automaticamente in base a una pianificazione definita dall'utente.	Continuo: il mirroring viene eseguito automaticamente in modo continuo, copiando i dati da ogni scrittura host.
Distanza	Supporta lunghe distanze tra gli array. In genere, la distanza è limitata solo dalle capacità della rete e dalla tecnologia di estensione del canale.	Limitato a distanze più brevi tra gli array. In genere, la distanza deve essere entro circa 10 km (6,2 miglia) dall'array di storage locale per soddisfare i requisiti di latenza e prestazioni dell'applicazione.
Metodo di comunicazione	Una rete IP o Fibre Channel standard.	Solo rete Fibre Channel.
Tipi di volume	Standard o thin.	Solo standard.

Flussi di lavoro di configurazione del mirroring SANtricity

È possibile configurare il mirroring asincrono o sincrono in SANtricity Unified Manager e quindi utilizzare SANtricity System Manager per gestire le sincronizzazioni.

Flusso di lavoro di mirroring asincrono

La replica asincrona prevede il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Selezionare l'array di storage locale come origine per il trasferimento dei dati.
   b. Crea o seleziona un gruppo di coerenza mirror esistente, che è un container per il volume primario sull'array locale e il volume secondario sull'array remoto. I volumi primario e secondario sono indicati come la "coppia mirrorata". Se stai creando il gruppo di coerenza mirror per la prima volta, specifichi se desideri eseguire sincronizzazioni manuali o pianificate.
   c. Seleziona un volume primario dall'array di storage locale, quindi determina la sua capacità riservata. La capacità riservata è la capacità fisica allocata da utilizzare per l'operazione di copia.
   d. Selezionare un array di storage remoto come destinazione del trasferimento, un volume secondario e quindi determinarne la capacità riservata.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, questo trasferimento iniziale potrebbe richiedere diverse ore.
2. Verifica lo stato di avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avvia System Manager per l'array locale.
   b. In System Manager, visualizza lo stato dell'operazione di mirroring. Quando il mirroring è completo, lo stato della coppia mirrorata è "Ottimale".
3. Facoltativamente, è possibile riprogrammare o eseguire manualmente i successivi trasferimenti di dati in System Manager. Solo i nuovi e i blocchi modificati vengono trasferiti dal volume primario al volume secondario.

> Grazie alla periodicità della replica asincrona, il sistema può consolidare i blocchi modificati e risparmiare larghezza di banda di rete. L'impatto sul throughput di scrittura e sulla latenza di scrittura è minimo.

Flusso di lavoro di mirroring sincrono

Il mirroring sincrono prevede il seguente flusso di lavoro:

1. Eseguire la configurazione iniziale in Unified Manager:
   a. Seleziona un array di storage locale come origine per il trasferimento dei dati.
   b. Selezionare un volume primario dall'array di storage locale.
   c. Selezionare un array storage remoto come destinazione per il trasferimento dei dati, quindi selezionare un volume secondario.
   d. Seleziona le priorità di sincronizzazione e risincronizzazione.
   e. Avviare il trasferimento iniziale dei dati dal volume primario al volume secondario. A seconda delle dimensioni del volume, questo trasferimento iniziale potrebbe richiedere diverse ore.
2. Verifica lo stato di avanzamento della sincronizzazione iniziale:
   a. In Unified Manager, avvia System Manager per l'array locale.
   b. In System Manager, visualizza lo stato dell'operazione di mirroring. Quando il mirroring è completo, lo stato della coppia mirrorata è "Ottimale". I due array tentano di rimanere sincronizzati durante le normali operazioni. Solo i nuovi blocchi e i blocchi modificati vengono trasferiti dal volume primario al volume secondario.
3. Facoltativamente, puoi modificare le impostazioni di sincronizzazione in System Manager.

Poiché la replica sincrona è continua, il collegamento di replica tra i due siti deve fornire una larghezza di banda sufficiente.

Scopri la terminologia del mirroring in SANtricity Unified Manager

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

Termine	Descrizione
Array di archiviazione locale	L'array di archiviazione locale è l'array di archiviazione su cui si sta operando.
Gruppo di coerenza mirror	Un mirror consistency group è un container per una o più coppie mirror. Per le operazioni di mirroring asincrono, è necessario creare un mirror consistency group. Tutte le coppie mirror in un gruppo vengono risincronizzate simultaneamente, preservando così un punto di ripristino coerente. Il mirroring sincrono non utilizza mirror consistency groups.
Coppia specchiata	Una coppia speculare è composta da due volumi, un volume primario e un volume secondario. Nel mirroring asincrono, una coppia mirrorata appartiene sempre a un mirror consistency group. Le operazioni di scrittura vengono eseguite prima sul volume primario e poi replicate sul volume secondario. Ogni coppia mirrorata in un mirror consistency group condivide le stesse impostazioni di sincronizzazione.
Volume primario	Il volume primario di una coppia speculare è il volume di origine da sottoporre a mirroring.
array di storage remoto	L'array di storage remoto viene solitamente designato come sito secondario, che di solito contiene una replica dei dati in una configurazione di mirroring.
Capacità riservata	La capacità riservata è la capacità fisica allocata utilizzata per qualsiasi operazione di copia del servizio e oggetto di archiviazione. Non è direttamente leggibile dall'host. Questi volumi sono necessari affinché il controller possa salvare in modo permanente le informazioni indispensabili per mantenere il mirroring in uno stato operativo. Contengono informazioni quali i log delta e i dati copy-on-write.
Volume secondario	Il volume secondario di una coppia speculare si trova solitamente in una sede secondaria e contiene una replica dei dati.
Sincronizzazione	La sincronizzazione avviene al momento della sincronizzazione iniziale tra l'array di storage locale e l'array di storage remoto. La sincronizzazione si verifica anche quando i volumi primario e secondario si desincronizzano a seguito di un'interruzione della comunicazione. Quando il collegamento di comunicazione viene ripristinato, tutti i dati non replicati vengono sincronizzati con l'array di storage del volume secondario.

Requisiti per l'utilizzo del mirroring in SANtricity Unified Manager

Se si intende configurare il mirroring, tenere presenti i seguenti requisiti.

Unified Manager

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Array di archiviazione

La funzione di mirroring sincrono non è disponibile sull'array di storage EF600/EF600C o EF300/EF300C.

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- I due array di storage devono essere rilevati in Unified Manager.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

Requisiti di connettività

Il mirroring tramite un'interfaccia FC (asincrona o sincrona) richiede quanto segue:

- Ciascun controller dell'array di storage dedica la sua porta host FC con il numero più alto alle operazioni di mirroring.
- Se il controller dispone sia di porte FC di base che di porte FC sulla scheda di interfaccia verso gli host (HIC), la porta con il numero più alto si trova sulla HIC. Qualsiasi host connesso alla porta dedicata viene disconnesso e non vengono accettate richieste di accesso host. Le richieste di I/O su questa porta sono accettate solo dai controller che partecipano alle operazioni di mirroring.
- Le porte di mirroring dedicate devono essere collegate a un ambiente FC fabric che supporti le interfacce directory service e name service. In particolare, FC-AL e point-to-point non sono supportati come opzioni di connettività tra i controller che partecipano alle relazioni di mirroring.

Il mirroring tramite un'interfaccia iSCSI (solo asincrono) richiede quanto segue:

- A differenza di FC, iSCSI non richiede una porta dedicata. Quando si utilizza il mirroring asincrono in ambienti iSCSI, non è necessario dedicare nessuna delle porte iSCSI front-end dell'array di storage al mirroring asincrono; tali porte sono condivise sia per il traffico di mirroring asincrono che per le connessioni

I/O host-array.

- Il controller mantiene un elenco di sistemi di storage remoti con cui l'iSCSI initiator tenta di stabilire una sessione. La prima porta che riesce a stabilire una connessione iSCSI viene utilizzata per tutte le comunicazioni successive con tale array di storage remoto. Se la comunicazione fallisce, viene tentata una nuova sessione utilizzando tutte le porte disponibili.

> I controller E4000 non supportano il mirroring iSCSI.

- Le porte iSCSI sono configurate a livello di array su base porta per porta. La comunicazione tra controller per la messaggistica di configurazione e il trasferimento dei dati utilizza le impostazioni globali, incluse le impostazioni per:
  - VLAN: Sia il sistema locale che quello remoto devono avere la stessa impostazione VLAN per comunicare
  - porta di ascolto iSCSI
  - Frame jumbo
  - Priorità Ethernet

> La comunicazione iSCSI tra i controller deve utilizzare una porta di connessione host e non la porta Ethernet di gestione.

Candidati al volume mirrorato

- Il livello RAID, i parametri di caching e la dimensione dei segmenti possono essere diversi sui volumi primario e secondario di una coppia con mirroring.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona in mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie asincrone in mirroring non ammissibili non appariranno nell'elenco dei volumi disponibili.

- Il volume secondario deve essere almeno grande quanto il volume primario.
- Un volume può partecipare a una sola relazione mirror.
- Per una coppia con mirroring sincrono, i volumi primario e secondario devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring sincrono, esistono dei limiti al numero di volumi supportati su un determinato array di storage. Assicurati che il numero di volumi configurati sul tuo array di storage sia inferiore al limite supportato. Quando il mirroring sincrono è attivo, i due volumi di capacità riservata che vengono creati vengono conteggiati ai fini del limite di volumi.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità Drive Security.
  - Se il volume primario è FIPS capable, il volume secondario deve essere FIPS capable.
  - Se il volume primario è FDE capable, anche il volume secondario deve essere FDE capable.
  - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.
- I volumi primari e secondari non devono avere la partizione delle risorse abilitata.

Capacità riservata

Mirroring asincrono:

- È necessario un volume di capacità riservato sia per il volume primario che per il volume secondario in una coppia mirrorata per registrare le informazioni di scrittura e recuperare dai reset del controller e altre interruzioni temporanee.
- Poiché sia il volume primario che il volume secondario in una coppia mirrorata richiedono capacità riservata aggiuntiva, è necessario assicurarsi di disporre di capacità libera su entrambi gli array di storage nella relazione di mirror.

Mirroring sincrono:

- La capacità riservata è necessaria per un volume primario e per un volume secondario per registrare le informazioni di scrittura e recuperare dai reset del controller e altre interruzioni temporanee.
- I volumi con capacità riservata vengono creati automaticamente quando il mirroring sincrono è attivato. Poiché sia il volume primario che il volume secondario in una coppia con mirroring richiedono capacità riservata, è necessario assicurarsi di disporre di capacità libera sufficiente su entrambi gli array di storage che partecipano alla relazione di mirroring sincrono.

Funzione di sicurezza dell'unità

- Se si utilizzano unità con funzionalità di sicurezza, il volume primario e il volume secondario devono avere impostazioni di sicurezza compatibili. Questa restrizione non viene applicata; pertanto, è necessario verificarla autonomamente.
- Se si utilizzano unità compatibili con Secure, il volume primario e il volume secondario devono utilizzare lo stesso tipo di unità. Questa restrizione non è applicata; pertanto, è necessario verificarla autonomamente.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse impostazioni DA.

Configura il mirroring

Creare una coppia speculare asincrona in SANtricity Unified Manager

Per configurare il mirroring asincrono, si crea una coppia mirrorata che include un volume primario sull'array locale e un volume secondario sull'array remoto.

Prima di iniziare

Prima di creare una coppia speculare, soddisfa i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Assicurati inoltre di soddisfare i seguenti requisiti per gli array di storage e i volumi:

- Ogni array di storage deve avere due controller.
- I due array di storage devono essere rilevati in Unified Manager.

- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel o un'interfaccia iSCSI.
- Hai creato sia il volume primario che il volume secondario che desideri utilizzare nella relazione di mirroring asincrono.
- Il volume secondario deve essere almeno grande quanto il volume primario.

Informazioni su questa attività

Il processo per creare una coppia mirror asincrona è una procedura in più fasi.

Passaggio 1: crea o seleziona un gruppo di coerenza speculare

In questa fase, si crea un nuovo gruppo di coerenza mirror o se ne seleziona uno esistente. Un gruppo di coerenza mirror è un container per i volumi primario e secondario (la coppia mirror) e specifica il metodo di risincronizzazione desiderato (manuale o automatico) per tutte le coppie nel gruppo.

Passaggi

1. Dalla pagina **Manage**, seleziona l'array di storage locale che desideri utilizzare come origine.
2. Selezionare **Actions › Crea coppia speculare asincrona**.

   Si apre la procedura guidata Create Asynchronous Mirrored Pair.

3. Seleziona un gruppo di coerenza mirror esistente o creane uno nuovo.

   Per selezionare un gruppo esistente, assicurarsi che sia selezionata l'opzione **An existing mirror consistency group** e quindi selezionare il gruppo dalla tabella. Un gruppo di coerenza può includere più coppie speculari.

   Per creare un nuovo gruppo, procedi come segue:

   a. Seleziona **A new mirror consistency group** e poi fai clic su **Avanti**.
   b. Inserisci un nome univoco che descriva al meglio i dati presenti sui volumi che verranno replicati tra i due array di storage. Un nome può contenere solo lettere, numeri e i caratteri speciali underscore (_), trattino (-) e cancelletto (#). Un nome non può superare i 30 caratteri e non può contenere spazi.
   c. Seleziona l'array di storage remoto su cui desideri stabilire una relazione mirror con l'array di storage locale.

      Se il tuo array di storage remoto è protetto da password, il sistema richiederà una password.

   d. Scegli se vuoi sincronizzare le coppie speculari manualmente o automaticamente:
      - **Manuale** — Selezionare questa opzione per avviare manualmente la sincronizzazione per tutte le coppie replicate all'interno di questo gruppo. Si noti che quando si desidera eseguire una risincronizzazione in un secondo momento, è necessario avviare System Manager per lo storage

primario, quindi accedere al **Storage › Mirroring asincrono**, selezionare il gruppo dalla scheda **Mirror Consistency Groups** e quindi selezionare **More › Risincronizza manualmente**.

- **Automatico** — Seleziona l'intervallo desiderato in **Minuti**, **Ore** o **Giorni**, dall'inizio dell'aggiornamento precedente all'inizio dell'aggiornamento successivo. Ad esempio, se l'intervallo di sincronizzazione è impostato su 30 minuti e il processo di sincronizzazione inizia alle 16:00, il processo successivo inizia alle 16:30.

e. Seleziona le impostazioni di avviso desiderate:

- Per le sincronizzazioni manuali, specificare la soglia (definita dalla percentuale di capacità rimanente) per quando si ricevono gli avvisi.
- Per le sincronizzazioni automatiche, puoi impostare tre metodi di avviso: quando la sincronizzazione non è stata completata entro un determinato periodo di tempo, quando i dati del punto di ripristino sull'array remoto sono più vecchi di un determinato limite di tempo e quando la capacità riservata si sta avvicinando a una determinata soglia (definita dalla percentuale di capacità rimanente).

4. Seleziona **Avanti** e vai a Passaggio 2: Seleziona il volume primario.

   Se si definisce un nuovo gruppo di coerenza mirror, Unified Manager crea il gruppo di coerenza mirror prima sull'array di storage locale e poi sull'array di storage remoto. È possibile visualizzare e gestire il gruppo di coerenza mirror avviando System Manager per ciascun array.

> Se Unified Manager crea correttamente il gruppo di coerenza mirror sull'array di storage locale, ma non riesce a crearlo sull'array di storage remoto, elimina automaticamente il gruppo di coerenza mirror dall'array di storage locale. Se si verifica un errore mentre Unified Manager tenta di eliminare il gruppo di coerenza mirror, è necessario eliminarlo manualmente.

Passaggio 2: Seleziona il volume primario

In questa fase, si seleziona il volume primario da utilizzare nella relazione di mirroring e si alloca la sua capacità riservata. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per quella coppia con mirroring. I volumi che non sono idonei per l'uso non vengono visualizzati in tale elenco.

Tutti i volumi che aggiungi al gruppo di coerenza mirror sull'array di storage locale avranno il ruolo primario nella relazione di mirror.

Passaggi

1. Dall'elenco dei volumi idonei, seleziona un volume che desideri utilizzare come volume primario, quindi fai clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, seleziona la capacità riservata per lo storage primario.

   Tenete presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume base e, di solito, questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Refresh Candidates**.
   - La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sul volume primario e di quanto tempo è necessario mantenere la capacità.
   - In generale, scegli una capacità maggiore per la capacità di riserva se una o entrambe queste condizioni esistono:

- Intendi mantenere la coppia mirrorata per un lungo periodo di tempo.
- Una percentuale elevata di blocchi di dati subirà modifiche sul volume primario a causa di un'intensa attività di I/O. Utilizza i dati storici sulle prestazioni o altre utilità del sistema operativo per aiutarti a determinare l'attività di I/O tipica sul volume primario.

3. Seleziona **Avanti** e vai a Passaggio 3: Seleziona il volume secondario.

Passaggio 3: Seleziona il volume secondario

In questa fase, si seleziona il volume secondario da utilizzare nella relazione di mirroring e si alloca la sua capacità riservata. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per quella coppia con mirroring. I volumi che non sono idonei all'uso non vengono visualizzati in tale elenco.

Tutti i volumi che aggiungi al gruppo di coerenza mirror sull'array di storage remoto avranno il ruolo secondario nella relazione di mirroring.

Passaggi

1. Dall'elenco dei volumi idonei, seleziona un volume che desideri utilizzare come volume secondario nella coppia con mirroring, quindi fai clic su **Avanti** per allocare la capacità riservata.
2. Dall'elenco dei candidati idonei, seleziona la capacità riservata per il volume secondario.

   Tenete presenti le seguenti linee guida:

   - L'impostazione predefinita per la capacità riservata è il 20% della capacità del volume base e, di solito, questa capacità è sufficiente. Se si modifica la percentuale, fare clic su **Refresh Candidates**.
   - La capacità necessaria varia a seconda della frequenza e della dimensione delle scritture di I/O sul volume primario e di quanto tempo è necessario mantenere la capacità.
   - In generale, scegli una capacità maggiore per la capacità di riserva se una o entrambe queste condizioni esistono:
     - Intendi mantenere la coppia mirrorata per un lungo periodo di tempo.
     - Una percentuale elevata di blocchi di dati subirà modifiche sul volume primario a causa di un'intensa attività di I/O. Utilizza i dati storici sulle prestazioni o altre utilità del sistema operativo per aiutarti a determinare l'attività di I/O tipica sul volume primario.
3. Selezionare **Fine** per completare la sequenza di mirroring asincrono.

Risultati

Unified Manager esegue le seguenti azioni:

- Avvia la sincronizzazione iniziale tra l'array di archiviazione locale e l'array di archiviazione remoto.
- Crea la capacità riservata per la coppia mirrorata sull'array di storage locale e sull'array di storage remoto.

> Se il volume di cui si esegue il mirroring è un volume thin, solo i blocchi di cui è stato effettuato il provisioning (capacità allocata anziché capacità dichiarata) vengono trasferiti al volume secondario durante la sincronizzazione iniziale. Ciò riduce la quantità di dati che devono essere trasferiti per completare la sincronizzazione iniziale.

Creare una coppia mirrorata sincrona in SANtricity Unified Manager

Per configurare il mirroring sincrono, si crea una coppia mirrorata che include un volume

primario sull'array locale e un volume secondario sull'array remoto.

Questa funzionalità non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Prima di iniziare

Prima di creare una coppia speculare, soddisfa i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Assicurati inoltre di soddisfare i seguenti requisiti per gli array di storage e i volumi:

- I due array di storage che si intende utilizzare per il mirroring vengono rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel.
- Hai creato sia il volume primario che il volume secondario che desideri utilizzare nella relazione di mirroring sincrono.
- Il volume primario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere un volume standard. Non può essere un volume thin o un volume snapshot.
- Il volume secondario deve essere almeno grande quanto il volume primario.

Informazioni su questa attività

Il processo per creare coppie mirrorate sincrone è una procedura in più fasi.

Passaggio 1: Selezionare il volume primario

In questa fase, si seleziona il volume primario da utilizzare nella relazione di mirroring sincrono. Quando si seleziona un volume primario sull'array di storage locale, il sistema visualizza un elenco di tutti i volumi idonei per quella coppia mirrorata. I volumi che non sono idonei per l'uso non vengono visualizzati in tale elenco. Il volume selezionato assume il ruolo primario nella relazione di mirroring.

Passaggi

1. Dalla pagina **Manage**, seleziona l'array di storage locale che desideri utilizzare come origine.
2. Selezionare **Actions › Crea Synchronous Mirrored Pair**.

   Si apre la procedura guidata Create Synchronous Mirrored Pair.

3. Dall'elenco dei volumi idonei, seleziona un volume che desideri utilizzare come volume principale nel

mirror.

4. Seleziona **Avanti** e vai a Passaggio 2: selezionare il volume secondario.

Passaggio 2: selezionare il volume secondario

In questa fase, si seleziona il volume secondario da utilizzare nella relazione di mirror. Quando si seleziona un volume secondario sull'array di storage remoto, il sistema visualizza un elenco di tutti i volumi idonei per quella coppia mirrorata. I volumi che non sono idonei per l'uso non vengono visualizzati in tale elenco. Il volume selezionato assumerà il ruolo di volume secondario nella relazione di mirror.

Passaggi

1. Seleziona l'array di storage remoto su cui desideri stabilire una relazione mirror con l'array di storage locale.

   Se il tuo array di storage remoto è protetto da password, il sistema richiederà una password.

   - Gli array di storage vengono elencati in base al loro nome di array di storage. Se non hai assegnato un nome a un array di storage, verrà visualizzato come "unnamed."
   - Se l'array di storage che si desidera utilizzare non è presente nell'elenco, assicurarsi che sia stato rilevato in Unified Manager.

2. Dall'elenco dei volumi idonei, seleziona un volume che desideri utilizzare come volume secondario nel mirror.

   Se si sceglie un volume secondario con una capacità maggiore rispetto al volume primario, la capacità utilizzabile è limitata alla dimensione del volume primario.

3. Fai clic su **Avanti** e vai a Passaggio 3: Seleziona le impostazioni di sincronizzazione.

Passaggio 3: Seleziona le impostazioni di sincronizzazione

In questa fase, si selezionano le impostazioni che determinano come i dati vengono sincronizzati dopo un'interruzione della comunicazione. È possibile impostare la priorità con cui il controller proprietario del volume primario risincronizza i dati con il volume secondario dopo un'interruzione della comunicazione. È inoltre necessario selezionare la politica di risincronizzazione, manuale o automatica.

Passaggi

1. Utilizza la barra di scorrimento per impostare la priorità di sincronizzazione.

   La priorità di sincronizzazione determina quante risorse di sistema vengono utilizzate per completare la sincronizzazione iniziale e l'operazione di risincronizzazione dopo un'interruzione della comunicazione rispetto alle richieste di I/O del servizio.

   La priorità impostata in questa finestra di dialogo si applica sia al volume primario che al volume secondario. È possibile modificare la velocità sul volume primario in un secondo momento accedendo a System Manager e selezionando **Storage › Synchronous Mirroring › More › Edit Settings**.

   Esistono cinque livelli di priorità di sincronizzazione:

   - Più basso
   - Basso
   - Medio

- Alto
- Più alto

  Se la priorità di sincronizzazione è impostata sul valore più basso, l'attività di I/O ha la priorità e l'operazione di risincronizzazione richiede più tempo. Se la priorità di sincronizzazione è impostata sul valore più alto, l'operazione di risincronizzazione ha la priorità, ma l'attività di I/O per l'array di storage potrebbe essere influenzata.

2. Scegli se desideri risincronizzare le coppie mirrorate sull'array di storage remoto manualmente o automaticamente.
   - **Manuale** (opzione consigliata) — Selezionare questa opzione per richiedere che la sincronizzazione venga ripresa manualmente dopo il ripristino della comunicazione con una coppia mirror. Questa opzione offre la migliore opportunità per il recupero dei dati.
   - **Automatico** — Selezionare questa opzione per avviare automaticamente la risincronizzazione dopo il ripristino della comunicazione con una coppia mirrorata.

     Per riprendere manualmente la sincronizzazione, vai a System Manager e seleziona **Storage › Mirroring sincrono**, evidenzia la coppia mirrorata nella tabella e seleziona **Riprendi** in **Altro**.
3. Fai clic su **Fine** per completare la sequenza di mirroring sincrono.

Risultati

Una volta attivato il mirroring, il sistema esegue le seguenti azioni:

- Avvia la sincronizzazione iniziale tra l'array di archiviazione locale e l'array di archiviazione remoto.
- Imposta la priorità di sincronizzazione e la policy di risincronizzazione.
- Riserva la porta con il numero più alto dell'HIC del controller per la trasmissione dei dati mirrorati.

  Le richieste di I/O ricevute su questa porta sono accettate solo dal controller remoto preferito proprietario del volume secondario nella coppia mirrorata. (Le prenotazioni sul volume primario sono consentite.)

- Crea due volumi di capacità riservata, uno per ciascun controller, che vengono utilizzati per registrare le informazioni di scrittura per il ripristino da reset del controller e altre interruzioni temporanee.

  La capacità di ciascun volume è 128 MiB. Tuttavia, se i volumi vengono inseriti in un pool, saranno riservati 4 GiB per ciascun volume.

Dopo aver finito

Accedere a System Manager e selezionare **Home › Visualizza operazioni in corso** per visualizzare lo stato di avanzamento dell'operazione di mirroring sincrono. Questa operazione può richiedere molto tempo e potrebbe influire sulle prestazioni del sistema.

Domande frequenti sul mirroring dello storage per SANtricity Unified Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Cosa devo sapere prima di creare un mirror consistency group?

Segui queste linee guida prima di creare un mirror consistency group.

Soddisfare i seguenti requisiti per Unified Manager:

- Il servizio Web Services Proxy deve essere in esecuzione.
- Unified Manager deve essere in esecuzione sul tuo host locale tramite una connessione HTTPS.
- Unified Manager deve visualizzare certificati SSL validi per lo storage array. È possibile accettare un certificato autofirmato o installare un certificato di sicurezza personalizzato tramite Unified Manager e accedendo a **Certificate › Certificate Management**.

Assicurati inoltre di soddisfare i seguenti requisiti per gli array di storage:

- I due array di storage devono essere rilevati in Unified Manager.
- Ogni array di storage deve avere due controller.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- I tuoi array di storage locali e remoti sono collegati tramite una fabric Fibre Channel o un'interfaccia iSCSI.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Cosa devo sapere prima di creare una coppia speculare?

Prima di creare una coppia speculare, seguire queste linee guida.

- È necessario disporre di due storage array.
- Ogni array di storage deve avere due controller.
- I due array di storage devono essere rilevati in Unified Manager.
- Ciascun controller, sia nell'array primario che in quello secondario, deve avere una porta di gestione Ethernet configurata e deve essere connesso alla rete.
- Gli array di storage hanno una versione minima del firmware pari a 7.84. (Ciascuno può eseguire diverse versioni del sistema operativo.)
- È necessario conoscere la password per gli array di storage locali e remoti.
- È necessario disporre di una capacità libera sufficiente sull'array di storage remoto per creare un volume secondario uguale o superiore al volume primario che si desidera replicare.
- Il mirroring asincrono è supportato sui controller con porte host Fibre Channel (FC) o iSCSI, mentre il mirroring sincrono è supportato solo sui controller con porte host FC.

> La funzione di mirroring sincrono non è disponibile sui sistemi storage EF600/EF600C o EF300/EF300C.

Perché dovrei cambiare questa percentuale?

La capacità riservata corrisponde in genere al 20 percento del volume di base per le operazioni di mirroring asincrono. Di solito questa capacità è sufficiente.

La capacità necessaria varia a seconda della frequenza e delle dimensioni delle scritture di I/O sul volume di base e di quanto tempo si intende utilizzare l'operazione di servizio di copia dell'oggetto di storage. In

generale, scegliere una percentuale maggiore per la capacità riservata se si verifica una o entrambe queste condizioni:

- Se la durata dell'operazione di copy service di un particolare oggetto storage sarà molto lunga.
- Se una grande percentuale di blocchi di dati cambierà sul volume di base a causa di un'intensa attività di I/O. Utilizzare i dati storici sulle prestazioni o altre utility del sistema operativo per aiutare a determinare l'attività di I/O tipica del volume di base.

Perché vedo più di un candidato a capacità riservata?

Se in un pool o in un gruppo di volumi sono presenti più volumi che soddisfano la percentuale di capacità selezionata per lo storage object, verranno visualizzati più candidati.

È possibile aggiornare l'elenco dei candidati consigliati modificando la percentuale di spazio fisico dell'unità che si desidera riservare sul volume di base per le operazioni di copy service. I candidati migliori vengono visualizzati in base alla selezione effettuata.

Perché non vedo tutti i miei volumi?

Quando si seleziona un volume primario per una coppia con mirroring, un elenco mostra tutti i volumi idonei.

I volumi che non sono idonei all'utilizzo non vengono visualizzati in tale elenco. I volumi potrebbero non essere idonei per uno qualsiasi dei seguenti motivi:

- Il volume non è ottimale.
- Il volume partecipa già a una relazione di mirroring.
- Per il mirroring sincrono, i volumi primario e secondario di una coppia speculare devono essere volumi standard. Non possono essere volumi thin o volumi snapshot.
- Per il mirroring asincrono, i volumi thin devono avere autoespansione abilitata.

> Per i controller EF600 e EF300, i volumi primari e secondari di una coppia asincrona in mirroring devono corrispondere allo stesso protocollo, livello di vassoio, dimensione del segmento, tipo di sicurezza e livello RAID. Le coppie asincrone in mirroring non ammissibili non appariranno nell'elenco dei volumi disponibili.

Perché non vedo tutti i volumi sull'array di storage remoto?

Quando si seleziona un volume secondario sull'array di storage remoto, un elenco mostra tutti i volumi idonei per quella coppia di mirroring.

I volumi che non sono idonei all'utilizzo non vengono visualizzati in tale elenco. I volumi possono non essere idonei per uno qualsiasi dei seguenti motivi:

- Il volume è un volume non standard, ad esempio un volume snapshot.
- Il volume non è ottimale.
- Il volume partecipa già a una relazione di mirroring.
- Per il mirroring asincrono, gli attributi del volume sottile tra il volume primario e il volume secondario non corrispondono.
- Se si utilizza Data Assurance (DA), il volume primario e il volume secondario devono avere le stesse impostazioni DA.

    - Se il volume primario è abilitato per DA, il volume secondario deve essere abilitato per DA.
    - Se il volume primario non è abilitato per DA, il volume secondario non deve essere abilitato per DA.
- Per il mirroring asincrono, il volume primario e il volume secondario devono avere le stesse funzionalità Drive Security.
    - Se il volume primario è FIPS capable, il volume secondario deve essere FIPS capable.
    - Se il volume primario è FDE capable, anche il volume secondario deve essere FDE capable.
    - Se il volume primario non utilizza Drive Security, il volume secondario non deve utilizzare Drive Security.

Che impatto ha la priorità di sincronizzazione sulle velocità di sincronizzazione?

La priorità di sincronizzazione definisce la quantità di tempo di elaborazione allocata alle attività di sincronizzazione rispetto alle prestazioni del sistema.

Il controller proprietario del volume primario esegue questa operazione in background. Contemporaneamente, il controller proprietario elabora le scritture I/O locali sul volume primario e le relative scritture remote sul volume secondario. Poiché la risincronizzazione distoglie le risorse di elaborazione del controller dall'attività di I/O, la risincronizzazione può avere un impatto sulle prestazioni dell'applicazione host.

Tenete a mente queste linee guida per aiutarvi a determinare quanto tempo potrebbe richiedere una priorità di sincronizzazione e in che modo le priorità di sincronizzazione possono influire sulle prestazioni del sistema.

Queste tariffe prioritarie sono disponibili:

- Più basso
- Basso
- Medio
- Alto
- Più alto

La velocità di priorità più bassa supporta le prestazioni del sistema, ma la risincronizzazione richiede più tempo. La velocità di priorità più alta supporta la risincronizzazione, ma le prestazioni del sistema potrebbero essere compromesse.

Queste linee guida approssimativamente approssimano le differenze tra le priorità.

Tariffa prioritaria per la sincronizzazione completa	Tempo trascorso rispetto alla velocità di sincronizzazione più elevata
Più basso	Circa otto volte più a lungo rispetto al tasso di priorità più alto.
Basso	Circa sei volte più a lungo rispetto al tasso di priorità più alto.
Medio	Circa tre volte e mezzo più a lungo rispetto al tasso di priorità più alto.

Tariffa prioritaria per la sincronizzazione completa	Tempo trascorso rispetto alla velocità di sincronizzazione più elevata
Alto	Circa il doppio del tempo rispetto alla velocità di priorità più alta.

Le dimensioni del volume e i carichi di I/O dell'host influenzano i confronti dei tempi di sincronizzazione.

Perché è consigliato utilizzare una policy di sincronizzazione manuale?

Si consiglia la risincronizzazione manuale perché consente di gestire il processo di risincronizzazione in modo da offrire la migliore opportunità per il recupero dei dati.

Se si utilizza una policy di risincronizzazione automatica e si verificano problemi di comunicazione intermittenti durante la risincronizzazione, i dati sul volume secondario potrebbero essere temporaneamente danneggiati. Al termine della risincronizzazione, i dati vengono corretti.

Certificati

Panoramica dei certificati

La gestione dei certificati consente di creare richieste di firma dei certificati (CSRs), importare certificati e gestire i certificati esistenti.

Cosa sono i certificati?

I *certificati* sono file digitali che identificano entità online, come siti web e server, per comunicazioni sicure su internet. Esistono due tipi di certificati: un *certificato firmato* è convalidato da un'autorità di certificazione (CA) e un *certificato autofirmato* è convalidato dal proprietario dell'entità invece che da una terza parte.

Per saperne di più:

- "Come funzionano i certificati"
- "Terminologia dei certificati"

Come configuro i certificati?

Da Certificate Management, puoi configurare i certificati per la stazione di gestione che ospita Unified Manager e anche importare i certificati per i controller negli array.

Per saperne di più:

- "Utilizzare certificati firmati da CA per il sistema di gestione"
- "Importa certificati per array"

Concetti

Come funzionano i certificati in SANtricity Unified Manager

I certificati sono file digitali che identificano entità online, come siti web e server, per comunicazioni sicure su internet.

Certificati firmati

I certificati garantiscono che le comunicazioni web vengano trasmesse in forma crittografata, private e inalterate, esclusivamente tra il server e il client specificati. Utilizzando Unified Manager, puoi gestire i certificati per il browser su un sistema di gestione host e per i controller negli array di storage rilevati.

Un certificato può essere firmato da un'autorità fidata, oppure può essere autofirmato. "Firmare" significa semplicemente che qualcuno ha convalidato l'identità del proprietario e ha stabilito che i suoi dispositivi possono essere considerati affidabili. Gli array di storage vengono forniti con un certificato autofirmato generato automaticamente su ciascun controller. Puoi continuare a utilizzare i certificati autofirmati oppure ottenere certificati firmati da una CA per una connessione più sicura tra i controller e i sistemi host.

> Sebbene i certificati firmati da una CA offrano una maggiore protezione della sicurezza (ad esempio, prevenendo gli attacchi man-in-the-middle), comportano anche costi che possono essere elevati se si dispone di una rete di grandi dimensioni. Al contrario, i certificati autofirmati sono meno sicuri, ma sono gratuiti. Pertanto, i certificati autofirmati vengono utilizzati più spesso per ambienti di test interni, non in ambienti di produzione.

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

Quando apri un browser e inserisci un indirizzo web, il tuo sistema esegue in background un processo di verifica del certificato per determinare se ti stai connettendo a un sito web che include un certificato valido, CA-signed. In genere, un sito protetto da un certificato firmato presenta un'icona a forma di lucchetto e una designazione https nell'indirizzo. Se tenti di connetterti a un sito web che non contiene un certificato CA-signed, il browser visualizza un avviso che il sito non è sicuro.

L'autorità di certificazione (CA) adotta delle misure per verificare la tua identità durante il processo di richiesta. Potrebbe inviare un'e-mail alla tua azienda registrata, verificare l'indirizzo della tua azienda ed eseguire una verifica HTTP o DNS. Una volta completata la procedura di richiesta, la CA ti invia dei file digitali da caricare su un sistema di gestione host. In genere, questi file includono una catena di fiducia, come segue:

- **Root** — Al vertice della gerarchia si trova il certificato root, che contiene una chiave privata utilizzata per firmare altri certificati. Il root identifica una specifica organizzazione CA. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato root.
- **Intermedi** — Dalla radice si diramano i certificati intermedi. La CA emette uno o più certificati intermedi che fungono da intermediari tra una radice protetta e i certificati del server.
- **Server** — Alla base della catena si trova il certificato del server, che identifica la tua entità specifica, come un sito web o un altro dispositivo. Ogni controller in un storage array richiede un certificato server separato.

Certificati autofirmati

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

I certificati autofirmati non sono "trusted" dai browser. Ogni volta che si tenta di connettersi a un sito web che contiene solo un certificato autofirmato, il browser visualizza un messaggio di avviso. È necessario fare clic su un collegamento nel messaggio di avviso che consente di procedere al sito web; così facendo, si accetta il certificato autofirmato.

Certificati per Unified Manager

L'interfaccia di Unified Manager viene installata insieme al Web Services Proxy su un sistema host. Quando si apre un browser e si tenta di connettersi a Unified Manager, il browser cerca di verificare che l'host sia una fonte attendibile controllando la presenza di un certificato digitale. Se il browser non trova un certificato firmato da una CA per il server, visualizza un messaggio di avviso. Da lì, è possibile continuare al sito web per accettare il certificato autofirmato per quella sessione. Oppure, è possibile ottenere certificati digitali firmati da una CA così da non visualizzare più il messaggio di avviso.

Certificati per i controller

Durante una sessione di Unified Manager, potrebbero essere visualizzati messaggi di sicurezza aggiuntivi quando si tenta di accedere a un controller privo di un certificato firmato da una CA. In tal caso, è possibile considerare attendibile in modo permanente il certificato autofirmato oppure importare i certificati firmati da una CA per i controller, in modo che il server Web Services Proxy possa autenticare le richieste client in entrata provenienti da questi controller.

Scopri la terminologia dei certificati in SANtricity Unified Manager

I seguenti termini si applicano alla gestione dei certificati.

Termine	Descrizione
CA	Un'autorità di certificazione (CA) è un'entità fidata che rilascia documenti elettronici, chiamati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti web, il che consente connessioni sicure tra client e server.
CSR	Una richiesta di firma del certificato (CSR) è un messaggio inviato da un richiedente a un'autorità di certificazione (CA). La CSR convalida le informazioni richieste dalla CA per rilasciare un certificato.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli aggressori di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e sull'identità dell'entità di fiducia che certifica (firma) queste informazioni.
Catena di certificati	Una gerarchia di file che aggiunge un livello di sicurezza ai certificati. In genere, la catena include un certificato radice al vertice della gerarchia, uno o più certificati intermedi e i certificati del server che identificano le entità.
Certificato intermedio	Uno o più certificati intermedi si diramano dal certificato radice nella catena di certificati. La CA emette uno o più certificati intermedi che fungono da intermediari tra un certificato radice protetto e i certificati del server.
Keystore	Un keystore è un repository sul sistema di gestione host che contiene chiavi private, insieme alle corrispondenti chiavi pubbliche e certificati. Queste chiavi e certificati identificano le proprie entità, come i controller.

Termine	Descrizione
Certificato radice	Il certificato radice si trova al vertice della gerarchia nella catena di certificati e contiene una chiave privata utilizzata per firmare altri certificati. Il root identifica una particolare organizzazione CA. Se si utilizza la stessa CA per tutti i dispositivi di rete, è necessario un solo certificato radice.
Certificato firmato	Un certificato convalidato da un'autorità di certificazione (CA). Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Inoltre, un certificato firmato include dettagli relativi al proprietario dell'entità (in genere, un server o un sito web) e una firma digitale composta da lettere e numeri. Un certificato firmato utilizza una catena di fiducia e pertanto viene utilizzato più spesso in ambienti di produzione. È anche noto come "CA-signed certificate" o "management certificate".
Certificato autofirmato	Un certificato autofirmato viene convalidato dal proprietario dell'entità. Questo file di dati contiene una chiave privata e garantisce che i dati vengano inviati in forma crittografata tra un server e un client tramite una connessione HTTPS. Include anche una firma digitale composta da lettere e numeri. Un certificato autofirmato non utilizza la stessa catena di fiducia di un certificato firmato da una CA e pertanto viene spesso utilizzato in ambienti di test. Viene anche definito come certificato "preinstallato".
Certificato del server	Il certificato del server si trova alla base della catena di certificati. Identifica la tua entità specifica, come un sito web o un altro dispositivo. Ogni controller in un sistema storage richiede un certificato server separato.
Truststore	Un truststore è un repository che contiene certificati provenienti da terze parti fidate, come le CA.

Utilizzare certificati firmati da CA per il sistema di gestione

È possibile ottenere e importare certificati firmati da CA per accedere in modo sicuro al sistema di gestione che ospita SANtricity Unified Manager.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.

Informazioni su questa attività

L'utilizzo di certificati firmati da una CA è una procedura in tre fasi.

Passaggio 1: Completare un file CSR

È necessario innanzitutto generare un file di richiesta di firma del certificato (CSR), che identifica la propria organizzazione e il sistema host in cui sono installati Web Services Proxy e Unified Manager.

In alternativa, puoi generare un file CSR utilizzando uno strumento come OpenSSL e passare a Passaggio 2: invia il file CSR.

Passaggi

1. Seleziona **Certificate Management**.
2. Dalla scheda Management, selezionare **Complete CSR**.
3. Inserisci le seguenti informazioni, quindi fai clic su **Avanti**:
   - **Organizzazione** — Il nome legale completo della tua azienda o organizzazione. Includi i suffissi, come Inc. o Corp.
   - **Unità organizzativa (facoltativa)** — La divisione della tua organizzazione che si occupa del certificato.
   - **Città/Località** — La città in cui si trova il tuo sistema host o la tua azienda.
   - **Stato/Regione (facoltativo)** — Lo stato o la regione in cui si trova il sistema host o la tua azienda.
   - **Codice ISO del Paese** — Il codice ISO (International Organization for Standardization) a due cifre del tuo Paese, ad esempio US.
4. Inserisci le seguenti informazioni sul sistema host su cui è installato il Web Services Proxy:
   - **Nome comune** — L'indirizzo IP o il nome DNS del sistema host in cui è installato il Web Services Proxy. Assicurati che questo indirizzo sia corretto; deve corrispondere esattamente a quello che inserisci per accedere a Unified Manager nel browser. Non includere http:// o https://. Il nome DNS non può iniziare con un carattere jolly.
   - **Indirizzi IP alternativi** — Se il nome comune è un indirizzo IP, puoi facoltativamente inserire eventuali indirizzi IP aggiuntivi o alias per il sistema host. Per più voci, usa un formato separato da virgole.
   - **Nomi DNS alternativi** — Se il nome comune è un nome DNS, inserire eventuali nomi DNS aggiuntivi per il sistema host. Per più voci, utilizzare il formato separato da virgole. Se non ci sono nomi DNS alternativi, ma hai inserito un nome DNS nel primo campo, copia quel nome qui. Il nome DNS non può iniziare con un carattere jolly.
5. Assicurati che le informazioni sull'host siano corrette. Se non lo sono, i certificati restituiti dalla CA non riusciranno quando proverai a importarli.
6. Fare clic su **Fine**.
7. Vai a Passaggio 2: invia il file CSR.

Passaggio 2: invia il file CSR

Dopo aver creato un file di richiesta di firma del certificato (CSR), lo si invia a una Certificate Authority (CA) per ricevere certificati di gestione firmati per il sistema che ospita Unified Manager e il Web Services Proxy.

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

Passaggi

1. Individua il file CSR scaricato.

   La posizione della cartella del download dipende dal browser.

2. Invia il file CSR a una CA (ad esempio, Verisign o DigiCert) e richiedi i certificati firmati in formato PEM.

Dopo aver inviato un file CSR alla CA, NON generare un altro file CSR. Ogni volta che generi un CSR, il sistema crea una coppia di chiavi privata e pubblica. La chiave pubblica fa parte del CSR, mentre la chiave privata viene conservata nel keystore del sistema. Quando ricevi i certificati firmati e li importi, il sistema garantisce che sia la chiave privata che quella pubblica siano la coppia originale. Se le chiavi non corrispondono, i certificati firmati non funzioneranno e devi richiedere nuovi certificati alla CA.

3. Quando la CA restituisce i certificati firmati, vai su Passaggio 3: Importa i certificati di gestione.

Passaggio 3: Importa i certificati di gestione

Dopo aver ricevuto i certificati firmati dall'Autorità di Certificazione (CA), importa i certificati nel sistema host in cui sono installati il Web Services Proxy e l'interfaccia di Unified Manager.

Prima di iniziare

- Hai ricevuto i certificati firmati dall'autorità di certificazione (CA). Questi file includono il certificato radice, uno o più certificati intermedi e il certificato del server.
- Se la CA ha fornito un file di certificati concatenati (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'utilità Windows `certmgr` per decomprimere i file (fare clic con il pulsante destro del mouse e selezionare **Tutte le attività › Esporta**). Si consiglia la codifica Base-64. Al termine dell'esportazione, viene visualizzato un file CER per ciascun file di certificato nella catena.
- Hai copiato i file del certificato sul sistema host in cui è in esecuzione il Web Services Proxy.

Passaggi

1. Seleziona **Certificate Management**.
2. Dalla scheda Management, selezionare **Import**.

   Si apre una finestra di dialogo per l'importazione dei file del certificato.

3. Fai clic su **Sfoglia** per selezionare prima i file del certificato radice e intermedio, quindi seleziona il certificato del server. Se hai generato la CSR da uno strumento esterno, devi anche importare il file della chiave privata creato insieme alla CSR.

   I nomi dei file vengono visualizzati nella finestra di dialogo.

4. Fai clic su **Import**.

Risultati

I file vengono caricati e convalidati. Le informazioni sul certificato vengono visualizzate nella pagina Certificate Management.

Reimposta i certificati di gestione

È possibile ripristinare il certificato di gestione allo stato originale, autofirmato di fabbrica.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.

Informazioni su questa attività

Questa operazione elimina il certificato di gestione corrente dal sistema host in cui sono installati Web Services Proxy e Unified Manager. Dopo il ripristino del certificato, il sistema host torna a utilizzare il certificato autofirmato.

Passaggi

1. Seleziona **Impostazioni > Certificati**.
2. Seleziona la scheda **Array Management**, quindi seleziona **Reset**.

   Si apre una finestra di dialogo Confirm Reset Management Certificate.

3. Digita `reset` nel campo, quindi fai clic su **Ripristina**.

   Dopo l'aggiornamento della pagina, 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 a utilizzare certificati autofirmati. Per eliminare la condizione che blocca l'accesso alla destinazione, è necessario cancellare i dati di navigazione dal browser.

Risultati

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

Utilizzare certificati array

Importa i certificati per gli array in SANtricity Unified Manager

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

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.
- Se si importano certificati attendibili, i certificati devono essere importati per i controller dell'array di storage utilizzando System Manager.

Passaggi

1. Seleziona **Certificate Management**.
2. Seleziona la scheda **Trusted**.

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

3. Selezionare **Import › Certificates** per importare un certificato CA oppure **Import › Self-signed storage array certificates** per importare un certificato autofirmato.

   Per limitare la visualizzazione, puoi utilizzare il campo di filtro **Mostra i certificati che sono…** oppure puoi ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, seleziona il certificato e quindi fai clic su **Import**.

   Il certificato viene caricato e convalidato.

Eliminare i certificati attendibili in SANtricity Unified Manager

È possibile eliminare uno o più certificati che non sono più necessari, ad esempio un certificato scaduto.

Prima di iniziare

Importa il nuovo certificato prima di eliminare quello vecchio.

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

Passaggi

1. Seleziona **Certificate Management**.
2. Seleziona la scheda **Trusted**.
3. Seleziona uno o più certificati nella tabella, quindi fai clic su **Delete**.

   > La funzione **Delete** non è disponibile per i certificati preinstallati.

   Si apre la finestra di dialogo Conferma eliminazione certificato attendibile.

4. Conferma l'eliminazione, quindi fai clic su **Elimina**.

   Il certificato viene rimosso dalla tabella.

Risolvere i certificati non attendibili

I certificati non attendibili si verificano quando un array di storage tenta di stabilire una connessione sicura a SANtricity Unified Manager, ma la connessione non riesce a confermarsi come sicura.

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

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni Security Admin.
- Se si intende importare un certificato firmato da una CA:
  - Hai generato una richiesta di firma del certificato (.CSR file) per ciascun controller nell'array di storage e l'hai inviata alla CA.
  - L'autorità di certificazione ha restituito file di certificati attendibili.
  - I file del certificato sono disponibili sul tuo sistema locale.

Informazioni su questa attività

Potrebbe essere necessario installare certificati CA attendibili aggiuntivi se una delle seguenti condizioni è vera:

- Hai aggiunto di recente un array di storage.
- Uno o entrambi i certificati sono scaduti.

- Uno o entrambi i certificati sono revocati.
- Uno o entrambi i certificati non dispongono di un certificato root o intermedio.

Passaggi

1. Seleziona **Certificate Management**.
2. Seleziona la scheda **Trusted**.

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

3. Selezionare **Import › Certificates** per importare un certificato CA oppure **Import › Self-Signed storage array certificates** per importare un certificato autofirmato.

   Per limitare la visualizzazione, puoi utilizzare il campo di filtro **Mostra i certificati che sono…** oppure puoi ordinare le righe dei certificati facendo clic su una delle intestazioni di colonna.

4. Nella finestra di dialogo, seleziona il certificato e quindi fai clic su **Import**.

   Il certificato viene caricato e convalidato.

Gestisci i certificati

Visualizza certificati

È possibile visualizzare le informazioni di riepilogo di 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 (identificativi univoci).

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni dei certificati non vengono visualizzate.

Passaggi

1. Seleziona **Certificate Management**.
2. Seleziona una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il Web Services Proxy. Un certificato di management può essere autofirmato o approvato da una certificate authority (CA). Consente l'accesso sicuro a Unified Manager.
   - **Attendibili** — Mostra i certificati a cui Unified Manager può accedere per gli array di storage e altri server remoti, come un LDAP server. I certificati possono essere emessi da una certificate authority (CA) o possono essere self-signed.
3. Per visualizzare maggiori informazioni su un certificato, selezionare la riga corrispondente, selezionare i puntini di sospensione alla fine della riga e quindi fare clic su **View** o **Export**.

Esporta certificati in SANtricity Unified Manager

È possibile esportare un certificato per visualizzarne tutti i dettagli completi.

Prima di iniziare

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

Passaggi

1. Seleziona **Certificate Management**.
2. Seleziona una delle seguenti schede:
   - **Management** — Mostra il certificato per il sistema che ospita il Web Services Proxy. Un certificato di management può essere autofirmato o approvato da una certificate authority (CA). Consente l'accesso sicuro a Unified Manager.
   - **Attendibili** — Mostra i certificati a cui Unified Manager può accedere per gli array di storage e altri server remoti, come un LDAP server. I certificati possono essere emessi da una certificate authority (CA) o possono essere self-signed.
3. Seleziona un certificato dalla pagina, quindi fai clic sui puntini di sospensione alla fine della riga.
4. Fai clic su **Export** e poi salva il file del certificato.
5. Apri il file nell'applicazione per la visualizzazione dei certificati.

Gestione degli accessi

Scopri la gestione degli accessi con SANtricity Unified Manager

Access Management è un metodo per configurare l'autenticazione degli utenti in SANtricity Unified Manager.

Quali metodi di autenticazione sono disponibili?

Sono disponibili i seguenti metodi di autenticazione:

- **Ruoli utente locali** — L'autenticazione viene gestita tramite funzionalità RBAC (controllo degli accessi in base al ruolo). I ruoli utente locali includono profili utente predefiniti e ruoli con autorizzazioni di accesso specifiche.
- **Servizi di directory** — L'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft Active Directory.
- **SAML** — L'autenticazione viene gestita tramite un Identity Provider (IdP) utilizzando SAML 2.0.

Per saperne di più:

- "Come funziona la gestione degli accessi"
- "Terminologia relativa alla gestione degli accessi"
- "Autorizzazioni per i ruoli mappati"
- "SAML"

Come si configura Access Management?

Il software SANtricity è preconfigurato per utilizzare i ruoli utente locali. Se si desidera utilizzare LDAP, è possibile configurarlo nella pagina Access Management.

Per saperne di più:

- "Gestione degli accessi con ruoli utente locali"
- "Gestione degli accessi con servizi di directory"

- "Configura SAML"

Concetti

Come funziona la gestione degli accessi in SANtricity Unified Manager

Utilizzare Access Management per stabilire l'autenticazione degli utenti in SANtricity Unified Manager.

Flusso di lavoro di configurazione

La configurazione di Access Management funziona come segue:

1. Un amministratore accede a Unified Manager con un profilo utente che include le autorizzazioni di Security admin.

   > Al primo accesso, il nome utente `admin` viene visualizzato automaticamente e non può essere modificato. L'utente `admin` ha pieno accesso a tutte le funzioni del sistema. La password deve essere impostata al primo accesso.

2. L'amministratore accede alla sezione Gestione accessi nell'interfaccia utente, che include ruoli utente locali preconfigurati. Questi ruoli rappresentano un'implementazione delle funzionalità di controllo degli accessi in base al ruolo (role-based access control, RBAC).
3. L'amministratore configura uno o più dei seguenti metodi di autenticazione:
   - **Ruoli utente locali** — L'autenticazione viene gestita tramite le funzionalità RBAC. I ruoli utente locali includono utenti e ruoli predefiniti con autorizzazioni di accesso specifiche. Gli amministratori possono utilizzare questi ruoli utente locali come unico metodo di autenticazione o utilizzarli in combinazione con un servizio di directory. Non è necessaria alcuna configurazione, tranne l'impostazione delle password per gli utenti.
   - **Servizi di directory** — L'autenticazione viene gestita tramite un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft's Active Directory. Un amministratore si connette al server LDAP e quindi associa gli utenti LDAP ai ruoli utente locali.
   - **SAML** — L'autenticazione viene gestita tramite un Identity Provider (IdP) utilizzando il Security Assertion Markup Language (SAML) 2.0. Un amministratore stabilisce la comunicazione tra il sistema IdP e l'array di storage, quindi associa gli utenti IdP ai ruoli utente locali incorporati nell'array di storage.
4. L'amministratore fornisce agli utenti le credenziali di accesso per Unified Manager.
5. Gli utenti accedono al sistema inserendo le proprie credenziali. Durante l'accesso, il sistema esegue le seguenti operazioni in background:
   - Autentica il nome utente e la password rispetto all'account utente.
   - Determina le autorizzazioni dell'utente in base ai ruoli assegnati.
   - Fornisce all'utente l'accesso alle funzioni dell'interfaccia utente.
   - Visualizza il nome utente nel banner superiore.

Funzioni disponibili in Unified Manager

L'accesso alle funzioni dipende dai ruoli assegnati all'utente, che includono i seguenti:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage sugli array, ma nessun accesso alla configurazione della sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management e Certificate Management.
- **Support admin** — Accesso a tutte le risorse hardware sugli array di storage, ai dati di errore e agli eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Una funzione non disponibile è visualizzata in grigio oppure non viene mostrata nell'interfaccia utente.

Scopri la terminologia relativa alla gestione degli accessi di SANtricity Unified Manager

Scopri come si applicano i termini di Access Management a SANtricity Unified Manager.

Termine	Descrizione
Active Directory	Active Directory (AD) è un servizio di directory Microsoft che utilizza LDAP per le reti di dominio Windows.
Legame	Le operazioni di bind vengono utilizzate per autenticare i client al directory server. Il bind richiede in genere credenziali di account e password, ma alcuni server consentono operazioni di bind anonime.
CA	Un'autorità di certificazione (CA) è un'entità fidata che rilascia documenti elettronici, chiamati certificati digitali, per la sicurezza di Internet. Questi certificati identificano i proprietari dei siti web, il che consente connessioni sicure tra client e server.
Certificato	Un certificato identifica il proprietario di un sito per motivi di sicurezza, impedendo agli aggressori di impersonare il sito. Il certificato contiene informazioni sul proprietario del sito e sull'identità dell'entità di fiducia che certifica (firma) queste informazioni.
LDAP	Il Lightweight Directory Access Protocol (LDAP) è un protocollo applicativo per l'accesso e la gestione di servizi di informazioni di directory distribuiti. Questo protocollo consente a numerose applicazioni e servizi di connettersi al LDAP server per validare gli utenti.
RBAC	Il controllo degli accessi in base al ruolo (RBAC) è un metodo per regolare l'accesso alle risorse di computer o di rete in base ai ruoli dei singoli utenti. Unified Manager include ruoli predefiniti.
SAML	Security Assertion Markup Language (SAML) è uno standard basato su XML per l'autenticazione e l'autorizzazione tra due entità. SAML consente l'autenticazione a più fattori, in cui gli utenti devono fornire due o più elementi per dimostrare la propria identità (ad esempio, una password e un'impronta digitale). La funzionalità SAML integrata nell'array di storage è conforme a SAML2.0 per l'asserzione dell'identità, l'autenticazione e l'autorizzazione.

Termine	Descrizione
SSO	Il single sign-on (SSO) è un servizio di autenticazione che consente di utilizzare un unico set di credenziali di accesso per accedere a più applicazioni.
Web Services Proxy	Il Web Services Proxy, che fornisce accesso tramite meccanismi HTTPS standard, consente agli amministratori di configurare i servizi di gestione per gli array di storage. Il proxy può essere installato su host Windows o Linux. L'interfaccia Unified Manager è disponibile con il Web Services Proxy.

Autorizzazioni per i ruoli mappati

Le funzionalità RBAC (in base al ruolo, controllo degli accessi basato sui ruoli) includono utenti predefiniti a cui sono associati uno o più ruoli. Ogni ruolo include autorizzazioni per l'accesso alle attività in SANtricity Unified Manager.

I ruoli forniscono agli utenti l'accesso alle attività, come segue:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage sugli array, ma nessun accesso alla configurazione della sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management e Certificate Management.
- **Support admin** — Accesso a tutte le risorse hardware sugli array di storage, ai dati di errore e agli eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.
- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Se un utente non dispone delle autorizzazioni per una determinata funzione, tale funzione è o non disponibile per la selezione oppure non viene visualizzata nell'interfaccia utente.

Gestione degli accessi con ruoli utente locali in SANtricity Unified Manager

Gli amministratori possono utilizzare le funzionalità RBAC (in base al ruolo) implementate in SANtricity Unified Manager. Queste funzionalità sono denominate "local user roles".

Flusso di lavoro di configurazione

I ruoli utente locali sono preconfigurati nel sistema. Per utilizzare i ruoli utente locali per l'autenticazione, gli amministratori possono fare quanto segue:

1. Un amministratore accede a Unified Manager con un profilo utente che include le autorizzazioni di Security admin.

   > L' `admin`utente ha pieno accesso a tutte le funzioni del sistema.

2. Un amministratore esamina i profili utente, che sono predefiniti e non possono essere modificati.
3. Facoltativamente, l'amministratore assegna nuove password per ciascun profilo utente.
4. Gli utenti accedono al sistema con le credenziali loro assegnate.

Gestione

Quando si utilizzano solo ruoli utente locali per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Cambia password.
- Imposta una lunghezza minima per le password.
- Consenti agli utenti di accedere senza password.

Gestione degli accessi con servizi di directory in SANtricity Unified Manager

Gli amministratori possono utilizzare un server LDAP (Lightweight Directory Access Protocol) e un servizio di directory, come Microsoft's Active Directory.

Flusso di lavoro di configurazione

Se nella rete vengono utilizzati un LDAP server e un servizio di directory, la configurazione funziona come segue:

1. Un amministratore accede a Unified Manager con un profilo utente che include le autorizzazioni di Security admin.

   L' `admin`utente ha pieno accesso a tutte le funzioni del sistema.

2. L'amministratore inserisce le impostazioni di configurazione per il LDAP server. Le impostazioni includono il domain name, l'URL e le informazioni sull'account Bind.
3. Se il LDAP server utilizza un protocollo sicuro (LDAPS), l'amministratore carica una catena di certificati di un'autorità di certificazione (CA) per l'autenticazione tra il LDAP server e il sistema host in cui è installato il Web Services Proxy.
4. Una volta stabilita la connessione al server, l'amministratore associa i gruppi di utenti ai ruoli utente locali. Questi ruoli sono predefiniti e non possono essere modificati.
5. L'amministratore verifica la connessione tra il LDAP server e il Web Services Proxy.
6. Gli utenti accedono al sistema con le credenziali LDAP/Directory Services loro assegnate.

Gestione

Quando si utilizzano i servizi di directory per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Aggiungi un server di directory.
- Modifica le impostazioni del server di directory.
- Associa gli utenti LDAP ai ruoli utente locali.
- Rimuovi un server di directory.
- Cambia password.
- Imposta una lunghezza minima per le password.
- Consenti agli utenti di accedere senza password.

Gestione degli accessi con SAML in SANtricity Unified Manager

Per Access Management, gli amministratori possono utilizzare le funzionalità Security Assertion Markup Language (SAML) 2.0 integrate nell'array.

Flusso di lavoro di configurazione

La configurazione SAML funziona come segue:

1. Un amministratore accede a Unified Manager con un profilo utente che include le autorizzazioni Security Admin.

   L `admin`utente ha pieno accesso a tutte le funzioni in System Manager.

2. L'amministratore va alla scheda **SAML** sotto Gestione accessi.
3. Un amministratore configura le comunicazioni con l'Identity Provider (IdP). Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è stato autenticato con successo. Per configurare le comunicazioni con l'array di storage, l'amministratore scarica il file di metadati dell'IdP dal sistema IdP e quindi utilizza Unified Manager per caricare il file sull'array di storage.
4. Un amministratore stabilisce una relazione di fiducia tra il Service Provider e l'IdP. Un Service Provider controlla l'autorizzazione degli utenti; in questo caso, il controller nell'array di storage funge da Service Provider. Per configurare le comunicazioni, l'amministratore utilizza Unified Manager per esportare un file di metadati del Service Provider per il controller. Dal sistema IdP, l'amministratore importa quindi il file di metadati nell'IdP.

   Gli amministratori devono inoltre assicurarsi che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.

5. L'amministratore associa i ruoli dell'array di storage agli attributi utente definiti nell'IdP. Per fare ciò, l'amministratore utilizza Unified Manager per creare le associazioni.
6. L'amministratore verifica l'accesso SSO all'URL dell'IdP. Questo test garantisce che l'array di storage e l'IdP possano comunicare.

   Una volta abilitato SAML, *non è possibile* disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

7. Da Unified Manager, l'amministratore abilita SAML per l'array di storage.
8. Gli utenti accedono al sistema con le proprie credenziali SSO.

Gestione

Quando si utilizza SAML per l'autenticazione, gli amministratori possono eseguire le seguenti attività di gestione:

- Modifica o crea nuove mappature dei ruoli
- Esporta file del Service Provider

Restrizioni di accesso

Quando SAML è abilitato, gli utenti non possono individuare o gestire lo storage per quell'array dall'interfaccia legacy Storage Manager.

Inoltre, i seguenti client non possono accedere ai servizi e alle risorse dell'array di storage:

- Enterprise Management Window (EMW)
- Interfaccia a riga di comando (CLI)
- Client dei Software Developer Kits (SDK)
- Clienti in banda
- Client REST API con autenticazione HTTP Basic
- Accedi utilizzando l'endpoint REST API standard

Utilizzare i ruoli utente locali

Visualizza i ruoli utente locali

Dalla scheda Ruoli utente locali, è possibile visualizzare le mappature degli utenti ai ruoli predefiniti. Queste mappature fanno parte del controllo degli accessi in base al ruolo (RBAC) applicato nel Web Services Proxy per SANtricity Unified Manager.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Informazioni su questa attività

Gli utenti e le mappature non possono essere modificati. Solo le password possono essere modificate.

Passaggi

1. Seleziona **Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.

   Gli utenti sono visualizzati nella tabella:

   - **admin** — Super amministratore con accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli.
   - **storage** — L'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **sicurezza** — L'utente responsabile della configurazione della sicurezza, inclusa Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor.
   - **support** — L'utente responsabile delle risorse hardware, dei dati relativi ai guasti e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor.
   - **monitor** — Un utente con accesso di sola lettura al sistema. Questo utente include solo il ruolo Monitor.
   - **rw** (lettura/scrittura) — Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor.
   - **ro** (read only) — Questo utente include solo il ruolo Monitor.

Modificare le password per i profili utente locali in SANtricity Unified Manager

È possibile modificare le password degli utenti per ciascun utente in Access Management.

Prima di iniziare

- È necessario aver effettuato l'accesso come amministratore locale, il che include i permessi di Root admin.
- È necessario conoscere la password dell'amministratore locale.

Informazioni su questa attività

Tieni a mente queste linee guida quando scegli una password:

- Le nuove password degli utenti locali devono soddisfare o superare l'impostazione corrente per la password minima (in Visualizza/Modifica impostazioni).
- Le password distinguono tra maiuscole e minuscole.
- Gli spazi finali non vengono rimossi dalle password quando vengono impostate. Fai attenzione a includere gli spazi se erano inclusi nella password.
- Per una maggiore sicurezza, usa almeno 15 caratteri alfanumerici e cambia la password frequentemente.

Passaggi

1. Seleziona **Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.
3. Seleziona un utente dalla tabella.

   Il pulsante Change Password diventa disponibile.

4. Seleziona **Change Password**.

   Si apre la finestra di dialogo Change Password.

5. Se non è impostata alcuna lunghezza minima per le password degli utenti locali, puoi selezionare la casella di controllo per richiedere all'utente di inserire una password per accedere al sistema.
6. Inserisci la nuova password per l'utente selezionato nei due campi.
7. Inserisci la password dell'amministratore locale per confermare questa operazione, quindi fai clic su **Cambia**.

Risultati

Se l'utente è attualmente connesso, la modifica della password causa la terminazione della sessione attiva dell'utente.

Modificare le impostazioni della password dell'utente locale in SANtricity Unified Manager

È possibile impostare la lunghezza minima richiesta per tutte le nuove password degli utenti locali o per quelle aggiornate. È inoltre possibile consentire agli utenti locali di accedere al sistema senza inserire una password.

Prima di iniziare

È necessario aver effettuato l'accesso come amministratore locale, il che include i permessi di Root admin.

Informazioni su questa attività

Tenete a mente queste linee guida quando impostate la lunghezza minima per le password degli utenti locali:

- Le modifiche alle impostazioni non influiscono sulle password degli utenti locali esistenti.
- La lunghezza minima richiesta per le password degli utenti locali deve essere compresa tra 0 e 30 caratteri.
- Qualsiasi nuova password utente locale deve soddisfare o superare l'impostazione attuale della lunghezza minima.
- Non impostare una lunghezza minima per la password se desideri che gli utenti locali accedano al sistema senza inserire una password.

Passaggi

1. Seleziona **Access Management**.
2. Seleziona la scheda **Ruoli utente locali**.
3. Seleziona **Visualizza/Modifica impostazioni**.

   Si apre la finestra di dialogo Impostazioni password utente locale.

4. Eseguire una delle seguenti operazioni:
   - Per consentire agli utenti locali di accedere al sistema *senza* inserire una password, deselezionare la casella di controllo "Require all local user passwords to be at least".
   - Per impostare una lunghezza minima per tutte le password degli utenti locali, selezionare la casella di controllo "Richiedi che tutte le password degli utenti locali siano almeno di" e quindi utilizzare la casella di selezione numerica per impostare la lunghezza minima richiesta per tutte le password degli utenti locali.

     Le nuove password degli utenti locali devono soddisfare o superare l'impostazione attuale.

5. Fare clic su **Save**.

Utilizzare i servizi di directory

Aggiungi server di directory in SANtricity Unified Manager

Per configurare l'autenticazione per Access Management, è necessario stabilire una comunicazione tra un LDAP server e l'host su cui è in esecuzione il Web Services Proxy per SANtricity Unified Manager. Successivamente, si mappano i gruppi di utenti LDAP ai ruoli utente locali.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali dell'LDAP server devono essere disponibili, inclusi il domain name, l'URL del server e, facoltativamente, il nome utente e la password dell'account di bind.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del LDAP server deve essere installata sul computer locale.

Informazioni su questa attività

L'aggiunta di un server di directory è un processo in due fasi. Innanzitutto, si inseriscono il domain name e l'URL. Se il server utilizza un protocollo sicuro, è necessario caricare anche un certificato CA per l'autenticazione, qualora sia firmato da un'autorità di certificazione non standard. Se si dispone delle credenziali per un bind account, è possibile inserire anche il nome utente e la password. Successivamente, si associano i gruppi di utenti del LDAP server ai ruoli utente locali.

Passaggi

1. Seleziona **Access Management**.
2. Dalla scheda **Directory Services**, selezionare **Add Directory Server**.

   Si apre la finestra di dialogo Add Directory Server.

3. Nella scheda **Impostazioni server**, inserire le credenziali per il LDAP server.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio(i)
Inserisci il domain name del LDAP server. Per più domain name, inseriscili in un elenco separato da virgole. Il domain name viene utilizzato nel login (*username@domain*) per specificare quale directory server utilizzare per l'autenticazione.	URL del server
Inserire l'URL per accedere al LDAP server nel formato `ldap[s]://**host**:*port*`.	Carica certificato (facoltativo)
Questo campo viene visualizzato solo se nel campo Server URL sopra è specificato un protocollo LDAPS. Fai clic su **Sfoglia** e seleziona un certificato CA da caricare. Si tratta del certificato attendibile o della catena di certificati attendibili utilizzati per autenticare il LDAP server.	Account di bind (facoltativo)

Impostazione	Descrizione
Inserire un account utente di sola lettura per le query di ricerca sul LDAP server e per la ricerca all'interno dei gruppi. Inserire il nome dell'account in un formato di tipo LDAP. Ad esempio, se l'utente di bind si chiama "bindacct", allora si potrebbe inserire un valore come `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Password di bind (facoltativa)
Questo campo viene visualizzato quando si inserisce un bind account. Inserisci la password per l'account bind.	Verifica la connessione al server prima di aggiungere

Impostazione	Descrizione
Seleziona questa casella di controllo se desideri assicurarti che il sistema possa comunicare con la configurazione del LDAP server che hai inserito. Il test viene eseguito dopo aver fatto clic su **Aggiungi** in fondo alla finestra di dialogo. Se questa casella di controllo è selezionata e il test fallisce, la configurazione non viene aggiunta. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e aggiungere la configurazione.	**Impostazioni dei privilegi**
DN di base di ricerca	Inserire il contesto LDAP per cercare gli utenti, in genere nella forma `CN=Users, DC=cpoc, DC=local`.
Attributo username	Inserisci l'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i del gruppo	Inserisci un elenco di attributi di gruppo sull'utente, che viene utilizzato per la mappatura gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

4. Fai clic sulla scheda **Role Mapping**.
5. Assegna i gruppi LDAP ai ruoli predefiniti. Un gruppo può avere più ruoli assegnati.

Dettagli del campo

Impostazione	Descrizione
Mappature	DN gruppo
Specificare il nome distinto (DN) del gruppo per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	Fai clic nel campo e seleziona uno dei ruoli utente locali da associare al Group DN. Devi selezionare singolarmente ogni ruolo che desideri includere per questo gruppo. Il ruolo Monitor è necessario in combinazione con gli altri ruoli per accedere a SANtricity Unified Manager. I ruoli associati includono le seguenti autorizzazioni: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage sugli array, ma nessun accesso alla configurazione della sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management e Certificate Management. • **Support admin** — Accesso a tutte le risorse hardware sugli array di storage, ai dati di errore e agli eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è obbligatorio per tutti gli utenti, incluso l'amministratore.

6. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
7. Quando hai terminato con le mappature, fai clic su **Aggiungi**.

   Il sistema esegue una convalida, assicurandosi che l'array di storage e LDAP server possano comunicare. Se viene visualizzato un messaggio di errore, controlla le credenziali inserite nella finestra di dialogo e reinserisci le informazioni se necessario.

Modifica le impostazioni del server di directory e le mappature dei ruoli in SANtricity Unified Manager

Se in precedenza hai configurato un server di directory in Access Management, puoi modificarne le impostazioni in qualsiasi momento. Le impostazioni includono le informazioni di connessione al server e le associazioni tra gruppi e ruoli.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- È necessario definire un server di directory.

Passaggi

1. Seleziona **Access Management**.
2. Seleziona la scheda **Directory Services**.
3. Se sono definiti più server, selezionare il server che si desidera modificare dalla tabella.
4. Seleziona **Visualizza/Modifica impostazioni**.

   Si apre la finestra di dialogo Directory Server Settings.

5. Nella scheda **Server Settings**, modificare le impostazioni desiderate.

Dettagli del campo

Impostazione	Descrizione
Impostazioni di configurazione	Dominio(i)
Il domain name dei LDAP server. Per più domain name, inserirli in un elenco separato da virgole. Il domain name viene utilizzato nel login (*username* @*domain*) per specificare il directory server su cui autenticarsi.	URL del server
L'URL per accedere al LDAP server nel formato `ldap[s]://host:port`.	Account di bind (facoltativo)
Account utente di sola lettura per le query di ricerca contro il LDAP server e per la ricerca all'interno dei gruppi.	Password di bind (facoltativa)
La password per l'account di bind. (Questo campo viene visualizzato quando si inserisce un account di bind.)	Verifica la connessione al server prima di salvare

Impostazione	Descrizione
Verifica che il sistema possa comunicare con la configurazione del LDAP server. Il test viene eseguito dopo aver fatto clic su **Salva**. Se questa casella di controllo è selezionata e il test fallisce, la configurazione non viene modificata. È necessario risolvere l'errore o deselezionare la casella di controllo per saltare il test e modificare nuovamente la configurazione.	**Impostazioni dei privilegi**
DN di base di ricerca	Il contesto LDAP per la ricerca degli utenti, in genere nella forma di `CN=Users, DC=cpoc, DC=local`.
Attributo username	L'attributo associato all'ID utente per l'autenticazione. Ad esempio: `sAMAccountName`.
Attributo/i del gruppo	Un elenco di attributi di gruppo sull'utente, utilizzato per la mappatura gruppo-ruolo. Ad esempio: `memberOf, managedObjects`.

6. Nella scheda **Role Mapping**, modificare la mappatura desiderata.

Dettagli del campo

Impostazione	Descrizione
Mappature	DN gruppo
Il domain name per il gruppo di utenti LDAP da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	I ruoli da mappare al DN del gruppo. È necessario selezionare singolarmente ogni ruolo che si desidera includere per questo gruppo. Il ruolo Monitor è richiesto in combinazione con gli altri ruoli per accedere a SANtricity Unified Manager. I ruoli includono i seguenti: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage sugli array, ma nessun accesso alla configurazione della sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management e Certificate Management. • **Support admin** — Accesso a tutte le risorse hardware sugli array di storage, ai dati di errore e agli eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è obbligatorio per tutti gli utenti, incluso l'amministratore.

7. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
8. Fare clic su **Save**.

Risultati

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione utente corrente verrà mantenuta.

Rimuovi server di directory

Per interrompere la connessione tra un server di directory e il Web Services Proxy, è possibile rimuovere le informazioni del server dalla pagina Access Management. Potresti voler eseguire questa operazione se hai configurato un nuovo server e poi vuoi rimuovere quello vecchio.

Prima di iniziare

È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.

Informazioni su questa attività

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione utente corrente verrà mantenuta.

Passaggi

1. Seleziona **Access Management**.
2. Seleziona la scheda **Directory Services**.
3. Dall'elenco, seleziona il server di directory che vuoi eliminare.
4. Fai clic su **Remove**.

   Si apre la finestra di dialogo Remove Directory Server.

5. Digita `remove` nel campo e poi fai clic su **Rimuovi**.

   Le impostazioni di configurazione del server di directory, le impostazioni dei privilegi e le mappature dei ruoli vengono rimosse. Gli utenti non possono più accedere con le credenziali di questo server.

Usa SAML

Configura SAML in SANtricity Unified Manager

Per configurare l'autenticazione per Access Management, puoi utilizzare le funzionalità di Security Assertion Markup Language (SAML) integrate nell'array di storage. Questa configurazione stabilisce una connessione tra un Identity Provider e lo Storage Provider.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- È necessario conoscere l'indirizzo IP o domain name del controller nell'array di storage.
- Un amministratore IdP ha configurato un sistema IdP.
- Un amministratore dell'IdP ha verificato che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.
- Un amministratore ha verificato che l'orologio del server IdP e quello del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni dell'orologio del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP ed è disponibile sul sistema locale utilizzato per accedere a Unified Manager.

Informazioni su questa attività

Un Identity Provider (IdP) è un sistema esterno utilizzato per richiedere le credenziali a un utente e per determinare se quell'utente è stato autenticato con successo. L'IdP può essere configurato per fornire l'autenticazione a più fattori e per utilizzare qualsiasi database utente, come Active Directory. Il team di sicurezza è responsabile della manutenzione dell'IdP. Un Service Provider (SP) è un sistema che controlla l'autenticazione e l'accesso degli utenti. Quando Access Management è configurato con SAML, l'array di storage agisce come Service Provider per richiedere l'autenticazione all'Identity Provider. Per stabilire una connessione tra l'IdP e l'array di storage, si condividono i file di metadati tra queste due entità. Successivamente, si mappano le entità utente dell'IdP ai ruoli dell'array di storage. E infine, si testa la connessione e gli accessi SSO prima di abilitare SAML.

SAML e Directory Services. Se si abilita SAML quando Directory Services è configurato come metodo di autenticazione, SAML ha la precedenza su Directory Services in Unified Manager. Se in seguito si disabilita SAML, la configurazione di Directory Services torna alla configurazione precedente.

Modifica e disabilitazione. Una volta abilitato SAML, *non* è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

La configurazione dell'autenticazione SAML è una procedura in più fasi.

Passaggio 1: Carica il file dei metadati IdP

Per fornire all'array di storage le informazioni di connessione all'IdP, è necessario importare i metadati IdP in Unified Manager. Il sistema IdP necessita di questi metadati per reindirizzare le richieste di autenticazione all'URL corretto e per convalidare le risposte ricevute.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.

   La pagina mostra una panoramica dei passaggi di configurazione.

3. Fai clic sul collegamento **Import Identity Provider (IdP) file**.

   Si apre la finestra di dialogo Import Identity Provider File.

4. Fai clic su **Sfoglia** per selezionare e caricare il file di metadati dell'IdP che hai copiato sul tuo sistema locale.

   Dopo aver selezionato il file, viene visualizzato l'IdP Entity ID.

5. Fai clic su **Import**.

Passaggio 2: Esporta i file del Service Provider

Per stabilire una relazione di fiducia tra l'IdP e l'array di storage, è necessario importare i metadati del Service Provider nell'IdP. L'IdP necessita di questi metadati per stabilire una relazione di fiducia con il controller e per elaborare le richieste di autorizzazione. Il file include informazioni quali il domain name del controller o l'indirizzo IP, in modo che l'IdP possa comunicare con i Service Provider.

Passaggi

1. Fai clic sul collegamento **Export Service Provider files**.

   Si apre la finestra di dialogo Export Service Provider Files.

2. Inserisci l'indirizzo IP del controller o il nome DNS nel campo **Controller A**, quindi fai clic su **Esporta** per salvare il file di metadati sul tuo sistema locale.

   Dopo aver fatto clic su **Esporta**, i metadati del Service Provider vengono scaricati sul sistema locale. Prendi nota della posizione in cui viene salvato il file.

3. Dal sistema locale, individua il file di metadati del Service Provider in formato XML che hai esportato.
4. Dal server IdP, importa il file di metadati del Service Provider per stabilire la relazione di fiducia. Puoi importare il file direttamente oppure inserire manualmente le informazioni del controller dal file.

Passaggio 3: Mappa i ruoli

Per fornire agli utenti l'autorizzazione e l'accesso a Unified Manager, è necessario mappare gli attributi utente dell'IdP e le appartenenze ai gruppi ai ruoli predefiniti dello storage array.

Prima di iniziare

- Un amministratore dell'IdP ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- Il file dei metadati IdP viene importato in Unified Manager.
- Un file di metadati del Service Provider per il controller viene importato nel sistema IdP per la relazione di fiducia.

Passaggi

1. Fai clic sul collegamento per **mappare i ruoli di Unified Manager**.

   Si apre la finestra di dialogo Role Mapping.

2. Assegna attributi e gruppi utente dell'IdP ai ruoli predefiniti. A un gruppo possono essere assegnati più ruoli.

Dettagli del campo

Impostazione	Descrizione
Mappature	Attributo utente
Specificare l'attributo (ad esempio, "member of") per il gruppo SAML da mappare.	Valore attributo
Specificare il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (\ ) se non fanno parte di un modello di espressione regolare: \.[]{}()<>*+-=!?^$	
Ruoli	Fai clic nel campo e seleziona uno dei ruoli dell'array di storage da associare all'Attribute. Devi selezionare singolarmente ogni ruolo che desideri includere. Il ruolo Monitor è necessario in combinazione con gli altri ruoli per accedere a Unified Manager. Il ruolo Security Admin è inoltre necessario per almeno un gruppo. I ruoli mappati includono le seguenti autorizzazioni: • **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage (ad esempio, volumi e pool di dischi), ma nessun accesso alla configurazione di sicurezza. • **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management, gestione certificati, gestione audit log e possibilità di attivare o disattivare l'interfaccia di gestione legacy (SYMbol). • **Support admin** — Accesso a tutte le risorse hardware sull'array di storage, ai dati di errore, agli eventi MEL e agli aggiornamenti del firmware del controller. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza. • **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

3. Se lo desideri, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.

Le mappature dei ruoli possono essere modificate dopo che SAML è stato abilitato.

4. Quando hai terminato con le mappature, fai clic su **Salva**.

Passaggio 4: Test SSO login

Per garantire che il sistema IdP e l'array di storage possano comunicare, è possibile testare facoltativamente un accesso SSO. Questo test viene eseguito anche durante la fase finale per l'abilitazione di SAML.

Prima di iniziare

- Il file dei metadati IdP viene importato in Unified Manager.
- Un file di metadati del Service Provider per il controller viene importato nel sistema IdP per la relazione di fiducia.

Passaggi

1. Seleziona il link **Test SSO Login**.

   Si apre una finestra di dialogo per l'inserimento delle credenziali SSO.

2. Inserisci le credenziali di accesso per un utente con autorizzazioni sia di Security Admin sia di Monitor.

   Si apre una finestra di dialogo mentre il sistema verifica l'accesso.

3. Cerca un messaggio Test Successful. Se il test viene completato con successo, passa al passaggio successivo per abilitare SAML.

   Se il test non viene completato correttamente, viene visualizzato un messaggio di errore con ulteriori informazioni. Assicurarsi che:

   - L'utente appartiene a un gruppo con autorizzazioni per Security Admin e Monitor.
   - I metadati che hai caricato per il server IdP sono corretti.
   - L'indirizzo del controller nei file di metadati SP è corretto.

Passaggio 5: Abilita SAML

L'ultimo passaggio consiste nel completare la configurazione SAML per l'autenticazione degli utenti. Durante questo processo, il sistema richiede anche di testare un accesso SSO. La procedura di test dell'accesso SSO è descritta nel passaggio precedente.

Prima di iniziare

- Il file dei metadati IdP viene importato in Unified Manager.
- Un file di metadati del Service Provider per il controller viene importato nel sistema IdP per la relazione di fiducia.
- È configurata almeno una mappatura dei ruoli di Monitor e di Security Admin.

Modifica e disabilitazione. Una volta abilitato SAML, *non* è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza.

Passaggi

1. Dalla scheda **SAML**, selezionare il collegamento **Enable SAML**.

   Si apre la finestra di dialogo Conferma abilitazione SAML.

2. Digita `enable`, quindi fai clic su **Enable**.
3. Inserisci le credenziali utente per un test di login SSO.

Risultati

Dopo che il sistema abilita SAML, termina tutte le sessioni attive e inizia ad autenticare gli utenti tramite SAML.

Modificare le mappature dei ruoli SAML in SANtricity Unified Manager

Se in precedenza hai configurato SAML per Access Management, puoi modificare le mappature dei ruoli tra i gruppi IdP e i ruoli predefiniti dell'array di storage.

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- Un amministratore dell'IdP ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- SAML è configurato e abilitato.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.
3. Seleziona **Mappatura dei ruoli**.

   Si apre la finestra di dialogo Role Mapping.

4. Assegna attributi e gruppi utente dell'IdP ai ruoli predefiniti. A un gruppo possono essere assegnati più ruoli.

   Assicurati di non rimuovere le tue autorizzazioni mentre SAML è attivo, altrimenti perderai l'accesso a Unified Manager.

Dettagli del campo

Impostazione	Descrizione
Mappature	Attributo utente
Specificare l'attributo (ad esempio, "member of") per il gruppo SAML da mappare.	Valore attributo
Specificare il valore dell'attributo per il gruppo da mappare.	Ruoli

Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

5. Facoltativamente, fai clic su **Aggiungi un'altra mappatura** per inserire ulteriori mappature gruppo-ruolo.
6. Fare clic su **Save**.

Risultati

Dopo aver completato questa operazione, tutte le sessioni utente attive verranno terminate. Solo la sessione utente corrente verrà mantenuta.

Esporta i file Service Provider SAML in SANtricity Unified Manager

Se necessario, è possibile esportare i metadati del Service Provider per l'array di archiviazione e reimportare il file nel sistema dell'Identity Provider (IdP).

Prima di iniziare

- È necessario aver effettuato l'accesso con un profilo utente che includa le autorizzazioni di Security admin. In caso contrario, le funzioni di Access Management non vengono visualizzate.
- SAML è configurato e abilitato.

Informazioni su questa attività

In questa attività, si esportano i metadati dal controller. L'IdP necessita di questi metadati per stabilire una relazione di fiducia con il controller e per elaborare le richieste di autenticazione. Il file include informazioni come il domain name o l'indirizzo IP del controller che l'IdP può utilizzare per inviare le richieste.

Passaggi

1. Selezionare **Settings › Access Management**.
2. Seleziona la scheda **SAML**.
3. Seleziona **Export**.

   Si apre la finestra di dialogo Export Service Provider Files.

4. Fai clic su **Esporta** per salvare il file di metadati sul tuo sistema locale.

Il campo domain name è di sola lettura.

Prendi nota di dove è memorizzato il file.

5. Dal sistema locale, individua il file di metadati del Service Provider in formato XML che hai esportato.
6. Dal server IdP, importa il file di metadati del Service Provider. Puoi importare il file direttamente oppure inserire manualmente le informazioni del controller.
7. Fare clic su **Close**.

Domande frequenti sulla gestione degli accessi utente per SANtricity Unified Manager

Questa FAQ può esserti utile se stai cercando una risposta rapida a una domanda.

Perché non posso accedere?

Se ricevi un errore durante il tentativo di accesso, verifica queste possibili cause.

Gli errori di accesso possono verificarsi per uno dei seguenti motivi:

- Hai inserito un nome utente o una password errati.
- Non disponi di privilegi sufficienti.
- Hai tentato di accedere senza successo più volte, il che ha attivato la modalità di blocco. Attendi 10 minuti per accedere nuovamente.
- L'autenticazione SAML è abilitata. Aggiorna il browser per accedere.

Cosa devo sapere prima di aggiungere un server di directory?

Prima di aggiungere un server di directory in Access Management, è necessario soddisfare determinati requisiti.

- I gruppi di utenti devono essere definiti nel servizio di directory.
- Le credenziali dell'LDAP server devono essere disponibili, inclusi il domain name, l'URL del server e, facoltativamente, il nome utente e la password dell'account di bind.
- Per i server LDAPS che utilizzano un protocollo sicuro, la catena di certificati del LDAP server deve essere installata sul computer locale.

Cosa devo sapere sulla mappatura ai ruoli degli array di storage?

Prima di associare i gruppi ai ruoli, rivedere le linee guida.

Le funzionalità RBAC (role-based access control) includono i seguenti ruoli:

- **Amministratore dello storage** — Accesso completo in lettura/scrittura agli oggetti di storage sugli array, ma nessun accesso alla configurazione della sicurezza.
- **Amministratore della sicurezza** — Accesso alla configurazione della sicurezza in Access Management e Certificate Management.
- **Support admin** — Accesso a tutte le risorse hardware sugli array di storage, ai dati di errore e agli eventi MEL. Nessun accesso agli oggetti di storage o alla configurazione di sicurezza.

- **Monitor** — Accesso in sola lettura a tutti gli oggetti di archiviazione, ma nessun accesso alla configurazione di sicurezza.

> Il ruolo Monitor è obbligatorio per tutti gli utenti, incluso l'amministratore.

Se si utilizza un server LDAP (Lightweight Directory Access Protocol) e Directory Services, assicurarsi che:

- Un amministratore ha definito i gruppi di utenti nel servizio di directory.
- Conosci i domain name dei gruppi per i gruppi di utenti LDAP.

SAML

Se si utilizzano le funzionalità Security Assertion Markup Language (SAML) incorporate nell'array di storage, assicurarsi che:

- Un amministratore del provider di identità (IdP) ha configurato gli attributi utente e l'appartenenza ai gruppi nel sistema IdP.
- Conosci i nomi dei gruppi di appartenenza.
- Conosci il valore dell'attributo per il gruppo da mappare. Sono supportate le espressioni regolari. Questi caratteri speciali delle espressioni regolari devono essere preceduti da una barra rovesciata (`\` se non fanno parte di un modello di espressione regolare:

```
\.[]{}()<>*+-=!?^$|
```

- Il ruolo Monitor è richiesto per tutti gli utenti, incluso l'amministratore. Unified Manager non funzionerà correttamente per nessun utente senza il ruolo Monitor.

Cosa devo sapere prima di configurare e abilitare SAML?

Prima di configurare e abilitare le funzionalità Security Assertion Markup Language (SAML) per l'autenticazione, assicurati di soddisfare i seguenti requisiti e di comprendere le restrizioni SAML.

Requisiti

Prima di iniziare, assicurati che:

- Un Identity Provider (IdP) è configurato nella tua rete. Un IdP è un sistema esterno utilizzato per richiedere le credenziali a un utente e determinare se l'utente è stato autenticato con successo. Il tuo team di sicurezza è responsabile della manutenzione dell'IdP.
- Un amministratore IdP ha configurato gli attributi utente e i gruppi nel sistema IdP.
- Un amministratore dell'IdP ha verificato che l'IdP supporti la possibilità di restituire un Name ID al momento dell'autenticazione.
- Un amministratore ha verificato che l'orologio del server IdP e quello del controller siano sincronizzati (tramite un server NTP o regolando le impostazioni dell'orologio del controller).
- Un file di metadati IdP viene scaricato dal sistema IdP e reso disponibile sul sistema locale utilizzato per accedere a Unified Manager.
- Conosci l'indirizzo IP o il domain name del controller nell'array di storage.

Restrizioni

Oltre ai requisiti sopra indicati, assicurati di comprendere le seguenti restrizioni:

- Una volta abilitato SAML, non è possibile disabilitarlo tramite l'interfaccia utente, né modificare le impostazioni dell'IdP. Se è necessario disabilitare o modificare la configurazione SAML, contattare Technical Support per assistenza. Si consiglia di testare gli accessi SSO prima di abilitare SAML nella fase finale della configurazione. (Il sistema esegue anche un test di accesso SSO prima di abilitare SAML.)
- Se in futuro si disabilita SAML, il sistema ripristina automaticamente la configurazione precedente (Local User Roles e/o Directory Services).
- Se Directory Services sono attualmente configurati per l'autenticazione degli utenti, SAML sovrascrive tale configurazione.
- Quando SAML è configurato, i seguenti client non possono accedere alle risorse dello storage array:
  - Enterprise Management Window (EMW)
  - Interfaccia a riga di comando (CLI)
  - Client dei Software Developer Kits (SDK)
  - Clienti in banda
  - Client REST API con autenticazione HTTP Basic
  - Accedi utilizzando l'endpoint REST API standard

Quali sono gli utenti locali?

Gli utenti locali sono predefiniti nel sistema e includono autorizzazioni specifiche.

Gli utenti locali includono:

- **admin** — Super amministratore con accesso a tutte le funzioni del sistema. Questo utente include tutti i ruoli. La password deve essere impostata al primo accesso.
- **storage** — L'amministratore responsabile di tutto il provisioning dello storage. Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account è disabilitato finché non viene impostata una password.
- **sicurezza** — L'utente responsabile della configurazione della sicurezza, inclusi Access Management e Certificate Management. Questo utente include i seguenti ruoli: Security Admin e Monitor. Questo account è disabilitato finché non viene impostata una password.
- **support** — L'utente responsabile delle risorse hardware, dei dati relativi ai guasti e degli aggiornamenti del firmware. Questo utente include i seguenti ruoli: Support Admin e Monitor. Questo account è disabilitato finché non viene impostata una password.
- **monitor** — Un utente con accesso di sola lettura al sistema. Questo utente include solo il ruolo Monitor. Questo account è disabilitato finché non viene impostata una password.
- **rw** (lettura/scrittura) — Questo utente include i seguenti ruoli: Storage Admin, Support Admin e Monitor. Questo account è disabilitato finché non viene impostata una password.
- **ro** (sola lettura) — Questo utente include solo il ruolo Monitor. Questo account è disabilitato finché non viene impostata una password.

Versioni precedenti

Consulta i link sottostanti per accedere alla documentazione relativa alle versioni precedenti dell'hardware E-Series e del software SANtricity. I link ti condurranno a un sito di documentazione diverso.

Documentazione hardware per le versioni precedenti

- "Installare i controller-drive trays E2712, E2724, E5612, E5624 e i DE1600 e DE5600 expansion drive trays"
- "Installa i vassoi controller-drive E2760 ed E5660 e i vassoi di espansione drive DE6600"
- "Installare gli array flash EF560 e i vassoi di espansione flash DE5600"
- "Installare sistemi meno recenti"
- "Mantieni i sistemi più vecchi"
- "Aggiungere un secondo controller a E2600 e E2700"
- "Modificare o aggiungere protocolli host"
- "Convertire da corrente alternata (CA) a corrente continua (CC)"
- "Guida all'aggiornamento del controller - Legacy controller models"

Documentazione software per le versioni precedenti

SANtricity Release 11.8

- "Guida di System Manager"
- "Guida di Unified Manager"

SANtricity Release 11.7

- "Guida di System Manager"
- "Guida di Unified Manager"

SANtricity Release 11.6

- "Guida di System Manager"
- "Guida di Unified Manager"

SANtricity Release 11.5

- "Guida di System Manager"

SANtricity Release 11.4

- "AMW (E2700, E5600/EF560) assistenza"
- "Guida EMW (E2700, E5600/EF560)"

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi, brevetti e altro.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi di NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono 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

Informativa sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp.

"Avviso per E-Series/EF-Series SANtricity OS"

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.