Gestisci lo storage con il software Element

Element Software

NetApp
November 12, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software-128/storage/index.html on November 12, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestisci lo storage con il software Element

Gestisci lo storage con il software Element

Utilizza il software Element per configurare l'archiviazione SolidFire , monitorare la capacità e le prestazioni del cluster e gestire l'attività di archiviazione in un'infrastruttura multi-tenant.

Element è il sistema operativo di archiviazione al centro di un cluster SolidFire . Il software Element viene eseguito in modo indipendente su tutti i nodi del cluster e consente ai nodi del cluster di combinare le risorse e di presentarsi come un unico sistema di archiviazione ai client esterni. Element Software è responsabile del coordinamento, della scalabilità e della gestione del cluster nel suo complesso.

L'interfaccia software è basata sull'API Element.

- "Accedi all'interfaccia utente del software Element"
- "Configurare le opzioni del sistema SolidFire dopo la distribuzione"
- "Aggiornare i componenti del sistema di archiviazione"
- "Utilizzare le opzioni di base nell'interfaccia utente del software Element"
- "Gestire gli account"
- "Gestisci il tuo sistema"
- "Gestire volumi e volumi virtuali"
- "Proteggi i tuoi dati"
- "Risolvi i problemi del tuo sistema"

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Accedi all'interfaccia utente del software Element

È possibile accedere all'interfaccia utente di Element utilizzando l'indirizzo IP virtuale di gestione (MVIP) del nodo del cluster primario.

Devi assicurarti che i blocchi popup e le impostazioni NoScript siano disattivati nel tuo browser.

È possibile accedere all'interfaccia utente utilizzando l'indirizzamento IPv4 o IPv6, a seconda della configurazione effettuata durante la creazione del cluster.

1. Scegli una delle seguenti opzioni:
   - IPv6: immettere https://[indirizzo IPv6 MVIP] Ad esempio:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

- IPv4: immettere https://[indirizzo IPv4 MVIP] Ad esempio:

```
https://10.123.456.789/
```

2. Per DNS, immettere il nome host.
3. Fare clic su tutti i messaggi del certificato di autenticazione.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Dopo aver configurato il sistema SolidFire , potresti voler eseguire alcune attività facoltative.

Se modifichi le credenziali nel sistema, potresti voler conoscere l'impatto sugli altri componenti.

Inoltre, è possibile configurare le impostazioni per l'autenticazione a più fattori, la gestione delle chiavi esterne e la sicurezza FIPS (Federal Information Processing Standards). Dovresti anche aggiornare le password quando necessario.

Trova maggiori informazioni

- "Modificare le credenziali in NetApp HCI e NetApp SolidFire"
- "Cambia il certificato SSL predefinito del software Element"
- "Cambia la password IPMI per i nodi"
- "Abilita l'autenticazione a più fattori"
- "Inizia con la gestione delle chiavi esterne"
- "Creare un cluster che supporti le unità FIPS"

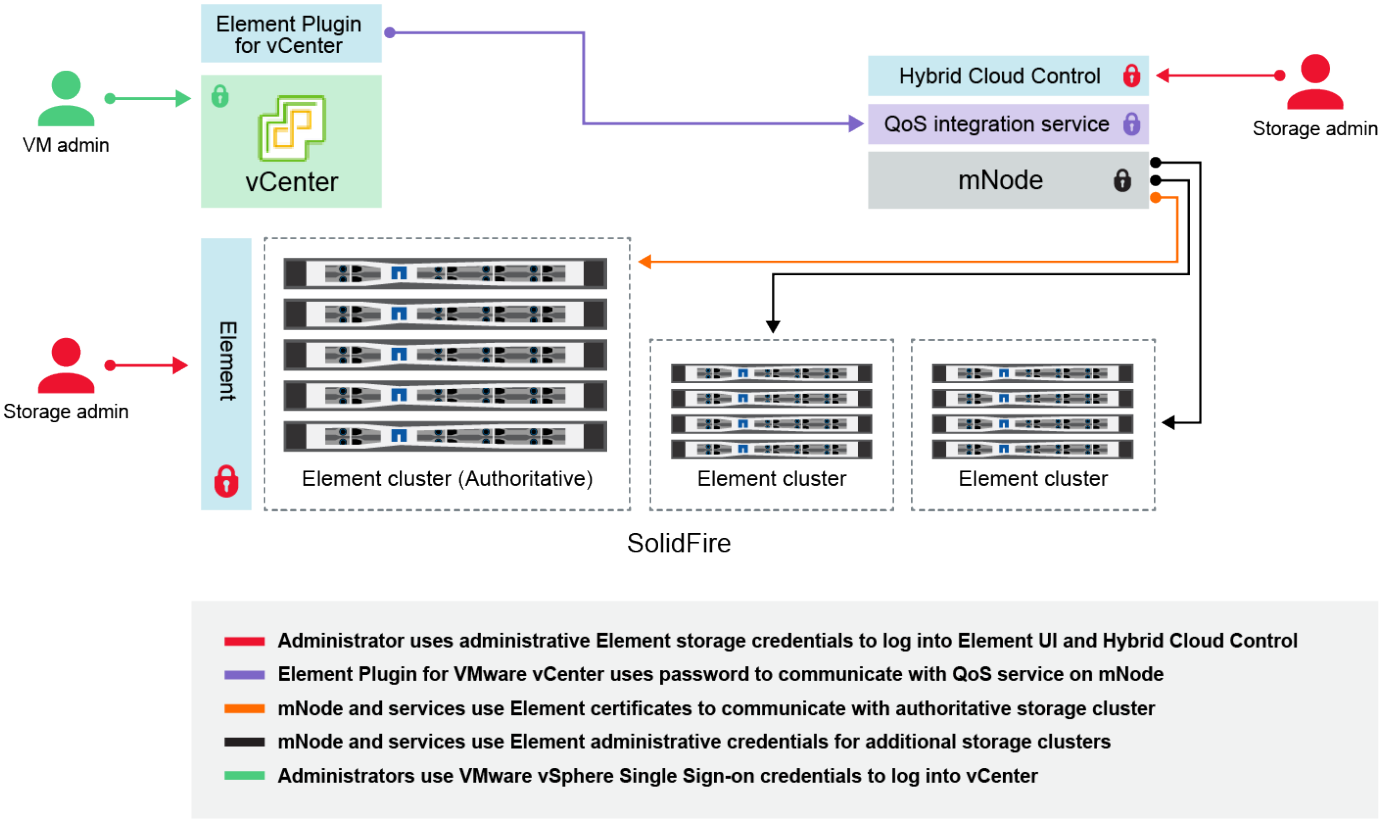
Modificare le credenziali in NetApp HCI e NetApp SolidFire

A seconda delle policy di sicurezza dell'organizzazione che ha implementato NetApp HCI o NetApp SolidFire, la modifica delle credenziali o delle password rientra solitamente nelle pratiche di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nella distribuzione.

Se si modificano le credenziali per un componente di una distribuzione NetApp HCI o NetApp SolidFire , la tabella seguente fornisce indicazioni sull'impatto sugli altri componenti.

Interazioni dei componenti NetApp SolidFire

:



Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali dell'elemento	**Si applica a**: NetApp HCI e SolidFire Gli amministratori utilizzano queste credenziali per accedere a: • Interfaccia utente Element sul cluster di archiviazione Element • Controllo del cloud ibrido sul nodo di gestione (mnode) Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noti come *cluster autorevole* per cui il mnode è stato inizialmente configurato. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se vengono modificate le credenziali per i cluster di archiviazione aggiunti successivamente, è necessario aggiornarle anche nel mnode utilizzando l'API mnode.	• "Aggiornare le password di amministrazione del cluster di archiviazione." • Aggiornare le credenziali di amministratore del cluster di archiviazione nel mnode utilizzando"API di modifica cluster admin" .

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali vSphere Single Sign-on 	**Si applica a**: solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI , le credenziali vengono configurate in NetApp Deployment Engine come segue: • username@vsphere.local con la password specificata e • administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per distribuire NetApp HCI, le credenziali di vSphere Single Sign-on vengono gestite dagli amministratori IT VMware.	"Aggiorna le credenziali vCenter ed ESXi".
Credenziali del controller di gestione della scheda madre (BMC) 	**Si applica a**: solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di elaborazione NetApp in una distribuzione NetApp HCI . BMC fornisce funzionalità di monitoraggio hardware di base e di console virtuale. Le credenziali BMC (talvolta denominate *IPMI*) per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni NetApp HCI . NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con il BMC nei nodi di elaborazione durante gli aggiornamenti del firmware dei nodi di elaborazione. Quando si modificano le credenziali BMC , è necessario aggiornare anche le credenziali per i rispettivi nodi di elaborazione sul nodo m per mantenere tutte le funzionalità di Hybrid Cloud Control.	• "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C,"cambiare la password IPMI predefinita" . • Per i nodi H410S e H610S,"cambia la password IPM predefinita" . • "Modificare le credenziali BMC sul nodo di gestione".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali ESXi 	**Si applica a**: solo NetApp HCI Gli amministratori possono accedere agli host ESXi tramite SSH o tramite la DCUI locale con un account root locale. Nelle distribuzioni NetApp HCI , il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione in NetApp Deployment Engine. Le credenziali root ESXi per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni NetApp HCI . NetApp Hybrid Cloud Control utilizza le credenziali in una capacità di account di servizio per comunicare direttamente con gli host ESXi durante gli aggiornamenti del firmware del nodo di elaborazione e i controlli di integrità. Quando le credenziali di root ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di elaborazione devono essere aggiornate sul mnode per mantenere la funzionalità Hybrid Cloud Control.	"Aggiornare le credenziali per gli host vCenter ed ESXi".
Password di integrazione QoS 	**Si applica a**: NetApp HCI e facoltativo in SolidFire Non utilizzato per accessi interattivi da parte degli amministratori. L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite: • Plug-in Element per vCenter Server e • Servizio QoS sul mnode. Per l'autenticazione, il servizio QoS utilizza una password utilizzata esclusivamente in questo contesto. La password QoS viene specificata durante l'installazione iniziale del plug-in Element per vCenter Server oppure generata automaticamente durante la distribuzione di NetApp HCI . Nessun impatto sugli altri componenti.	"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server". La password SIOC del plug-in NetApp Element per vCenter Server è nota anche come *password QoSSIOC*. Consultare l'articolo della Knowledge Base sul plug-in Element per vCenter Server.

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali di vCenter Service Applianc e 	**Si applica a**: NetApp HCI solo se configurato da NetApp Deployment Engine Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle distribuzioni NetApp HCI , il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione nel NetApp Deployment Engine. A seconda della versione di VMware vSphere distribuita, anche alcuni amministratori nel dominio vSphere Single Sign-on possono accedere all'appliance. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.
Credenziali di amministratore del nodo di gestione NetApp 	**Si applica a**: NetApp HCI e facoltativo in SolidFire Gli amministratori possono accedere alle macchine virtuali del nodo di gestione NetApp per la configurazione avanzata e la risoluzione dei problemi. A seconda della versione del nodo di gestione implementata, l'accesso tramite SSH non è abilitato per impostazione predefinita. Nelle distribuzioni NetApp HCI , il nome utente e la password venivano specificati dall'utente durante l'installazione iniziale del nodo di elaborazione in NetApp Deployment Engine. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.

Trova maggiori informazioni

- "Cambia il certificato SSL predefinito del software Element"
- "Cambia la password IPMI per i nodi"
- "Abilita l'autenticazione a più fattori"
- "Inizia con la gestione delle chiavi esterne"
- "Creare un cluster che supporti le unità FIPS"

Cambia il certificato SSL predefinito del software Element

È possibile modificare il certificato SSL predefinito e la chiave privata del nodo di archiviazione nel cluster utilizzando l'API NetApp Element .

Quando viene creato un cluster software NetApp Element , il cluster crea un certificato Secure Sockets Layer (SSL) autofirmato univoco e una chiave privata che vengono utilizzati per tutte le comunicazioni HTTPS tramite l'interfaccia utente Element, l'interfaccia utente per nodo o le API. Il software Element supporta sia i certificati autofirmati sia i certificati emessi e verificati da un'autorità di certificazione (CA) attendibile.

È possibile utilizzare i seguenti metodi API per ottenere maggiori informazioni sul certificato SSL predefinito e

apportare modifiche.

- **OttieniCertificatoSSL**

  Puoi usare il"Metodo GetSSLCertificate" per recuperare informazioni sul certificato SSL attualmente installato, compresi tutti i dettagli del certificato.

- **SetSSLCertificate**

  Puoi usare il"Metodo SetSSLCertificate" per impostare i certificati SSL del cluster e per nodo sul certificato e sulla chiave privata forniti. Il sistema convalida il certificato e la chiave privata per impedire che venga applicato un certificato non valido.

- **RimuoviCertificatoSSL**

  IL"Metodo RemoveSSLCertificate" rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una chiave privata.

> Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Qualsiasi nodo rimosso dal cluster torna a essere un certificato autofirmato e tutte le informazioni sui certificati e sulle chiavi definite dall'utente vengono rimosse dal nodo.

Trova maggiori informazioni

- "Modificare il certificato SSL predefinito del nodo di gestione"
- "Quali sono i requisiti per l'impostazione di certificati SSL personalizzati in Element Software?"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Cambia la password IPMI predefinita per i nodi

È possibile modificare la password predefinita dell'amministratore dell'Intelligent Platform Management Interface (IPMI) non appena si ottiene l'accesso IPMI remoto al nodo. Potrebbe essere opportuno farlo se ci sono aggiornamenti di installazione.

Per i dettagli sulla configurazione dell'accesso IPM per i nodi, vedere"Configurare IPMI per ogni nodo" .

È possibile modificare la password IPM per questi nodi:

- Nodi H410S
- Nodi H610S

Modificare la password IPMI predefinita per i nodi H410S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `ADMIN` e password `ADMIN` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, fare clic sulla scheda **Configurazione**.
4. Fare clic su **Utenti**.
5. Seleziona il `ADMIN` utente e fare clic su **Modifica utente**.
6. Selezionare la casella di controllo **Cambia password**.
7. Inserisci una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modifica**, quindi su **OK**.
9. Ripetere questa procedura per tutti gli altri nodi H410S con password IPMI predefinite.

Modificare la password IPMI predefinita per i nodi H610S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `root` e password `calvin` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, clicca sull'icona di navigazione del menu in alto a sinistra della pagina per aprire il cassetto della barra laterale.
4. Fare clic su **Impostazioni**.
5. Fare clic su **Gestione utenti**.
6. Selezionare l'utente **Amministratore** dall'elenco.
7. Abilitare la casella di controllo **Cambia password**.
8. Inserisci una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Salva** in fondo alla pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Utilizzare le opzioni di base nell'interfaccia utente del software Element

Utilizzare le opzioni di base nell'interfaccia utente del software Element

L'interfaccia utente Web del software NetApp Element (Element UI) consente di monitorare ed eseguire attività comuni sul sistema SolidFire .

Le opzioni di base includono la visualizzazione dei comandi API attivati dall'attività dell'interfaccia utente e la fornitura di feedback.

- "Visualizza l'attività API"
- "Icone nell'interfaccia Element"
- "Fornire feedback"

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Attività API

Visualizza l'attività API

Il sistema Element utilizza l'API NetApp Element come base per le sue caratteristiche e funzionalità. L'interfaccia utente Element consente di visualizzare vari tipi di attività API in tempo reale sul sistema mentre si utilizza l'interfaccia. Grazie al registro API, puoi visualizzare l'attività API di sistema avviata dall'utente e in background, nonché le chiamate API effettuate sulla pagina che stai visualizzando.

È possibile utilizzare il registro API per identificare quali metodi API vengono utilizzati per determinate attività e vedere come utilizzare i metodi e gli oggetti API per creare applicazioni personalizzate.

Per informazioni su ciascun metodo, vedere "Riferimento API di Element Software".

1. Dalla barra di navigazione dell'interfaccia utente dell'elemento, fare clic su **Registro API**.
2. Per modificare il tipo di attività API visualizzata nella finestra Registro API, procedere come segue:
   a. Selezionare **Richieste** per visualizzare il traffico delle richieste API.
   b. Selezionare **Risposte** per visualizzare il traffico di risposta API.
   c. Filtra i tipi di traffico API selezionando una delle seguenti opzioni:
      - **Avviato dall'utente**: traffico API generato dalle tue attività durante questa sessione dell'interfaccia utente web.
      - **Background Polling**: traffico API generato dall'attività del sistema in background.
      - **Pagina corrente**: traffico API generato dalle attività sulla pagina che stai visualizzando.

Trova maggiori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Frequenza di aggiornamento dell'interfaccia influenzata dal carico del cluster

A seconda dei tempi di risposta dell'API, il cluster potrebbe regolare automaticamente l'intervallo di aggiornamento dei dati per determinate parti della pagina del software NetApp Element visualizzata.

L'intervallo di aggiornamento viene ripristinato al valore predefinito quando si ricarica la pagina nel browser. È possibile visualizzare l'intervallo di aggiornamento corrente facendo clic sul nome del cluster nell'angolo in alto a destra della pagina. Si noti che l'intervallo controlla la frequenza con cui vengono effettuate le richieste API, non la rapidità con cui i dati vengono restituiti dal server.

Quando un cluster è sottoposto a un carico elevato, potrebbe mettere in coda le richieste API dall'interfaccia utente di Element. In rare circostanze, quando la risposta del sistema subisce un ritardo significativo, ad esempio a causa di una connessione di rete lenta combinata con un cluster occupato, è possibile che si venga disconnessi dall'interfaccia utente di Element se il sistema non risponde alle richieste API in coda con sufficiente rapidità. Se vieni reindirizzato alla schermata di disconnessione, puoi effettuare nuovamente l'accesso dopo aver ignorato la richiesta iniziale di autenticazione del browser. Una volta tornati alla pagina di panoramica, potrebbero venirti richieste le credenziali del cluster se non sono state salvate dal tuo browser.

Icone nell'interfaccia Element

L'interfaccia del software NetApp Element visualizza icone che rappresentano le azioni che è possibile intraprendere sulle risorse di sistema.

La seguente tabella fornisce un rapido riferimento:

Icona	Descrizione
	Azioni
	Backup su
	Clona o copia
	Elimina o elimina
	Modificare
	Filtro
	Paio

	Aggiorna
	Ripristinare
	Ripristina da
	Ripristino
	Istantanea

Fornire feedback

Puoi contribuire a migliorare l'interfaccia utente web del software Element e risolvere eventuali problemi dell'interfaccia utente utilizzando il modulo di feedback accessibile in tutta l'interfaccia utente.

1. Da qualsiasi pagina dell'interfaccia utente di Element, fare clic sul pulsante **Feedback**.
2. Inserisci le informazioni rilevanti nei campi Riepilogo e Descrizione.
3. Allega eventuali screenshot utili.
4. Inserisci un nome e un indirizzo email.
5. Seleziona la casella di controllo per includere i dati relativi al tuo ambiente attuale.
6. Fare clic su **Invia**.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestire gli account

Gestire gli account

Nei sistemi di archiviazione SolidFire , i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi su un cluster. Quando si crea un volume, questo viene assegnato a un account specifico. È anche possibile gestire gli account degli amministratori del cluster per un sistema di archiviazione SolidFire .

- "Lavorare con gli account utilizzando CHAP"
- "Gestire gli account utente dell'amministratore del cluster"

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Lavorare con gli account utilizzando CHAP

Nei sistemi di archiviazione SolidFire , i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi su un cluster. Un account contiene l'autenticazione CHAP (Challenge-Handshake Authentication Protocol) necessaria per accedere ai volumi a esso assegnati. Quando si crea un volume, questo viene assegnato a un account specifico.

A un account possono essere assegnati fino a duemila volumi, ma un volume può appartenere a un solo account.

Algoritmi CHAP

A partire da Element 12.7, sono supportati gli algoritmi CHAP sicuri conformi a FIPS SHA1, SHA-256 e SHA3-256. Quando un iniziatore iSCSI host crea una sessione iSCSI con un target iSCSI Element, richiede un elenco di algoritmi CHAP da utilizzare. La destinazione Element iSCSI sceglie il primo algoritmo supportato dall'elenco richiesto dall'iniziatore iSCSI host. Per confermare che la destinazione Element iSCSI scelga l'algoritmo più sicuro, è necessario configurare l'iniziatore iSCSI host per inviare un elenco di algoritmi ordinati dal più sicuro, ad esempio SHA3-256, al meno sicuro, ad esempio SHA1 o MD5. Quando gli algoritmi SHA non vengono richiesti dall'iniziatore iSCSI host, la destinazione iSCSI Element sceglie MD5, presupponendo che l'elenco degli algoritmi proposti dall'host contenga MD5. Potrebbe essere necessario aggiornare la configurazione dell'iniziatore iSCSI dell'host per abilitare il supporto per gli algoritmi sicuri.

Durante un aggiornamento a Element 12.7 o versione successiva, se è già stata aggiornata la configurazione dell'iniziatore iSCSI host per inviare una richiesta di sessione con un elenco che include algoritmi SHA, quando i nodi di archiviazione si riavviano, i nuovi algoritmi sicuri vengono attivati e vengono stabilite sessioni iSCSI nuove o riconnesse utilizzando il protocollo più sicuro. Durante l'aggiornamento, tutte le sessioni iSCSI esistenti passano da MD5 a SHA. Se non si aggiorna la configurazione dell'iniziatore iSCSI host per richiedere SHA, le sessioni iSCSI esistenti continueranno a utilizzare MD5. In un secondo momento, dopo aver aggiornato gli algoritmi CHAP dell'iniziatore iSCSI host, le sessioni iSCSI dovrebbero passare gradualmente da MD5 a SHA nel tempo, in base alle attività di manutenzione che determinano la riconnessione delle sessioni iSCSI.

Ad esempio, l'iniziatore iSCSI host predefinito in Red Hat Enterprise Linux (RHEL) 8.3 ha `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` impostazione commentata, il che fa sì che l'iniziatore iSCSI utilizzi solo MD5. Rimuovendo il commento da questa impostazione sull'host e riavviando l'iniziatore iSCSI, le sessioni iSCSI da quell'host inizieranno a utilizzare SHA3-256.

Se necessario, è possibile utilizzare il "ElencoISCSISessioni" Metodo API per visualizzare gli algoritmi CHAP utilizzati per ogni sessione.

Creare un account

È possibile creare un account per consentire l'accesso ai volumi.

Ogni nome di account nel sistema deve essere univoco.

1. Selezionare **Gestione** > **Account**.

2. Fare clic su **Crea account**.
3. Inserisci un **Nome utente**.
4. Nella sezione **Impostazioni CHAP**, immettere le seguenti informazioni:

   Lasciare vuoti i campi delle credenziali per generare automaticamente una delle due password.

   - **Segreto dell'iniziatore** per l'autenticazione della sessione del nodo CHAP.
   - **Segreto di destinazione** per l'autenticazione della sessione del nodo CHAP.
5. Fare clic su **Crea account**.

Visualizza i dettagli dell'account

È possibile visualizzare l'attività di performance per singoli account in formato grafico.

Le informazioni del grafico forniscono informazioni su I/O e produttività per l'account. I livelli di attività media e massima vengono mostrati in incrementi di periodi di segnalazione di 10 secondi. Queste statistiche includono l'attività per tutti i volumi assegnati all'account.

1. Selezionare **Gestione** > **Account**.
2. Fare clic sull'icona Azioni per un account.
3. Fare clic su **Visualizza dettagli**.

Ecco alcuni dettagli:

- **Stato**: Lo stato dell'account. Valori possibili:
  - attivo: un account attivo.
  - bloccato: Un account bloccato.
  - rimosso: un account che è stato eliminato e ripulito.
- **Volumi attivi**: numero di volumi attivi assegnati all'account.
- **Compressione**: punteggio di efficienza della compressione per i volumi assegnati all'account.
- **Deduplicazione**: punteggio di efficienza della deduplicazione per i volumi assegnati all'account.
- **Thin Provisioning**: punteggio di efficienza del thin provisioning per i volumi assegnati all'account.
- **Efficienza complessiva**: punteggio di efficienza complessiva per i volumi assegnati all'account.

Modifica un account

È possibile modificare un account per cambiarne lo stato, cambiare i segreti CHAP o modificare il nome dell'account.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali modifiche alle impostazioni dell'iniziatore e del cluster.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **Account**.
2. Fare clic sull'icona Azioni per un account.
3. Nel menu che si apre, seleziona **Modifica**.
4. **Facoltativo:** modifica il **Nome utente**.
5. **Facoltativo:** fare clic sull'elenco a discesa **Stato** e selezionare uno stato diverso.

   Modificando lo stato in **bloccato**, tutte le connessioni iSCSI all'account vengono interrotte e l'account non è più accessibile. I volumi associati all'account vengono mantenuti; tuttavia, i volumi non sono rilevabili tramite iSCSI.

6. **Facoltativo:** in **Impostazioni CHAP**, modifica le credenziali **Segreto iniziatore** e **Segreto destinazione** utilizzate per l'autenticazione della sessione del nodo.

   Se non modifichi le credenziali **Impostazioni CHAP**, queste rimarranno invariate. Se si lasciano vuoti i campi delle credenziali, il sistema genera nuove password.

7. Fare clic su **Salva modifiche**.

Elimina un account

Puoi eliminare un account quando non ti serve più.

Eliminare e ripulire tutti i volumi associati all'account prima di eliminarlo.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **Account**.
2. Fare clic sull'icona Azioni relativa all'account che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestire gli account utente dell'amministratore del cluster

È possibile gestire gli account degli amministratori del cluster per un sistema di archiviazione SolidFire creando, eliminando e modificando gli account degli amministratori del cluster, cambiando la password degli amministratori del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

Tipi di account amministratore del cluster di archiviazione

In un cluster di storage che esegue il software NetApp Element possono esistere due tipi di account amministratore: l'account amministratore del cluster primario e un account amministratore del cluster.

- **Account amministratore del cluster primario**

  Questo account amministratore viene creato quando viene creato il cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo all'utente root in un sistema Linux. Puoi modificare la password per questo account amministratore.

- **Account amministratore del cluster**

  È possibile concedere a un account amministratore del cluster un intervallo limitato di accessi amministrativi per eseguire attività specifiche all'interno di un cluster. Le credenziali assegnate a ciascun account amministratore del cluster vengono utilizzate per autenticare le richieste API e Element UI all'interno del sistema di archiviazione.

Per accedere ai nodi attivi in un cluster tramite l'interfaccia utente per nodo è necessario un account amministratore del cluster locale (non LDAP). Per accedere a un nodo che non fa ancora parte di un cluster non sono necessarie le credenziali dell'account.

Visualizza i dettagli dell'amministratore del cluster

1. Per creare un account amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **Utenti** > **Amministratori cluster**.
2. Nella pagina Amministratori cluster della scheda Utenti, è possibile visualizzare le seguenti informazioni.
   - **ID**: Numero sequenziale assegnato all'account dell'amministratore del cluster.
   - **Nome utente**: il nome assegnato all'account dell'amministratore del cluster al momento della sua creazione.
   - **Accesso**: le autorizzazioni utente assegnate all'account utente. Valori possibili:
     - Leggere
     - segnalazione
     - nodi
     - unità
     - volumi
     - conti
     - amministratori del cluster
     - amministratore
     - supportoAdmin

Tutte le autorizzazioni sono disponibili per il tipo di accesso amministratore.

Sono disponibili tipi di accesso tramite l'API che non sono disponibili nell'interfaccia utente di Element.

+

- **Tipo**: Tipo di amministratore del cluster. Valori possibili:
  - Grappolo
  - Ldap
- **Attributi**: se l'account dell'amministratore del cluster è stato creato utilizzando l'API Element, questa colonna mostra tutte le coppie nome-valore impostate utilizzando tale metodo.

  Vedere"Riferimento API del software NetApp Element" .

Crea un account amministratore del cluster

È possibile creare nuovi account di amministratore del cluster con autorizzazioni per consentire o limitare l'accesso ad aree specifiche del sistema di archiviazione. Quando si impostano le autorizzazioni dell'account amministratore del cluster, il sistema concede diritti di sola lettura per tutte le autorizzazioni non assegnate all'amministratore del cluster.

Se si desidera creare un account amministratore del cluster LDAP, assicurarsi che LDAP sia configurato sul cluster prima di iniziare.

"Abilita l'autenticazione LDAP con l'interfaccia utente Element"

In seguito è possibile modificare i privilegi dell'account amministratore del cluster per la creazione di report, nodi, unità, volumi, account e accesso a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

In seguito è anche possibile rimuovere qualsiasi account utente amministratore del cluster creato da un amministratore di sistema. Non è possibile rimuovere l'account amministratore del cluster primario creato al momento della creazione del cluster.

1. Per creare un account amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **Utenti** > **Amministratori cluster**.
   b. Fare clic su **Crea amministratore cluster**.
   c. Selezionare il tipo di utente **Cluster**.
   d. Inserisci un nome utente e una password per l'account e conferma la password.
   e. Seleziona le autorizzazioni utente da applicare all'account.
   f. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.
   g. Fare clic su **Crea amministratore cluster**.
2. Per creare un account amministratore del cluster nella directory LDAP, eseguire le seguenti azioni:
   a. Fare clic su **Cluster** > **LDAP**.
   b. Assicurarsi che l'autenticazione LDAP sia abilitata.
   c. Fare clic su **Test autenticazione utente** e copiare il nome distinto visualizzato per l'utente o per uno dei gruppi di cui l'utente è membro, in modo da poterlo incollare in seguito.
   d. Fare clic su **Utenti** > **Amministratori cluster**.

e. Fare clic su **Crea amministratore cluster**.

f. Selezionare il tipo di utente LDAP.

g. Nel campo Nome distinto, seguire l'esempio nella casella di testo per immettere un nome distinto completo per l'utente o il gruppo. In alternativa, incollalo dal nome distinto che hai copiato in precedenza.

   Se il nome distinto fa parte di un gruppo, qualsiasi utente membro di quel gruppo sul server LDAP avrà le autorizzazioni di questo account amministratore.

Per aggiungere utenti o gruppi LDAP Cluster Admin, il formato generale del nome utente è "LDAP:<Nome distinto completo>".

a. Seleziona le autorizzazioni utente da applicare all'account.

b. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.

c. Fare clic su **Crea amministratore cluster**.

Modifica le autorizzazioni dell'amministratore del cluster

È possibile modificare i privilegi dell'account amministratore del cluster per la creazione di report, nodi, unità, volumi, account e accesso a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

1. Fare clic su **Utenti** > **Amministratori cluster**.
2. Fare clic sull'icona Azioni relativa all'amministratore del cluster che si desidera modificare.
3. Fare clic su **Modifica**.
4. Seleziona le autorizzazioni utente da applicare all'account.
5. Fare clic su **Salva modifiche**.

Cambiare le password per gli account degli amministratori del cluster

È possibile utilizzare l'interfaccia utente di Element per modificare le password degli amministratori del cluster.

1. Fare clic su **Utenti** > **Amministratori cluster**.
2. Fare clic sull'icona Azioni relativa all'amministratore del cluster che si desidera modificare.
3. Fare clic su **Modifica**.
4. Nel campo Cambia password, inserisci una nuova password e confermala.
5. Fare clic su **Salva modifiche**.

Informazioni correlate

- "Scopri i tipi di accesso disponibili per le API Element"
- "Abilita l'autenticazione LDAP con l'interfaccia utente Element"
- "Disabilitare LDAP"
- "Plug-in NetApp Element per vCenter Server"

Gestisci LDAP

È possibile configurare il protocollo LDAP (Lightweight Directory Access Protocol) per abilitare la funzionalità di accesso sicura basata su directory allo storage SolidFire . È possibile configurare LDAP a livello di cluster e autorizzare utenti e gruppi LDAP.

La gestione di LDAP implica la configurazione dell'autenticazione LDAP su un cluster SolidFire utilizzando un ambiente Microsoft Active Directory esistente e il test della configurazione.

È possibile utilizzare sia indirizzi IPv4 che IPv6.

L'abilitazione di LDAP prevede i seguenti passaggi generali, descritti in dettaglio:

1. **Completare i passaggi di preconfigurazione per il supporto LDAP**. Verificare di disporre di tutti i dettagli necessari per configurare l'autenticazione LDAP.
2. **Abilita l'autenticazione LDAP**. Utilizzare l'interfaccia utente Element o l'API Element.
3. **Convalidare la configurazione LDAP**. Facoltativamente, verificare che il cluster sia configurato con i valori corretti eseguendo il metodo API GetLdapConfiguration o controllando la configurazione LCAP tramite l'interfaccia utente dell'elemento.
4. **Testare l'autenticazione LDAP** (con `readonly` utente). Verificare che la configurazione LDAP sia corretta eseguendo il metodo API TestLdapAuthentication oppure utilizzando l'interfaccia utente dell'elemento. Per questo test iniziale, utilizzare il nome utente "sAMAccountName" del `readonly` utente. Ciò convaliderà che il cluster è configurato correttamente per l'autenticazione LDAP e convaliderà anche che `readonly` le credenziali e l'accesso sono corretti. Se questo passaggio non riesce, ripetere i passaggi da 1 a 3.
5. **Testa l'autenticazione LDAP** (con un account utente che desideri aggiungere). Ripetere la procedura descritta al punto 4 con un account utente che si desidera aggiungere come amministratore del cluster Element. Copia il `distinguished` nome (DN) o l'utente (o il gruppo). Questo DN verrà utilizzato nel passaggio 6.
6. **Aggiungere l'amministratore del cluster LDAP** (copiare e incollare il DN dal passaggio di autenticazione LDAP di prova). Utilizzando l'interfaccia utente Element o il metodo API AddLdapClusterAdmin, creare un nuovo utente amministratore del cluster con il livello di accesso appropriato. Per il nome utente, incolla il DN completo che hai copiato nel passaggio 5. Ciò garantisce che il DN sia formattato correttamente.
7. **Testare l'accesso dell'amministratore del cluster**. Accedere al cluster utilizzando l'utente amministratore del cluster LDAP appena creato. Se hai aggiunto un gruppo LDAP, puoi accedere come qualsiasi utente di quel gruppo.

Completare i passaggi di preconfigurazione per il supporto LDAP

Prima di abilitare il supporto LDAP in Element, è necessario configurare un server Windows Active Directory ed eseguire altre attività di preconfigurazione.

Passi

1. Configurare un server Windows Active Directory.
2. **Facoltativo:** abilitare il supporto LDAPS.
3. Crea utenti e gruppi.
4. Creare un account di servizio di sola lettura (ad esempio "sfreadonly") da utilizzare per la ricerca nella directory LDAP.

Abilita l'autenticazione LDAP con l'interfaccia utente Element

È possibile configurare l'integrazione del sistema di archiviazione con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso degli utenti al sistema di archiviazione.

È possibile configurare LDAP tramite l'interfaccia utente Element o tramite l'API Element. Questa procedura descrive come configurare LDAP utilizzando l'interfaccia utente Element.

Questo esempio mostra come configurare l'autenticazione LDAP su SolidFire e utilizza `SearchAndBind` come tipo di autenticazione. Nell'esempio viene utilizzato un singolo server Active Directory Windows Server 2012 R2.

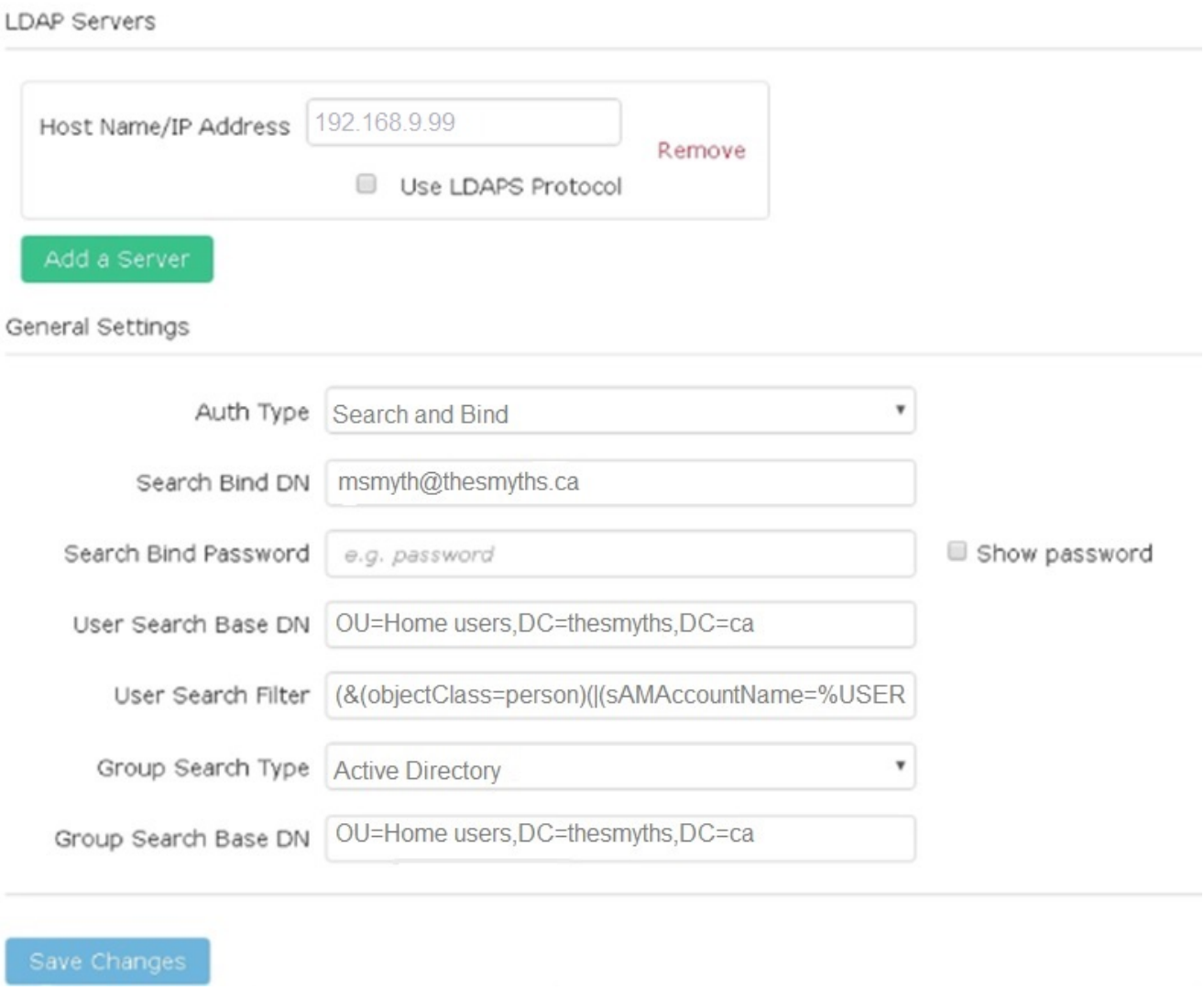
Passi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **Sì** per abilitare l'autenticazione LDAP.
3. Fare clic su **Aggiungi un server**.
4. Inserisci **Nome host/Indirizzo IP**.

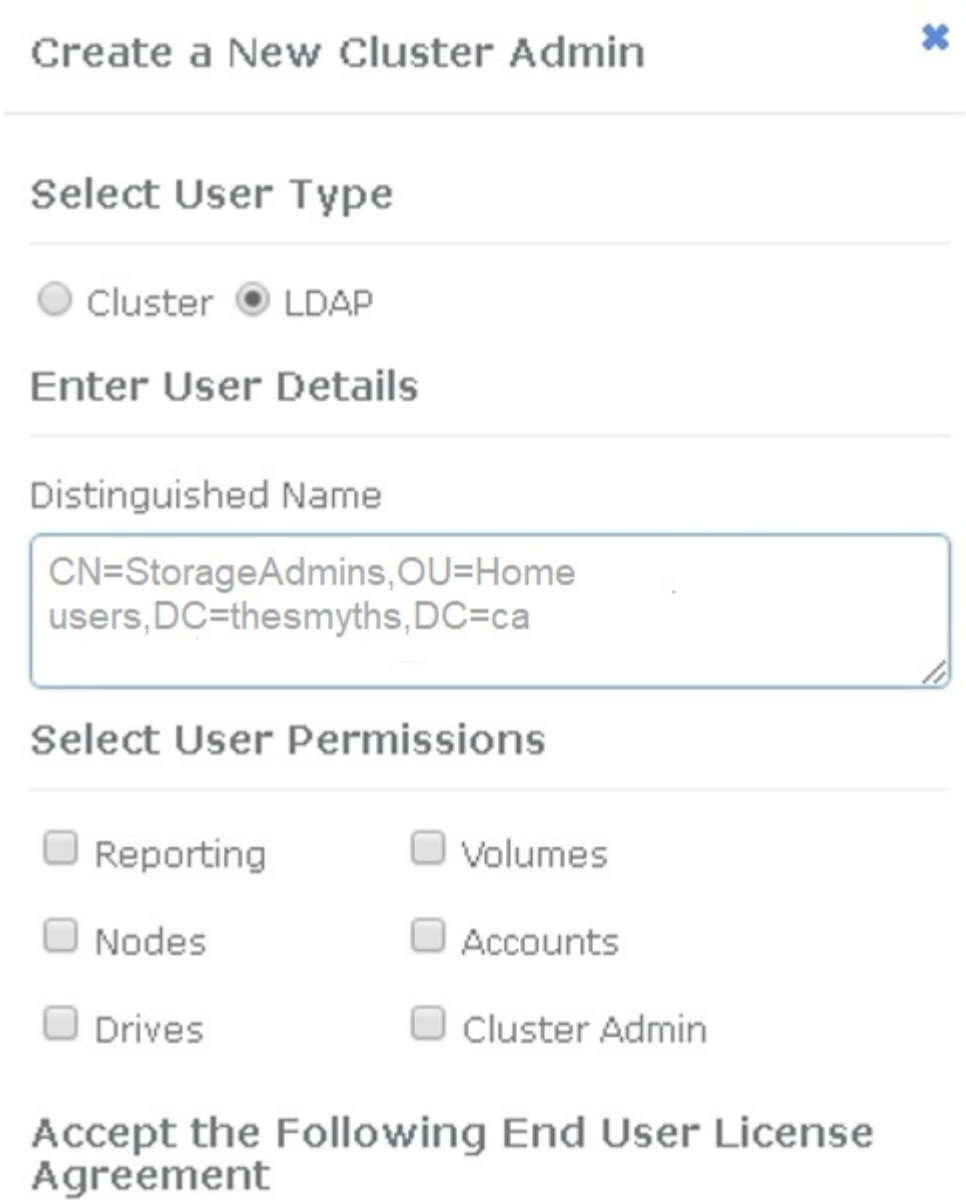
   È anche possibile immettere un numero di porta personalizzato facoltativo.

   Ad esempio, per aggiungere un numero di porta personalizzato, immettere <nome host o indirizzo IP>:<numero di porta>

5. **Facoltativo:** seleziona **Usa protocollo LDAPS**.
6. Inserisci le informazioni richieste in **Impostazioni generali**.



7. Fare clic su **Abilita LDAP**.
8. Fare clic su **Test autenticazione utente** se si desidera testare l'accesso al server per un utente.
9. Copiare il nome distinto e le informazioni sul gruppo utente che vengono visualizzate per utilizzarle in seguito durante la creazione degli amministratori del cluster.
10. Fare clic su **Salva modifiche** per salvare le nuove impostazioni.
11. Per creare un utente in questo gruppo in modo che chiunque possa accedere, completa quanto segue:
    a. Fare clic su **Utente** > **Visualizza**.



b. Per il nuovo utente, fare clic su **LDAP** per Tipo utente e incollare il gruppo copiato nel campo Nome distinto.
c. Selezionare le autorizzazioni, in genere tutte le autorizzazioni.
d. Scorri verso il basso fino al Contratto di licenza con l'utente finale e fai clic su **Accetto**.
e. Fare clic su **Crea amministratore cluster**.

   Ora hai un utente con il valore di un gruppo Active Directory.

Per testarlo, disconnettiti dall'interfaccia utente di Element e accedi nuovamente come utente di quel gruppo.

Abilita l'autenticazione LDAP con l'API Element

È possibile configurare l'integrazione del sistema di archiviazione con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso degli utenti al sistema di archiviazione.

È possibile configurare LDAP tramite l'interfaccia utente Element o tramite l'API Element. Questa procedura descrive come configurare LDAP utilizzando l'API Element.

Per sfruttare l'autenticazione LDAP su un cluster SolidFire , abilitare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.

Passi

1. Abilitare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.
2. Inserisci le informazioni richieste.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Modificare i valori dei seguenti parametri:

Parametri utilizzati	Descrizione
authType: SearchAndBind	Stabilisce che il cluster utilizzerà l'account di servizio di sola lettura per cercare prima l'utente da autenticare e successivamente associare tale utente se trovato e autenticato.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifica la posizione nell'albero LDAP da cui iniziare la ricerca dei gruppi. Per questo esempio abbiamo utilizzato la radice del nostro albero. Se l'albero LDAP è molto grande, potrebbe essere opportuno impostarlo su un sottoalbero più granulare per ridurre i tempi di ricerca.
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifica la posizione nell'albero LDAP da cui iniziare la ricerca degli utenti. Per questo esempio abbiamo utilizzato la radice del nostro albero. Se l'albero LDAP è molto grande, potrebbe essere opportuno impostarlo su un sottoalbero più granulare per ridurre i tempi di ricerca.

Parametri utilizzati	Descrizione
groupSearchType: ActiveDirectory	Utilizza il server Windows Active Directory come server LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Per utilizzare userPrincipalName (indirizzo email per l'accesso) puoi modificare userSearchFilter in:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
In alternativa, per cercare sia userPrincipalName che sAMAccountName, è possibile utilizzare il seguente userSearchFilter:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Utilizza sAMAccountName come nome utente per accedere al cluster SolidFire . Queste impostazioni indicano a LDAP di cercare il nome utente specificato durante l'accesso nell'attributo sAMAccountName e di limitare la ricerca alle voci che hanno "person" come valore nell'attributo objectClass.	searchBindDN
Questo è il nome distinto dell'utente di sola lettura che verrà utilizzato per cercare nella directory LDAP. Per Active Directory è solitamente più semplice utilizzare userPrincipalName (formato indirizzo email) per l'utente.	cercaBindPassword

Per testarlo, disconnettiti dall'interfaccia utente di Element e accedi nuovamente come utente di quel gruppo.

Visualizza i dettagli LDAP

Visualizzare le informazioni LDAP nella pagina LDAP nella scheda Cluster.

Per visualizzare queste impostazioni di configurazione LDAP è necessario abilitare LDAP.

1. Per visualizzare i dettagli LDAP con l'interfaccia utente Element, fare clic su **Cluster** > **LDAP**.
   - **Nome host/Indirizzo IP**: Indirizzo di un server di directory LDAP o LDAPS.

- **Tipo di autenticazione**: metodo di autenticazione dell'utente. Valori possibili:
  - Legame diretto
  - Cerca e collega
- **DN di binding di ricerca**: un DN completamente qualificato con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente (richiede l'accesso a livello di binding alla directory LDAP).
- **Cerca password di associazione**: password utilizzata per autenticare l'accesso al server LDAP.
- **DN base ricerca utente**: il DN base dell'albero utilizzato per avviare la ricerca utente. Il sistema esegue la ricerca nel sottoalbero dalla posizione specificata.
- **Filtro di ricerca utente**: inserisci quanto segue utilizzando il tuo nome di dominio:

  ```
  (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
  ```

- **Tipo di ricerca di gruppo**: tipo di ricerca che controlla il filtro di ricerca di gruppo predefinito utilizzato. Valori possibili:
  - Active Directory: appartenenza nidificata di tutti i gruppi LDAP di un utente.
  - Nessun gruppo: nessun supporto di gruppo.
  - Membro DN: gruppi in stile Membro DN (livello singolo).
- **DN base ricerca gruppo**: il DN base dell'albero utilizzato per avviare la ricerca di gruppo. Il sistema esegue la ricerca nel sottoalbero dalla posizione specificata.
- **Test di autenticazione utente**: dopo aver configurato LDAP, utilizzare questa opzione per testare l'autenticazione del nome utente e della password per il server LDAP. Inserisci un account già esistente per testarlo. Vengono visualizzate le informazioni sul nome distinto e sul gruppo utente, che è possibile copiare per un utilizzo successivo durante la creazione degli amministratori del cluster.

Testare la configurazione LDAP

Dopo aver configurato LDAP, dovresti testarlo utilizzando l'interfaccia utente Element o l'API Element `TestLdapAuthentication` metodo.

Passi

1. Per testare la configurazione LDAP con Element UI, procedere come segue:
   a. Fare clic su **Cluster** > **LDAP**.
   b. Fare clic su **Test autenticazione LDAP**.
   c. Risolvi eventuali problemi utilizzando le informazioni nella tabella sottostante:

Messaggio di errore	Descrizione
`xLDAPUserNotFound`	• L'utente sottoposto a test non è stato trovato nella configurazione `userSearchBaseDN` sottoalbero. • IL `userSearchFilter` è configurato in modo errato.

Messaggio di errore	Descrizione
`xLDAPBindFailed (Error: Invalid credentials)`	• Il nome utente testato è un utente LDAP valido, ma la password fornita non è corretta. • Il nome utente testato è un utente LDAP valido, ma l'account è attualmente disabilitato.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	L'URI del server LDAP non è corretto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Il nome utente o la password di sola lettura non sono configurati correttamente.
`xLDAPSearchFailed (Error: No such object)`	IL `userSearchBaseDN` non è una posizione valida all'interno dell'albero LDAP.
`xLDAPSearchFailed (Error: Referral)`	• IL `userSearchBaseDN` non è una posizione valida all'interno dell'albero LDAP. • IL `userSearchBaseDN` E `groupSearchBaseDN` si trovano in una OU annidata. Ciò può causare problemi di autorizzazione. La soluzione alternativa è quella di includere l'OU nelle voci DN di base dell'utente e del gruppo (ad esempio: `ou=storage, cn=company, cn=com`)

2. Per testare la configurazione LDAP con l'API Element, procedere come segue:
   a. Chiamare il metodo TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

   b. Esaminare i risultati. Se la chiamata API ha esito positivo, i risultati includono il nome distinto dell'utente specificato e un elenco dei gruppi di cui l'utente è membro.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Disabilitare LDAP

È possibile disattivare l'integrazione LDAP tramite l'interfaccia utente di Element.

Prima di iniziare, è opportuno annotare tutte le impostazioni di configurazione, poiché disabilitando LDAP tutte le impostazioni vengono cancellate.

Passi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **No**.
3. Fare clic su **Disabilita LDAP**.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestisci il tuo sistema

Gestisci il tuo sistema

Puoi gestire il tuo sistema nell'interfaccia utente Element. Ciò include l'abilitazione dell'autenticazione a più fattori, la gestione delle impostazioni del cluster, il supporto degli standard federali di elaborazione delle informazioni (FIPS) e l'utilizzo della gestione delle chiavi esterne.

- "Abilita l'autenticazione a più fattori"
- "Configurare le impostazioni del cluster"
- "Creare un cluster che supporti le unità FIPS"
- "Inizia con la gestione delle chiavi esterne"

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Abilita l'autenticazione a più fattori

Configurare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) utilizza un Identity Provider (IdP) di terze parti tramite Security Assertion Markup Language (SAML) per gestire le sessioni utente. L'MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, a seconda delle necessità, come password e messaggio di testo oppure password e messaggio di posta elettronica.

È possibile utilizzare questi passaggi di base tramite l'API Element per configurare il cluster in modo che utilizzi l'autenticazione a più fattori.

I dettagli di ciascun metodo API possono essere trovati in "Riferimento API dell'elemento".

1. Creare una nuova configurazione dell'Identity Provider (IdP) di terze parti per il cluster chiamando il seguente metodo API e passando i metadati IdP in formato JSON: `CreateIdpConfiguration`

   I metadati IdP, in formato testo normale, vengono recuperati dall'IdP di terze parti. Questi metadati devono essere convalidati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni di formattazione JSON che puoi utilizzare, ad esempio: https://freeformatter.com/json-escape.html.

2. Recupera i metadati del cluster tramite spMetadataUrl per copiarli nell'IdP di terze parti chiamando il seguente metodo API: `ListIdpConfigurations`

   spMetadataUrl è un URL utilizzato per recuperare i metadati del provider di servizi dal cluster per l'IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull'IdP di terze parti in modo da includere l'attributo "NameID" per identificare in modo univoco un utente per la registrazione degli audit e per il corretto funzionamento di Single Logout.
4. Creare uno o più account utente amministratore del cluster autenticati da un IdP di terze parti per l'autorizzazione chiamando il seguente metodo API:`AddIdpClusterAdmin`

   > Il nome utente per l'amministratore del cluster IdP deve corrispondere alla mappatura Nome/Valore dell'attributo SAML per ottenere l'effetto desiderato, come mostrato negli esempi seguenti:

   - email=bob@company.com — dove l'IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
   - group=cluster-administrator - dove l'IdP è configurato per rilasciare una proprietà di gruppo a cui tutti gli utenti dovrebbero avere accesso. Si noti che l'abbinamento Nome/Valore dell'attributo SAML è sensibile alle maiuscole e alle minuscole per motivi di sicurezza.
5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Informazioni aggiuntive per l'autenticazione a più fattori

È opportuno tenere presente le seguenti avvertenze in relazione all'autenticazione a più fattori.

- Per aggiornare i certificati IdP non più validi, è necessario utilizzare un utente non amministratore IdP per chiamare il seguente metodo API: `UpdateIdpConfiguration`
- L'MFA non è compatibile con i certificati di lunghezza inferiore a 2048 bit. Per impostazione predefinita, sul cluster viene creato un certificato SSL a 2048 bit. Dovresti evitare di impostare un certificato di dimensioni inferiori quando chiami il metodo API: `SetSSLCertificate`

> Se il cluster utilizza un certificato inferiore a 2048 bit prima dell'aggiornamento, il certificato del cluster deve essere aggiornato con un certificato da 2048 bit o superiore dopo l'aggiornamento a Element 12.0 o versione successiva.

- Gli utenti amministratori IdP non possono essere utilizzati per effettuare chiamate API direttamente (ad esempio, tramite SDK o Postman) o per altre integrazioni (ad esempio, OpenStack Cinder o vCenter Plug-in). Se è necessario creare utenti dotati di queste capacità, aggiungere utenti amministratori del cluster LDAP o utenti amministratori del cluster locale.

Trova maggiori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Configurare le impostazioni del cluster

Abilitare e disabilitare la crittografia a riposo per un cluster

Con i cluster SolidFire è possibile crittografare tutti i dati inattivi archiviati sulle unità del cluster. È possibile abilitare la protezione a livello di cluster delle unità auto-crittografanti (SED) utilizzando"crittografia a riposo basata su hardware o software" .

È possibile abilitare la crittografia hardware a riposo tramite l'interfaccia utente o l'API di Element. L'abilitazione della funzionalità di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile abilitare la crittografia software a riposo solo tramite l'API Element.

La crittografia basata su hardware a riposo non è abilitata per impostazione predefinita durante la creazione del cluster e può essere abilitata e disabilitata dall'interfaccia utente di Element.

> Per i cluster di archiviazione all-flash SolidFire , la crittografia software a riposo deve essere abilitata durante la creazione del cluster e non può essere disabilitata dopo la creazione del cluster.

Cosa ti servirà

- Si dispone dei privilegi di amministratore del cluster per abilitare o modificare le impostazioni di crittografia.
- Per la crittografia a riposo basata su hardware, è necessario assicurarsi che il cluster sia in uno stato di integrità prima di modificare le impostazioni di crittografia.
- Se si disabilita la crittografia, è necessario che due nodi partecipino a un cluster per accedere alla chiave per disabilitare la crittografia su un'unità.

Controllare lo stato di crittografia a riposo

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo sul cluster, utilizzare"Ottieni informazioni sul cluster" metodo. Puoi usare il"Ottieni informazioni sulla crittografia software a riposo" metodo per ottenere le informazioni che il cluster utilizza per crittografare i dati a riposo.

> La dashboard dell'interfaccia utente del software Element su `https://<MVIP>/` attualmente mostra solo lo stato di crittografia a riposo per la crittografia basata su hardware.

Opzioni

- Abilita la crittografia basata su hardware a riposo
- Abilita la crittografia basata su software a riposo
- Disabilitare la crittografia basata su hardware a riposo

Abilita la crittografia basata su hardware a riposo

> Per abilitare la crittografia a riposo utilizzando una configurazione di gestione delle chiavi esterna, è necessario abilitare la crittografia a riposo tramite"API" . L'abilitazione tramite il pulsante Element UI esistente ripristinerà l'utilizzo delle chiavi generate internamente.

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster** > **Impostazioni**.
2. Selezionare **Abilita crittografia a riposo**.

Abilita la crittografia basata su software a riposo

> La crittografia software a riposo non può essere disabilitata dopo essere stata abilitata sul cluster.

1. Durante la creazione del cluster, eseguire il comando"metodo di creazione del cluster" con `enableSoftwareEncryptionAtRest` impostato su `true` .

Disabilitare la crittografia basata su hardware a riposo

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster** > **Impostazioni**.
2. Selezionare **Disabilita crittografia a riposo**.

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Imposta la soglia di riempimento del cluster

È possibile modificare il livello al quale il sistema genera un avviso di riempimento del cluster di blocchi seguendo i passaggi indicati di seguito. Inoltre, è possibile utilizzare il metodo API ModifyClusterFullThreshold per modificare il livello in cui il sistema genera un avviso di blocco o di metadati.

Cosa ti servirà

È necessario disporre dei privilegi di amministratore del cluster.

Passi

1. Fare clic su **Cluster** > **Impostazioni**.
2. Nella sezione Impostazioni complete del cluster, immettere una percentuale in **Genera un avviso quando rimane _% di capacità prima che Helix non riesca a riprendersi da un errore del nodo**.
3. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

"Come vengono calcolate le soglie di blockSpace per Element"

Abilita e disabilita il bilanciamento del carico del volume

A partire da Element 12.8, è possibile utilizzare Volume Load Balancing per bilanciare i volumi tra i nodi in base agli IOPS effettivi di ciascun volume anziché agli IOPS minimi configurati nella policy QoS. È possibile abilitare e disabilitare il bilanciamento del carico del volume, disabilitato per impostazione predefinita, tramite l'interfaccia utente o l'API di Element.

Passi

1. Selezionare **Cluster** > **Impostazioni**.
2. Nella sezione Cluster Specific, modifica lo stato per Volume Load Balancing:

   Abilita il bilanciamento del carico del volume

   Selezionare **Abilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

   Disabilita il bilanciamento del carico del volume:

   Selezionare **Disabilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

3. Facoltativamente, selezionare **Reporting** > **Panoramica** per confermare la modifica dello stato per il saldo sugli IOPS effettivi. Potrebbe essere necessario scorrere verso il basso le informazioni sullo stato del cluster per visualizzarne lo stato.

Trova maggiori informazioni

- "Abilita il bilanciamento del carico del volume tramite l'API"
- "Disabilitare il bilanciamento del carico del volume tramite l'API"
- "Creare e gestire policy QoS del volume"

Abilita e disabilita l'accesso al supporto

È possibile abilitare l'accesso al supporto per consentire temporaneamente al personale di supporto NetApp di accedere ai nodi di storage tramite SSH per la risoluzione dei problemi.

Per modificare l'accesso al supporto è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **Cluster** > **Impostazioni**.
2. Nella sezione Abilita/Disabilita accesso supporto, inserisci la durata (in ore) per cui desideri consentire l'accesso al supporto.
3. Fare clic su **Abilita accesso supporto**.
4. **Facoltativo:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestisci il banner Termini di utilizzo

È possibile abilitare, modificare o configurare un banner contenente un messaggio per l'utente.

Opzioni

Abilita il banner Termini di utilizzo Modifica il banner dei Termini di utilizzo Disattiva il banner Termini di utilizzo

Abilita il banner Termini di utilizzo

È possibile abilitare un banner con i Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente clicca sul banner, viene visualizzata una finestra di dialogo di testo contenente il messaggio configurato per il cluster. Il banner può essere rimosso in qualsiasi momento.

Per abilitare la funzionalità Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **Utenti** > **Termini di utilizzo**.
2. Nel modulo **Termini di utilizzo**, immettere il testo da visualizzare nella finestra di dialogo Termini di utilizzo.

   Non superare i 4096 caratteri.

3. Fare clic su **Abilita**.

Modifica il banner dei Termini di utilizzo

Puoi modificare il testo che un utente vede quando seleziona il banner di accesso ai Termini di utilizzo.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che la funzione Termini di utilizzo sia abilitata.

Passi

1. Fare clic su **Utenti** > **Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modifica il testo che desideri visualizzare.

Non superare i 4096 caratteri.

3. Fare clic su **Salva modifiche**.

Disattiva il banner Termini di utilizzo

Puoi disattivare il banner Termini di utilizzo. Con il banner disabilitato, all'utente non viene più richiesto di accettare i termini di utilizzo quando utilizza Element UI.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che i Termini di utilizzo siano abilitati.

Passi

1. Fare clic su **Utenti** > **Termini di utilizzo**.
2. Fare clic su **Disabilita**.

Imposta il protocollo di tempo di rete

Configurare i server Network Time Protocol affinché il cluster esegua le query

È possibile istruire ciascun nodo di un cluster a interrogare un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede loro informazioni NTP.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

Configurare NTP sul cluster in modo che punti a un server NTP locale. È possibile utilizzare l'indirizzo IP o il nome host FQDN. Il server NTP predefinito al momento della creazione del cluster è impostato su us.pool.ntp.org; tuttavia, a seconda della posizione fisica del cluster SolidFire , non è sempre possibile stabilire una connessione a questo sito.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di archiviazione siano corrette e operative. Per farlo, configura i server DNS su ogni nodo di archiviazione e assicurati che le porte siano aperte consultando la pagina Requisiti delle porte di rete.

È possibile inserire fino a cinque server NTP diversi.

È possibile utilizzare sia indirizzi IPv4 che IPv6.

Cosa ti servirà

Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.

Passi

1. Configurare un elenco di IP e/o FQDN nelle impostazioni del server.
2. Assicurarsi che il DNS sia impostato correttamente sui nodi.
3. Fare clic su **Cluster** > **Impostazioni**.
4. In Impostazioni Network Time Protocol, seleziona **No**, che utilizza la configurazione NTP standard.

5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- "Configurare il cluster per ascoltare le trasmissioni NTP"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Configurare il cluster per ascoltare le trasmissioni NTP

Utilizzando la modalità broadcast, è possibile istruire ciascun nodo di un cluster ad ascoltare sulla rete i messaggi broadcast NTP (Network Time Protocol) provenienti da un server specifico.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

Cosa ti servirà

- Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.
- È necessario configurare un server NTP sulla rete come server broadcast.

Passi

1. Fare clic su **Cluster** > **Impostazioni**.
2. Inserire nell'elenco dei server il server o i server NTP che utilizzano la modalità broadcast.
3. In Impostazioni Network Time Protocol, seleziona **Sì** per utilizzare un client broadcast.
4. Per impostare il client broadcast, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- "Configurare i server Network Time Protocol affinché il cluster esegua le query"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestisci SNMP

Scopri di più su SNMP

È possibile configurare il protocollo SNMP (Simple Network Management Protocol) nel cluster.

È possibile selezionare un richiedente SNMP, selezionare la versione di SNMP da utilizzare, identificare l'utente USM (User-based Security Model) SNMP e configurare trap per monitorare il cluster SolidFire . È inoltre possibile visualizzare e accedere ai file della base dati di gestione.

È possibile utilizzare sia indirizzi IPv4 che IPv6.

Dettagli SNMP

Nella pagina SNMP della scheda Cluster è possibile visualizzare le seguenti informazioni.

- **MIB SNMP**

  I file MIB disponibili per la visualizzazione o il download.

- **Impostazioni SNMP generali**

  È possibile abilitare o disabilitare SNMP. Dopo aver abilitato SNMP, puoi scegliere quale versione utilizzare. Se si utilizza la versione 2, è possibile aggiungere richiedenti, mentre se si utilizza la versione 3, è possibile impostare utenti USM.

- **Impostazioni trap SNMP**

  Puoi identificare le trappole che vuoi catturare. È possibile impostare l'host, la porta e la stringa della community per ciascun destinatario della trap.

Configurare un richiedente SNMP

Quando è abilitata la versione 2 di SNMP, è possibile abilitare o disabilitare un richiedente e configurare i richiedenti per ricevere richieste SNMP autorizzate.

1. Fare clic sul **Cluster › SNMP**.
2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 2**.
4. Nella sezione **Richiedenti**, immettere le informazioni **Stringa della community** e **Rete**.

   Per impostazione predefinita, la stringa della community è public e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Facoltativo:** per aggiungere un altro richiedente, fare clic su **Aggiungi un richiedente** e immettere le informazioni **Stringa della community** e **Rete**.
6. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- Configurare le trappole SNMP
- Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

Configurare un utente USM SNMP

Quando si abilita SNMP versione 3, è necessario configurare un utente USM per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster** > **SNMP**.
2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 3**.

4. Nella sezione **Utenti USM**, immettere il nome, la password e la passphrase.
5. **Facoltativo:** per aggiungere un altro utente USM, fare clic su **Aggiungi un utente USM** e immettere nome, password e passphrase.
6. Fare clic su **Salva modifiche**.

Configurare le trappole SNMP

Gli amministratori di sistema possono utilizzare trap SNMP, note anche come notifiche, per monitorare lo stato di salute del cluster SolidFire .

Quando le trap SNMP sono abilitate, il cluster SolidFire genera trap associate alle voci del registro eventi e agli avvisi di sistema. Per ricevere le notifiche SNMP, è necessario scegliere le trappole da generare e identificare i destinatari delle informazioni sulle trappole. Per impostazione predefinita, non vengono generate trappole.

1. Fare clic su **Cluster** > **SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
   - Cluster Fault Traps
   - Cluster Resolved Fault Traps
   - Trappole per eventi cluster
3. Nella sezione **Destinatari trap**, immettere le informazioni relative all'host, alla porta e alla stringa di community per un destinatario.
4. **Facoltativo**: per aggiungere un altro destinatario della trappola, fare clic su **Aggiungi un destinatario della trappola** e immettere le informazioni relative a host, porta e stringa della community.
5. Fare clic su **Salva modifiche**.

Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

È possibile visualizzare e scaricare i file MIB (Management Information Base) utilizzati per definire ciascuno degli oggetti gestiti. La funzionalità SNMP supporta l'accesso in sola lettura agli oggetti definiti in SolidFire-StorageCluster-MIB.

I dati statistici forniti nel MIB mostrano l'attività del sistema per quanto segue:

- Statistiche del cluster
- Statistiche di volume
- Volumi per statistiche di conto
- Statistiche del nodo
- Altri dati come report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente i punti di accesso di livello superiore (OIDS) ai prodotti della serie SF.

Passi

1. Fare clic su **Cluster** > **SNMP**.
2. In **SNMP MIB**, fare clic sul file MIB che si desidera scaricare.
3. Nella finestra di download visualizzata, apri o salva il file MIB.

Gestisci unità

Ogni nodo contiene una o più unità fisiche utilizzate per archiviare una parte dei dati del cluster. Il cluster utilizza la capacità e le prestazioni dell'unità dopo che questa è stata aggiunta correttamente a un cluster. È possibile utilizzare l'interfaccia utente di Element per gestire le unità.

Dettagli delle unità

La pagina Unità nella scheda Cluster fornisce un elenco delle unità attive nel cluster. È possibile filtrare la pagina selezionando tra le schede Attivo, Disponibile, Rimozione, Cancellazione e Non riuscito.

Quando si inizializza per la prima volta un cluster, l'elenco delle unità attive è vuoto. È possibile aggiungere unità non assegnate a un cluster ed elencate nella scheda Disponibili dopo la creazione di un nuovo cluster SolidFire .

Nell'elenco delle unità attive compaiono i seguenti elementi.

- **ID unità**

  Numero sequenziale assegnato all'unità.

- **ID nodo**

  Numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

  Il nome del nodo che ospita l'unità.

- **Fessura**

  Il numero dello slot in cui si trova fisicamente l'unità.

- **Capacità**

  La dimensione dell'unità, in GB.

- **Seriale**

  Il numero di serie dell'unità.

- **Usura rimanente**

  L'indicatore del livello di usura.

  Il sistema di archiviazione segnala la quantità approssimativa di usura disponibile su ciascuna unità a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un'unità che ha consumato il 5 percento dei cicli di scrittura e cancellazione previsti segnala un'usura residua del 95 percento. Il sistema non aggiorna automaticamente le informazioni sull'usura dell'unità; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

  Il tipo di unità. Il tipo può essere blocco o metadati.

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestisci nodi

Gestisci nodi

È possibile gestire lo storage SolidFire e i nodi Fibre Channel dalla pagina Nodi della scheda Cluster.

Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo si blocca, viene generato un errore di cluster appropriato.

Trova maggiori informazioni

Aggiungere un nodo a un cluster

Aggiungere un nodo a un cluster

È possibile aggiungere nodi a un cluster quando è necessario più spazio di archiviazione o dopo la creazione del cluster. I nodi richiedono una configurazione iniziale quando vengono accesi per la prima volta. Dopo aver configurato il nodo, questo viene visualizzato nell'elenco dei nodi in sospeso ed è possibile aggiungerlo a un cluster.

La versione del software su ciascun nodo di un cluster deve essere compatibile. Quando si aggiunge un nodo a un cluster, il cluster installa la versione cluster del software NetApp Element sul nuovo nodo, secondo necessità.

È possibile aggiungere nodi di capacità più piccole o più grandi a un cluster esistente. È possibile aggiungere capacità di nodi maggiori a un cluster per consentire la crescita della capacità. I nodi più grandi aggiunti a un cluster con nodi più piccoli devono essere aggiunti a coppie. Ciò consente a Double Helix di disporre di spazio sufficiente per spostare i dati nel caso in cui uno dei nodi più grandi dovesse guastarsi. È possibile aggiungere capacità di nodi più piccole a un cluster di nodi più grande per migliorare le prestazioni.

> Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo diventa inutilizzabile, viene generato l'errore cluster strandedCapacity.

"Video NetApp : Scalabilità in base alle tue esigenze: espansione di un cluster SolidFire"

È possibile aggiungere nodi agli appliance NetApp HCI .

Passi

1. Selezionare **Cluster** > **Nodi**.
2. Fare clic su **In attesa** per visualizzare l'elenco dei nodi in attesa.

   Una volta completato il processo di aggiunta dei nodi, questi vengono visualizzati nell'elenco Nodi attivi. Fino ad allora, i nodi in sospeso vengono visualizzati nell'elenco Attivi in sospeso.

   SolidFire installa la versione software Element del cluster sui nodi in sospeso quando li aggiungi a un cluster. Potrebbero volerci alcuni minuti.

3. Eseguire una delle seguenti operazioni:
   - Per aggiungere singoli nodi, fare clic sull'icona **Azioni** relativa al nodo che si desidera aggiungere.
   - Per aggiungere più nodi, seleziona la casella di controllo dei nodi da aggiungere, quindi **Azioni in blocco**. **Nota:** se il nodo che stai aggiungendo ha una versione del software Element diversa da quella in esecuzione sul cluster, il cluster aggiorna in modo asincrono il nodo alla versione del software Element in esecuzione sul master del cluster. Dopo l'aggiornamento, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo sarà nello stato pendingActive.
4. Fare clic su **Aggiungi**.

   Il nodo appare nell'elenco dei nodi attivi.

Trova maggiori informazioni

Versionamento e compatibilità dei nodi

Versionamento e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione del software Element installata su un nodo. I cluster di storage basati sul software Element creano automaticamente un'immagine di un nodo nella versione del software Element sul cluster se il nodo e il cluster non hanno versioni compatibili.

L'elenco seguente descrive i livelli di significatività della versione software che compongono il numero di versione del software Element:

- **Maggiore**

  Il primo numero indica la versione del software. Un nodo con un numero di componente principale non può essere aggiunto a un cluster contenente nodi con un numero di patch principale diverso, né è possibile creare un cluster con nodi con versioni principali miste.

- **Minore**

  Il secondo numero indica funzionalità software minori o miglioramenti alle funzionalità software esistenti che sono stati aggiunti a una versione principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa versione incrementale non è compatibile con nessun'altra versione incrementale del software Element con un componente secondario diverso. Ad esempio, 11.0 non è compatibile con 11.1 e 11.1 non è compatibile con 11.2.

- **Micro**

  Il terzo numero indica una patch compatibile (release incrementale) con la versione del software Element

rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0.2 e 11.0.2 è compatibile con 11.0.3.

Per garantire la compatibilità, i numeri di versione principale e secondaria devono corrispondere. Per garantire la compatibilità, i micronumeri non devono necessariamente corrispondere.

Capacità del cluster in un ambiente di nodi misti

È possibile combinare diversi tipi di nodi in un cluster. Le serie SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 e la serie H possono coesistere in un cluster.

La serie H è composta dai nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi supportano sia 10GbE che 25GbE.

È meglio non mescolare nodi crittografati e non crittografati. In un cluster con nodi misti, nessun nodo può essere più grande del 33 percento della capacità totale del cluster. Ad esempio, in un cluster con quattro nodi SF-Series 4805, il nodo più grande che può essere aggiunto da solo è un SF-Series 9605. La soglia di capacità del cluster viene calcolata in base alla potenziale perdita del nodo più grande in questa situazione.

A seconda della versione del software Element, i seguenti nodi di archiviazione della serie SF non sono supportati:

A partire da…	Nodo di archiviazione non supportato…
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x.

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio tag di servizio, dettagli dell'unità e grafici per l'utilizzo e statistiche dell'unità. La pagina Nodi della scheda Cluster fornisce la colonna Versione in cui è possibile visualizzare la versione software di ciascun nodo.

Passi

1. Fare clic su **Cluster** > **Nodi**.

2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **Azioni** per un nodo.
3. Fare clic su **Visualizza dettagli**.
4. Esaminare i dettagli del nodo:
   - **ID nodo**: ID generato dal sistema per il nodo.
   - **Nome nodo**: il nome host del nodo.
   - **Ruolo del nodo**: il ruolo che il nodo ha nel cluster. Valori possibili:
     - Cluster Master: il nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
     - Nodo ensemble: un nodo che partecipa al cluster. A seconda della dimensione del cluster, sono presenti 3 o 5 nodi ensemble.
     - Fibre Channel: un nodo del cluster.
   - **Tipo di nodo**: il tipo di modello del nodo.
   - **Unità attive**: numero di unità attive nel nodo.
   - **Utilizzo del nodo**: percentuale di utilizzo del nodo in base a nodeHeat. Il valore visualizzato è recentPrimaryTotalHeat in percentuale. Disponibile a partire da Element 12.8.
   - **IP di gestione**: indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione di rete da 1 GbE o 10 GbE.
   - **IP del cluster**: l'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi nello stesso cluster.
   - **IP di archiviazione**: l'indirizzo IP di archiviazione (SIP) assegnato al nodo utilizzato per la scoperta della rete iSCSI e per tutto il traffico dati della rete.
   - **ID VLAN di gestione**: ID virtuale per la rete locale di gestione.
   - **ID VLAN di archiviazione**: ID virtuale per la rete locale di archiviazione.
   - **Versione**: la versione del software in esecuzione su ciascun nodo.
   - **Porta di replicazione**: la porta utilizzata sui nodi per la replica remota.
   - **Tag di servizio**: il numero univoco del tag di servizio assegnato al nodo.
   - **Dominio di protezione personalizzato**: il dominio di protezione personalizzato assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

È possibile visualizzare i dettagli delle porte Fibre Channel, come lo stato, il nome e l'indirizzo della porta, dalla pagina Porte FC.

Visualizza le informazioni sulle porte Fibre Channel connesse al cluster.

Passi

1. Fare clic su **Cluster** > **Porte FC**.
2. Per filtrare le informazioni in questa pagina, clicca su **Filtra**.
3. Esamina i dettagli:
   - **ID nodo**: il nodo che ospita la sessione per la connessione.
   - **Nome nodo**: Nome del nodo generato dal sistema.
   - **Slot**: Numero dello slot in cui si trova la porta Fibre Channel.

- **Porta HBA**: porta fisica sull'adattatore bus host (HBA) Fibre Channel.
- **WWNN**: Nome del nodo mondiale.
- **WWPN**: Nome della porta mondiale di destinazione.
- **Switch WWN**: Nome mondiale dello switch Fibre Channel.
- **Stato del porto**: Stato attuale del porto.
- **nPort ID**: ID della porta del nodo sulla struttura Fibre Channel.
- **Velocità**: la velocità Fibre Channel negoziata. I valori possibili sono i seguenti:
  - 4Gbps
  - 8Gbps
  - 16Gbps

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestire reti virtuali

Gestire reti virtuali

La rete virtuale nello storage SolidFire consente di connettere a un unico cluster il traffico tra più client che si trovano su reti logiche separate. Le connessioni al cluster sono separate nello stack di rete tramite l'uso del tagging VLAN.

Trova maggiori informazioni

- Aggiungi una rete virtuale
- Abilita il routing e l'inoltro virtuali
- Modifica una rete virtuale
- Modifica VLAN VRF
- Elimina una rete virtuale

Aggiungi una rete virtuale

È possibile aggiungere una nuova rete virtuale a una configurazione cluster per abilitare una connessione di ambiente multi-tenant a un cluster che esegue il software Element.

Cosa ti servirà

- Identificare il blocco di indirizzi IP che verrà assegnato alle reti virtuali sui nodi del cluster.
- Identificare un indirizzo IP di rete di storage (SVIP) che verrà utilizzato come endpoint per tutto il traffico di storage NetApp Element .

Per questa configurazione è necessario considerare i seguenti criteri:

- Le VLAN che non sono abilitate per VRF richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP.

- Le VLAN abilitate per VRF non richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.
- L'SVIP predefinito non richiede che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.

Quando si aggiunge una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascuno richiede un indirizzo IP di rete virtuale. Il numero di indirizzi IP specificato durante la creazione di una nuova rete virtuale deve essere uguale o maggiore del numero di nodi nel cluster. Gli indirizzi di rete virtuale vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi del cluster.

Passi

1. Fare clic su **Cluster** > **Rete**.
2. Fare clic su **Crea VLAN**.
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:
    - **Nome VLAN**
    - **Tag VLAN**
    - **SVIP**
    - **Maschera di rete**
    - (Facoltativo) **Descrizione**
4. Immettere l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **Blocchi di indirizzi IP**.
5. Immettere la **Dimensione** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
6. Fare clic su **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
7. Fare clic su **Crea VLAN**.

Visualizza i dettagli della rete virtuale

Passi

1. Fare clic su **Cluster** > **Rete**.
2. Esamina i dettagli.
    - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
    - **Nome**: Nome univoco assegnato dall'utente per la rete VLAN.
    - **Tag VLAN**: tag VLAN assegnato al momento della creazione della rete virtuale.
    - **SVIP**: Indirizzo IP virtuale di archiviazione assegnato alla rete virtuale.
    - **Netmask**: Maschera di rete per questa rete virtuale.
    - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere abilitato.
    - **VRF abilitato**: Indica se il routing e l'inoltro virtuali sono abilitati o meno.
    - **IP utilizzati**: intervallo di indirizzi IP di rete virtuale utilizzati per la rete virtuale.

Abilita il routing e l'inoltro virtuali

È possibile abilitare il routing e l'inoltro virtuali (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di funzionare simultaneamente. Questa funzionalità è disponibile solo per le reti di archiviazione.

È possibile abilitare VRF solo al momento della creazione di una VLAN. Se si desidera tornare a non-VRF, è necessario eliminare e ricreare la VLAN.

1. Fare clic su **Cluster** > **Rete**.
2. Per abilitare VRF su una nuova VLAN, selezionare **Crea VLAN**.
   a. Inserire le informazioni rilevanti per il nuovo VRF/VLAN. Vedere Aggiunta di una rete virtuale.
   b. Selezionare la casella di controllo **Abilita VRF**.
   c. **Facoltativo**: Inserisci un gateway.
3. Fare clic su **Crea VLAN**.

Trova maggiori informazioni

Aggiungi una rete virtuale

Modifica una rete virtuale

È possibile modificare gli attributi VLAN, come il nome VLAN, la netmask e la dimensione dei blocchi di indirizzi IP. Il tag VLAN e SVIP non possono essere modificati per una VLAN. L'attributo gateway non è un parametro valido per le VLAN non VRF.

Se sono presenti sessioni iSCSI, di replica remota o di altra rete, la modifica potrebbe non riuscire.

Quando si gestisce la dimensione degli intervalli di indirizzi IP VLAN, è necessario tenere presenti le seguenti limitazioni:

- È possibile rimuovere gli indirizzi IP solo dall'intervallo di indirizzi IP iniziale assegnato al momento della creazione della VLAN.
- È possibile rimuovere un blocco di indirizzi IP aggiunto dopo l'intervallo di indirizzi IP iniziale, ma non è possibile ridimensionare un blocco IP rimuovendo gli indirizzi IP.
- Quando si tenta di rimuovere indirizzi IP, dall'intervallo di indirizzi IP iniziale o da un blocco IP, utilizzati dai nodi del cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare specifici indirizzi IP in uso ad altri nodi del cluster.

È possibile aggiungere un blocco di indirizzi IP utilizzando la seguente procedura:

1. Selezionare **Cluster** > **Rete**.
2. Selezionare l'icona Azioni per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **Modifica VLAN**, immettere i nuovi attributi per la VLAN.
5. Selezionare **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per la rete virtuale.
6. Selezionare **Salva modifiche**.

Collegamento agli articoli della Knowledge Base sulla risoluzione dei problemi

Collegamento agli articoli della Knowledge Base per assistenza nella risoluzione dei problemi relativi alla gestione degli intervalli di indirizzi IP della VLAN.

- "Avviso di IP duplicato dopo l'aggiunta di un nodo di archiviazione nella VLAN sul cluster Element"

- "Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati tali IP in Element"

Modifica VLAN VRF

È possibile modificare gli attributi VLAN VRF, come il nome VLAN, la netmask, il gateway e i blocchi di indirizzi IP.

1. Fare clic su **Cluster** > **Rete**.
2. Fare clic sull'icona Azioni per la VLAN che si desidera modificare.
3. Fare clic su **Modifica**.
4. Immettere i nuovi attributi per la VLAN VRF nella finestra di dialogo **Modifica VLAN**.
5. Fare clic su **Salva modifiche**.

Elimina una rete virtuale

È possibile rimuovere un oggetto di rete virtuale. Prima di rimuovere una rete virtuale, è necessario aggiungere i blocchi di indirizzi a un'altra rete virtuale.

1. Fare clic su **Cluster** > **Rete**.
2. Fare clic sull'icona Azioni relativa alla VLAN che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Trova maggiori informazioni

Modifica una rete virtuale

Creare un cluster che supporti le unità FIPS

Prepara il cluster Element per la funzionalità delle unità FIPS

La sicurezza sta diventando sempre più critica per l'implementazione di soluzioni in molti ambienti dei clienti. Gli standard federali per l'elaborazione delle informazioni (FIPS) sono standard per la sicurezza e l'interoperabilità informatica. La crittografia certificata FIPS 140-2 per i dati inattivi è un componente della soluzione di sicurezza complessiva.

Per preparare l'abilitazione della funzionalità delle unità FIPS, è opportuno evitare di mischiare nodi in cui alcuni sono compatibili con le unità FIPS e altri no.

Un cluster è considerato conforme alle unità FIPS in base alle seguenti condizioni:

- Tutte le unità sono certificate FIPS.
- Tutti i nodi sono nodi unità FIPS.
- La crittografia a riposo (EAR) è abilitata.
- La funzionalità delle unità FIPS è abilitata. Tutte le unità e i nodi devono essere compatibili con FIPS e la crittografia a riposo deve essere abilitata per abilitare la funzionalità unità FIPS.

Abilita la crittografia a riposo

È possibile abilitare e disabilitare la crittografia a livello di cluster quando è inattivo. Questa funzione non è abilitata per impostazione predefinita. Per supportare le unità FIPS, è necessario abilitare la crittografia a riposo.

1. Nell'interfaccia utente del software NetApp Element , fare clic su **Cluster** > **Impostazioni**.
2. Fare clic su **Abilita crittografia a riposo**.

Trova maggiori informazioni

- Abilitare e disabilitare la crittografia per un cluster
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Identificare se i nodi sono pronti per la funzionalità delle unità FIPS

È necessario verificare se tutti i nodi nel cluster di storage sono pronti a supportare le unità FIPS utilizzando il metodo API GetFipsReport del software NetApp Element .

Il report risultante mostra uno dei seguenti stati:

- Nessuno: il nodo non è in grado di supportare la funzionalità delle unità FIPS.
- Parziale: il nodo supporta FIPS, ma non tutte le unità sono FIPS.
- Pronto: il nodo è compatibile con FIPS e tutte le unità sono unità FIPS oppure non è presente alcuna unità.

Passi

1. Utilizzando l'API Element, verificare se i nodi e le unità nel cluster di archiviazione sono compatibili con le unità FIPS immettendo:

   ```
   GetFipsReport
   ```

2. Esaminare i risultati, annotando tutti i nodi che non visualizzano lo stato Pronto.
3. Per tutti i nodi che non visualizzano lo stato Pronto, verificare se l'unità è in grado di supportare la funzionalità delle unità FIPS:
   - Utilizzando l'API Element, immettere: `GetHardwareList`
   - Prendere nota del valore di **DriveEncryptionCapabilityType**. Se è "fips", l'hardware può supportare la funzionalità delle unità FIPS.

     Vedi i dettagli su `GetFipsReport` O `ListDriveHardware` nel "Riferimento API dell'elemento".
4. Se l'unità non supporta la funzionalità unità FIPS, sostituire l'hardware con hardware FIPS (nodo o unità).

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Abilita la funzionalità delle unità FIPS

È possibile abilitare la funzionalità delle unità FIPS utilizzando il software NetApp Element `EnableFeature` Metodo API.

La crittografia a riposo deve essere abilitata sul cluster e tutti i nodi e le unità devono essere compatibili con FIPS, come indicato quando GetFipsReport visualizza lo stato Pronto per tutti i nodi.

Fare un passo

1. Utilizzando l'API Element, abilitare FIPS su tutte le unità immettendo:

   ```
   EnableFeature params: FipsDrives
   ```

Trova maggiori informazioni

- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Controllare lo stato dell'unità FIPS

È possibile verificare se la funzionalità delle unità FIPS è abilitata sul cluster utilizzando il software NetApp Element `GetFeatureStatus` Metodo API che mostra se lo stato FIPS Drives Enabled è vero o falso.

1. Utilizzando l'API Element, verificare la funzionalità delle unità FIPS sul cluster immettendo:

   ```
   GetFeatureStatus
   ```

2. Esaminare i risultati del `GetFeatureStatus` Chiamata API. Se il valore Unità FIPS abilitate è Vero, la funzionalità Unità FIPS è abilitata.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Trova maggiori informazioni

- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Risolvere i problemi della funzionalità dell'unità FIPS

Utilizzando l'interfaccia utente del software NetApp Element , è possibile visualizzare avvisi per informazioni su guasti o errori del cluster nel sistema correlati alla funzionalità delle unità FIPS.

1. Utilizzando l'interfaccia utente di Element, seleziona **Reporting** > **Avvisi**.
2. Cercare guasti del cluster, tra cui:
   - Unità FIPS non corrispondenti
   - FIPS non rispetta la conformità
3. Per suggerimenti sulla risoluzione, vedere le informazioni sul codice di errore del cluster.

Trova maggiori informazioni

- Codici di errore del cluster
- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Stabilire una comunicazione sicura

Abilita FIPS 140-2 per HTTPS sul tuo cluster

È possibile utilizzare il metodo API EnableFeature per abilitare la modalità operativa FIPS 140-2 per le comunicazioni HTTPS.

Con il software NetApp Element , puoi scegliere di abilitare la modalità operativa Federal Information Processing Standards (FIPS) 140-2 sul tuo cluster. L'abilitazione di questa modalità attiva il NetApp Cryptographic Security Module (NCSM) e sfrutta la crittografia certificata FIPS 140-2 Livello 1 per tutte le comunicazioni tramite HTTPS all'interfaccia utente e all'API NetApp Element .

> Dopo aver abilitato la modalità FIPS 140-2, non è più possibile disattivarla. Quando la modalità FIPS 140-2 è abilitata, ogni nodo del cluster si riavvia ed esegue un autotest per verificare che NCSM sia correttamente abilitato e funzioni nella modalità certificata FIPS 140-2. Ciò provoca un'interruzione sia delle connessioni di gestione che di archiviazione sul cluster. È opportuno pianificare attentamente e abilitare questa modalità solo se l'ambiente in uso necessita del meccanismo di crittografia offerto.

Per ulteriori informazioni, consultare le informazioni sull'API Element.

Di seguito è riportato un esempio di richiesta API per abilitare FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Dopo aver abilitato questa modalità operativa, tutte le comunicazioni HTTPS utilizzano i cifrari approvati FIPS 140-2.

Trova maggiori informazioni

- Cifrari SSL
- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Cifrari SSL

I cifrari SSL sono algoritmi di crittografia utilizzati dagli host per stabilire una comunicazione sicura. Esistono cifrari standard supportati dal software Element e cifrari non standard quando è abilitata la modalità FIPS 140-2.

Gli elenchi seguenti forniscono i cifrari Secure Socket Layer (SSL) standard supportati dal software Element e i cifrari SSL supportati quando è abilitata la modalità FIPS 140-2:

- **FIPS 140-2 disabilitato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C

TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- **FIPS 140-2 abilitato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (sect571r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (sect571r1) - A

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A

  TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A

  TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

Trova maggiori informazioni

Abilita FIPS 140-2 per HTTPS sul tuo cluster

Inizia con la gestione delle chiavi esterne

Inizia con la gestione delle chiavi esterne

La gestione delle chiavi esterne (EKM) garantisce una gestione sicura delle chiavi di

autenticazione (AK) in combinazione con un server di chiavi esterne (EKS) esterno al cluster. Gli AK vengono utilizzati per bloccare e sbloccare le unità auto-crittografanti (SED) quando"crittografia a riposo" è abilitato sul cluster. L'EKS garantisce la generazione e l'archiviazione sicura degli AK. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito da OASIS, per comunicare con l'EKS.

- "Impostare la gestione esterna"
- "Crittografia software di reimpostazione della chiave principale a riposo"
- "Recupera le chiavi di autenticazione inaccessibili o non valide"
- "Comandi API di gestione delle chiavi esterne"

Trova maggiori informazioni

- "API CreateCluster che può essere utilizzata per abilitare la crittografia del software a riposo"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Impostare la gestione delle chiavi esterne

È possibile seguire questi passaggi e utilizzare i metodi API Element elencati per configurare la funzionalità di gestione delle chiavi esterne.

Cosa ti servirà

- Se si sta configurando la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, è stata abilitata la crittografia software a riposo utilizzando"Crea cluster" metodo su un nuovo cluster che non contiene volumi.

Passi

1. Stabilire una relazione di fiducia con l'External Key Server (EKS).
   a. Creare una coppia di chiavi pubblica/privata per il cluster Element che verrà utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API:"Crea coppia di chiavi pubbliche e private"
   b. Ottieni la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. Il CSR consente al server delle chiavi di verificare che il cluster Element che accederà alle chiavi sia autenticato come cluster Element. Chiamare il seguente metodo API:"Ottieni richiesta di firma del certificato del client"
   c. Utilizzare EKS/Autorità di certificazione per firmare il CSR recuperato. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un fornitore di chiavi definisce dove ottenere una chiave, mentre un server definisce gli attributi specifici dell'EKS con cui verrà comunicata.
   a. Crea un fornitore di chiavi in cui risiederanno i dettagli del server delle chiavi chiamando il seguente metodo API:"CreateKeyProviderKmip"
   b. Creare un server di chiavi che fornisca il certificato firmato e il certificato di chiave pubblica dell'Autorità di certificazione chiamando i seguenti metodi API:"CreateKeyServerKmip" "TestKeyServerKmip"

      Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

c. Aggiungere il server delle chiavi al contenitore del provider delle chiavi chiamando i seguenti metodi API:"AggiungiKeyServerAlProviderKmip" "TestKeyProviderKmip"

   Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

3. Come passaggio successivo per la crittografia a riposo, eseguire una delle seguenti operazioni:
   a. (Per la crittografia hardware a riposo) Abilita"crittografia hardware a riposo" fornendo l'ID del fornitore di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il"Abilita crittografia a riposo" Metodo API.

      È necessario abilitare la crittografia a riposo tramite"API" . Abilitando la crittografia a riposo tramite il pulsante Element UI esistente, la funzionalità tornerà a utilizzare chiavi generate internamente.

   b. (Per la crittografia software a riposo) Per"crittografia software a riposo" per utilizzare il fornitore di chiavi appena creato, passare l'ID del fornitore di chiavi al"RekeySoftwareEncryptionAtRestMasterKey" Metodo API.

Trova maggiori informazioni

- "Abilitare e disabilitare la crittografia per un cluster"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Crittografia software di reimpostazione della chiave principale a riposo

È possibile utilizzare l'API Element per rigenerare una chiave esistente. Questo processo crea una nuova chiave master sostitutiva per il server di gestione delle chiavi esterno. Le chiavi principali vengono sempre sostituite da nuove chiavi principali e non vengono mai duplicate o sovrascritte.

Potrebbe essere necessario rinominare la chiave come parte di una delle seguenti procedure:

- Creare una nuova chiave come parte di un passaggio dalla gestione delle chiavi interne alla gestione delle chiavi esterne.
- Crea una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.

Questo processo è asincrono e restituisce una risposta prima che l'operazione di reimpostazione delle chiavi sia completata. Puoi usare il"Ottieni risultato asincrono" metodo per interrogare il sistema per vedere quando il processo è stato completato.

Cosa ti servirà

- Hai abilitato la crittografia software a riposo utilizzando"Crea cluster" metodo su un nuovo cluster che non contiene volumi e non ha I/O. Utilizzare il collegamento:../api/reference_element_api_getsoftwareencryptionatrestinfo.html[`GetSoftwareEncryptionatRestInfo`] per confermare che lo stato è `enabled` prima di procedere.
- Hai"ha stabilito un rapporto di fiducia" tra il cluster SolidFire e un External Key Server (EKS). Esegui il"TestKeyProviderKmip" metodo per verificare che sia stata stabilita una connessione con il fornitore della chiave.

Passi

1. Esegui il"ListKeyProvidersKmip" comando e copia l'ID del fornitore della chiave(`keyProviderID`).
2. Esegui il"RekeySoftwareEncryptionAtRestMasterKey" con il `keyManagementType` parametro come `external` E `keyProviderID` come numero ID del fornitore della chiave dal passaggio precedente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copia il `asyncHandle` valore dal `RekeySoftwareEncryptionAtRestMasterKey` risposta al comando.
4. Esegui il"Ottieni risultato asincrono" comando con il `asyncHandle` valore del passaggio precedente per confermare la modifica nella configurazione. Dalla risposta al comando dovresti vedere che la vecchia configurazione della chiave principale è stata aggiornata con le nuove informazioni sulla chiave. Copiare l'ID del nuovo fornitore di chiavi per utilizzarlo in un passaggio successivo.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Esegui il `GetSoftwareEncryptionatRestInfo` comando per confermare i nuovi dettagli della chiave, incluso il `keyProviderID` , sono stati aggiornati.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Trova maggiori informazioni

- "Gestisci l'archiviazione con l'API Element"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Recupera le chiavi di autenticazione inaccessibili o non valide

Occasionalmente può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, verrà generato un errore del cluster (denominato codice di errore del cluster). Qui vengono descritti i due casi più probabili.

Il cluster non è in grado di sbloccare le unità a causa di un errore del cluster KmipServerFault.

Ciò può verificarsi quando il cluster si avvia per la prima volta e il server delle chiavi non è accessibile o la chiave richiesta non è disponibile.

1. Seguire i passaggi di ripristino indicati nei codici di errore del cluster (se presenti).

Potrebbe essere impostato un errore sliceServiceUnhealthy perché le unità dei metadati sono state contrassegnate come non riuscite e impostate sullo stato "Disponibile".

Passaggi per la cancellazione:

1. Aggiungere nuovamente le unità.
2. Dopo 3 o 4 minuti, verificare che il `sliceServiceUnhealthy` il guasto è stato risolto.

Vedere"codici di errore del cluster" per maggiori informazioni.

Comandi API di gestione delle chiavi esterne

Elenco di tutte le API disponibili per la gestione e la configurazione di EKM.

Utilizzato per stabilire una relazione di fiducia tra il cluster e i server esterni di proprietà del cliente:

- Crea coppia di chiavi pubbliche e private
- Ottieni richiesta di firma del certificato del client

Utilizzato per definire i dettagli specifici dei server esterni di proprietà del cliente:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

Utilizzato per creare e gestire i fornitori di chiavi che gestiscono server di chiavi esterni:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AggiungiKeyServerAlProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Per informazioni sui metodi API, vedere "Informazioni di riferimento API".

Gestire volumi e volumi virtuali

Scopri di più sulla gestione dei volumi e dei volumi virtuali

È possibile gestire i dati in un cluster che esegue il software Element dalla scheda Gestione nell'interfaccia utente di Element. Le funzioni di gestione dei cluster disponibili includono la creazione e la gestione di volumi di dati, gruppi di accesso ai volumi, iniziatori e criteri di qualità del servizio (QoS).

Lavorare con i volumi

Il sistema SolidFire fornisce spazio di archiviazione tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel. Dalla pagina Volumi nella scheda Gestione, è possibile creare, modificare, clonare ed eliminare volumi su un nodo. È anche possibile visualizzare statistiche sulla larghezza di banda del volume e sull'utilizzo di I/O.

"Scopri come lavorare con i volumi"

Lavorare con volumi virtuali

È possibile visualizzare informazioni ed eseguire attività per volumi virtuali e relativi contenitori di archiviazione, endpoint di protocollo, associazioni e host utilizzando l'interfaccia utente di Element.

Il sistema di archiviazione software NetApp Element viene fornito con la funzionalità Virtual Volumes (VVols) disabilitata. È necessario eseguire un'attività una tantum di abilitazione manuale della funzionalità vSphere VVol tramite l'interfaccia utente di Element.

Dopo aver abilitato la funzionalità VVol, nell'interfaccia utente viene visualizzata la scheda VVols, che offre opzioni di monitoraggio e gestione limitate relative a VVols. Inoltre, un componente software lato storage noto come VASA Provider funge da servizio di storage awareness per vSphere. La maggior parte dei comandi VVol, come la creazione, la clonazione e la modifica di VVol, vengono avviati da un vCenter Server o da un host ESXi e tradotti dal provider VASA nelle API Element per il sistema di archiviazione software Element. I comandi per creare, eliminare e gestire contenitori di archiviazione ed eliminare volumi virtuali possono essere avviati tramite l'interfaccia utente di Element.

La maggior parte delle configurazioni necessarie per utilizzare la funzionalità Virtual Volumes con i sistemi di storage software Element vengono eseguite in vSphere. Consultare la *Guida alla configurazione di VMware vSphere Virtual Volumes for SolidFire Storage* per registrare il provider VASA in vCenter, creare e gestire datastore VVol e gestire l'archiviazione in base ai criteri.

> Per Element 12.5 e versioni precedenti, non registrare più di un provider NetApp Element VASA su una singola istanza di vCenter. Se viene aggiunto un secondo provider NetApp Element VASA, tutti i datastore VVOL diventano inaccessibili.

> Il supporto VASA per più vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con il tuo vCenter. Per installare, scaricare il file VASA39 .tar.gz dal "Download del software NetApp" sito e seguire le istruzioni riportate nel manifesto. Il provider NetApp Element VASA utilizza un certificato NetApp . Con questa patch, il certificato viene utilizzato senza modifiche da vCenter per supportare più vCenter per l'utilizzo di VASA e VVol. Non modificare il certificato. I certificati SSL personalizzati non sono supportati da VASA.

"Scopri come lavorare con i volumi virtuali"

Lavorare con gruppi di accesso al volume e iniziatori

È possibile utilizzare gli iniziatori iSCSI o gli iniziatori Fibre Channel per accedere ai volumi definiti all'interno dei gruppi di accesso ai volumi.

È possibile creare gruppi di accesso mappando gli IQN dell'iniziatore iSCSI o i WWPN Fibre Channel in una raccolta di volumi. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza richiedere l'autenticazione CHAP.

Esistono due tipi di metodi di autenticazione CHAP:

- Autenticazione CHAP a livello di account: è possibile assegnare l'autenticazione CHAP all'account.
- Autenticazione CHAP a livello di iniziatore: è possibile assegnare segreti e target CHAP univoci per iniziatori specifici senza essere vincolati a un singolo CHAP per un singolo account. Questa autenticazione CHAP a livello di iniziatore sostituisce le credenziali a livello di account.

Facoltativamente, con CHAP per iniziatore, è possibile applicare l'autorizzazione dell'iniziatore e

l'autenticazione CHAP per iniziatore. Queste opzioni possono essere definite per ogni iniziatore e un gruppo di accesso può contenere un mix di iniziatori con opzioni diverse.

Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso alla rete Fibre Channel ai volumi nel gruppo di accesso.

I gruppi di accesso al volume hanno i seguenti limiti:

- In un gruppo di accesso sono consentiti al massimo 64 IQN o WWPN.
- Un gruppo di accesso può essere composto da un massimo di 2000 volumi.
- Un IQN o WWPN può appartenere a un solo gruppo di accesso.
- Un singolo volume può appartenere a un massimo di quattro gruppi di accesso.

"Scopri come lavorare con i gruppi di accesso al volume e gli iniziatori"

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Lavorare con i volumi

Gestire le politiche di qualità del servizio

Un criterio di qualità del servizio (QoS) consente di creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi. È possibile creare, modificare ed eliminare i criteri QoS dalla pagina Criteri QoS nella scheda Gestione.

Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.

"Video NetApp : Criteri di qualità del servizio SolidFire"

Vedere"Prestazioni e qualità del servizio" .

- Creare una policy QoS
- Modifica una policy QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare criteri QoS e applicarli durante la creazione dei volumi.

1. Selezionare **Gestione** > **Criteri QoS**.
2. Fare clic su **Crea criterio QoS**.
3. Inserisci il **Nome della polizza**.

4. Immettere i valori **MIN IOPS**, **MAX IOPS** e **Burst IOPS**.
5. Fare clic su **Crea criterio QoS**.

Modifica una policy QoS

È possibile modificare il nome di un criterio QoS esistente o modificare i valori associati al criterio. La modifica di una policy QoS influisce su tutti i volumi associati alla policy.

1. Selezionare **Gestione** > **Criteri QoS**.
2. Fare clic sull'icona Azioni per il criterio QoS che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica criterio QoS**, modificare le seguenti proprietà come richiesto:
   - Nome della polizza
   - IOPS minimi
   - IOPS massimi
   - IOPS a raffica
5. Fare clic su **Salva modifiche**.

Eliminare una policy QoS

È possibile eliminare un criterio QoS se non è più necessario. Quando si elimina un criterio QoS, tutti i volumi associati al criterio mantengono le impostazioni QoS ma non vengono più associati al criterio.

> Se invece si sta tentando di dissociare un volume da una policy QoS, è possibile modificare le impostazioni QoS per quel volume in personalizzate.

1. Selezionare **Gestione** > **Criteri QoS**.
2. Fare clic sull'icona Azioni per il criterio QoS che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.

Trova maggiori informazioni

- "Rimuovere l'associazione della policy QoS di un volume"
- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Gestire i volumi

Il sistema SolidFire fornisce spazio di archiviazione tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel.

Dalla pagina Volumi nella scheda Gestione, è possibile creare, modificare, clonare ed eliminare volumi su un nodo.

Crea un volume

È possibile creare un volume e associarlo a un determinato account. Ogni volume deve essere associato a un account. Questa associazione consente all'account di accedere al volume tramite gli iniziatori iSCSI utilizzando le credenziali CHAP.

È possibile specificare le impostazioni QoS per un volume durante la creazione.

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic su **Crea volume**.
3. Nella finestra di dialogo **Crea un nuovo volume**, immettere il **Nome del volume**.
4. Inserisci la dimensione totale del volume.

   La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

   - 1 GB = 1 000 000 000 byte
   - 1 GiB = 1 073 741 824 byte
5. Selezionare una **Dimensione blocco** per il volume.
6. Fare clic sull'elenco a discesa **Account** e selezionare l'account che deve avere accesso al volume.

   Se non esiste un account, fare clic sul collegamento **Crea account**, immettere un nuovo nome account e fare clic su **Crea**. L'account viene creato e associato al nuovo volume.

   Se ci sono più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico ti mostrerà i possibili valori tra cui scegliere.
7. Per impostare la **Qualità del servizio**, procedere in uno dei seguenti modi:
   a. In **Criterio** è possibile selezionare un criterio QoS esistente, se disponibile.
   b. In **Impostazioni personalizzate**, imposta i valori minimi, massimi e burst personalizzati per IOPS oppure utilizza i valori QoS predefiniti.

      I volumi con un valore Max o Burst IOPS superiore a 20.000 IOPS potrebbero richiedere un'elevata profondità di coda o più sessioni per raggiungere questo livello di IOPS su un singolo volume.
8. Fare clic su **Crea volume**.

Visualizza i dettagli del volume

1. Selezionare **Gestione** > **Volumi**.
2. Esamina i dettagli.
   - **ID**: ID generato dal sistema per il volume.
   - **Nome**: il nome assegnato al volume al momento della sua creazione.
   - **Account**: Nome dell'account assegnato al volume.
   - **Gruppi di accesso**: il nome del gruppo o dei gruppi di accesso al volume a cui appartiene il volume.
   - **Accesso**: tipo di accesso assegnato al volume al momento della sua creazione. Valori possibili:
     - Lettura/Scrittura: sono accettate tutte le letture e le scritture.

        - Sola lettura: sono consentite tutte le attività di lettura; non sono consentite le attività di scrittura.
        - Bloccato: è consentito solo l'accesso dell'amministratore.
        - ReplicationTarget: designato come volume di destinazione in una coppia di volumi replicati.
    - **Utilizzato**: percentuale di spazio utilizzato nel volume.
    - **Dimensione**: la dimensione totale (in GB) del volume.
    - **ID nodo primario**: il nodo primario per questo volume.
    - **ID nodo secondario**: elenco dei nodi secondari per questo volume. Possono assumere più valori durante gli stati transitori, come il cambio dei nodi secondari, ma solitamente avranno un singolo valore.
    - **QoS Throttle**: identifica se il volume è stato limitato a causa dell'elevato carico sul nodo di archiviazione primario.
    - **Criterio QoS**: nome e collegamento al criterio QoS definito dall'utente.
    - **MIN IOPS**: numero minimo di IOPS garantiti per il volume.
    - **IOPS massimi**: numero massimo di IOPS consentiti per il volume.
    - **Burst IOPS**: il numero massimo di IOPS consentiti in un breve periodo di tempo per il volume. Predefinito = 15.000.
    - **Snapshot**: numero di snapshot creati per il volume.
    - **Attributi**: attributi assegnati al volume come coppia chiave/valore tramite un metodo API.
    - **512e**: Indica se 512e è abilitato su un volume. Valori possibili:
        - SÌ
        - NO
    - **Creato il**: data e ora in cui è stato creato il volume.

Visualizza i dettagli dei singoli volumi

È possibile visualizzare le statistiche sulle prestazioni per singoli volumi.

1. Selezionare **Reporting** > **Prestazioni volume**.
2. Nell'elenco dei volumi, fare clic sull'icona Azioni per un volume.
3. Fare clic su **Visualizza dettagli**.

   Nella parte inferiore della pagina viene visualizzata una barra contenente informazioni generali sul volume.

4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi altri dettagli**.

   Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Modifica volumi attivi

È possibile modificare gli attributi del volume, quali i valori QoS, le dimensioni del volume e l'unità di misura in cui vengono calcolati i valori dei byte. È anche possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

È possibile ridimensionare un volume quando c'è spazio sufficiente sul cluster nelle seguenti condizioni:

- Condizioni operative normali.
- Vengono segnalati errori o guasti del volume.
- Il volume è in fase di clonazione.
- Il volume è in fase di risincronizzazione.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Nella finestra **Attiva**, fare clic sull'icona Azioni per il volume che si desidera modificare.
3. Fare clic su **Modifica**.
4. **Facoltativo:** modifica la dimensione totale del volume.
   - È possibile aumentare, ma non diminuire, la dimensione del volume. È possibile ridimensionare un solo volume in un'unica operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.
   - Se si desidera modificare le dimensioni del volume per la replica, è necessario innanzitutto aumentare le dimensioni del volume assegnato come destinazione della replica. Quindi puoi ridimensionare il volume sorgente. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

     La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

   - 1 GB = 1 000 000 000 byte
   - 1 GiB = 1 073 741 824 byte
5. **Facoltativo:** seleziona un livello di accesso all'account diverso tra i seguenti:
   - Solo lettura
   - Lettura/scrittura
   - Bloccato
   - Obiettivo di replicazione
6. **Facoltativo:** seleziona l'account che deve avere accesso al volume.

   Se l'account non esiste, fare clic sul collegamento **Crea account**, immettere un nuovo nome account e fare clic su **Crea**. L'account viene creato e associato al volume.

   Se ci sono più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico ti mostrerà i possibili valori tra cui scegliere.

7. **Facoltativo:** per modificare la selezione in **Qualità del servizio**, procedere in uno dei seguenti modi:
   a. In **Criterio** è possibile selezionare un criterio QoS esistente, se disponibile.
   b. In **Impostazioni personalizzate**, imposta i valori minimi, massimi e burst personalizzati per IOPS oppure utilizza i valori QoS predefiniti.

      Se si utilizzano criteri QoS su un volume, è possibile impostare un QoS personalizzato per rimuovere l'affiliazione del criterio QoS al volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.

Quando si modificano i valori IOPS, è necessario incrementarli in decine o centinaia. I valori di input richiedono numeri interi validi.

Configurare volumi con un valore burst estremamente elevato. Ciò consente al sistema di elaborare più rapidamente carichi di lavoro sequenziali occasionali di grandi blocchi, limitando comunque gli IOPS sostenuti per un volume.

8. Fare clic su **Salva modifiche**.

Elimina un volume

È possibile eliminare uno o più volumi da un cluster di archiviazione Element.

Il sistema non elimina immediatamente un volume eliminato; il volume rimane disponibile per circa otto ore. Se si ripristina un volume prima che il sistema lo elimini, il volume torna online e le connessioni iSCSI vengono ripristinate.

Se un volume utilizzato per creare uno snapshot viene eliminato, gli snapshot associati diventano inattivi. Quando i volumi di origine eliminati vengono eliminati, anche gli snapshot inattivi associati vengono rimossi dal sistema.

I volumi persistenti associati ai servizi di gestione vengono creati e assegnati a un nuovo account durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare i volumi o l'account associato.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Per eliminare un singolo volume, procedere come segue:
   a. Fare clic sull'icona Azioni relativa al volume che si desidera eliminare.
   b. Nel menu che si apre, fare clic su **Elimina**.
   c. Conferma l'azione.

   Il sistema sposta il volume nell'area **Eliminati** nella pagina **Volumi**.
3. Per eliminare più volumi, procedere come segue:
   a. Nell'elenco dei volumi, seleziona la casella accanto ai volumi che desideri eliminare.
   b. Fare clic su **Azioni in blocco**.
   c. Nel menu che si apre, fare clic su **Elimina**.
   d. Conferma l'azione.

   Il sistema sposta i volumi nell'area **Eliminati** nella pagina **Volumi**.

Ripristina un volume eliminato

È possibile ripristinare un volume nel sistema se è stato eliminato ma non ancora ripulito. Il sistema elimina automaticamente un volume circa otto ore dopo la sua eliminazione. Se il sistema ha eliminato il volume, non è possibile ripristinarlo.

1. Selezionare **Gestione** > **Volumi**.

2. Fare clic sulla scheda **Eliminati** per visualizzare l'elenco dei volumi eliminati.
3. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
4. Nel menu che si apre, fare clic su **Ripristina**.
5. Conferma l'azione.

   Il volume viene inserito nell'elenco dei volumi **Attivi** e le connessioni iSCSI al volume vengono ripristinate.

Svuota un volume

Quando un volume viene eliminato, viene rimosso definitivamente dal sistema. Tutti i dati nel volume andranno persi.

Il sistema elimina automaticamente i volumi eliminati otto ore dopo l'eliminazione. Tuttavia, se si desidera eliminare un volume prima dell'orario programmato, è possibile farlo.

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic sul pulsante **Eliminato**.
3. Eseguire i passaggi per eliminare un singolo volume o più volumi.

Opzione	Passi
Svuotare un singolo volume	a. Fare clic sull'icona Azioni relativa al volume che si desidera eliminare. b. Fare clic su **Elimina**. c. Conferma l'azione.
Svuota più volumi	a. Selezionare i volumi che si desidera eliminare. b. Fare clic su **Azioni in blocco**. c. Nel menu che si apre, seleziona **Elimina**. d. Conferma l'azione.

Clonare un volume

È possibile creare un clone di un singolo volume o di più volumi per realizzare una copia dei dati in un dato momento. Quando si clona un volume, il sistema crea uno snapshot del volume e quindi crea una copia dei dati a cui fa riferimento lo snapshot. Si tratta di un processo asincrono e la quantità di tempo richiesta dipende dalle dimensioni del volume che si sta clonando e dal carico attuale del cluster.

Il cluster supporta fino a due richieste di clonazione in esecuzione per volume alla volta e fino a otto operazioni di clonazione di volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per essere elaborate in un secondo momento.

> I sistemi operativi differiscono nel modo in cui gestiscono i volumi clonati. VMware ESXi tratterà un volume clonato come una copia del volume o un volume snapshot. Il volume sarà un dispositivo disponibile da utilizzare per creare un nuovo datastore. Per ulteriori informazioni sul montaggio di volumi clone e sulla gestione di LUN snapshot, consultare la documentazione VMware su "montaggio di una copia del datastore VMFS" E "gestione di datastore VMFS duplicati" .

Prima di troncare un volume clonato clonandolo in una dimensione più piccola, assicurarsi di preparare le partizioni in modo che si adattino al volume più piccolo.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Per clonare un singolo volume, procedere come segue:
   a. Nell'elenco dei volumi nella pagina **Attivi**, fare clic sull'icona Azioni per il volume che si desidera clonare.
   b. Nel menu che si apre, fare clic su **Clona**.
   c. Nella finestra **Clona volume**, immettere un nome per il volume appena clonato.
   d. Selezionare una dimensione e una misura per il volume utilizzando la casella di selezione e l'elenco **Dimensione volume**.

      La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

      - 1 GB = 1 000 000 000 byte
      - 1 GiB = 1 073 741 824 byte

   e. Selezionare il tipo di accesso per il volume appena clonato.
   f. Selezionare un account da associare al volume appena clonato dall'elenco **Account**.

      Puoi creare un account durante questa fase cliccando sul link **Crea account**, inserendo un nome account e cliccando su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'account all'elenco **Account**.

3. Per clonare più volumi, procedere come segue:
   a. Nell'elenco dei volumi nella pagina **Attivi**, seleziona la casella accanto ai volumi che desideri clonare.
   b. Fare clic su **Azioni in blocco**.
   c. Nel menu che si apre, seleziona **Clona**.
   d. Nella finestra di dialogo **Clona più volumi**, immettere un prefisso per i volumi clonati nel campo **Nuovo prefisso nome volume**.
   e. Selezionare un account da associare ai volumi clonati dall'elenco **Account**.
   f. Selezionare il tipo di accesso per i volumi clonati.
4. Fare clic su **Avvia clonazione**.

Aumentando la dimensione del volume di un clone si ottiene un nuovo volume con spazio libero aggiuntivo alla fine del volume. A seconda di come si utilizza il volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per sfruttarlo.

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Assegnare LUN ai volumi Fibre Channel

È possibile modificare l'assegnazione LUN per un volume Fibre Channel in un gruppo di accesso al volume. È anche possibile effettuare assegnazioni LUN del volume Fibre Channel quando si crea un gruppo di accesso al volume.

L'assegnazione di nuovi LUN Fibre Channel è una funzione avanzata e potrebbe avere conseguenze sconosciute sull'host connesso. Ad esempio, il nuovo ID LUN potrebbe non essere rilevato automaticamente sull'host e l'host potrebbe richiedere una nuova scansione per rilevarlo.

1. Selezionare **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. In **Assegna ID LUN** nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Assegnazioni LUN**.
5. Per ogni volume nell'elenco a cui si desidera assegnare un LUN, immettere un nuovo valore nel campo **LUN** corrispondente.
6. Fare clic su **Salva modifiche**.

Applicare una policy QoS ai volumi

È possibile applicare in blocco una policy QoS esistente a uno o più volumi.

Deve esistere la policy QoS che si desidera applicare in blocco.

1. Selezionare **Gestione** > **Volumi**.
2. Nell'elenco dei volumi, seleziona la casella accanto ai volumi a cui desideri applicare la policy QoS.
3. Fare clic su **Azioni in blocco**.
4. Nel menu visualizzato, fare clic su **Applica criterio QoS**.
5. Selezionare il criterio QoS dall'elenco a discesa.
6. Fare clic su **Applica**.

Trova maggiori informazioni

Politiche di qualità del servizio

Rimuovere l'associazione della policy QoS di un volume

È possibile rimuovere un'associazione di criteri QoS da un volume selezionando le impostazioni QoS personalizzate.

Il volume che si desidera modificare deve essere associato a una policy QoS.

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic sull'icona Azioni per un volume che contiene un criterio QoS che si desidera modificare.
3. Fare clic su **Modifica**.
4. Nel menu visualizzato in **Qualità del servizio**, fare clic su **Impostazioni personalizzate**.

5. Modificare **Min IOPS**, **Max IOPS** e **Burst IOPS** oppure mantenere le impostazioni predefinite.
6. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

Eliminare una policy QoS

Lavorare con volumi virtuali

Abilita volumi virtuali

È necessario abilitare manualmente la funzionalità vSphere Virtual Volumes (VVols) tramite il software NetApp Element . Il sistema software Element è dotato di funzionalità VVols disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento. L'abilitazione della funzionalità VVols è un'attività di configurazione che deve essere eseguita una sola volta.

Cosa ti servirà

- Il cluster deve eseguire Element 9.0 o versione successiva.
- Il cluster deve essere connesso a un ambiente ESXi 6.0 o successivo compatibile con VVols.
- Se si utilizza Element 11.3 o versione successiva, il cluster deve essere connesso a un ambiente ESXi 6.0 aggiornamento 3 o versione successiva.

> L'abilitazione della funzionalità vSphere Virtual Volumes modifica in modo permanente la configurazione del software Element. È opportuno abilitare la funzionalità VVols solo se il cluster è connesso a un ambiente compatibile con VMware ESXi VVols. È possibile disattivare la funzionalità VVols e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica, eliminando così tutti i dati presenti sul sistema.

Passi

1. Selezionare **Cluster** > **Impostazioni**.
2. Trova le impostazioni specifiche del cluster per i volumi virtuali.
3. Fare clic su **Abilita volumi virtuali**.
4. Fare clic su **Sì** per confermare la modifica alla configurazione dei volumi virtuali.

   La scheda **VVols** viene visualizzata nell'interfaccia utente di Element.

   > Quando la funzionalità VVols è abilitata, il cluster SolidFire avvia il provider VASA, apre la porta 8444 per il traffico VASA e crea endpoint di protocollo che possono essere rilevati da vCenter e da tutti gli host ESXi.

5. Copiare l'URL del provider VASA dalle impostazioni dei volumi virtuali (VVol) in **Cluster** > **Impostazioni**. Utilizzerai questo URL per registrare il provider VASA in vCenter.
6. Creare un contenitore di archiviazione in **VVols** > **Contenitori di archiviazione**.

   > È necessario creare almeno un contenitore di archiviazione affinché le VM possano essere fornite a un datastore VVol.

7. Selezionare **VVols** > **Endpoint protocollo**.
8. Verificare che sia stato creato un endpoint del protocollo per ciascun nodo del cluster.

> In vSphere sono necessarie ulteriori attività di configurazione. Consultare la *Guida alla configurazione di VMware vSphere Virtual Volumes for SolidFire Storage* per registrare il provider VASA in vCenter, creare e gestire datastore VVol e gestire l'archiviazione in base ai criteri.

Trova maggiori informazioni

"Guida alla configurazione di VMware vSphere Virtual Volumes per SolidFire Storage"

Visualizza i dettagli del volume virtuale

È possibile esaminare le informazioni sui volumi virtuali per tutti i volumi virtuali attivi nel cluster nell'interfaccia utente di Element. È inoltre possibile visualizzare l'attività delle prestazioni per ciascun volume virtuale, inclusi input, output, throughput, latenza, profondità della coda e informazioni sul volume.

Cosa ti servirà

- Dovresti aver abilitato la funzionalità VVols nell'interfaccia utente Element per il cluster.
- Dovresti aver creato un contenitore di archiviazione associato.
- Dovresti aver configurato il tuo cluster vSphere per utilizzare la funzionalità VVols del software Element.
- Dovresti aver creato almeno una VM in vSphere.

Passi

1. Fare clic su **VVols** > **Volumi virtuali**.

   Vengono visualizzate le informazioni per tutti i volumi virtuali attivi.

2. Fare clic sull'icona **Azioni** per il volume virtuale che si desidera esaminare.
3. Nel menu visualizzato, seleziona **Visualizza dettagli**.

Dettagli

La pagina Volumi virtuali della scheda VVols fornisce informazioni su ciascun volume virtuale attivo nel cluster, ad esempio ID volume, ID snapshot, ID volume virtuale padre e ID volume virtuale.

- **ID volume**: ID del volume sottostante.
- **ID snapshot**: ID dello snapshot del volume sottostante. Il valore è 0 se il volume virtuale non rappresenta uno snapshot SolidFire .
- **ID volume virtuale padre**: ID del volume virtuale padre. Se l'ID è composto da soli zeri, il volume virtuale è indipendente e non ha alcun collegamento con un elemento padre.
- **ID volume virtuale**: UUID del volume virtuale.
- **Nome**: il nome assegnato al volume virtuale.
- **Contenitore di archiviazione**: il contenitore di archiviazione che possiede il volume virtuale.
- **Tipo di sistema operativo guest**: sistema operativo associato al volume virtuale.

- **Tipo di volume virtuale**: il tipo di volume virtuale: Configurazione, Dati, Memoria, Swap o Altro.
- **Accesso**: autorizzazioni di lettura-scrittura assegnate al volume virtuale.
- **Dimensione**: la dimensione del volume virtuale in GB o GiB.
- **Snapshot**: numero di snapshot associati. Fare clic sul numero per collegarsi ai dettagli dello snapshot.
- **IOPS minimi**: impostazione QoS IOPS minima del volume virtuale.
- **IOPS massimi**: impostazione QoS IOPS massima del volume virtuale.
- **Burst IOPS**: impostazione QoS burst massima del volume virtuale.
- **VMW_VmID**: le informazioni nei campi preceduti da "VMW_" sono definite da VMware.
- **Ora di creazione**: ora in cui è stata completata l'attività di creazione del volume virtuale.

Dettagli individuali del volume virtuale

La pagina Volumi virtuali nella scheda VVols fornisce le seguenti informazioni sui volumi virtuali quando si seleziona un singolo volume virtuale e ne si visualizzano i dettagli.

- **VMW_XXX**: Le informazioni nei campi preceduti da "VMW_" sono definite da VMware.
- **ID volume virtuale padre**: ID del volume virtuale padre. Se l'ID è composto da soli zeri, il volume virtuale è indipendente e non ha alcun collegamento con un elemento padre.
- **ID volume virtuale**: UUID del volume virtuale.
- **Tipo di volume virtuale**: il tipo di volume virtuale: Configurazione, Dati, Memoria, Swap o Altro.
- **ID volume**: ID del volume sottostante.
- **Accesso**: autorizzazioni di lettura-scrittura assegnate al volume virtuale.
- **Nome account**: Nome dell'account contenente il volume.
- **Gruppi di accesso**: gruppi di accesso al volume associati.
- **Dimensione totale del volume**: capacità totale fornita in byte.
- **Blocchi diversi da zero**: numero totale di blocchi da 4 KiB con dati dopo il completamento dell'ultima operazione di garbage collection.
- **Zero Blocchi**: numero totale di blocchi da 4 KiB senza dati dopo il completamento dell'ultimo ciclo di operazioni di garbage collection.
- **Snapshot**: numero di snapshot associati. Fare clic sul numero per collegarsi ai dettagli dello snapshot.
- **IOPS minimi**: impostazione QoS IOPS minima del volume virtuale.
- **IOPS massimi**: impostazione QoS IOPS massima del volume virtuale.
- **Burst IOPS**: impostazione QoS burst massima del volume virtuale.
- **Abilita 512**: poiché i volumi virtuali utilizzano sempre l'emulazione della dimensione del blocco da 512 byte, il valore è sempre sì.
- **Volumi accoppiati**: indica se un volume è accoppiato.
- **Ora di creazione**: ora in cui è stata completata l'attività di creazione del volume virtuale.
- **Dimensione blocchi**: dimensione dei blocchi sul volume.
- **Scritture non allineate**: per i volumi 512e, il numero di operazioni di scrittura che non si sono svolte su un limite di settore di 4k. Un numero elevato di scritture non allineate potrebbe indicare un allineamento non corretto delle partizioni.

- **Letture non allineate**: per i volumi 512e, il numero di operazioni di lettura che non si trovavano su un confine di settore 4k. Un numero elevato di letture non allineate potrebbe indicare un allineamento non corretto delle partizioni.
- **scsiEUIDeviceID**: identificatore univoco globale del dispositivo SCSI per il volume nel formato a 16 byte basato su EUI-64.
- **scsiNAADeviceID**: identificatore univoco globale del dispositivo SCSI per il volume nel formato NAA IEEE Registered Extended.
- **Attributi**: Elenco di coppie nome-valore nel formato oggetto JSON.

Elimina un volume virtuale

Sebbene i volumi virtuali debbano sempre essere eliminati dal VMware Management Layer, la funzionalità per eliminare i volumi virtuali è abilitata dall'interfaccia utente di Element. È opportuno eliminare un volume virtuale dall'interfaccia utente di Element solo quando assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire .

1. Selezionare **VVols** > **Volumi virtuali**.
2. Fare clic sull'icona Azioni relativa al volume virtuale che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.

> È necessario eliminare un volume virtuale dal VMware Management Layer per garantire che il volume virtuale sia correttamente scollegato prima dell'eliminazione. È opportuno eliminare un volume virtuale dall'interfaccia utente di Element solo quando assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire . Se si elimina un volume virtuale dall'interfaccia utente di Element, il volume verrà eliminato immediatamente.

4. Conferma l'azione.
5. Aggiornare l'elenco dei volumi virtuali per confermare che il volume virtuale è stato rimosso.
6. **Facoltativo**: selezionare **Segnalazione** > **Registro eventi** per confermare che la cancellazione è avvenuta correttamente.

Gestire i contenitori di stoccaggio

Un contenitore di archiviazione è una rappresentazione del datastore vSphere creata su un cluster che esegue il software Element.

I contenitori di archiviazione vengono creati e associati agli account NetApp Element . Un contenitore di archiviazione creato su Element Storage viene visualizzato come un datastore vSphere in vCenter ed ESXi. I contenitori di archiviazione non allocano alcuno spazio nell'archiviazione Element. Vengono semplicemente utilizzati per associare logicamente volumi virtuali.

Sono supportati al massimo quattro contenitori di archiviazione per cluster. Per abilitare la funzionalità VVols è necessario almeno un contenitore di archiviazione.

Creare un contenitore di archiviazione

È possibile creare contenitori di archiviazione nell'interfaccia utente di Element e individuarli in vCenter. È

necessario creare almeno un contenitore di archiviazione per iniziare il provisioning delle macchine virtuali supportate da VVol.

Prima di iniziare, abilitare la funzionalità VVols nell'interfaccia utente di Element per il cluster.

Passi

1. Selezionare **VVols** > **Contenitori di archiviazione**.
2. Fare clic sul pulsante **Crea contenitori di archiviazione**.
3. Immettere le informazioni sul contenitore di archiviazione nella finestra di dialogo **Crea un nuovo contenitore di archiviazione**:
   a. Immettere un nome per il contenitore di archiviazione.
   b. Configurare i segreti dell'iniziatore e della destinazione per CHAP.

      Lasciare vuoti i campi Impostazioni CHAP per generare automaticamente i segreti.

   c. Fare clic sul pulsante **Crea contenitore di archiviazione**.
4. Verificare che il nuovo contenitore di archiviazione appaia nell'elenco nella sotto-scheda **Contenitori di archiviazione**.

   Poiché un ID account NetApp Element viene creato automaticamente e assegnato al contenitore di archiviazione, non è necessario creare manualmente un account.

Visualizza i dettagli del contenitore di stoccaggio

Nella pagina Contenitori di archiviazione della scheda VVols, è possibile visualizzare le informazioni relative a tutti i contenitori di archiviazione attivi nel cluster.

- **ID account**: ID dell'account NetApp Element associato al contenitore di archiviazione.
- **Nome**: Nome del contenitore di archiviazione.
- **Stato**: Stato del contenitore di archiviazione. Valori possibili:
  - Attivo: il contenitore di stoccaggio è in uso.
  - Bloccato: il contenitore di stoccaggio è bloccato.
- **Tipo PE**: tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile per il software Element).
- **ID contenitore di archiviazione**: UUID del contenitore di archiviazione del volume virtuale.
- **Volumi virtuali attivi**: numero di volumi virtuali attivi associati al contenitore di archiviazione.

Visualizza i dettagli dei singoli contenitori di stoccaggio

È possibile visualizzare le informazioni relative a un singolo contenitore di archiviazione selezionandolo dalla pagina Contenitori di archiviazione nella scheda VVols.

- **ID account**: ID dell'account NetApp Element associato al contenitore di archiviazione.
- **Nome**: Nome del contenitore di archiviazione.
- **Stato**: Stato del contenitore di archiviazione. Valori possibili:
  - Attivo: il contenitore di stoccaggio è in uso.
  - Bloccato: il contenitore di stoccaggio è bloccato.

- **Segreto dell'iniziatore CHAP**: Il segreto CHAP esclusivo dell'iniziatore.
- **Segreto del bersaglio CHAP**: Il segreto CHAP univoco per il bersaglio.
- **ID contenitore di archiviazione**: UUID del contenitore di archiviazione del volume virtuale.
- **Tipo di endpoint del protocollo**: indica il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile).

Modifica un contenitore di archiviazione

È possibile modificare l'autenticazione CHAP del contenitore di archiviazione nell'interfaccia utente dell'elemento.

1. Selezionare **VVols** > **Contenitori di archiviazione**.
2. Fare clic sull'icona **Azioni** relativa al contenitore di archiviazione che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. In Impostazioni CHAP, modifica le credenziali Segreto iniziatore e Segreto destinazione utilizzate per l'autenticazione.

   Se non modifichi le credenziali delle impostazioni CHAP, queste rimarranno invariate. Se si lasciano vuoti i campi delle credenziali, il sistema genera automaticamente nuovi segreti.

5. Fare clic su **Salva modifiche**.

Elimina un contenitore di archiviazione

È possibile eliminare i contenitori di archiviazione dall'interfaccia utente dell'elemento.

Cosa ti servirà

Assicurarsi che tutte le macchine virtuali siano state rimosse dal datastore VVol.

Passi

1. Selezionare **VVols** > **Contenitori di archiviazione**.
2. Fare clic sull'icona **Azioni** relativa al contenitore di archiviazione che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.
5. Aggiornare l'elenco dei contenitori di archiviazione nella sotto-scheda **Contenitori di archiviazione** per confermare che il contenitore di archiviazione è stato rimosso.

Endpoint del protocollo

Scopri di più sugli endpoint del protocollo

Gli endpoint del protocollo sono punti di accesso utilizzati da un host per indirizzare lo storage su un cluster che esegue il software NetApp Element . Gli endpoint del protocollo non possono essere eliminati o modificati da un utente, non sono associati a un account e non possono essere aggiunti a un gruppo di accesso al volume.

Un cluster che esegue il software Element crea automaticamente un endpoint di protocollo per ogni nodo di archiviazione nel cluster. Ad esempio, un cluster di storage a sei nodi ha sei endpoint di protocollo mappati su

ciascun host ESXi. Gli endpoint del protocollo vengono gestiti dinamicamente dal software Element e vengono creati, spostati o rimossi in base alle necessità, senza alcun intervento. Gli endpoint del protocollo sono l'obiettivo del multi-pathing e fungono da proxy I/O per le LUN sussidiarie. Ogni endpoint del protocollo utilizza un indirizzo SCSI disponibile, proprio come una destinazione iSCSI standard. Gli endpoint del protocollo vengono visualizzati come un dispositivo di archiviazione a blocco singolo (512 byte) nel client vSphere, ma questo dispositivo di archiviazione non è disponibile per essere formattato o utilizzato come archiviazione.

iSCSI è l'unico protocollo supportato. Il protocollo Fibre Channel non è supportato.

Dettagli degli endpoint del protocollo

La pagina Endpoint del protocollo nella scheda VVols fornisce informazioni sugli endpoint del protocollo.

- **ID fornitore principale**

  ID del fornitore dell'endpoint del protocollo primario.

- **ID fornitore secondario**

  ID del provider dell'endpoint del protocollo secondario.

- **ID endpoint protocollo**

  L'UUID dell'endpoint del protocollo.

- **Stato dell'endpoint del protocollo**

  Lo stato dell'endpoint del protocollo. I valori possibili sono i seguenti:

  - Attivo: l'endpoint del protocollo è in uso.
  - Inizio: l'endpoint del protocollo è in fase di avvio.
  - Failover: l'endpoint del protocollo ha subito un failover.
  - Riservato: l'endpoint del protocollo è riservato.

- **Tipo di fornitore**

  Il tipo di provider dell'endpoint del protocollo. I valori possibili sono i seguenti:

  - Primario
  - Secondario

- **ID dispositivo SCSI NAA**

  Identificatore univoco globale del dispositivo SCSI per l'endpoint del protocollo nel formato NAA IEEE Registered Extended.

Rilegature

Scopri di più sulle associazioni

Per eseguire operazioni di I/O con un volume virtuale, un host ESXi deve prima associare il volume virtuale.

Il cluster SolidFire sceglie un endpoint di protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint di protocollo e restituisce il binding all'host ESXi. Dopo l'associazione, l'host ESXi può eseguire operazioni di I/O con il volume virtuale associato.

Dettagli degli attacchi

La pagina Associazioni nella scheda VVols fornisce informazioni di associazione su ciascun volume virtuale.

Vengono visualizzate le seguenti informazioni:

- **ID host**

  L'UUID dell'host ESXi che ospita i volumi virtuali ed è noto al cluster.

- **ID endpoint protocollo**

  ID endpoint del protocollo che corrispondono a ciascun nodo nel cluster SolidFire .

- **Endpoint del protocollo nell'ID banda**

  ID del dispositivo SCSI NAA dell'endpoint del protocollo.

- **Tipo di endpoint del protocollo**

  Il tipo di endpoint del protocollo.

- **ID associazione VVol**

  L'UUID di associazione del volume virtuale.

- **ID VVol**

  Identificatore univoco universale (UUID) del volume virtuale.

- **ID secondario VVol**

  ID secondario del volume virtuale che è un ID LUN SCSI di secondo livello.

Dettagli dell'host

La pagina Host nella scheda VVols fornisce informazioni sugli host VMware ESXi che ospitano volumi virtuali.

Vengono visualizzate le seguenti informazioni:

- **ID host**

  L'UUID dell'host ESXi che ospita i volumi virtuali ed è noto al cluster.

- **Indirizzo host**

  L'indirizzo IP o il nome DNS dell'host ESXi.

- **Legami**

  ID di associazione per tutti i volumi virtuali associati dall'host ESXi.

- **ID cluster ESX**

  ID del cluster host vSphere o GUID di vCenter.

- **Iniziatori IQN**

  IQN dell'iniziatore per l'host del volume virtuale.

- * ID endpoint del protocollo SolidFire *

  Gli endpoint del protocollo attualmente visibili all'host ESXi.

Lavorare con gruppi di accesso al volume e iniziatori

Creare un gruppo di accesso al volume

È possibile creare gruppi di accesso al volume mappando gli iniziatori a una raccolta di volumi per un accesso protetto. È quindi possibile concedere l'accesso ai volumi nel gruppo con un segreto di avvio CHAP dell'account e un segreto di destinazione.

Se si utilizza CHAP basato sull'iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso al volume, garantendo maggiore sicurezza. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

Passi

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic su **Crea gruppo di accesso**.
3. Immettere un nome per il gruppo di accesso al volume nel campo **Nome**.
4. Aggiungere un iniziatore al gruppo di accesso al volume in uno dei seguenti modi:

Opzione	Descrizione
Aggiunta di un iniziatore Fibre Channel	a. In Aggiungi iniziatori, seleziona un iniziatore Fibre Channel esistente dall'elenco Iniziatori Fibre Channel non associati. b. Fare clic su **Aggiungi iniziatore FC**. È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento **Crea iniziatore**, inserendo un nome per l'iniziatore e facendo clic su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco Iniziatori. Un esempio del formato è il seguente: `5f:47:ac:c0:5c:74:d4:02`
Aggiunta di un iniziatore iSCSI	In Aggiungi iniziatori, seleziona un iniziatore esistente dall'elenco Iniziatori. **Nota:** puoi creare un iniziatore durante questo passaggio cliccando sul link **Crea iniziatore**, immettendo un nome per l'iniziatore e cliccando su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco Iniziatori. Un esempio del formato è il seguente: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` È possibile trovare l'IQN dell'iniziatore per ciascun volume selezionando **Visualizza dettagli** nel menu Azioni per il volume nell'elenco **Gestione** > **Volumi** > **Attivi**. Quando si modifica un iniziatore, è possibile impostare l'attributo requiredCHAP su True, consentendo di impostare il segreto dell'iniziatore di destinazione. Per maggiori dettagli, vedere le informazioni API sul metodo API ModifyInitiator. "Gestisci l'archiviazione con l'API Element"

5. **Facoltativo:** aggiungere altri iniziatori secondo necessità.
6. In Aggiungi volumi, seleziona un volume dall'elenco **Volumi**.

   Il volume viene visualizzato nell'elenco **Volumi allegati**.

7. **Facoltativo:** aggiungere altri volumi secondo necessità.
8. Fare clic su **Crea gruppo di accesso**.

Trova maggiori informazioni

Aggiungere volumi a un gruppo di accesso

Visualizza i dettagli del gruppo di accesso individuale

È possibile visualizzare i dettagli di un singolo gruppo di accesso, ad esempio volumi e iniziatori collegati, in formato grafico.

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona Azioni per un gruppo di accesso.
3. Fare clic su **Visualizza dettagli**.

Dettagli del gruppo di accesso al volume

La pagina Gruppi di accesso nella scheda Gestione fornisce informazioni sui gruppi di accesso al volume.

Vengono visualizzate le seguenti informazioni:

- **ID**: ID generato dal sistema per il gruppo di accesso.
- **Nome**: il nome assegnato al gruppo di accesso al momento della sua creazione.
- **Volumi attivi**: numero di volumi attivi nel gruppo di accesso.
- **Compressione**: punteggio di efficienza della compressione per il gruppo di accesso.
- **Deduplicazione**: punteggio di efficienza della deduplicazione per il gruppo di accesso.
- **Thin Provisioning**: punteggio di efficienza del thin provisioning per il gruppo di accesso.
- **Efficienza complessiva**: punteggio di efficienza complessiva per il gruppo di accesso.
- **Iniziatori**: numero di iniziatori connessi al gruppo di accesso.

Aggiungere volumi a un gruppo di accesso

È possibile aggiungere volumi a un gruppo di accesso ai volumi. Ogni volume può appartenere a più di un gruppo di accesso al volume; è possibile visualizzare i gruppi a cui appartiene ogni volume nella pagina Volumi **Attivi**.

È possibile utilizzare questa procedura anche per aggiungere volumi a un gruppo di accesso al volume Fibre Channel.

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso a cui si desidera aggiungere volumi.
3. Fare clic sul pulsante **Modifica**.
4. In Aggiungi volumi, seleziona un volume dall'elenco **Volumi**.

   È possibile aggiungere altri volumi ripetendo questo passaggio.

5. Fare clic su **Salva modifiche**.

Rimuovere volumi da un gruppo di accesso

Quando si rimuove un volume da un gruppo di accesso, il gruppo non ha più accesso a quel volume.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettersi sempre dalle sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali modifiche alle impostazioni dell'iniziatore e del cluster.

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso da cui si desidera rimuovere i volumi.
3. Fare clic su **Modifica**.
4. In Aggiungi volumi nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Volumi collegati**.
5. Selezionare il volume che si desidera rimuovere dall'elenco e fare clic sull'icona **x** per rimuovere il volume dall'elenco.

   È possibile rimuovere altri volumi ripetendo questo passaggio.

6. Fare clic su **Salva modifiche**.

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnare loro degli alias.

È anche possibile assegnare attributi CHAP basati sull'iniziatore utilizzando una chiamata API. Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare `CreateInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP. L'accesso dell'iniziatore può essere limitato a una o più VLAN specificando uno o più virtualNetworkID tramite `CreateInitiators` E `ModifyInitiators` Chiamate API. Se non viene specificata alcuna rete virtuale, l'iniziatore può accedere a tutte le reti.

Per maggiori dettagli, consultare le informazioni di riferimento dell'API. "Gestisci l'archiviazione con l'API Element"

Passi

1. Fare clic su **Gestione** > **Iniziatori**.
2. Fare clic su **Crea iniziatore**.
3. Eseguire i passaggi per creare un singolo iniziatore o più iniziatori:

Opzione	Passi
Creare un singolo iniziatore	a. Fare clic su **Crea un singolo iniziatore**. b. Inserire l'IQN o il WWPN dell'iniziatore nel campo **IQN/WWPN**. c. Inserisci un nome descrittivo per l'iniziatore nel campo **Alias**. d. Fare clic su **Crea iniziatore**.

Opzione	Passi
Crea più iniziatori	a. Fare clic su **Crea iniziatori in blocco**. b. Inserire un elenco di IQN o WWPN nella casella di testo. c. Fare clic su **Aggiungi iniziatori**. d. Selezionare un iniziatore dall'elenco risultante e fare clic sull'icona Aggiungi corrispondente nella colonna **Alias** per aggiungere un alias per l'iniziatore. e. Fare clic sul segno di spunta per confermare il nuovo alias. f. Fare clic su **Crea iniziatori**.

Modifica un iniziatore

È possibile modificare l'alias di un iniziatore esistente o aggiungerne uno nuovo se non ne esiste già uno.

Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare `ModifyInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP.

Vedere"Gestisci l'archiviazione con l'API Element" .

Passi

1. Fare clic su **Gestione** > **Iniziatori**.
2. Fare clic sull'icona Azioni relativa all'iniziatore che si desidera modificare.
3. Fare clic su **Modifica**.
4. Immettere un nuovo alias per l'iniziatore nel campo **Alias**.
5. Fare clic su **Salva modifiche**.

Aggiungere un singolo iniziatore a un gruppo di accesso al volume

È possibile aggiungere un iniziatore a un gruppo di accesso al volume esistente.

Quando si aggiunge un iniziatore a un gruppo di accesso al volume, l'iniziatore ha accesso a tutti i volumi in quel gruppo di accesso al volume.

È possibile trovare l'iniziatore per ciascun volume facendo clic sull'icona Azioni e selezionando quindi **Visualizza dettagli** per il volume nell'elenco dei volumi attivi.

Se si utilizza CHAP basato sull'iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso al volume, garantendo maggiore sicurezza. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

Passi

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera modificare.
3. Fare clic su **Modifica**.

4. Per aggiungere un iniziatore Fibre Channel al gruppo di accesso al volume, procedere come segue:

   a. In Aggiungi iniziatori, seleziona un iniziatore Fibre Channel esistente dall'elenco **Iniziatori Fibre Channel non associati**.

   b. Fare clic su **Aggiungi iniziatore FC**.

   È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento **Crea iniziatore**, inserendo un nome per l'iniziatore e facendo clic su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco **Iniziatori**.

   Un esempio del formato è il seguente:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Per aggiungere un iniziatore iSCSI al gruppo di accesso al volume, in Aggiungi iniziatori, seleziona un iniziatore esistente dall'elenco **Iniziatori**.

   È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento **Crea iniziatore**, inserendo un nome per l'iniziatore e facendo clic su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco **Iniziatori**.

   Il formato accettato di un IQN di avvio è il seguente: iqn.aaaa-mm, in cui y e m sono cifre, seguite da testo che deve contenere solo cifre, caratteri alfabetici minuscoli, un punto (.), due punti (:) o un trattino (-).

   Un esempio del formato è il seguente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

   È possibile trovare l'IQN dell'iniziatore per ciascun volume nella pagina **Gestione** > **Volumi** Volumi attivi facendo clic sull'icona Azioni e selezionando quindi **Visualizza dettagli** per il volume.

6. Fare clic su **Salva modifiche**.

Aggiungere più iniziatori a un gruppo di accesso al volume

È possibile aggiungere più iniziatori a un gruppo di accesso al volume esistente per consentire l'accesso ai volumi nel gruppo di accesso al volume con o senza la necessità dell'autenticazione CHAP.

Quando si aggiungono iniziatori a un gruppo di accesso al volume, gli iniziatori hanno accesso a tutti i volumi in quel gruppo di accesso al volume.

È possibile trovare l'iniziatore per ciascun volume facendo clic sull'icona Azioni e quindi su **Visualizza dettagli** per il volume nell'elenco dei volumi attivi.

È possibile aggiungere più iniziatori a un gruppo di accesso al volume esistente per abilitare l'accesso ai volumi e assegnare credenziali CHAP univoche per ciascun iniziatore all'interno di tale gruppo di accesso al

volume. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

È possibile assegnare attributi CHAP basati sull'iniziatore utilizzando una chiamata API. Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare la chiamata API ModifyInitiator per rimuovere e aggiungere l'accesso e gli attributi CHAP.

Per i dettagli, vedere"Gestisci l'archiviazione con l'API Element" .

Passi

1. Fare clic su **Gestione** > **Iniziatori**.
2. Seleziona gli iniziatori che desideri aggiungere a un gruppo di accesso.
3. Fare clic sul pulsante **Azioni in blocco**.
4. Fare clic su **Aggiungi al gruppo di accesso al volume**.
5. Nella finestra di dialogo Aggiungi al gruppo di accesso al volume, selezionare un gruppo di accesso dall'elenco **Gruppo di accesso al volume**.
6. Fare clic su **Aggiungi**.

Rimuovere gli iniziatori da un gruppo di accesso

Quando si rimuove un iniziatore da un gruppo di accesso, non potrà più accedere ai volumi in quel gruppo di accesso al volume. L'accesso normale dell'account al volume non viene interrotto.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettersi sempre dalle sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali modifiche alle impostazioni dell'iniziatore e del cluster.

Passi

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera rimuovere.
3. Nel menu che si apre, seleziona **Modifica**.
4. In Aggiungi iniziatori nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Iniziatori**.
5. Selezionare l'icona x per ogni iniziatore che si desidera rimuovere dal gruppo di accesso.
6. Fare clic su **Salva modifiche**.

Elimina un gruppo di accesso

È possibile eliminare un gruppo di accesso quando non è più necessario. Non è necessario eliminare gli ID iniziatore e gli ID volume dal gruppo di accesso al volume prima di eliminare il gruppo. Dopo aver eliminato il gruppo di accesso, l'accesso del gruppo ai volumi viene interrotto.

1. Fare clic su **Gestione** > **Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera eliminare.

3. Nel menu che si apre, fare clic su **Elimina**.
4. Per eliminare anche gli iniziatori associati a questo gruppo di accesso, selezionare la casella di controllo **Elimina iniziatori in questo gruppo di accesso**.
5. Conferma l'azione.

Elimina un iniziatore

È possibile eliminare un iniziatore quando non è più necessario. Quando si elimina un iniziatore, il sistema lo rimuove da tutti i gruppi di accesso al volume associati. Tutte le connessioni che utilizzano l'iniziatore rimangono valide finché la connessione non viene reimpostata.

Passi

1. Fare clic su **Gestione** > **Iniziatori**.
2. Eseguire i passaggi per eliminare un singolo iniziatore o più iniziatori:

Opzione	Passi
Elimina singolo iniziatore	a. Fare clic sull'icona **Azioni** relativa all'iniziatore che si desidera eliminare. b. Fare clic su **Elimina**. c. Conferma l'azione.
Elimina più iniziatori	a. Seleziona le caselle di controllo accanto agli iniziatori che desideri eliminare. b. Fare clic sul pulsante **Azioni in blocco**. c. Nel menu che appare, seleziona **Elimina**. d. Conferma l'azione.

Proteggi i tuoi dati

Proteggi i tuoi dati

Il software NetApp Element consente di proteggere i dati in vari modi, grazie a funzionalità quali snapshot per singoli volumi o gruppi di volumi, replica tra cluster e volumi in esecuzione su Element e replica su sistemi ONTAP .

- **Istantanee**

  La protezione dei dati basata solo su snapshot replica i dati modificati in momenti specifici su un cluster remoto. Vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non lo sono.

  Utilizzare snapshot del volume per la protezione dei dati

- **Replica remota tra cluster e volumi in esecuzione su Element**

È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in una coppia di cluster, entrambi in esecuzione su Element per scenari di failover e failback.

Eseguire la replica remota tra cluster che eseguono il software NetApp Element

- *Replica tra cluster Element e ONTAP utilizzando la tecnologia SnapMirror *

  Grazie alla tecnologia NetApp SnapMirror , è possibile replicare gli snapshot acquisiti tramite Element su ONTAP per scopi di disaster recovery. In una relazione SnapMirror , Element è un endpoint e ONTAP è l'altro.

  Utilizzare la replica SnapMirror tra i cluster Element e ONTAP

- **Esegui il backup e il ripristino dei volumi dagli archivi di oggetti SolidFire, S3 o Swift**

  È possibile eseguire il backup e il ripristino dei volumi su altri storage SolidFire , nonché su archivi di oggetti secondari compatibili con Amazon S3 o OpenStack Swift.

  Eseguire il backup e il ripristino dei volumi negli archivi di oggetti SolidFire, S3 o Swift

Per maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"

Utilizzare snapshot del volume per la protezione dei dati

Utilizzare snapshot del volume per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un dato momento. È possibile acquisire uno snapshot di un volume e utilizzarlo in un secondo momento se è necessario riportare un volume allo stato in cui si trovava al momento della creazione dello snapshot.

Gli snapshot sono simili ai cloni di volume. Tuttavia, gli snapshot sono semplicemente repliche dei metadati del volume, quindi non è possibile montarli o scriverci sopra. La creazione di uno snapshot del volume richiede inoltre solo una piccola quantità di risorse di sistema e spazio, il che rende la creazione di snapshot più rapida della clonazione.

È possibile acquisire un'istantanea di un singolo volume o di un set di volumi.

Facoltativamente, replicare gli snapshot su un cluster remoto e utilizzarli come copia di backup del volume. Ciò consente di ripristinare un volume a un punto specifico nel tempo utilizzando lo snapshot replicato. In alternativa, è possibile creare un clone di un volume da uno snapshot replicato.

Trova maggiori informazioni

- Utilizzare snapshot di volumi individuali per la protezione dei dati
- Utilizzo di snapshot di gruppo per attività di protezione dei dati
- Pianificazione di uno snapshot

Utilizzare snapshot di volumi individuali per la protezione dei dati

Utilizzare snapshot di volumi individuali per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un dato momento. Per lo snapshot è possibile utilizzare un singolo volume anziché un gruppo di volumi.

Trova maggiori informazioni

- Crea uno snapshot del volume
- Modifica la conservazione degli snapshot
- Eliminazione di uno snapshot
- Clonazione di un volume da uno snapshot
- Ripristino di un volume in uno snapshot
- Backup di uno snapshot del volume in un archivio oggetti Amazon S3
- Backup di uno snapshot del volume in un archivio oggetti OpenStack Swift
- Backup di uno snapshot del volume su un cluster SolidFire

Crea uno snapshot del volume

È possibile creare uno snapshot di un volume attivo per preservare l'immagine del volume in qualsiasi momento. È possibile creare fino a 32 snapshot per un singolo volume.

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera utilizzare per lo snapshot.
3. Nel menu che si apre, seleziona **Snapshot**.
4. Nella finestra di dialogo **Crea snapshot del volume**, immettere il nome del nuovo snapshot.
5. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando associato** per garantire che lo snapshot venga acquisito nella replica quando il volume padre viene associato.
6. Per impostare la conservazione per lo snapshot, selezionare una delle seguenti opzioni:
   - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
   - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
7. Per acquisire un singolo snapshot immediato, procedere come segue:
   a. Fare clic su **Scatta istantanea ora**.
   b. Fare clic su **Crea snapshot**.
8. Per pianificare l'esecuzione dello snapshot in un momento futuro, procedere come segue:
   a. Fare clic su **Crea pianificazione snapshot**.
   b. Inserisci un **Nome nuovo programma**.
   c. Selezionare un **Tipo di pianificazione** dall'elenco.
   d. **Facoltativo:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.

e. Fare clic su **Crea pianificazione**.

Trova maggiori informazioni

Pianifica uno snapshot

Modifica la conservazione degli snapshot

È possibile modificare il periodo di conservazione di uno snapshot per controllare quando e se il sistema elimina gli snapshot. Il periodo di conservazione specificato inizia quando si immette il nuovo intervallo. Quando si imposta un periodo di conservazione, è possibile selezionare un periodo che inizia all'ora corrente (la conservazione non viene calcolata in base all'ora di creazione dello snapshot). È possibile specificare intervalli in minuti, ore e giorni.

Passi

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot che si desidera modificare.
3. Nel menu che si apre, fare clic su **Modifica**.
4. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando associato** per garantire che lo snapshot venga acquisito nella replica quando il volume padre è associato.
5. **Facoltativo:** seleziona un'opzione di conservazione per lo snapshot:
   - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
   - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per selezionare un periodo di tempo durante il quale il sistema conserverà lo snapshot.
6. Fare clic su **Salva modifiche**.

Elimina uno snapshot

È possibile eliminare uno snapshot del volume da un cluster di archiviazione che esegue il software Element. Quando si elimina uno snapshot, il sistema lo rimuove immediatamente.

È possibile eliminare gli snapshot replicati dal cluster di origine. Se uno snapshot è in fase di sincronizzazione con il cluster di destinazione quando lo elimini, la replica di sincronizzazione viene completata e lo snapshot viene eliminato dal cluster di origine. Lo snapshot non viene eliminato dal cluster di destinazione.

È anche possibile eliminare gli snapshot replicati sulla destinazione dal cluster di destinazione. Lo snapshot eliminato viene conservato in un elenco di snapshot eliminati sulla destinazione finché il sistema non rileva che lo snapshot è stato eliminato sul cluster di origine. Quando la destinazione rileva che hai eliminato lo snapshot di origine, interrompe la replica dello snapshot.

Quando si elimina uno snapshot dal cluster di origine, lo snapshot del cluster di destinazione non viene influenzato (vale anche il contrario).

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.

4. Conferma l’azione.

Clonare un volume da uno snapshot

È possibile creare un nuovo volume da uno snapshot di un volume. Quando si esegue questa operazione, il sistema utilizza le informazioni dello snapshot per clonare un nuovo volume utilizzando i dati contenuti nel volume al momento della creazione dello snapshot. Questo processo memorizza le informazioni su altri snapshot del volume nel volume appena creato.

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull’icona **Azioni** per lo snapshot che si desidera utilizzare per il clone del volume.
3. Nel menu visualizzato, fare clic su **Clona volume da snapshot**.
4. Immettere un **Nome volume** nella finestra di dialogo **Clona volume da snapshot**.
5. Selezionare una **Dimensione totale** e le unità di misura per il nuovo volume.
6. Selezionare un tipo di **Accesso** per il volume.
7. Selezionare un **Account** dall’elenco da associare al nuovo volume.
8. Fare clic su **Avvia clonazione**.

Ripristinare un volume a uno snapshot

È possibile ripristinare un volume a uno snapshot precedente in qualsiasi momento. In questo modo vengono annullate tutte le modifiche apportate al volume dalla creazione dello snapshot.

Passi

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull’icona **Azioni** per lo snapshot che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, seleziona **Rollback Volume To Snapshot**.
4. **Facoltativo:** per salvare lo stato corrente del volume prima di tornare allo snapshot:
   a. Nella finestra di dialogo **Rollback a snapshot**, seleziona **Salva lo stato corrente del volume come snapshot**.
   b. Inserisci un nome per il nuovo snapshot.
5. Fare clic su **Rollback Snapshot**.

Eseguire il backup di uno snapshot del volume

Eseguire il backup di uno snapshot del volume

È possibile utilizzare la funzionalità di backup integrata per eseguire il backup di uno snapshot del volume. È possibile eseguire il backup degli snapshot da un cluster SolidFire a un archivio oggetti esterno o a un altro cluster SolidFire . Quando si esegue il backup di uno snapshot in un archivio oggetti esterno, è necessario disporre di una connessione all’archivio oggetti che consenta operazioni di lettura/scrittura.

- "Eseguire il backup di uno snapshot del volume in un archivio oggetti Amazon S3"
- "Eseguire il backup di uno snapshot del volume in un archivio oggetti OpenStack Swift"
- "Eseguire il backup di uno snapshot del volume su un cluster SolidFire"

Eseguire il backup di uno snapshot del volume in un archivio oggetti Amazon S3

È possibile eseguire il backup degli snapshot SolidFire su archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **S3**.
5. Selezionare un'opzione in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
7. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
8. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
9. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
10. **Facoltativo**: inserisci un'etichetta da aggiungere al prefisso nel campo **Etichetta**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di uno snapshot del volume in un archivio oggetti OpenStack Swift

È possibile eseguire il backup degli snapshot SolidFire in archivi di oggetti secondari compatibili con OpenStack Swift.

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **Swift**.
5. Selezionare un'opzione in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Inserisci un **URL** da utilizzare per accedere all'archivio oggetti.
7. Inserisci un **Nome utente** per l'account.
8. Inserisci la **Chiave di autenticazione** per l'account.
9. Immettere il **Contenitore** in cui archiviare il backup.
10. **Facoltativo**: Inserisci un **tag**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di uno snapshot del volume su un cluster SolidFire

È possibile eseguire il backup di snapshot di volumi residenti su un cluster SolidFire su un cluster SolidFire remoto.

Assicurarsi che i cluster di origine e di destinazione siano accoppiati.

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **Ripristina da**.
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare * SolidFire*.
5. Selezionare un formato dati in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copia la chiave dalla casella **Chiave di scrittura volume in blocco** negli appunti.
8. Nel cluster di origine, fare clic su **Protezione dati** > **Snapshot**.
9. Fare clic sull'icona Azioni relativa allo snapshot che si desidera utilizzare per il backup.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare * SolidFire*.
12. Selezionare lo stesso formato dati selezionato in precedenza nel campo **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.
14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Nel campo **Chiave di scrittura volume di massa**, incollare la chiave generata in precedenza sul cluster di destinazione.
17. Fare clic su **Inizia a leggere**.

Utilizzare snapshot di gruppo per la protezione dei dati

Utilizzo di snapshot di gruppo per attività di protezione dei dati

È possibile creare uno snapshot di gruppo di un set correlato di volumi per conservare una copia puntuale dei metadati per ciascun volume. È possibile utilizzare lo snapshot del gruppo in futuro come backup o rollback per ripristinare lo stato del gruppo di volumi a uno stato precedente.

Trova maggiori informazioni

- Crea uno snapshot di gruppo
- Modifica istantanee di gruppo
- Modifica i membri dello snapshot del gruppo
- Eliminare uno snapshot di gruppo
- Ripristina i volumi in uno snapshot di gruppo
- Clona più volumi
- Clona più volumi da uno snapshot di gruppo

Dettagli dello snapshot del gruppo

La pagina Snapshot di gruppo nella scheda Protezione dati fornisce informazioni sugli snapshot di gruppo.

- **ID**

  ID generato dal sistema per lo snapshot del gruppo.

- **UUID**

  ID univoco dello snapshot del gruppo.

- **Nome**

  Nome definito dall'utente per l'istantanea del gruppo.

- **Crea tempo**

  Ora in cui è stato creato lo snapshot del gruppo.

- **Stato**

  Lo stato attuale dello snapshot. Valori possibili:

  - Preparazione: lo snapshot è in fase di preparazione per l'uso e non è ancora scrivibile.
  - Fatto: la preparazione di questo snapshot è terminata ed è ora utilizzabile.
  - Attivo: lo snapshot è il ramo attivo.

- **# Volumi**

  Il numero di volumi nel gruppo.

- **Conservare fino a**

  Giorno e ora in cui lo snapshot verrà eliminato.

- **Replica remota**

  Indica se lo snapshot è abilitato o meno per la replica su un cluster SolidFire remoto. Valori possibili:

  - Abilitato: lo snapshot è abilitato per la replica remota.

- Disabilitato: lo snapshot non è abilitato per la replica remota.

Creazione di uno snapshot di gruppo

È possibile creare uno snapshot di un gruppo di volumi e anche creare una pianificazione di snapshot di gruppo per automatizzare gli snapshot di gruppo. Un singolo snapshot di gruppo può eseguire snapshot costanti di un massimo di 32 volumi contemporaneamente.

Passi

1. Fare clic su **Gestione** > **Volumi**.
2. Utilizzare le caselle di controllo per selezionare più volumi per un gruppo di volumi.
3. Fare clic su **Azioni in blocco**.
4. Fare clic su **Snapshot di gruppo**.
5. Immettere un nuovo nome per lo snapshot di gruppo nella finestra di dialogo Crea snapshot di gruppo dei volumi.
6. **Facoltativo:** selezionare la casella di controllo **Includi ciascun membro dello snapshot di gruppo nella replica quando associato** per garantire che ogni snapshot venga acquisito nella replica quando il volume padre viene associato.
7. Seleziona un'opzione di conservazione per lo snapshot del gruppo:
   - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
   - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
8. Per acquisire un singolo snapshot immediato, procedere come segue:
   a. Fare clic su **Acquisisci istantanea di gruppo ora**.
   b. Fare clic su **Crea snapshot di gruppo**.
9. Per pianificare l'esecuzione dello snapshot in un momento futuro, procedere come segue:
   a. Fare clic su **Crea pianificazione snapshot di gruppo**.
   b. Inserisci un **Nome nuovo programma**.
   c. Selezionare un **Tipo di pianificazione** dall'elenco.
   d. **Facoltativo:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
   e. Fare clic su **Crea pianificazione**.

Modifica degli snapshot di gruppo

È possibile modificare le impostazioni di replica e conservazione per gli snapshot di gruppo esistenti.

1. Fare clic su **Protezione dati** > **Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per l'istantanea del gruppo che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. **Facoltativo:** per modificare l'impostazione di replica per lo snapshot del gruppo:

a. Fare clic su **Modifica** accanto a **Replica corrente**.

b. Selezionare la casella di controllo **Includi ciascun membro dello snapshot di gruppo nella replica quando abbinato** per garantire che ogni snapshot venga acquisito nella replica quando il volume padre viene abbinato.

5. **Facoltativo:** per modificare l'impostazione di conservazione per lo snapshot del gruppo, seleziona una delle seguenti opzioni:

   a. Fare clic su **Modifica** accanto a **Conservazione corrente**.

   b. Seleziona un'opzione di conservazione per lo snapshot del gruppo:

      - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
      - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.

6. Fare clic su **Salva modifiche**.

Eliminazione di uno snapshot di gruppo

È possibile eliminare uno snapshot di gruppo dal sistema. Quando elimini lo snapshot del gruppo, puoi scegliere se tutti gli snapshot associati al gruppo devono essere eliminati o conservati come snapshot individuali.

Se si elimina un volume o uno snapshot che fa parte di uno snapshot di gruppo, non sarà più possibile eseguire il rollback allo snapshot di gruppo. Tuttavia, è possibile ripristinare ogni volume singolarmente.

1. Fare clic su **Protezione dati** > **Snapshot di gruppo**.
2. Fare clic sull'icona Azioni relativa allo snapshot che si desidera eliminare.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Selezionare una delle seguenti opzioni nella finestra di dialogo di conferma:
   - Fare clic su **Elimina snapshot di gruppo E tutti i membri dello snapshot di gruppo** per eliminare lo snapshot di gruppo e tutti gli snapshot dei membri.
   - Fare clic su **Mantieni i membri dello snapshot del gruppo come snapshot individuali** per eliminare lo snapshot del gruppo ma conservare tutti gli snapshot dei membri.
5. Conferma l'azione.

Ripristina i volumi in uno snapshot di gruppo

È possibile ripristinare un gruppo di volumi in qualsiasi momento trasformandolo in uno snapshot di gruppo.

Quando si esegue il rollback di un gruppo di volumi, tutti i volumi del gruppo vengono ripristinati allo stato in cui si trovavano al momento della creazione dello snapshot del gruppo. Il rollback ripristina anche le dimensioni del volume a quelle registrate nello snapshot originale. Se il sistema ha eliminato un volume, al momento dell'eliminazione sono stati eliminati anche tutti gli snapshot di quel volume; il sistema non ripristina nessuno snapshot del volume eliminato.

1. Fare clic su **Protezione dati** > **Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per lo snapshot di gruppo che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, selezionare **Esegui rollback dei volumi nello snapshot di gruppo**.

4. **Facoltativo**: per salvare lo stato corrente dei volumi prima di tornare allo snapshot:
   a. Nella finestra di dialogo **Rollback a snapshot**, selezionare **Salva lo stato corrente dei volumi come snapshot di gruppo**.
   b. Inserisci un nome per il nuovo snapshot.
5. Fare clic su **Ripristina snapshot gruppo**.

Modifica dei membri dello snapshot del gruppo

È possibile modificare le impostazioni di conservazione per i membri di uno snapshot di gruppo esistente.

1. Fare clic su **Protezione dati** > **Snapshot**.
2. Fare clic sulla scheda **Membri**.
3. Fare clic sull'icona Azioni relativa al membro dello snapshot di gruppo che si desidera modificare.
4. Nel menu che si apre, seleziona **Modifica**.
5. Per modificare l'impostazione di replica per lo snapshot, selezionare una delle seguenti opzioni:
   - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
   - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
6. Fare clic su **Salva modifiche**.

Clona più volumi

È possibile creare più cloni di volume in un'unica operazione per creare una copia puntuale dei dati su un gruppo di volumi.

Quando si clona un volume, il sistema crea uno snapshot del volume e poi crea un nuovo volume dai dati nello snapshot. È possibile montare e scrivere sul nuovo clone del volume. La clonazione di più volumi è un processo asincrono e richiede una quantità di tempo variabile a seconda delle dimensioni e del numero dei volumi da clonare.

Le dimensioni del volume e il carico attuale del cluster influiscono sul tempo necessario per completare un'operazione di clonazione.

Passi

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sulla scheda **Attivo**.
3. Utilizzare le caselle di controllo per selezionare più volumi, creando un gruppo di volumi.
4. Fare clic su **Azioni in blocco**.
5. Fare clic su **Clona** nel menu visualizzato.
6. Immettere un **Nuovo prefisso nome volume** nella finestra di dialogo **Clona più volumi**.

   Il prefisso viene applicato a tutti i volumi del gruppo.

7. **Facoltativo:** seleziona un account diverso a cui apparterrà il clone.

   Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

8. **Facoltativo:** selezionare un metodo di accesso diverso per i volumi nel clone.

   Se non si seleziona un metodo di accesso, il sistema utilizza l'accesso al volume corrente.

9. Fare clic su **Avvia clonazione**.

Clonazione di più volumi da uno snapshot di gruppo

È possibile clonare un gruppo di volumi da uno snapshot di gruppo in un dato momento. Questa operazione richiede che esista già uno snapshot di gruppo dei volumi, poiché lo snapshot di gruppo viene utilizzato come base per creare i volumi. Dopo aver creato i volumi, è possibile utilizzarli come qualsiasi altro volume nel sistema.

Le dimensioni del volume e il carico attuale del cluster influiscono sul tempo necessario per completare un'operazione di clonazione.

1. Fare clic su **Protezione dati** > **Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per lo snapshot di gruppo che si desidera utilizzare per i cloni del volume.
3. Nel menu visualizzato, selezionare **Clona volumi da snapshot di gruppo**.
4. Immettere un **Nuovo prefisso nome volume** nella finestra di dialogo **Clona volumi da snapshot di gruppo**.

   Il prefisso viene applicato a tutti i volumi creati dallo snapshot del gruppo.

5. **Facoltativo:** seleziona un account diverso a cui apparterrà il clone.

   Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

6. **Facoltativo:** selezionare un metodo di accesso diverso per i volumi nel clone.

   Se non si seleziona un metodo di accesso, il sistema utilizza l'accesso al volume corrente.

7. Fare clic su **Avvia clonazione**.

Pianifica uno snapshot

Pianifica uno snapshot

È possibile proteggere i dati su un volume o un gruppo di volumi pianificando l'esecuzione di snapshot del volume a intervalli specifici. È possibile pianificare l'esecuzione automatica di snapshot di singoli volumi o di snapshot di gruppo.

Quando si configura una pianificazione degli snapshot, è possibile scegliere tra intervalli di tempo basati sui giorni della settimana o sui giorni del mese. È anche possibile specificare i giorni, le ore e i minuti prima che venga eseguito lo snapshot successivo. Se il volume viene replicato, è possibile archiviare gli snapshot risultanti su un sistema di archiviazione remoto.

Trova maggiori informazioni

- Creare una pianificazione snapshot
- Modificare una pianificazione di snapshot

- Elimina una pianificazione snapshot
- Copia una pianificazione snapshot

Dettagli della pianificazione degli snapshot

Nella pagina Protezione dati > Pianificazioni, è possibile visualizzare le seguenti informazioni nell'elenco delle pianificazioni degli snapshot.

- **ID**

  ID generato dal sistema per lo snapshot.

- **Tipo**

  Il tipo di programma. Attualmente l'unico tipo supportato è Snapshot.

- **Nome**

  Nome assegnato alla pianificazione al momento della sua creazione. I nomi delle pianificazioni snapshot possono avere una lunghezza massima di 223 caratteri e contenere caratteri az, 0-9 e trattino (-).

- **Frequenza**

  La frequenza con cui viene eseguita la pianificazione. La frequenza può essere impostata in ore e minuti, settimane o mesi.

- **Ricorrente**

  Indica se la pianificazione deve essere eseguita una sola volta o a intervalli regolari.

- **Messo in pausa manualmente**

  Indica se la pianificazione è stata sospesa manualmente o meno.

- **ID volume**

  ID del volume che la pianificazione utilizzerà quando verrà eseguita.

- **Ultima corsa**

  L'ultima volta che è stato eseguito il programma.

- **Stato dell'ultima esecuzione**

  L'esito dell'ultima esecuzione programmata. Valori possibili:

  - Successo
  - Fallimento

Creare una pianificazione snapshot

È possibile pianificare l'esecuzione automatica di uno snapshot di uno o più volumi a intervalli specificati.

Quando si configura una pianificazione degli snapshot, è possibile scegliere tra intervalli di tempo basati sui giorni della settimana o sui giorni del mese. È anche possibile creare una pianificazione ricorrente e specificare i giorni, le ore e i minuti prima che venga eseguito lo snapshot successivo.

Se si pianifica l'esecuzione di uno snapshot in un intervallo di tempo non divisibile per 5 minuti, lo snapshot verrà eseguito nel successivo intervallo di tempo divisibile per 5 minuti. Ad esempio, se si pianifica l'esecuzione di uno snapshot alle 12:42:00 UTC, questo verrà eseguito alle 12:45:00 UTC. Non è possibile pianificare l'esecuzione di uno snapshot a intervalli inferiori a 5 minuti.

A partire da Element 12.5, è possibile abilitare la creazione seriale e scegliere di conservare gli snapshot in base al metodo First-In-First-Out (FIFO) dall'interfaccia utente.

- L'opzione **Abilita creazione seriale** specifica che viene replicato solo uno snapshot alla volta. La creazione di un nuovo snapshot non riesce quando è ancora in corso la replica di uno snapshot precedente. Se la casella di controllo non è selezionata, è consentita la creazione di uno snapshot quando è ancora in corso un'altra replica dello snapshot.
- L'opzione **FIFO** aggiunge la possibilità di conservare un numero coerente degli snapshot più recenti. Quando la casella di controllo è selezionata, gli snapshot vengono conservati secondo il metodo FIFO. Una volta che la coda di snapshot FIFO raggiunge la sua profondità massima, lo snapshot FIFO più vecchio viene scartato quando viene inserito un nuovo snapshot FIFO.

Passi

1. Selezionare **Protezione dati** > **Pianificazioni**.
2. Seleziona **Crea pianificazione**.
3. Nel campo **ID volume CSV**, immettere un singolo ID volume o un elenco di ID volume separati da virgole da includere nell'operazione di snapshot.
4. Inserisci un nuovo nome per la pianificazione.
5. Selezionare un tipo di pianificazione e impostare la pianificazione tra le opzioni fornite.
6. **Facoltativo:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione degli snapshot indefinitamente.
7. **Facoltativo:** inserisci un nome per il nuovo snapshot nel campo **Nome nuovo snapshot**.

   Se si lascia vuoto il campo, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.
8. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per garantire che gli snapshot vengano acquisiti nella replica quando il volume padre è accoppiato.
9. **Facoltativo:** selezionare la casella di controllo **Abilita creazione seriale** per garantire che venga replicato solo uno snapshot alla volta.
10. Per impostare la conservazione per lo snapshot, selezionare una delle seguenti opzioni:
    - **Facoltativo:** selezionare la casella di controllo **FIFO (First In First out)** per conservare un numero coerente degli snapshot più recenti.
    - Selezionare **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
    - Selezionare **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
11. Seleziona **Crea pianificazione**.

Modificare una pianificazione di snapshot

È possibile modificare le pianificazioni degli snapshot esistenti. Dopo la modifica, la prossima volta che la pianificazione verrà eseguita, utilizzerà gli attributi aggiornati. Tutti gli snapshot creati dalla pianificazione originale rimangono sul sistema di archiviazione.

Passi

1. Fare clic su **Protezione dati** > **Pianificazioni**.
2. Fare clic sull'icona **Azioni** relativa alla pianificazione che si desidera modificare.
3. Nel menu che si apre, fare clic su **Modifica**.
4. Nel campo **ID volume CSV**, modificare l'ID del singolo volume o l'elenco separato da virgole degli ID del volume attualmente inclusi nell'operazione di snapshot.
5. Per mettere in pausa o riprendere la pianificazione, seleziona una delle seguenti opzioni:
   - Per mettere in pausa una pianificazione attiva, selezionare **Sì** dall'elenco **Metti in pausa manualmente la pianificazione**.
   - Per riprendere una pianificazione sospesa, selezionare **No** dall'elenco **Sospendi manualmente la pianificazione**.
6. Se lo si desidera, immettere un nome diverso per la pianificazione nel campo **Nuovo nome pianificazione**.
7. Per modificare la pianificazione in modo che venga eseguita in giorni diversi della settimana o del mese, selezionare **Tipo di pianificazione** e modificare la pianificazione dalle opzioni fornite.
8. **Facoltativo:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione degli snapshot indefinitamente.
9. **Facoltativo:** immettere o modificare il nome del nuovo snapshot nel campo **Nome nuovo snapshot**.

   Se si lascia vuoto il campo, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.
10. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per garantire che gli snapshot vengano acquisiti nella replica quando il volume padre è accoppiato.
11. Per modificare l'impostazione di conservazione, selezionare una delle seguenti opzioni:
    - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
    - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per selezionare un periodo di tempo durante il quale il sistema conserverà lo snapshot.
12. Fare clic su **Salva modifiche**.

Copia una pianificazione snapshot

È possibile copiare una pianificazione e mantenerne gli attributi correnti.

1. Fare clic su **Protezione dati** > **Pianificazioni**.
2. Fare clic sull'icona Azioni relativa alla pianificazione che si desidera copiare.
3. Nel menu che si apre, fare clic su **Crea una copia**.

   Viene visualizzata la finestra di dialogo **Crea pianificazione**, compilata con gli attributi correnti della pianificazione.

4. **Facoltativo:** inserisci un nome e gli attributi aggiornati per la nuova pianificazione.
5. Fare clic su **Crea pianificazione**.

Elimina una pianificazione snapshot

È possibile eliminare una pianificazione snapshot. Dopo aver eliminato la pianificazione, non verranno eseguiti più snapshot pianificati. Tutti gli snapshot creati dalla pianificazione rimangono nel sistema di archiviazione.

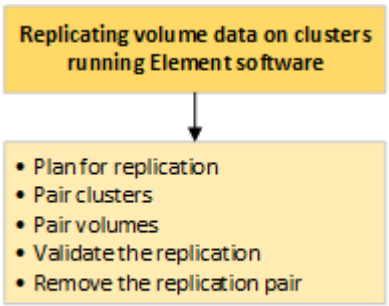
1. Fare clic su **Protezione dati** > **Pianificazioni**.
2. Fare clic sull'icona **Azioni** relativa alla pianificazione che si desidera eliminare.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Conferma l'azione.

Eseguire la replica remota tra cluster che eseguono il software NetApp Element

Eseguire la replica remota tra cluster che eseguono il software NetApp Element

Per i cluster che eseguono il software Element, la replica in tempo reale consente la rapida creazione di copie remote dei dati del volume. È possibile associare un cluster di archiviazione a un massimo di altri quattro cluster di archiviazione. È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in una coppia di cluster per scenari di failover e failback.

Il processo di replicazione comprende i seguenti passaggi:



- "Pianifica l'associazione di cluster e volumi per la replica in tempo reale"
- "Cluster di coppie per la replicazione"
- "Volumi di coppia"
- "Convalida la replica del volume"
- "Elimina una relazione di volume dopo la replica"
- "Gestire le relazioni di volume"

Pianifica l'associazione di cluster e volumi per la replica in tempo reale

Per la replica remota in tempo reale è necessario associare due cluster di storage che

eseguono il software Element, associare i volumi su ciascun cluster e convalidare la replica. Una volta completata la replica, è necessario eliminare la relazione del volume.

Cosa ti servirà

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.
- Tutti gli indirizzi IP dei nodi sulle reti di gestione e di archiviazione per i cluster accoppiati vengono instradati l'uno verso l'altro.
- L'MTU di tutti i nodi accoppiati deve essere lo stesso e supportato end-to-end tra i cluster.
- Entrambi i cluster di archiviazione devono avere nomi di cluster, MVIP, SVIP e tutti gli indirizzi IP dei nodi univoci.
- La differenza tra le versioni del software Element sui cluster non è maggiore di una versione principale. Se la differenza è maggiore, è necessario aggiornare uno dei cluster per eseguire la replica dei dati.

> Gli apparecchi WAN Accelerator non sono stati qualificati da NetApp per l'uso durante la replica dei dati. Questi dispositivi possono interferire con la compressione e la deduplicazione se distribuiti tra due cluster che replicano i dati. Assicuratevi di valutare attentamente gli effetti di qualsiasi dispositivo WAN Accelerator prima di distribuirlo in un ambiente di produzione.

Trova maggiori informazioni

- Cluster di coppie per la replicazione
- Volumi di coppia
- Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Cluster di coppie per la replicazione

Cluster di coppie per la replicazione

Per utilizzare la funzionalità di replica in tempo reale, è necessario innanzitutto associare due cluster. Dopo aver associato e connesso due cluster, è possibile configurare i volumi attivi su un cluster in modo che vengano replicati continuamente su un secondo cluster, garantendo una protezione continua dei dati (CDP).

Cosa ti servirà

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.
- Tutti i MIP e i SIP dei nodi vengono instradati l'uno verso l'altro.
- Meno di 2000 ms di latenza di andata e ritorno tra i cluster.
- Entrambi i cluster di storage devono avere nomi di cluster, MVIP, SVIP e tutti gli indirizzi IP dei nodi univoci.
- La differenza tra le versioni del software Element sui cluster non è maggiore di una versione principale. Se la differenza è maggiore, è necessario aggiornare uno dei cluster per eseguire la replica dei dati.

> L'associazione dei cluster richiede la piena connettività tra i nodi sulla rete di gestione. La replica richiede la connettività tra i singoli nodi sulla rete del cluster di archiviazione.

È possibile associare un cluster a un massimo di altri quattro cluster per replicare i volumi. È anche possibile associare tra loro i cluster all'interno del gruppo di cluster.

Accoppiare i cluster utilizzando MVIP o una chiave di associazione

È possibile associare un cluster di origine e uno di destinazione utilizzando l'MVIP del cluster di destinazione se è presente l'accesso dell'amministratore del cluster a entrambi i cluster. Se l'accesso dell'amministratore del cluster è disponibile solo su un cluster in una coppia di cluster, è possibile utilizzare una chiave di associazione sul cluster di destinazione per completare l'associazione del cluster.

1. Selezionare uno dei seguenti metodi per associare i cluster:
   - "Cluster di coppie tramite MVIP": Utilizzare questo metodo se l'amministratore del cluster ha accesso a entrambi i cluster. Questo metodo utilizza l'MVIP del cluster remoto per accoppiare due cluster.
   - "Accoppia i cluster utilizzando una chiave di associazione": Utilizzare questo metodo se l'amministratore del cluster ha accesso solo a uno dei cluster. Questo metodo genera una chiave di associazione che può essere utilizzata sul cluster di destinazione per completare l'associazione del cluster.

Trova maggiori informazioni

Requisiti delle porte di rete

Cluster di coppie tramite MVIP

È possibile associare due cluster per la replica in tempo reale utilizzando l'MVIP di un cluster per stabilire una connessione con l'altro cluster. Per utilizzare questo metodo è necessario l'accesso come amministratore del cluster su entrambi i cluster. Il nome utente e la password dell'amministratore del cluster vengono utilizzati per autenticare l'accesso al cluster prima che i cluster possano essere associati.

1. Nel cluster locale, selezionare **Protezione dati** > **Coppie cluster**.
2. Fare clic su **Cluster di coppie**.
3. Fare clic su **Avvia associazione** e quindi su **Sì** per indicare che si ha accesso al cluster remoto.
4. Immettere l'indirizzo MVIP del cluster remoto.
5. Fare clic su **Completa associazione sul cluster remoto**.

   Nella finestra **Autenticazione richiesta**, immettere il nome utente e la password dell'amministratore del cluster remoto.

6. Nel cluster remoto, selezionare **Protezione dati** > **Coppie cluster**.
7. Fare clic su **Cluster di coppie**.
8. Fare clic su **Completa associazione**.
9. Fare clic sul pulsante **Completa associazione**.

Trova maggiori informazioni

- Accoppia i cluster utilizzando una chiave di associazione
- "Accoppiamento di cluster tramite MVIP (video)"

Accoppia i cluster utilizzando una chiave di associazione

Se si dispone dell'accesso come amministratore del cluster a un cluster locale ma non a

quello remoto, è possibile associare i cluster utilizzando una chiave di associazione. Una chiave di associazione viene generata su un cluster locale e quindi inviata in modo sicuro a un amministratore del cluster in un sito remoto per stabilire una connessione e completare l'associazione del cluster per la replica in tempo reale.

1. Nel cluster locale, selezionare **Protezione dati** > **Coppie cluster**.
2. Fare clic su **Cluster di coppie**.
3. Fare clic su **Avvia associazione** e poi su **No** per indicare che non si ha accesso al cluster remoto.
4. Fare clic su **Genera chiave**.

> Questa azione genera una chiave di testo per l'associazione e crea una coppia di cluster non configurata sul cluster locale. Se non si completa la procedura, sarà necessario eliminare manualmente la coppia di cluster.

5. Copia la chiave di associazione del cluster negli appunti.
6. Rendere la chiave di associazione accessibile all'amministratore del cluster nel sito remoto del cluster.

> La chiave di associazione del cluster contiene una versione dell'MVIP, del nome utente, della password e delle informazioni del database per consentire le connessioni del volume per la replica remota. Questa chiave deve essere trattata in modo sicuro e non conservata in un modo che possa consentire l'accesso accidentale o non protetto al nome utente o alla password.

> Non modificare nessuno dei caratteri nella chiave di associazione. La chiave diventa non valida se viene modificata.

7. Nel cluster remoto, selezionare **Protezione dati** > **Coppie cluster**.
8. Fare clic su **Cluster di coppie**.
9. Fare clic su **Completa associazione** e immettere la chiave di associazione nel campo **Chiave di associazione** (il metodo consigliato è incollare).
10. Fare clic su **Completa associazione**.

Trova maggiori informazioni

- Cluster di coppie tramite MVIP
- "Associazione di cluster tramite una chiave di associazione cluster (video)"

Convalida la connessione della coppia di cluster

Una volta completata l'associazione dei cluster, potrebbe essere opportuno verificare la connessione della coppia di cluster per garantire il successo della replica.

1. Nel cluster locale, selezionare **Protezione dati** > **Coppie cluster**.
2. Nella finestra **Coppie di cluster**, verificare che la coppia di cluster sia connessa.
3. **Facoltativo:** tornare al cluster locale e alla finestra **Coppie di cluster** e verificare che la coppia di cluster sia connessa.

Volumi di coppia

Volumi di coppia

Dopo aver stabilito una connessione tra i cluster in una coppia di cluster, è possibile associare un volume su un cluster con un volume sull'altro cluster nella coppia. Quando viene stabilita una relazione di associazione di volumi, è necessario identificare quale volume è la destinazione della replica.

È possibile associare due volumi per la replica in tempo reale archiviati su cluster di archiviazione diversi in una coppia di cluster connessi. Dopo aver associato due cluster, è possibile configurare i volumi attivi su un cluster in modo che vengano replicati continuamente su un secondo cluster, garantendo una protezione continua dei dati (CDP). È anche possibile assegnare uno dei due volumi come origine o destinazione della replica.

Gli abbinamenti di volume sono sempre uno a uno. Dopo che un volume fa parte di un abbinamento con un volume su un altro cluster, non è possibile abbinarlo nuovamente a nessun altro volume.

Cosa ti servirà

- Hai stabilito una connessione tra i cluster in una coppia di cluster.
- Si dispone dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.

Passi

1. Crea un volume di destinazione con accesso in lettura o scrittura
2. Associare i volumi utilizzando un ID volume o una chiave di associazione
3. Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Crea un volume di destinazione con accesso in lettura o scrittura

Il processo di replicazione coinvolge due endpoint: il volume di origine e quello di destinazione. Quando si crea il volume di destinazione, il volume viene automaticamente impostato sulla modalità di lettura/scrittura per accettare i dati durante la replica.

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic su **Crea volume**.
3. Nella finestra di dialogo Crea un nuovo volume, immettere il nome del volume.
4. Immettere la dimensione totale del volume, selezionare una dimensione di blocco per il volume e selezionare l'account che deve avere accesso al volume.
5. Fare clic su **Crea volume**.
6. Nella finestra Attiva, fare clic sull'icona Azioni per il volume.
7. Fare clic su **Modifica**.
8. Modificare il livello di accesso dell'account in Destinazione replica.
9. Fare clic su **Salva modifiche**.

Associare i volumi utilizzando un ID volume o una chiave di associazione

Abbinare i volumi utilizzando un ID volume

È possibile associare un volume a un altro volume su un cluster remoto se si dispone dell'accesso come amministratore del cluster a entrambi i cluster su cui si desidera associare i volumi. Questo metodo utilizza l'ID del volume sul cluster remoto per avviare una connessione.

Cosa ti servirà

- Assicurarsi che i cluster contenenti i volumi siano accoppiati.
- Creare un nuovo volume sul cluster remoto.

> Dopo il processo di associazione è possibile assegnare un'origine e una destinazione di replicazione. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione della dimensione del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

- Conoscere l'ID del volume di destinazione.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera associare.
3. Fare clic su **Associa**.
4. Nella finestra di dialogo **Volume di associazione**, selezionare **Avvia associazione**.
5. Selezionare **Lo voglio** per indicare che si ha accesso al cluster remoto.
6. Selezionare una **Modalità di replicazione** dall'elenco:
   - **In tempo reale (asincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.
   - **In tempo reale (sincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
   - **Solo snapshot**: vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Selezionare un cluster remoto dall'elenco.
8. Scegli un ID volume remoto.
9. Fare clic su **Avvia associazione**.

   Il sistema apre una scheda del browser Web che si connette all'interfaccia utente Element del cluster remoto. Potrebbe essere necessario accedere al cluster remoto con le credenziali di amministratore del cluster.

10. Nell'interfaccia utente dell'elemento del cluster remoto, selezionare **Completa associazione**.
11. Confermare i dettagli in **Conferma associazione volume**.
12. Fare clic su **Completa associazione**.

Dopo aver confermato l'associazione, i due cluster avviano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Stato volume** della finestra **Coppie di volumi**. La coppia di volumi viene visualizzata `PausedMisconfigured` finché non vengono assegnate la coppia di volumi sorgente e destinazione.

Dopo aver completato correttamente l'associazione, si consiglia di aggiornare la tabella Volumi per rimuovere l'opzione **Associa** dall'elenco **Azioni** per il volume associato. Se non si aggiorna la tabella, l'opzione **Coppia** rimane disponibile per la selezione. Se si seleziona nuovamente l'opzione **Associa**, si apre una nuova scheda e poiché il volume è già associato, il sistema segnala un `StartVolumePairing Failed: xVolumeAlreadyPaired` messaggio di errore nella finestra **Volume coppia** della pagina Element UI.

Trova maggiori informazioni

- Messaggi di associazione del volume
- Avvisi di associazione del volume
- Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Abbinare i volumi utilizzando una chiave di associazione

Se si dispone dell'accesso come amministratore del cluster solo al cluster di origine (non si dispone delle credenziali di amministratore del cluster per un cluster remoto), è possibile associare un volume a un altro volume su un cluster remoto utilizzando una chiave di associazione.

Cosa ti servirà

- Assicurarsi che i cluster contenenti i volumi siano accoppiati.
- Assicurarsi che sul cluster remoto sia presente un volume da utilizzare per l'associazione.

Dopo il processo di associazione è possibile assegnare un'origine e una destinazione di replicazione. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione della dimensione del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera associare.
3. Fare clic su **Associa**.
4. Nella finestra di dialogo **Volume di associazione**, selezionare **Avvia associazione**.
5. Selezionare **Non** per indicare che non si ha accesso al cluster remoto.
6. Selezionare una **Modalità di replicazione** dall'elenco:
   - **In tempo reale (asincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.

- **In tempo reale (sincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
- **Solo snapshot**: vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.

7. Fare clic su **Genera chiave**.

   Questa azione genera una chiave di testo per l'associazione e crea una coppia di volumi non configurati sul cluster locale. Se non si completa la procedura, sarà necessario eliminare manualmente la coppia di volumi.

8. Copia la chiave di associazione negli appunti del tuo computer.
9. Rendere la chiave di associazione accessibile all'amministratore del cluster nel sito remoto del cluster.

   La chiave di associazione del volume deve essere trattata in modo sicuro e non utilizzata in un modo che possa consentire un accesso accidentale o non protetto.

   Non modificare nessuno dei caratteri nella chiave di associazione. La chiave diventa non valida se viene modificata.

10. Nell'interfaccia utente dell'elemento del cluster remoto, selezionare **Gestione** > **Volumi**.
11. Fare clic sull'icona Azioni per il volume che si desidera associare.
12. Fare clic su **Associa**.
13. Nella finestra di dialogo **Volume di associazione**, selezionare **Completa associazione**.
14. Incolla la chiave di associazione dall'altro cluster nella casella **Chiave di associazione**.
15. Fare clic su **Completa associazione**.

    Dopo aver confermato l'associazione, i due cluster avviano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Stato volume** della finestra **Coppie di volumi**. La coppia di volumi viene visualizzata `PausedMisconfigured` finché non vengono assegnate la coppia di volumi sorgente e destinazione.

    Dopo aver completato correttamente l'associazione, si consiglia di aggiornare la tabella Volumi per rimuovere l'opzione **Associa** dall'elenco **Azioni** per il volume associato. Se non si aggiorna la tabella, l'opzione **Coppia** rimane disponibile per la selezione. Se si seleziona nuovamente l'opzione **Associa**, si apre una nuova scheda e poiché il volume è già associato, il sistema segnala un `StartVolumePairing Failed: xVolumeAlreadyPaired` messaggio di errore nella finestra **Volume coppia** della pagina Element UI.

Trova maggiori informazioni

- Messaggi di associazione del volume
- Avvisi di associazione del volume
- Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Dopo aver associato i volumi, è necessario assegnare un volume di origine e il relativo

volume di destinazione della replica. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È possibile utilizzare questa procedura anche per reindirizzare i dati inviati a un volume di origine a un volume di destinazione remoto nel caso in cui il volume di origine non sia più disponibile.

Cosa ti servirà

Hai accesso ai cluster contenenti i volumi di origine e di destinazione.

Passi

1. Preparare il volume sorgente:
   a. Dal cluster che contiene il volume che si desidera assegnare come origine, selezionare **Gestione** > **Volumi**.
   b. Fare clic sull'icona **Azioni** per il volume che si desidera assegnare come origine e fare clic su **Modifica**.
   c. Nell'elenco a discesa **Accesso**, selezionare **Lettura/Scrittura**.

   Se si inverte l'assegnazione di origine e destinazione, questa azione farà sì che la coppia di volumi visualizzi il seguente messaggio finché non verrà assegnata una nuova destinazione di replica: `PausedMisconfigured`

   La modifica dell'accesso interrompe la replicazione del volume e causa l'interruzione della trasmissione dei dati. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

   a. Fare clic su **Salva modifiche**.
2. Preparare il volume di destinazione:
   a. Dal cluster che contiene il volume che si desidera assegnare come destinazione, selezionare **Gestione** > **Volumi**.
   b. Fare clic sull'icona Azioni per il volume che si desidera assegnare come destinazione e fare clic su **Modifica**.
   c. Nell'elenco a discesa **Accesso**, selezionare **Destinazione replica**.

   Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Dovresti utilizzare un nuovo volume di destinazione che non contenga dati e abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione 512e e configurazione QoS. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

   d. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- Abbinare i volumi utilizzando un ID volume
- Abbinare i volumi utilizzando una chiave di associazione

Convalida la replica del volume

Dopo aver replicato un volume, è necessario assicurarsi che i volumi di origine e di destinazione siano attivi. Quando sono in stato attivo, i volumi vengono accoppiati, i dati

vengono inviati dal volume di origine a quello di destinazione e i dati sono sincronizzati.

1. Da entrambi i cluster, selezionare **Protezione dati** > **Coppie di volumi**.
2. Verificare che lo stato del volume sia Attivo.

Trova maggiori informazioni

Avvisi di associazione del volume

Elimina una relazione di volume dopo la replica

Una volta completata la replica e non più necessaria la relazione tra coppie di volumi, è possibile eliminare la relazione tra volumi.

1. Selezionare **Protezione dati** > **Coppie di volumi**.
2. Fare clic sull'icona **Azioni** relativa alla coppia di volumi che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Gestire le relazioni di volume

Sospendi la replicazione

È possibile sospendere manualmente la replicazione se è necessario interrompere l'elaborazione I/O per un breve periodo. Potrebbe essere necessario sospendere la replicazione in caso di aumento dell'elaborazione I/O e se si desidera ridurre il carico di elaborazione.

1. Selezionare **Protezione dati** > **Coppie di volumi**.
2. Fare clic sull'icona Azioni per la coppia di volumi.
3. Fare clic su **Modifica**.
4. Nel riquadro **Modifica coppia di volumi**, sospendere manualmente il processo di replica.

> La sospensione o la ripresa manuale della replicazione del volume determina l'interruzione o la ripresa della trasmissione dei dati. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Salva modifiche**.

Cambia la modalità di replicazione

È possibile modificare le proprietà della coppia di volumi per cambiare la modalità di replica della relazione tra coppie di volumi.

1. Selezionare **Protezione dati** > **Coppie di volumi**.
2. Fare clic sull'icona Azioni per la coppia di volumi.
3. Fare clic su **Modifica**.
4. Nel riquadro **Modifica coppia di volumi**, seleziona una nuova modalità di replica:

- **In tempo reale (asincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.
- **In tempo reale (sincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
- **Solo snapshot**: vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate. **Attenzione:** La modifica della modalità di replicazione modifica immediatamente la modalità. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Salva modifiche**.

Elimina coppie di volumi

È possibile eliminare una coppia di volumi se si desidera rimuovere un'associazione di coppia tra due volumi.

1. Selezionare **Protezione dati** > **Coppie di volumi**.
2. Fare clic sull'icona Azioni relativa alla coppia di volumi che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Elimina una coppia di cluster

È possibile eliminare una coppia di cluster dall'interfaccia utente dell'elemento di uno qualsiasi dei cluster nella coppia.

1. Fare clic su **Protezione dati** > **Coppie cluster**.
2. Fare clic sull'icona Azioni per una coppia di cluster.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Conferma l'azione.
5. Ripetere i passaggi dal secondo cluster nell'associazione di cluster.

Dettagli della coppia di cluster

La pagina Coppie di cluster nella scheda Protezione dati fornisce informazioni sui cluster che sono stati associati o che sono in fase di associazione. Il sistema visualizza messaggi di associazione e di avanzamento nella colonna Stato.

- **ID**

  Un ID generato dal sistema assegnato a ciascuna coppia di cluster.

- **Nome del cluster remoto**

  Il nome dell'altro cluster nella coppia.

- **MVIP remoto**

  L'indirizzo IP virtuale di gestione dell'altro cluster nella coppia.

- **Stato**

  Stato di replicazione del cluster remoto

- **Replica dei volumi**

  Numero di volumi contenuti nel cluster che vengono accoppiati per la replica.

- **UUID**

  Un ID univoco assegnato a ciascun cluster nella coppia.

Coppie di volumi

Dettagli della coppia di volumi

La pagina Coppie di volumi nella scheda Protezione dati fornisce informazioni sui volumi che sono stati associati o sono in fase di associazione. Il sistema visualizza messaggi di associazione e di avanzamento nella colonna Stato volume.

- **ID**

  ID generato dal sistema per il volume.

- **Nome**

  Nome dato al volume al momento della sua creazione. I nomi dei volumi possono contenere fino a 223 caratteri e contenere az, 0-9 e trattino (-).

- **Account**

  Nome dell'account assegnato al volume.

- **Stato del volume**

  Stato di replicazione del volume

- **Stato dell'istantanea**

  Stato del volume snapshot.

- **Modalità**

  Metodo di replicazione della scrittura del client. I valori possibili sono i seguenti:

  - Asincrono
  - Solo snapshot
  - Sincronizzazione

- **Direzione**

  La direzione dei dati del volume:

  - Icona del volume sorgente (→) indica che i dati vengono scritti su una destinazione esterna al cluster.

- Icona del volume di destinazione ( ) indica che i dati vengono scritti sul volume locale da una fonte esterna.

- **Ritardo asincrono**

  Intervallo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è abbinato, il valore è nullo.

- **Cluster remoto**

  Nome del cluster remoto su cui risiede il volume.

- **ID volume remoto**

  ID volume del volume sul cluster remoto.

- **Nome del volume remoto**

  Nome assegnato al volume remoto al momento della sua creazione.

Messaggi di associazione del volume

È possibile visualizzare i messaggi di associazione del volume durante il processo di associazione iniziale dalla pagina Coppie di volumi nella scheda Protezione dati. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia nella vista elenco dei volumi di replica.

- **PausaDisconnesso**

  Timeout della replica di origine o delle RPC di sincronizzazione. La connessione al cluster remoto è stata persa. Controllare le connessioni di rete al cluster.

- **Ripresa della connessione**

  La sincronizzazione della replica remota è ora attiva. Avvio del processo di sincronizzazione e attesa dei dati.

- **Ripresa di RRSync**

  Viene creata una singola copia elicoidale dei metadati del volume nel cluster associato.

- **Ripresa della sincronizzazione locale**

  Viene eseguita una copia a doppia elica dei metadati del volume nel cluster associato.

- **Ripresa del trasferimento dati**

  Il trasferimento dei dati è ripreso.

- **Attivo**

  I volumi vengono accoppiati e i dati vengono inviati dal volume di origine a quello di destinazione, sincronizzandoli.

- **Oziare**

Non si verifica alcuna attività di replicazione.

Avvisi di associazione del volume

La pagina Coppie di volumi nella scheda Protezione dati fornisce questi messaggi dopo aver associato i volumi. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia (salvo diversa indicazione) nella vista elenco dei volumi di replica.

- **PausedClusterFull**

  Poiché il cluster di destinazione è pieno, la replicazione di origine e il trasferimento di dati in blocco non possono procedere. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedExceededMaxSnapshotCount**

  Il volume di destinazione ha già il numero massimo di snapshot e non può replicare snapshot aggiuntivi.

- **PausaManuale**

  Il volume locale è stato messo in pausa manualmente. È necessario riattivarla prima che la replicazione riprenda.

- **PausedManualRemote**

  Il volume remoto è in modalità di pausa manuale. È necessario un intervento manuale per riattivare il volume remoto prima che la replica riprenda.

- **PausaNon configurato correttamente**

  In attesa di una sorgente e di una destinazione attive. Per riprendere la replicazione è necessario un intervento manuale.

- **QoS in pausa**

  La QoS di destinazione non è riuscita a sostenere l'I/O in entrata. La replicazione riprende automaticamente. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedSlowLink**

  È stato rilevato un collegamento lento e la replica è stata interrotta. La replicazione riprende automaticamente. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedVolumeSizeMismatch**

  Il volume di destinazione non ha le stesse dimensioni del volume di origine.

- **PausedXCopy**

  Un comando SCSI XCOPY viene inviato a un volume sorgente. Il comando deve essere completato prima che la replicazione possa riprendere. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **ArrestatoNon configurato correttamente**

È stato rilevato un errore di configurazione permanente. Il volume remoto è stato eliminato o disaccoppiato. Non è possibile alcuna azione correttiva; è necessario stabilire un nuovo abbinamento.

Utilizzare la replica SnapMirror tra cluster Element e ONTAP (interfaccia utente Element)

Utilizzare la replica SnapMirror tra cluster Element e ONTAP (interfaccia utente Element)

È possibile creare relazioni SnapMirror dalla scheda Protezione dati nell'interfaccia utente NetApp Element . Per visualizzarlo nell'interfaccia utente, è necessario abilitare la funzionalità SnapMirror .

IPv6 non è supportato per la replica SnapMirror tra il software NetApp Element e i cluster ONTAP .

"Video NetApp : SnapMirror per NetApp HCI e Element Software"

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare copie Snapshot con i sistemi NetApp ONTAP . Il motivo principale per cui si utilizza questa tecnologia è il ripristino di emergenza di NetApp HCI su ONTAP. Gli endpoint includono ONTAP, ONTAP Select e Cloud Volumes ONTAP. Vedere TR-4641 Protezione dei dati NetApp HCI .

"Rapporto tecnico NetApp 4641: Protezione dei dati NetApp HCI"

Trova maggiori informazioni

- "Creazione del tuo Data Fabric con NetApp HCI, ONTAP e Converged Infrastructure"
- "Replica tra NetApp Element Software e ONTAP (ONTAP CLI)"

Panoramica SnapMirror

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare snapshot con i sistemi NetApp ONTAP .

I sistemi che eseguono Element possono comunicare direttamente con SnapMirror sui sistemi ONTAP 9.3 o versioni successive. L'API NetApp Element fornisce metodi per abilitare la funzionalità SnapMirror su cluster, volumi e snapshot. Inoltre, l'interfaccia utente di Element include tutte le funzionalità necessarie per gestire le relazioni SnapMirror tra il software Element e i sistemi ONTAP .

È possibile replicare i volumi originati ONTAP nei volumi Element in casi d'uso specifici con funzionalità limitate. Per maggiori informazioni, vedere "Replica tra il software Element e ONTAP (ONTAP CLI)".

Abilita SnapMirror sul cluster

È necessario abilitare manualmente la funzionalità SnapMirror a livello di cluster tramite l'interfaccia utente NetApp Element . Il sistema è dotato di funzionalità SnapMirror disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento. L'abilitazione della funzionalità SnapMirror è un'operazione di configurazione che va eseguita una sola volta.

SnapMirror può essere abilitato solo per i cluster che eseguono il software Element utilizzato insieme ai volumi su un sistema NetApp ONTAP . È necessario abilitare la funzionalità SnapMirror solo se il cluster è connesso

per l'uso con volumi NetApp ONTAP .

Cosa ti servirà

Il cluster di storage deve eseguire il software NetApp Element .

Passi

1. Fare clic su **Cluster** > **Impostazioni**.
2. Trova le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Abilita SnapMirror**.

> L'abilitazione della funzionalità SnapMirror modifica in modo permanente la configurazione del software Element. È possibile disattivare la funzionalità SnapMirror e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica.

4. Fare clic su **Sì** per confermare la modifica alla configurazione SnapMirror .

Abilita SnapMirror sul volume

È necessario abilitare SnapMirror sul volume nell'interfaccia utente di Element. Ciò consente la replica dei dati su volumi ONTAP specificati. Si tratta dell'autorizzazione concessa dall'amministratore del cluster che esegue il software NetApp Element affinché SnapMirror controlli un volume.

Cosa ti servirà

- Hai abilitato SnapMirror nell'interfaccia utente Element per il cluster.
- È disponibile un endpoint SnapMirror .
- Il volume deve avere una dimensione di blocco di 512e.
- Il volume non partecipa alla replica remota.
- Il tipo di accesso al volume non è Destinazione replica.

> È possibile impostare questa proprietà anche durante la creazione o la clonazione di un volume.

Passi

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume per cui si desidera abilitare SnapMirror .
3. Nel menu che si apre, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica volume**, selezionare la casella di controllo **Abilita SnapMirror**.
5. Fare clic su **Salva modifiche**.

Crea un endpoint SnapMirror

Prima di poter creare una relazione, è necessario creare un endpoint SnapMirror nell'interfaccia utente NetApp Element .

Un endpoint SnapMirror è un cluster ONTAP che funge da destinazione di replica per un cluster che esegue il software Element. Prima di creare una relazione SnapMirror , è necessario creare un endpoint SnapMirror .

È possibile creare e gestire fino a quattro endpoint SnapMirror su un cluster di archiviazione che esegue il software Element.

> Se un endpoint esistente è stato originariamente creato utilizzando l'API e le credenziali non sono state salvate, è possibile visualizzare l'endpoint nell'interfaccia utente dell'elemento e verificarne l'esistenza, ma non può essere gestito utilizzando l'interfaccia utente dell'elemento. Questo endpoint può quindi essere gestito solo tramite l'API Element.

Per i dettagli sui metodi API, vedere "Gestisci l'archiviazione con l'API Element".

Cosa ti servirà

- Dovresti aver abilitato SnapMirror nell'interfaccia utente di Element per il cluster di archiviazione.
- Conosci le credenziali ONTAP per l'endpoint.

Passi

1. Fare clic su **Protezione dati** > *Endpoint SnapMirror *.
2. Fare clic su **Crea endpoint**.
3. Nella finestra di dialogo **Crea un nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster del sistema ONTAP .
4. Immettere le credenziali di amministratore ONTAP associate all'endpoint.
5. Esaminare i dettagli aggiuntivi:
   - LIF: elenca le interfacce logiche intercluster ONTAP utilizzate per comunicare con Element.
   - Stato: mostra lo stato corrente dell'endpoint SnapMirror . I valori possibili sono: connesso, disconnesso e non gestito.
6. Fare clic su **Crea endpoint**.

Crea una relazione SnapMirror

È necessario creare una relazione SnapMirror nell'interfaccia utente NetApp Element .

> Se un volume non è ancora abilitato per SnapMirror e si sceglie di creare una relazione dall'interfaccia utente dell'elemento, SnapMirror viene automaticamente abilitato su quel volume.

Cosa ti servirà

SnapMirror è abilitato sul volume.

Passi

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che deve far parte della relazione.
3. Fare clic su *Crea una relazione SnapMirror *.
4. Nella finestra di dialogo **Crea una relazione SnapMirror *, seleziona un endpoint dall'elenco *Endpoint**.
5. Selezionare se la relazione verrà creata utilizzando un nuovo volume ONTAP o un volume ONTAP esistente.
6. Per creare un nuovo volume ONTAP nell'interfaccia utente di Element, fare clic su **Crea nuovo volume**.

a. Selezionare la **Macchina virtuale di archiviazione** per questa relazione.
b. Selezionare **Aggregato** dall'elenco a discesa.
c. Nel campo **Suffisso nome volume**, immettere un suffisso.

> Il sistema rileva il nome del volume di origine e lo copia nel campo **Nome volume**. Il suffisso inserito aggiunge il nome.

d. Fare clic su **Crea volume di destinazione**.

7. Per utilizzare un volume ONTAP esistente, fare clic su **Usa volume esistente**.
   a. Selezionare la **Macchina virtuale di archiviazione** per questa relazione.
   b. Selezionare il volume di destinazione per questa nuova relazione.
8. Nella sezione **Dettagli relazione**, seleziona una policy. Se il criterio selezionato ha regole di mantenimento, la tabella Regole visualizza le regole e le etichette associate.
9. **Facoltativo**: seleziona una pianificazione.

   Ciò determina la frequenza con cui la relazione crea copie.

10. **Facoltativo**: Nel campo **Limita larghezza di banda a**, immettere la quantità massima di larghezza di banda che può essere utilizzata dai trasferimenti di dati associati a questa relazione.
11. Esaminare i dettagli aggiuntivi:
    - **Stato**: Stato attuale della relazione del volume di destinazione. I valori possibili sono:
      - non inizializzato: il volume di destinazione non è stato inizializzato.
      - snapmirrored: il volume di destinazione è stato inizializzato ed è pronto per ricevere gli aggiornamenti SnapMirror .
      - interrotto: il volume di destinazione è in lettura/scrittura e sono presenti snapshot.
    - **Stato**: Stato attuale della relazione. I valori possibili sono idle, transferring, checking, quiescing, quiesced, queued, preparing, finalizing, aborting e breaking.
    - **Tempo di ritardo**: quantità di tempo in secondi per cui il sistema di destinazione è in ritardo rispetto al sistema di origine. Il tempo di ritardo non deve essere superiore all'intervallo di pianificazione del trasferimento.
    - **Limite di larghezza di banda**: la quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
    - **Ultimo trasferimento**: timestamp dell'ultimo snapshot trasferito. Clicca per ulteriori informazioni.
    - **Nome policy**: il nome della policy ONTAP SnapMirror per la relazione.
    - **Tipo di policy**: tipo di policy ONTAP SnapMirror selezionata per la relazione. I valori possibili sono:
      - specchio asincrono
      - specchio_vault
    - **Nome pianificazione**: Nome della pianificazione preesistente sul sistema ONTAP selezionato per questa relazione.
12. Per non inizializzare in questo momento, assicurarsi che la casella di controllo **Inizializza** non sia selezionata.

L'inizializzazione può richiedere molto tempo. Potrebbe essere opportuno eseguirlo durante le ore non di punta. L'inizializzazione esegue un trasferimento di base; crea una copia snapshot del volume di origine, quindi trasferisce tale copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. È possibile inizializzare manualmente oppure utilizzare una pianificazione per avviare il processo di inizializzazione (e gli aggiornamenti successivi) in base alla pianificazione.

13. Fare clic su **Crea relazione**.
14. Fare clic su **Protezione dati** > *Relazioni SnapMirror * per visualizzare questa nuova relazione SnapMirror .

Azioni di relazione SnapMirror

È possibile configurare una relazione dalla pagina Relazioni SnapMirror della scheda Protezione dati. Qui vengono descritte le opzioni dell'icona Azioni.

- **Modifica**: modifica la policy utilizzata o la pianificazione per la relazione.
- **Elimina**: elimina la relazione SnapMirror . Questa funzione non elimina il volume di destinazione.
- **Inizializza**: esegue il primo trasferimento iniziale di dati di base per stabilire una nuova relazione.
- **Aggiorna**: esegue un aggiornamento su richiesta della relazione, replicando tutti i nuovi dati e le copie Snapshot inclusi dall'ultimo aggiornamento alla destinazione.
- **Quiesce**: impedisce ulteriori aggiornamenti per una relazione.
- **Riprendi**: Riprende una relazione sospesa.
- **Break**: imposta il volume di destinazione in lettura-scrittura e interrompe tutti i trasferimenti correnti e futuri. Verificare che i client non stiano utilizzando il volume sorgente originale, perché l'operazione di risincronizzazione inversa rende il volume sorgente originale di sola lettura.
- **Risincronizzazione**: ripristina una relazione interrotta nella stessa direzione prima che si verificasse l'interruzione.
- **Risincronizzazione inversa**: automatizza i passaggi necessari per creare e inizializzare una nuova relazione nella direzione opposta. Ciò è possibile solo se la relazione esistente è in uno stato di interruzione. Questa operazione non eliminerà la relazione corrente. Il volume di origine originale torna alla copia Snapshot comune più recente e si risincronizza con la destinazione. Tutte le modifiche apportate al volume sorgente originale dall'ultimo aggiornamento SnapMirror riuscito andranno perse. Tutte le modifiche apportate o i nuovi dati scritti nel volume di destinazione corrente vengono rispediti al volume di origine originale.
- **Annulla**: annulla un trasferimento in corso. Se viene emesso un aggiornamento SnapMirror per una relazione interrotta, la relazione continua con l'ultimo trasferimento dall'ultimo checkpoint di riavvio creato prima dell'interruzione.

Etichette SnapMirror

Etichette SnapMirror

Un'etichetta SnapMirror funge da marcatore per il trasferimento di uno snapshot specificato in base alle regole di conservazione della relazione.

L'applicazione di un'etichetta a uno snapshot lo contrassegna come destinazione per la replica SnapMirror . Il ruolo della relazione è quello di far rispettare le regole durante il trasferimento dei dati selezionando lo

snapshot etichettato corrispondente, copiandolo nel volume di destinazione e assicurando che venga conservato il numero corretto di copie. Si riferisce alla politica per determinare il conteggio dei dati da conservare e il periodo di conservazione. La policy può avere un numero qualsiasi di regole e ogni regola ha un'etichetta univoca. Questa etichetta funge da collegamento tra lo snapshot e la regola di conservazione.

È l'etichetta SnapMirror che indica quale regola viene applicata allo snapshot, allo snapshot di gruppo o alla pianificazione selezionati.

Aggiungi etichette SnapMirror agli snapshot

Le etichette SnapMirror specificano i criteri di conservazione degli snapshot sull'endpoint SnapMirror . È possibile aggiungere etichette agli snapshot e agli snapshot di gruppo.

È possibile visualizzare le etichette disponibili da una finestra di dialogo di relazione SnapMirror esistente o da NetApp ONTAP System Manager.

> Quando si aggiunge un'etichetta a uno snapshot di gruppo, tutte le etichette esistenti nei singoli snapshot vengono sovrascritte.

Cosa ti servirà

- SnapMirror è abilitato sul cluster.
- L'etichetta che vuoi aggiungere esiste già in ONTAP.

Passi

1. Fare clic sulla pagina **Protezione dati** > **Snapshot** o **Snapshot di gruppo**.
2. Fare clic sull'icona **Azioni** per lo snapshot o lo snapshot di gruppo a cui si desidera aggiungere un'etichetta SnapMirror .
3. Nella finestra di dialogo **Modifica istantanea**, immettere il testo nel campo *Etichetta SnapMirror *. L'etichetta deve corrispondere a un'etichetta di regola nel criterio applicato alla relazione SnapMirror .
4. Fare clic su **Salva modifiche**.

Aggiungere etichette SnapMirror alle pianificazioni degli snapshot

È possibile aggiungere etichette SnapMirror alle pianificazioni degli snapshot per garantire che venga applicata una policy SnapMirror . È possibile visualizzare le etichette disponibili da una finestra di dialogo di relazione SnapMirror esistente o da NetAppONTAP System Manager.

Cosa ti servirà

- SnapMirror deve essere abilitato a livello di cluster.
- L'etichetta che vuoi aggiungere esiste già in ONTAP.

Passi

1. Fare clic su **Protezione dati** > **Pianificazioni**.
2. Aggiungere un'etichetta SnapMirror a una pianificazione in uno dei seguenti modi:

Opzione	Passi
Creazione di un nuovo programma	a. Seleziona **Crea pianificazione**. b. Inserisci tutti gli altri dettagli rilevanti. c. Seleziona **Crea pianificazione**.
Modifica della pianificazione esistente	a. Fare clic sull'icona **Azioni** per la pianificazione a cui si desidera aggiungere un'etichetta e selezionare **Modifica**. b. Nella finestra di dialogo visualizzata, immettere il testo nel campo *Etichetta SnapMirror *. c. Selezionare **Salva modifiche**.

Trova maggiori informazioni

Creare una pianificazione snapshot

Ripristino di emergenza tramite SnapMirror

Ripristino di emergenza tramite SnapMirror

In caso di problemi con un volume o un cluster che esegue il software NetApp Element , utilizzare la funzionalità SnapMirror per interrompere la relazione ed eseguire il failover sul volume di destinazione.

Se il cluster originale è completamente guasto o non esiste più, contattare l'assistenza NetApp per ulteriore assistenza.

Eseguire un failover da un cluster Element

È possibile eseguire un failover dal cluster Element per rendere il volume di destinazione accessibile in lettura/scrittura agli host sul lato di destinazione. Prima di eseguire un failover dal cluster Element, è necessario interrompere la relazione SnapMirror .

Utilizzare l'interfaccia utente NetApp Element per eseguire il failover. Se l'interfaccia utente dell'elemento non è disponibile, è possibile utilizzare anche ONTAP System Manager o ONTAP CLI per emettere il comando di interruzione della relazione.

Cosa ti servirà

- Esiste una relazione SnapMirror e sul volume di destinazione è presente almeno uno snapshot valido.
- È necessario effettuare il failover sul volume di destinazione a causa di un'interruzione imprevista o di un evento pianificato nel sito principale.

Passi

1. Nell'interfaccia utente dell'elemento, fare clic su **Protezione dati** > *Relazioni SnapMirror *.
2. Trova la relazione con il volume di origine di cui vuoi eseguire il failover.
3. Fare clic sull'icona **Azioni**.

4. Fare clic su **Interruzione**.
5. Conferma l'azione.

   Il volume sul cluster di destinazione ora ha accesso in lettura/scrittura e può essere montato sugli host dell'applicazione per riprendere i carichi di lavoro di produzione. A seguito di questa azione, tutte le repliche SnapMirror vengono interrotte. La relazione mostra uno stato di rottura.

Eseguire un failback su Element

Scopri come eseguire un failback su Element

Una volta mitigato il problema sul lato primario, è necessario risincronizzare il volume di origine ed eseguire il failback sul software NetApp Element . I passaggi da eseguire variano a seconda che il volume di origine esista ancora o che sia necessario eseguire il failback su un volume appena creato.

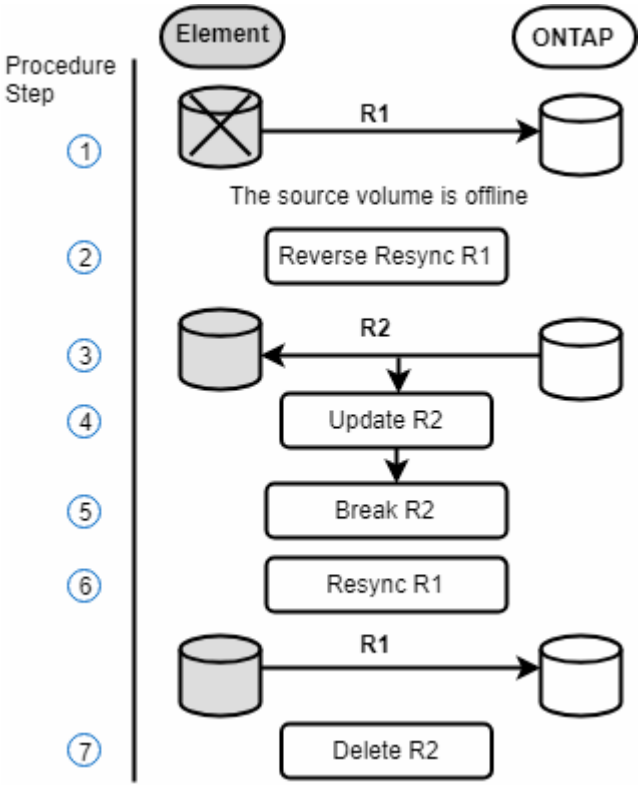
Scenari di failback SnapMirror

La funzionalità di disaster recovery SnapMirror è illustrata in due scenari di failback. Questi presuppongono che la relazione originale sia stata interrotta (interrotta).

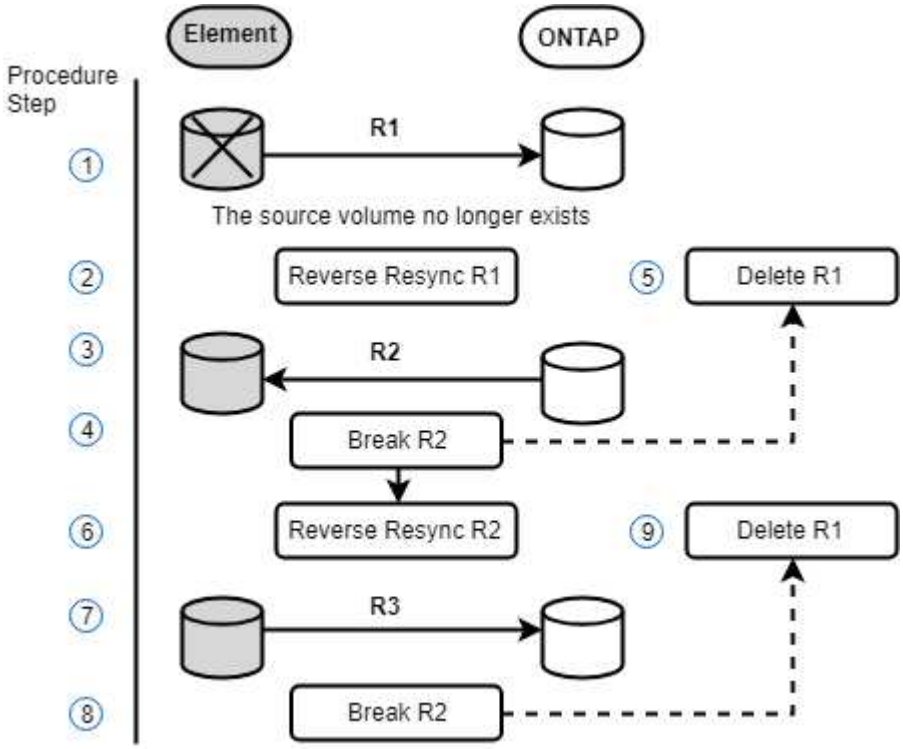
I passaggi delle procedure corrispondenti sono aggiunti a titolo di riferimento.

> Negli esempi qui riportati, R1 = la relazione originale in cui il cluster che esegue il software NetApp Element è il volume di origine originale (Element) e ONTAP è il volume di destinazione originale (ONTAP). R2 e R3 rappresentano le relazioni inverse create tramite l'operazione di risincronizzazione inversa.

L'immagine seguente mostra lo scenario di failback quando il volume di origine esiste ancora:



L'immagine seguente mostra lo scenario di failback quando il volume di origine non esiste più:



Trova maggiori informazioni

- Eseguire un failback quando il volume di origine esiste ancora
- Eseguire un failback quando il volume di origine non esiste più
- Scenari di failback SnapMirror

Eseguire un failback quando il volume di origine esiste ancora

È possibile risincronizzare il volume di origine originale ed eseguire il failback utilizzando l'interfaccia utente NetApp Element . Questa procedura si applica agli scenari in cui il volume sorgente originale esiste ancora.

1. Nell'interfaccia utente dell'elemento, individua la relazione che hai interrotto per eseguire il failover.
2. Fare clic sull'icona Azioni e quindi su **Risincronizzazione inversa**.
3. Conferma l'azione.

> L'operazione di risincronizzazione inversa crea una nuova relazione in cui i ruoli dei volumi di origine e di destinazione originali vengono invertiti (ciò determina due relazioni poiché la relazione originale persiste). Tutti i nuovi dati dal volume di destinazione originale vengono trasferiti al volume di origine originale come parte dell'operazione di risincronizzazione inversa. È possibile continuare ad accedere e scrivere dati sul volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host dal volume di origine ed eseguire un aggiornamento SnapMirror prima di reindirizzare al volume primario originale.

4. Fare clic sull'icona Azioni della relazione inversa appena creata e fare clic su **Aggiorna**.

Ora che hai completato la risincronizzazione inversa e verificato che non ci sono sessioni attive connesse al volume sul lato di destinazione e che i dati più recenti si trovano sul volume primario originale, puoi eseguire i seguenti passaggi per completare il failback e riattivare il volume primario originale:

5. Fare clic sull'icona Azioni della relazione inversa e fare clic su **Interrompi**.
6. Fare clic sull'icona Azioni della relazione originale e fare clic su **Risincronizza**.

> Ora è possibile montare il volume primario originale per riprendere i carichi di lavoro di produzione sul volume primario originale. La replica SnapMirror originale riprende in base ai criteri e alla pianificazione configurati per la relazione.

7. Dopo aver confermato che lo stato della relazione originale è "snapmirrored", fare clic sull'icona Azioni della relazione inversa e fare clic su **Elimina**.

Trova maggiori informazioni

Scenari di failback SnapMirror

Eseguire un failback quando il volume di origine non esiste più

È possibile risincronizzare il volume di origine originale ed eseguire il failback utilizzando l'interfaccia utente NetApp Element . Questa sezione si applica agli scenari in cui il volume sorgente originale è andato perso ma il cluster originale è ancora intatto. Per istruzioni su come ripristinare un nuovo cluster, consultare la documentazione sul sito di supporto NetApp .

Cosa ti servirà

- Si è verificata un'interruzione della relazione di replica tra i volumi Element e ONTAP .
- Il volume Element è irrimediabilmente perso.
- Il nome del volume originale risulta NON TROVATO.

Passi

1. Nell'interfaccia utente dell'elemento, individua la relazione che hai interrotto per eseguire il failover.

   Migliore pratica: prendi nota della politica SnapMirror e pianifica i dettagli della relazione interrotta originariamente. Queste informazioni saranno necessarie per ricreare la relazione.

2. Fare clic sull'icona **Azioni** e quindi su **Risincronizzazione inversa**.
3. Conferma l'azione.

> L'operazione Reverse Resync crea una nuova relazione in cui i ruoli del volume di origine originale e del volume di destinazione vengono invertiti (ciò determina due relazioni poiché la relazione originale persiste). Poiché il volume originale non esiste più, il sistema crea un nuovo volume Element con lo stesso nome e le stesse dimensioni del volume di origine originale. Al nuovo volume viene assegnata una policy QoS predefinita denominata sm-recovery ed è associato a un account predefinito denominato sm-recovery. Sarà necessario modificare manualmente l'account e la policy QoS per tutti i volumi creati da SnapMirror per sostituire i volumi di origine originali che sono stati distrutti.

I dati dell'ultimo snapshot vengono trasferiti al nuovo volume come parte dell'operazione di

risincronizzazione inversa. È possibile continuare ad accedere e scrivere dati sul volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host dal volume attivo ed eseguire un aggiornamento SnapMirror prima di ripristinare la relazione primaria originale in un passaggio successivo. Dopo aver completato la risincronizzazione inversa e aver verificato che non vi siano sessioni attive connesse al volume sul lato di destinazione e che i dati più recenti si trovino sul volume primario originale, continuare con i passaggi seguenti per completare il failback e riattivare il volume primario originale:

4. Fare clic sull'icona **Azioni** della relazione inversa creata durante l'operazione di risincronizzazione inversa e fare clic su **Interrompi**.
5. Fare clic sull'icona **Azioni** della relazione originale, in cui il volume di origine non esiste, e fare clic su **Elimina**.
6. Fare clic sull'icona **Azioni** della relazione inversa, che è stata interrotta nel passaggio 4, e fare clic su **Risincronizzazione inversa**.
7. In questo modo si invertono l'origine e la destinazione e si ottiene una relazione con lo stesso volume di origine e lo stesso volume di destinazione della relazione originale.
8. Fare clic sull'icona **Azioni** e su **Modifica** per aggiornare questa relazione con le impostazioni di pianificazione e i criteri QoS originali di cui si è preso nota.
9. Ora è possibile eliminare in sicurezza la relazione inversa che hai risincronizzato al passaggio 6.

Trova maggiori informazioni

Scenari di failback SnapMirror

Eseguire un trasferimento o una migrazione una tantum da ONTAP a Element

In genere, quando si utilizza SnapMirror per il disaster recovery da un cluster di storage SolidFire che esegue il software NetApp Element al software ONTAP , Element è l'origine e ONTAP la destinazione. Tuttavia, in alcuni casi il sistema di archiviazione ONTAP può fungere da origine e Element da destinazione.

- Esistono due scenari:
  - Non esiste alcuna relazione precedente di disaster recovery. Seguire tutti i passaggi di questa procedura.
  - Esiste una precedente relazione di disaster recovery, ma non tra i volumi utilizzati per questa mitigazione. In questo caso, seguire solo i passaggi 3 e 4 riportati di seguito.

Cosa ti servirà

- Il nodo di destinazione dell'elemento deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .

È necessario specificare il percorso di destinazione dell'elemento nel formato hostip:/lun/<id_number>, dove lun è la stringa effettiva "lun" e id_number è l'ID del volume dell'elemento.

Passi

1. Utilizzando ONTAP, creare la relazione con il cluster Element:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Verificare che la relazione SnapMirror sia stata creata utilizzando il comando ONTAP snapmirror show.

   Per informazioni sulla creazione di una relazione di replica, consultare la documentazione ONTAP e per la sintassi completa dei comandi, consultare la pagina man ONTAP .

3. Utilizzando il `ElementCreateVolume` API, crea il volume di destinazione e imposta la modalità di accesso al volume di destinazione su SnapMirror:

   Crea un volume Element utilizzando l'API Element

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Inizializzare la relazione di replicazione utilizzando ONTAP `snapmirror initialize` comando:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Replica tra il software NetApp Element e ONTAP (ONTAP CLI)

Panoramica della replica tra il software NetApp Element e ONTAP (ONTAP CLI)

È possibile garantire la continuità aziendale su un sistema Element utilizzando

SnapMirror per replicare copie snapshot di un volume Element su una destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP e quindi riattivare il sistema Element quando il servizio viene ripristinato.

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un nodo ONTAP su un sistema Element. Potresti aver creato una LUN durante un'interruzione nel sito Element oppure potresti utilizzare una LUN per migrare i dati da ONTAP al software Element.

Dovresti utilizzare il backup Element to ONTAP se si verificano le seguenti condizioni:

- È meglio utilizzare le best practice, non esplorare tutte le opzioni disponibili.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI) ONTAP , non System Manager o uno strumento di scripting automatizzato.
- Si utilizza iSCSI per fornire dati ai client.

Se hai bisogno di ulteriori informazioni sulla configurazione o concettuali SnapMirror , vedi"Panoramica sulla protezione dei dati" .

Informazioni sulla replica tra Element e ONTAP

A partire da ONTAP 9.3, è possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element in una destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un nodo ONTAP su un sistema Element. Potresti aver creato una LUN durante un'interruzione nel sito Element oppure potresti utilizzare una LUN per migrare i dati da ONTAP al software Element.

Tipi di rapporto di protezione dei dati

SnapMirror offre due tipi di rapporto di protezione dei dati. Per ogni tipo, SnapMirror crea una copia snapshot del volume sorgente dell'elemento prima di inizializzare o aggiornare la relazione:

- In una relazione di protezione dei dati di *disaster recovery (DR)*, il volume di destinazione contiene solo la copia snapshot creata da SnapMirror, dalla quale è possibile continuare a fornire dati in caso di catastrofe nel sito primario.
- In una relazione di protezione dei dati con *conservazione a lungo termine*, il volume di destinazione contiene copie snapshot point-in-time create dal software Element, nonché la copia snapshot creata da SnapMirror. Ad esempio, potresti voler conservare copie mensili degli snapshot creati in un arco di tempo di 20 anni.

Politiche predefinite

La prima volta che si richiama SnapMirror, viene eseguito un *trasferimento di base* dal volume di origine al volume di destinazione. La policy *SnapMirror* definisce il contenuto della baseline e tutti gli aggiornamenti.

Quando si crea una relazione di protezione dei dati, è possibile utilizzare una policy predefinita o personalizzata. Il *tipo di policy* determina quali copie snapshot includere e quante copie conservare.

La tabella seguente mostra le policy predefinite. Utilizzare il `MirrorLatest` politica per creare una relazione DR tradizionale. Utilizzare il `MirrorAndVault` O `Unified7year` policy per creare una relazione di replica unificata, in cui DR e conservazione a lungo termine sono configurati sullo stesso volume di destinazione.

Politica	Tipo di polizza	Aggiorna il comportamento
MirrorLatest	specchio asincrono	Trasferisci la copia snapshot creata da SnapMirror.
MirrorAndVault	specchio-volta	Trasferisci la copia snapshot creata da SnapMirror e tutte le copie snapshot meno recenti create dall'ultimo aggiornamento, a condizione che abbiano etichette SnapMirror "giornaliere" o "settimanali".
Unified7year	specchio-volta	Trasferisci la copia snapshot creata da SnapMirror e tutte le copie snapshot meno recenti create dall'ultimo aggiornamento, a condizione che abbiano le etichette SnapMirror "giornaliera", "settimanale" o "mensile".

Per informazioni di base complete sulle policy SnapMirror , inclusa una guida su quale policy utilizzare, vedere"Panoramica sulla protezione dei dati" .

Informazioni sulle etichette SnapMirror

Ogni policy con tipo di policy "mirror-vault" deve avere una regola che specifica quali copie snapshot replicare. La regola "daily", ad esempio, indica che devono essere replicate solo le copie snapshot a cui è stata assegnata l'etichetta SnapMirror "daily". L'etichetta SnapMirror viene assegnata quando si configurano le copie snapshot di Element.

Replica da un cluster di origine Element a un cluster di destinazione ONTAP

È possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element su un sistema di destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

Un volume Element è più o meno equivalente a un LUN ONTAP . SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP . SnapMirror replica i dati su una LUN esistente se la LUN soddisfa i requisiti per la replica da Element a ONTAP .

Le regole di replicazione sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume Element.
- Non è possibile replicare i dati da un volume ONTAP a più volumi Element.

Replica da un cluster di origine ONTAP a un cluster di destinazione Element

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un sistema ONTAP su un volume Element:

- Se esiste già una relazione SnapMirror tra un'origine Element e una destinazione ONTAP , un LUN creato mentre si forniscono dati dalla destinazione viene replicato automaticamente quando l'origine viene riattivata.
- In caso contrario, è necessario creare e inizializzare una relazione SnapMirror tra il cluster di origine ONTAP e il cluster di destinazione Element.

Le regole di replicazione sono le seguenti:

- La relazione di replicazione deve avere una policy di tipo “async-mirror”.

  I criteri di tipo “mirror-vault” non sono supportati.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Prerequisiti

Prima di configurare una relazione di protezione dei dati tra Element e ONTAP, è necessario aver completato le seguenti attività:

- Il cluster Element deve eseguire il software NetApp Element versione 10.1 o successiva.
- Il cluster ONTAP deve eseguire ONTAP 9.3 o versione successiva.
- SnapMirror deve essere concesso in licenza sul cluster ONTAP .
- È necessario aver configurato volumi sui cluster Element e ONTAP sufficientemente grandi da gestire i trasferimenti di dati previsti.
- Se si utilizza il tipo di criterio “mirror-vault”, è necessario che sia stata configurata un’etichetta SnapMirror per le copie snapshot dell’elemento da replicare.

  Puoi eseguire questa attività solo in"Interfaccia utente web del software Element" o utilizzando il"Metodi API" .

- È necessario assicurarsi che la porta 5010 sia disponibile.
- Se si prevede di dover spostare un volume di destinazione, è necessario assicurarsi che esista una connettività full-mesh tra l’origine e la destinazione. Ogni nodo del cluster di origine Element deve essere in grado di comunicare con ogni nodo del cluster di destinazione ONTAP .

Dettagli di supporto

La tabella seguente mostra i dettagli del supporto per il backup da Element a ONTAP .

Risorsa o funzionalità	Dettagli di supporto

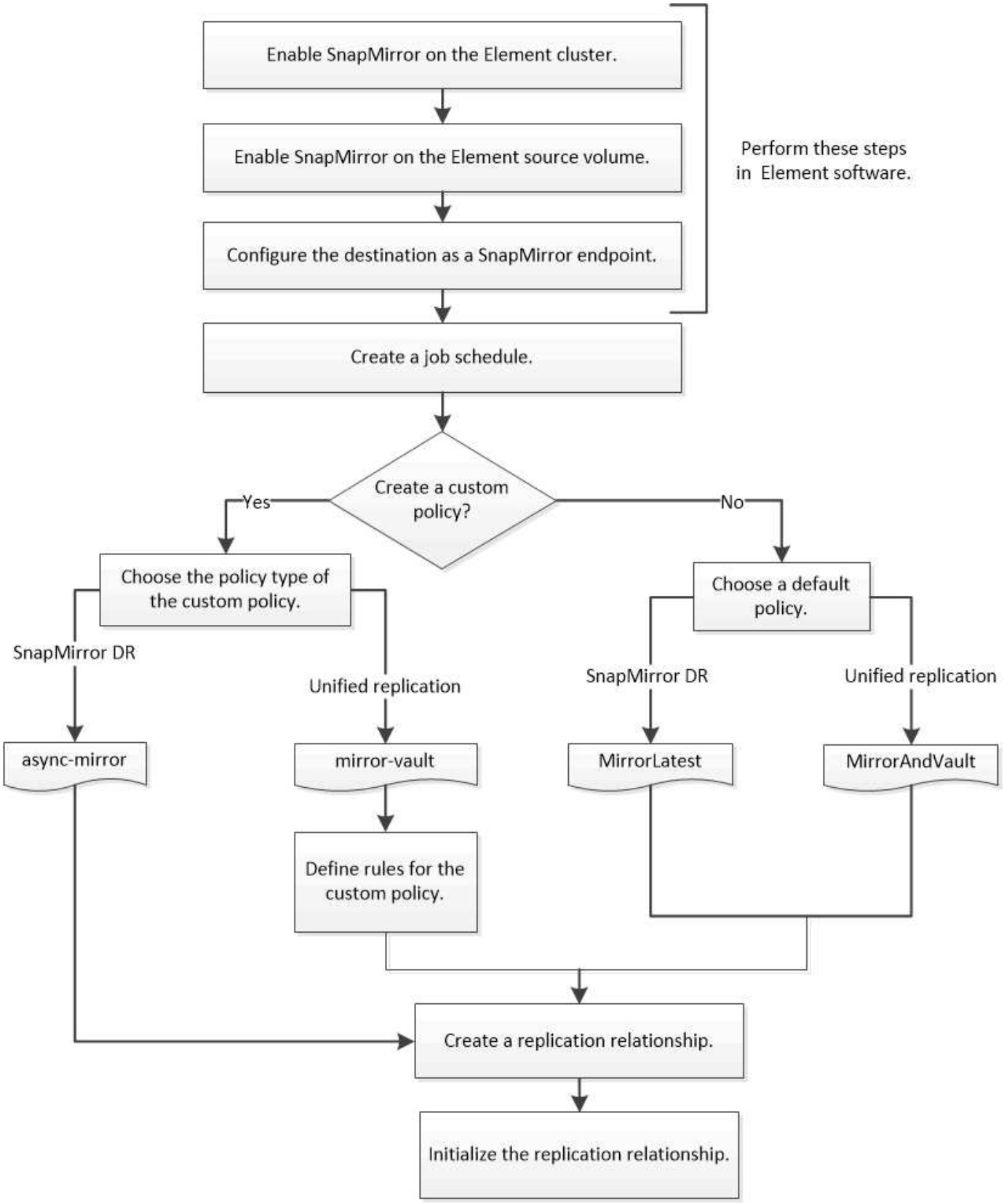
SnapMirror	• La funzione di ripristino SnapMirror non è supportata. • IL `MirrorAllSnapshots` E `XDPDefault` le policy non sono supportate. • Il tipo di criterio “vault” non è supportato. • La regola definita dal sistema “all_source_snapshots” non è supportata. • Il tipo di policy “mirror-vault” è supportato solo per la replica dal software Element a ONTAP. Utilizzare “async-mirror” per la replica da ONTAP al software Element. • IL `-schedule` E `-prefix` opzioni per `snapmirror policy add-rule` non sono supportati. • IL `-preserve` E `-quick-resync` opzioni per `snapmirror resync` non sono supportati. • L’efficienza di archiviazione non viene preservata. • Le distribuzioni di protezione dei dati a cascata e a fan-out non sono supportate.
ONTAP	• ONTAP Select è supportato a partire da ONTAP 9.4 ed Element 10.3. • Cloud Volumes ONTAP è supportato a partire da ONTAP 9.5 ed Element 11.0.
Elemento	• Il limite di dimensione del volume è 8 TiB. • La dimensione del blocco del volume deve essere 512 byte. Non è supportata una dimensione di blocco di 4K byte. • La dimensione del volume deve essere un multiplo di 1 MiB. • Gli attributi del volume non vengono conservati. • Il numero massimo di copie snapshot da replicare è 30.
Rete	• È consentita una singola connessione TCP per trasferimento. • Il nodo Elemento deve essere specificato come indirizzo IP. La ricerca del nome host DNS non è supportata. • Gli spazi IP non sono supportati.
SnapLock	I volumi SnapLock non sono supportati.
FlexGroup	I volumi FlexGroup non sono supportati.
SVM DR	I volumi ONTAP in una configurazione SVM DR non sono supportati.
MetroCluster	I volumi ONTAP in una configurazione MetroCluster non sono supportati.

Flusso di lavoro per la replica tra Element e ONTAP

Sia che si replichino dati da Element a ONTAP o da ONTAP a Element, è necessario

configurare una pianificazione dei processi, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare una policy predefinita o personalizzata.

Il flusso di lavoro presuppone che siano state completate le attività prerequisito elencate in"Prerequisiti" . Per informazioni di base complete sulle policy SnapMirror , inclusa una guida su quale policy utilizzare, vedere"Panoramica sulla protezione dei dati" .



Abilita SnapMirror nel software Element

Abilita SnapMirror sul cluster Element

È necessario abilitare SnapMirror sul cluster Element prima di poter creare una relazione

di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element o utilizzando "Metodo API".

Prima di iniziare

- Il cluster Element deve eseguire il software NetApp Element versione 10.1 o successiva.
- SnapMirror può essere abilitato solo per i cluster Element utilizzati con volumi NetApp ONTAP .

Informazioni su questo compito

Il sistema Element è dotato di SnapMirror disabilitato per impostazione predefinita. SnapMirror non viene abilitato automaticamente come parte di una nuova installazione o di un aggiornamento.

> Una volta abilitato, SnapMirror non può essere disabilitato. È possibile disattivare la funzionalità SnapMirror e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica.

Passi

1. Fare clic su **Cluster** > **Impostazioni**.
2. Trova le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Abilita SnapMirror**.

Abilita SnapMirror sul volume sorgente dell'elemento

È necessario abilitare SnapMirror sul volume di origine Element prima di poter creare una relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element o utilizzando"ModificaVolume" E"ModificaVolumi" Metodi API.

Prima di iniziare

- È necessario aver abilitato SnapMirror sul cluster Element.
- La dimensione del blocco del volume deve essere di 512 byte.
- Il volume non deve partecipare alla replica remota di Element.
- Il tipo di accesso al volume non deve essere "Replication Target".

Informazioni su questo compito

La procedura seguente presuppone che il volume esista già. È anche possibile abilitare SnapMirror quando si crea o si clona un volume.

Passi

1. Selezionare **Gestione** > **Volumi**.
2. Seleziona il pulsante per il volume.
3. Nel menu a discesa, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica volume**, seleziona **Abilita SnapMirror**.
5. Selezionare **Salva modifiche**.

Crea un endpoint SnapMirror

È necessario creare un endpoint SnapMirror prima di poter creare una relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software

Element o utilizzando "Metodi API SnapMirror".

Prima di iniziare

È necessario aver abilitato SnapMirror sul cluster Element.

Passi

1. Fare clic su **Protezione dati** > *Endpoint SnapMirror *.
2. Fare clic su **Crea endpoint**.
3. Nella finestra di dialogo **Crea un nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster ONTAP .
4. Immettere l'ID utente e la password dell'amministratore del cluster ONTAP .
5. Fare clic su **Crea endpoint**.

Configurare una relazione di replicazione

Creare una pianificazione di processi di replicazione

Sia che si replichino dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione dei processi, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare una policy predefinita o personalizzata.

Puoi usare il `job schedule cron create` comando per creare una pianificazione di processi di replicazione. La pianificazione dei lavori determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui è assegnata la pianificazione.

Informazioni su questo compito

Quando si crea una relazione di protezione dei dati, si assegna una pianificazione dei lavori. Se non si assegna una pianificazione dei lavori, è necessario aggiornare manualmente la relazione.

Fare un passo

1. Crea una pianificazione di lavoro:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Per `-month` , `-dayofweek` , E `-hour` , puoi specificare `all` per eseguire il lavoro rispettivamente ogni mese, giorno della settimana e ora.

   A partire da ONTAP 9.10.1, è possibile includere il Vserver nella pianificazione dei lavori:

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   L'esempio seguente crea una pianificazione di lavoro denominata `my_weekly` che si svolge il sabato alle 3:00 del mattino:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

Creare una politica di replica personalizzata

Quando si crea una relazione di replica, è possibile utilizzare un criterio predefinito o personalizzato. Per una policy di replica unificata personalizzata, è necessario definire una o più *regole* che stabiliscano quali copie snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

È possibile creare una policy di replica personalizzata se la policy predefinita per una relazione non è adatta. Ad esempio, potresti voler comprimere i dati in un trasferimento di rete o modificare il numero di tentativi effettuati SnapMirror per trasferire copie di snapshot.

Informazioni su questo compito

Il *tipo di policy* della policy di replica determina il tipo di relazione supportata. La tabella seguente mostra i tipi di polizza disponibili.

Tipo di polizza	Tipo di relazione
specchio asincrono	SnapMirror DR
specchio-volta	Replica unificata

Fare un passo

1. Crea una policy di replica personalizzata:

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
   low|normal -is-network-compression-enabled true|false
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia snapshot comune per le relazioni sincrone SnapMirror utilizzando `-common-snapshot-schedule` parametro. Per impostazione predefinita, la pianificazione comune della copia degli snapshot per le relazioni sincrone SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia degli snapshot per le relazioni sincrone SnapMirror .

   L'esempio seguente crea un criterio di replica personalizzato per SnapMirror DR che abilita la compressione di rete per i trasferimenti di dati:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment "DR with network compression
   enabled" -is-network-compression-enabled true
   ```

   L'esempio seguente crea un criterio di replica personalizzato per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Dopo aver finito

Per i tipi di policy “mirror-vault”, è necessario definire regole che determinino quali copie snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento.

Utilizzare il `snapmirror policy show` comando per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina man.

Definire una regola per una policy

Per le policy personalizzate con tipo di policy “mirror-vault”, è necessario definire almeno una regola che determini quali copie snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento. È anche possibile definire regole per policy predefinite con il tipo di policy “mirror-vault”.

Informazioni su questo compito

Ogni policy con tipo di policy “mirror-vault” deve avere una regola che specifica quali copie snapshot replicare. La regola “bi-monthly”, ad esempio, indica che devono essere replicate solo le copie snapshot a cui è stata assegnata l’etichetta SnapMirror “bi-monthly”. L’etichetta SnapMirror viene assegnata quando si configurano le copie snapshot di Element.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate automaticamente a una policy quando ne specifichi il tipo. La tabella seguente mostra le regole definite dal sistema.

Regola definita dal sistema	Utilizzato nei tipi di policy	Risultato
sm_creato	specchio asincrono, specchio-vault	Una copia snapshot creata da SnapMirror viene trasferita durante l’inizializzazione e l’aggiornamento.
quotidiano	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “daily” vengono trasferite durante l’inizializzazione e l’aggiornamento.
settimanale	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “weekly” vengono trasferite durante l’inizializzazione e l’aggiornamento.
mensile	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “mensile” vengono trasferite durante l’inizializzazione e l’aggiornamento.

È possibile specificare regole aggiuntive in base alle esigenze, per policy predefinite o personalizzate. Per esempio:

- Per impostazione predefinita `MirrorAndVault` policy, potresti creare una regola denominata “bi-monthly” per abbinare le copie snapshot sulla sorgente con l’etichetta SnapMirror “bi-monthly”.
- Per una policy personalizzata con il tipo di policy “mirror-vault”, è possibile creare una regola denominata “bi-weekly” per abbinare le copie snapshot sull’origine con l’etichetta SnapMirror “bi-weekly”.

Fare un passo

1. Definisci una regola per una policy:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   L’esempio seguente aggiunge una regola con l’etichetta SnapMirror `bi-monthly` al valore predefinito `MirrorAndVault` politica:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   L’esempio seguente aggiunge una regola con l’etichetta SnapMirror `bi-weekly` all’usanza `my_snapvault` politica:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   L’esempio seguente aggiunge una regola con l’etichetta SnapMirror `app_consistent` all’usanza `Sync` politica:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   È quindi possibile replicare copie snapshot dal cluster di origine che corrispondono a questa etichetta SnapMirror :

   ```
   cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
   snapshot1 -snapmirror-label app_consistent
   ```

Creare una relazione di replicazione

Crea una relazione da una sorgente Element a una destinazione ONTAP

La relazione tra il volume di origine nell’archiviazione primaria e il volume di destinazione

nell'archiviazione secondaria è chiamata *relazione di protezione dei dati*. Puoi usare il `snapmirror create` comando per creare una relazione di protezione dei dati da una sorgente Element a una destinazione ONTAP , o da una sorgente ONTAP a una destinazione Element.

È possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element su un sistema di destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .
- Se si utilizza il tipo di criterio "mirror-vault", è necessario che sia stata configurata un'etichetta SnapMirror per le copie snapshot dell'elemento da replicare.

> Puoi eseguire questa attività solo in"Interfaccia utente web del software Element" o utilizzando il"Metodi API" .

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

Un volume Element è più o meno equivalente a un LUN ONTAP . SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP . SnapMirror replica i dati su una LUN esistente se la LUN soddisfa i requisiti per la replica dal software Element a ONTAP.

Le regole di replicazione sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume Element.
- Non è possibile replicare i dati da un volume ONTAP a più volumi Element.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie snapshot.

Fare un passo

1. Dal cluster di destinazione, creare una relazione di replica da un'origine Element a una destinazione ONTAP :

   ```
   snapmirror create -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy
   <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente crea una relazione SnapMirror DR utilizzando l'impostazione predefinita `MirrorLatest` politica:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

L'esempio seguente crea una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` politica:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

L'esempio seguente crea una relazione di replica unificata utilizzando `Unified7year` politica:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

L'esempio seguente crea una relazione di replica unificata utilizzando il metodo personalizzato `my_unified` politica:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Creare una relazione da una sorgente ONTAP a una destinazione Element

A partire da ONTAP 9.4, è possibile utilizzare SnapMirror per replicare copie snapshot di una LUN creata su una sorgente ONTAP su una destinazione Element. Potresti utilizzare la LUN per migrare i dati da ONTAP al software Element.

Prima di iniziare

- Il nodo di destinazione dell'elemento deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .

Informazioni su questo compito

È necessario specificare il percorso di destinazione dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

Le regole di replicazione sono le seguenti:

- La relazione di replicazione deve avere una policy di tipo “async-mirror”.

  È possibile utilizzare una policy predefinita o personalizzata.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Fare un passo

1. Creare una relazione di replica da una sorgente ONTAP a una destinazione Element:

   ```
   snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
   <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L’esempio seguente crea una relazione SnapMirror DR utilizzando l’impostazione predefinita `MirrorLatest` politica:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   L’esempio seguente crea una relazione SnapMirror DR utilizzando il valore personalizzato `my_mirror` politica:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Inizializzare una relazione di replicazione

Per tutti i tipi di relazione, l’inizializzazione esegue un *trasferimento di base*: crea una copia snapshot del volume di origine, quindi trasferisce tale copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .
- Se si utilizza il tipo di criterio “mirror-vault”, è necessario che sia stata configurata un’etichetta SnapMirror per le copie snapshot dell’elemento da replicare.

Puoi eseguire questa attività solo in"Interfaccia utente web del software Element" o utilizzando il"Metodi API" .

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e *`name`* è il nome del volume Element.

L'inizializzazione può richiedere molto tempo. Potrebbe essere opportuno effettuare il trasferimento di base nelle ore non di punta.

Se per qualsiasi motivo l'inizializzazione di una relazione da una sorgente ONTAP a una destinazione Element non riesce, continuerà a non riuscire anche dopo aver corretto il problema (ad esempio, un nome LUN non valido). La soluzione alternativa è la seguente:

1. Elimina la relazione.
2. Eliminare il volume di destinazione dell'elemento.
3. Crea un nuovo volume di destinazione Element.
4. Crea e inizializza una nuova relazione dall'origine ONTAP al volume di destinazione Element.

Fare un passo

1. Inizializzare una relazione di replicazione:

   `snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path <SVM:volume|cluster://SVM/volume>`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente inizializza la relazione tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` SU `svm_backup` :

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Fornire dati da un volume di destinazione SnapMirror DR

Rendere scrivibile il volume di destinazione

Quando un disastro disabilita il sito primario per una relazione SnapMirror DR, è possibile fornire dati dal volume di destinazione con un'interruzione minima. È possibile riattivare il volume di origine quando il servizio viene ripristinato nel sito primario.

È necessario rendere scrivibile il volume di destinazione prima di poter fornire dati dal volume ai client. Puoi usare il `snapmirror quiesce` comando per interrompere i trasferimenti programmati verso la destinazione, il `snapmirror abort` comando per interrompere i trasferimenti in corso e il `snapmirror break` comando per rendere scrivibile la destinazione.

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

Passi

1. Interrompere i trasferimenti programmati verso la destinazione:

   ```
   snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente interrompe i trasferimenti pianificati tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` SU `svm_backup` :

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Interrompere i trasferimenti in corso verso la destinazione:

   ```
   snapmirror abort -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente interrompe i trasferimenti in corso tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` SU `svm_backup` :

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Interrompere la relazione SnapMirror DR:

   ```
   snapmirror break -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente interrompe la relazione tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` SU `svm_backup` e il volume di destinazione `volA_dst` SU `svm_backup` :

   ```
   cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Configurare il volume di destinazione per l'accesso ai dati

Dopo aver reso scrivibile il volume di destinazione, è necessario configurarlo per

l'accesso ai dati. Gli host SAN possono accedere ai dati dal volume di destinazione finché il volume di origine non viene riattivato.

1. Mappare l'Element LUN sul gruppo di iniziatori appropriato.
2. Creare sessioni iSCSI dagli iniziatori host SAN ai LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dell'archiviazione per rilevare la LUN connessa.

Riattivare il volume sorgente originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

Informazioni su questo compito

La procedura seguente presuppone che la linea di base nel volume sorgente originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

A partire da ONTAP 9.4, le copie snapshot di una LUN create durante la distribuzione dei dati dalla destinazione ONTAP vengono replicate automaticamente quando l'origine dell'elemento viene riattivata.

Le regole di replicazione sono le seguenti:

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Passi

1. Elimina la relazione di protezione dei dati originale:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente elimina la relazione tra il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, `volA_dst` SU `svm_backup` :

   ```
   cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```

2. Invertire la relazione originale di protezione dei dati:

   ```
   snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <hostip:>/lun/<name> -policy <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

Sebbene la risincronizzazione non richieda un trasferimento della linea di base, può richiedere molto tempo. Potresti voler eseguire la risincronizzazione nelle ore non di punta.

L'esempio seguente inverte la relazione tra il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, `volA_dst` SU `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Aggiorna la relazione invertita:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

> Il comando fallisce se non esiste una copia snapshot comune sull'origine e sulla destinazione. Utilizzo `snapmirror initialize` per reinizializzare la relazione.

L'esempio seguente aggiorna la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst` SU `svm_backup` e il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Interrompere i trasferimenti programmati per la relazione invertita:

```
snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti pianificati tra il volume da cui si stanno fornendo i dati, `volA_dst` SU `svm_backup` e il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Interrompere i trasferimenti in corso per la relazione invertita:

```
snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination
-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti in corso tra il volume da cui si stanno fornendo i dati, `volA_dst` SU `svm_backup` e il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Interrompi la relazione inversa:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination -path <hostip:>/lun/<name>`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente interrompe la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst` SU `svm_backup` e il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Eliminare la relazione di protezione dei dati invertita:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume> -destination-path <hostip:>/lun/<name> -policy <policy>`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente elimina la relazione invertita tra il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, `volA_dst` SU `svm_backup` :

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Ripristinare il rapporto originale di protezione dei dati:

   `snapmirror resync -source-path <hostip:>/lun/<name> -destination-path <SVM:volume>|<cluster://SVM/volume>`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente ristabilisce la relazione tra il volume sorgente originale, `0005` all'indirizzo IP 10.0.0.11 e il volume di destinazione originale, `volA_dst` SU `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Aggiornare manualmente una relazione di replicazione

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa di un errore di rete.

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

Passi

1. Aggiornare manualmente una relazione di replicazione:

   ```
   snapmirror update -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Il comando fallisce se non esiste una copia snapshot comune sull'origine e sulla destinazione. Utilizzo `snapmirror initialize` per reinizializzare la relazione.

   L'esempio seguente aggiorna la relazione tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` SU `svm_backup` :

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Risincronizzare una relazione di replicazione

È necessario risincronizzare una relazione di replica dopo aver reso scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione oppure se si desidera modificare i criteri di replica per la relazione.

Informazioni su questo compito

Sebbene la risincronizzazione non richieda un trasferimento della linea di base, può richiedere molto tempo. Potresti voler eseguire la risincronizzazione nelle ore non di punta.

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e `name` è il nome del volume Element.

Fare un passo

1. Risincronizzare i volumi di origine e di destinazione:

   ```
   snapmirror resync -source-path <hostip:>/lun/<name> -destination-path
   <SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente risincronizza la relazione tra il volume di origine `0005` all'indirizzo IP 10.0.0.11 e al

volume di destinazione `volA_dst` SU `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

Eseguire il backup e il ripristino dei volumi

Eseguire il backup e il ripristino dei volumi

È possibile eseguire il backup e il ripristino dei volumi su altri storage SolidFire , nonché su archivi di oggetti secondari compatibili con Amazon S3 o OpenStack Swift.

Quando si ripristinano volumi da OpenStack Swift o Amazon S3, sono necessarie le informazioni manifest del processo di backup originale. Se si ripristina un volume di cui è stato eseguito il backup su un sistema di archiviazione SolidFire , non sono necessarie informazioni sul manifesto.

Trova maggiori informazioni

- Eseguire il backup di un volume in un archivio oggetti Amazon S3
- Eseguire il backup di un volume in un archivio oggetti OpenStack Swift
- Eseguire il backup di un volume su un cluster di archiviazione SolidFire
- Ripristina un volume dal backup su un archivio oggetti Amazon S3
- Ripristina un volume dal backup su un archivio oggetti OpenStack Swift
- Ripristinare un volume dal backup su un cluster di archiviazione SolidFire

Eseguire il backup di un volume in un archivio oggetti Amazon S3

È possibile eseguire il backup dei volumi su archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona Azioni per il volume di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **S3**.
5. Selezionare un'opzione in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
7. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
8. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
9. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
10. Inserisci un'etichetta da aggiungere al prefisso nel campo **Etichetta**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di un volume in un archivio oggetti OpenStack Swift

È possibile eseguire il backup dei volumi su archivi di oggetti esterni compatibili con OpenStack Swift.

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona Azioni relativa al volume di cui eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **Swift**.
5. Selezionare un formato dati in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un URL da utilizzare per accedere all'archivio oggetti nel campo **URL**.
7. Inserisci un nome utente per l'account nel campo **Nome utente**.
8. Inserisci la chiave di autenticazione per l'account nel campo **Chiave di autenticazione**.
9. Immettere il contenitore in cui archiviare il backup nel campo **Contenitore**.
10. **Facoltativo**: inserisci un'etichetta con il nome da aggiungere al prefisso nel campo **Etichetta con il nome**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di un volume su un cluster di archiviazione SolidFire

È possibile eseguire il backup dei volumi residenti in un cluster su un cluster remoto per i cluster di archiviazione che eseguono il software Element.

Assicurarsi che i cluster di origine e di destinazione siano accoppiati.

Vedere"Cluster di coppie per la replicazione" .

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, **Gestione** > **Volumi**.
2. Fare clic sull'icona Azioni per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **Ripristina da**.
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare * SolidFire*.
5. Selezionare un'opzione in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copia la chiave dalla casella **Chiave di scrittura volume in blocco** negli appunti.
8. Nel cluster di origine, vai a **Gestione** > **Volumi**.

9. Fare clic sull'icona Azioni relativa al volume di cui eseguire il backup.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare * SolidFire*.
12. Seleziona la stessa opzione selezionata in precedenza nel campo **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.
14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Nel campo **Chiave di scrittura volume di massa**, incollare la chiave generata in precedenza sul cluster di destinazione.
17. Fare clic su **Inizia a leggere**.

Ripristina un volume dal backup su un archivio oggetti Amazon S3

È possibile ripristinare un volume da un backup su un archivio oggetti Amazon S3.

1. Fare clic su **Segnalazione** > **Registro eventi**.
2. Individua l'evento di backup che ha creato il backup che devi ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copia le informazioni del manifesto negli appunti.
5. Fare clic su **Gestione** > **Volumi**.
6. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Ripristina da**.
8. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **S3**.
9. Selezionare l'opzione corrispondente al backup in **Formato dati**:
   - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
   - **Non compresso**: formato non compresso compatibile con altri sistemi.
10. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
11. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
12. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
13. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
14. Incolla le informazioni del manifesto nel campo **Manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristina un volume dal backup su un archivio oggetti OpenStack Swift

È possibile ripristinare un volume da un backup su un archivio oggetti OpenStack Swift.

1. Fare clic su **Segnalazione** > **Registro eventi**.
2. Individua l'evento di backup che ha creato il backup che devi ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.

4. Copia le informazioni del manifesto negli appunti.
5. Fare clic su **Gestione** > **Volumi**.
6. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Ripristina da**.
8. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **Swift**.
9. Selezionare l'opzione corrispondente al backup in **Formato dati**:
    - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
    - **Non compresso**: formato non compresso compatibile con altri sistemi.
10. Immettere un URL da utilizzare per accedere all'archivio oggetti nel campo **URL**.
11. Inserisci un nome utente per l'account nel campo **Nome utente**.
12. Inserisci la chiave di autenticazione per l'account nel campo **Chiave di autenticazione**.
13. Immettere il nome del contenitore in cui è archiviato il backup nel campo **Contenitore**.
14. Incolla le informazioni del manifesto nel campo **Manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup su un cluster di archiviazione SolidFire

È possibile ripristinare un volume da un backup su un cluster di archiviazione SolidFire .

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
3. Nel menu visualizzato, fare clic su **Ripristina da**.
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare * SolidFire*.
5. Selezionare l'opzione corrispondente al backup in **Formato dati**:
    - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
    - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copiare le informazioni **Bulk Volume Write Key** negli appunti.
8. Nel cluster di origine, fare clic su **Gestione** > **Volumi**.
9. Fare clic sull'icona Azioni per il volume che si desidera utilizzare per il ripristino.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, selezionare * SolidFire* in **Backup su**.
12. Selezionare l'opzione corrispondente al backup in **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.

14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Incolla la chiave dagli appunti nel campo **Chiave di scrittura volume in blocco**.
17. Fare clic su **Inizia a leggere**.

Configurare domini di protezione personalizzati

Per i cluster Element che contengono più di due nodi di archiviazione, è possibile configurare domini di protezione personalizzati per ciascun nodo. Quando si configurano domini di protezione personalizzati, è necessario assegnare tutti i nodi del cluster a un dominio.

Quando si assegnano domini di protezione, inizia una sincronizzazione dei dati tra i nodi e alcune operazioni del cluster non sono disponibili finché la sincronizzazione dei dati non viene completata. Dopo aver configurato un dominio di protezione personalizzato per un cluster, quando si aggiunge un nuovo nodo di archiviazione, non è possibile aggiungere unità per il nuovo nodo finché non si assegna un dominio di protezione per il nodo e non si consente il completamento della sincronizzazione dei dati. Visita il"Documentazione sui domini di protezione" per saperne di più sui domini di protezione.

Affinché uno schema di dominio di protezione personalizzato sia utile per un cluster, tutti i nodi di archiviazione all'interno di ogni chassis devono essere assegnati allo stesso dominio di protezione personalizzato. Per ottenere questo risultato, è necessario creare tutti i domini di protezione personalizzati necessari (lo schema di dominio di protezione personalizzato più piccolo possibile è di tre domini). Come buona pratica, configura un numero uguale di nodi per dominio e prova a garantire che ogni nodo assegnato a un dominio specifico sia dello stesso tipo.

Passi

1. Fare clic su **Cluster** > **Nodi**.
2. Fare clic su **Configura domini di protezione**.

   Nella finestra **Configura domini di protezione personalizzati**, è possibile visualizzare i domini di protezione attualmente configurati (se presenti), nonché le assegnazioni dei domini di protezione per i singoli nodi.

3. Inserisci un nome per il nuovo dominio di protezione personalizzato e fai clic su **Crea**.

   Ripetere questo passaggio per tutti i nuovi domini di protezione che si desidera creare.

4. Per ogni nodo nell'elenco **Assegna nodi**, fare clic sul menu a discesa nella colonna **Dominio di protezione** e selezionare un dominio di protezione da assegnare a quel nodo.

   Prima di applicare le modifiche, assicurati di comprendere il layout del nodo e dello chassis, lo schema del dominio di protezione personalizzato configurato e gli effetti dello schema sulla protezione dei dati. Se si applica uno schema di dominio di protezione e si hanno immediatamente necessità di apportare modifiche, potrebbe volerci del tempo prima che sia possibile farlo a causa della sincronizzazione dei dati che avviene una volta applicata una configurazione.

5. Fare clic su **Configura domini di protezione**.

Risultato

A seconda delle dimensioni del cluster, la sincronizzazione dei dati tra i domini potrebbe richiedere del tempo. Una volta completata la sincronizzazione dei dati, è possibile visualizzare le assegnazioni personalizzate del dominio di protezione nella pagina **Cluster** > **Nodi** e la dashboard dell'interfaccia utente Web di Element mostra lo stato di protezione del cluster nel riquadro **Stato del dominio di protezione personalizzato**.

Possibili errori

Ecco alcuni errori che potresti visualizzare dopo aver applicato una configurazione personalizzata del dominio di protezione:

Errore	Descrizione	Risoluzione
Errore di SetProtectionDomainLayout: ProtectionDomainLayout renderebbe inutilizzabile NodeID {9}. Non è possibile utilizzare contemporaneamente nomi predefiniti e non predefiniti.	A un nodo non è assegnato alcun dominio di protezione.	Assegnare un dominio di protezione al nodo.
Errore SetProtectionDomainLayout: il tipo di dominio di protezione 'personalizzato' divide il tipo di dominio di protezione 'chassis'.	A un nodo in uno chassis multi-nodo viene assegnato un dominio di protezione diverso dagli altri nodi nello chassis.	Assicurarsi che a tutti i nodi nello chassis sia assegnato lo stesso dominio di protezione.

Trova maggiori informazioni

- "Domini di protezione personalizzati"
- "Gestisci l'archiviazione con l'API Element"

Risolvi i problemi del tuo sistema

Eventi di sistema

Visualizza informazioni sugli eventi di sistema

È possibile visualizzare informazioni sui vari eventi rilevati nel sistema. Il sistema aggiorna i messaggi degli eventi ogni 30 secondi. Il registro eventi visualizza gli eventi chiave del cluster.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting** > **Registro eventi**.

   Per ogni evento vengono visualizzate le seguenti informazioni:

Articolo	Descrizione
ID	ID univoco associato a ciascun evento.

Tipo di evento	Il tipo di evento registrato, ad esempio eventi API o eventi clone.
Messaggio	Messaggio associato all'evento.
Dettagli	Informazioni che aiutano a identificare il motivo per cui si è verificato l'evento.
ID del servizio	Il servizio che ha segnalato l'evento (se applicabile).
Nodo	Il nodo che ha segnalato l'evento (se applicabile).
ID unità	L'unità che ha segnalato l'evento (se applicabile).
Ora dell'evento	L'ora in cui si è verificato l'evento.

Trova maggiori informazioni

Tipi di eventi

Tipi di eventi

Il sistema segnala diversi tipi di eventi; ogni evento è un'operazione completata dal sistema. Gli eventi possono essere di routine, eventi normali o eventi che richiedono l'attenzione dell'amministratore. La colonna Tipi di evento nella pagina Registro eventi indica in quale parte del sistema si è verificato l'evento.

Il sistema non registra i comandi API di sola lettura nel registro eventi.

L'elenco seguente descrive i tipi di eventi che compaiono nel registro eventi:

- **apiEvent**

  Eventi avviati da un utente tramite un'API o un'interfaccia utente Web che modificano le impostazioni.

- **binAssegnazioniEvento**

  Eventi correlati all'assegnazione dei contenitori di dati. I contenitori sono essenzialmente contenitori che contengono dati e sono mappati nel cluster.

- **binSyncEvent**

  Eventi di sistema correlati a una riassegnazione di dati tra servizi a blocchi.

- **bsCheckEvent**

  Eventi di sistema correlati ai controlli del servizio di blocco.

- **bsKillEvent**

Eventi di sistema correlati alla cessazione del servizio di blocco.

- **bulkOpEvent**

  Eventi correlati alle operazioni eseguite su un intero volume, come un backup, un ripristino, uno snapshot o una clonazione.

- **cloneEvent**

  Eventi correlati alla clonazione del volume.

- **clusterMasterEvent**

  Eventi che si verificano durante l'inizializzazione del cluster o in seguito a modifiche della configurazione del cluster, come l'aggiunta o la rimozione di nodi.

- **cSumEvent**

  Eventi correlati al rilevamento di una mancata corrispondenza del checksum durante la convalida del checksum end-to-end.

  I servizi che rilevano una mancata corrispondenza del checksum vengono automaticamente arrestati e non riavviati dopo aver generato questo evento.

- **dataEvent**

  Eventi correlati alla lettura e alla scrittura dei dati.

- **dbEvent**

  Eventi correlati al database globale gestito dai nodi ensemble nel cluster.

- **driveEvent**

  Eventi correlati alle operazioni di azionamento.

- **encryptionAtRestEvent**

  Eventi correlati al processo di crittografia su un cluster.

- **eventoensemble**

  Eventi correlati all'aumento o alla diminuzione del numero di nodi in un ensemble.

- **fibreChannelEvent**

  Eventi relativi alla configurazione e alle connessioni ai nodi.

- **gcEvent**

  Gli eventi correlati ai processi vengono eseguiti ogni 60 minuti per recuperare spazio di archiviazione sulle unità a blocchi. Questo processo è noto anche come garbage collection.

- **ieEvent**

  Errore interno del sistema.

- **installEvent**

  Eventi di installazione automatica del software. Il software viene installato automaticamente su un nodo in sospeso.

- **iSCSIEvent**

  Eventi correlati a problemi iSCSI nel sistema.

- **limitEvent**

  Eventi correlati al numero di volumi o volumi virtuali in un account o nel cluster che si avvicinano al massimo consentito.

- **maintenanceModeEvent**

  Eventi correlati alla modalità di manutenzione del nodo, come la disabilitazione del nodo.

- **evento_di_rete**

  Eventi correlati alla segnalazione degli errori di rete per ciascuna interfaccia fisica della scheda di interfaccia di rete (NIC).

  Questi eventi vengono attivati quando un conteggio di errori per un'interfaccia supera la soglia predefinita di 1000 durante un intervallo di monitoraggio di 10 minuti. Questi eventi si applicano agli errori di rete quali mancate risposte ricevute, errori di controllo di ridondanza ciclico (CRC), errori di lunghezza, errori di overrun ed errori di frame.

- **piattaformaHardwareEvent**

  Eventi correlati a problemi rilevati sui dispositivi hardware.

- **eventoClusterremoto**

  Eventi correlati all'associazione di cluster remoti.

- **schedulerEvent**

  Eventi correlati agli snapshot pianificati.

- **servizioEvento**

  Eventi relativi allo stato del servizio di sistema.

- **sliceEvent**

  Eventi correlati a Slice Server, come la rimozione di un'unità o di un volume di metadati.

  Esistono tre tipi di eventi di riassegnazione delle sezioni, che includono informazioni sul servizio a cui è assegnato un volume:

  - flipping: cambiare il servizio primario in un nuovo servizio primario

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

◦ spostamento: modifica del servizio secondario in un nuovo servizio secondario

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

◦ potatura: rimozione di un volume da un insieme di servizi

```
sliceID {oldSecondaryServiceID(s)}
```

- **snmpTrapEvent**

  Eventi correlati alle trappole SNMP.

- **statEvent**

  Eventi relativi alle statistiche di sistema.

- **tsEvento**

  Eventi relativi al servizio di trasporto del sistema.

- **eccezione inaspettata**

  Eventi correlati a eccezioni di sistema impreviste.

- **ureEvent**

  Eventi correlati a errori di lettura irrecuperabili che si verificano durante la lettura dal dispositivo di archiviazione.

- **vasaProviderEvent**

  Eventi correlati a un provider VASA (vSphere APIs for Storage Awareness).

Visualizza lo stato delle attività in esecuzione

È possibile visualizzare nell'interfaccia utente Web lo stato di avanzamento e di completamento delle attività in esecuzione segnalate dai metodi API ListSyncJobs e ListBulkVolumeJobs. È possibile accedere alla pagina Attività in esecuzione dalla scheda Report dell'interfaccia utente dell'elemento.

Se il numero di attività è elevato, il sistema potrebbe metterle in coda ed eseguirle in batch. Nella pagina Attività in esecuzione vengono visualizzati i servizi attualmente sincronizzati. Una volta completata, un'attività viene sostituita dalla successiva attività di sincronizzazione in coda. Le attività di sincronizzazione potrebbero continuare ad apparire nella pagina Attività in esecuzione finché non ci saranno più attività da completare.

È possibile visualizzare i dati di sincronizzazione della replica per i volumi sottoposti a replica nella pagina Attività in esecuzione del cluster contenente il volume di destinazione.

Avvisi di sistema

Visualizza gli avvisi di sistema

È possibile visualizzare avvisi per informazioni su guasti o errori del cluster nel sistema. Gli avvisi possono essere informazioni, avvertenze o errori e sono un buon indicatore del funzionamento del cluster. La maggior parte degli errori si risolve automaticamente.

È possibile utilizzare il metodo API ListClusterFaults per automatizzare il monitoraggio degli avvisi. Ciò ti consente di essere informato su tutti gli avvisi che si verificano.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting** > **Avvisi**.

   Il sistema aggiorna gli avvisi sulla pagina ogni 30 secondi.

   Per ogni evento vengono visualizzate le seguenti informazioni:

Articolo	Descrizione
ID	ID univoco associato a un avviso cluster.
Gravità	Il grado di importanza dell'allerta. Valori possibili: • Attenzione: un problema minore che potrebbe presto richiedere attenzione. Gli aggiornamenti del sistema sono ancora consentiti. • errore: un errore che potrebbe causare un degrado delle prestazioni o la perdita di alta disponibilità (HA). In genere, gli errori non dovrebbero compromettere il servizio. • critico: un guasto grave che influisce sul servizio. Il sistema non è in grado di soddisfare le richieste API o I/O del client. Operare in questo stato potrebbe comportare una potenziale perdita di dati. • bestPractice: non viene utilizzata una delle best practice consigliate per la configurazione del sistema.
Tipo	Il componente interessato dal guasto. Può essere un nodo, un'unità, un cluster, un servizio o un volume.
Nodo	ID del nodo a cui si riferisce questo errore. Incluso per errori di nodo e unità, altrimenti impostato su - (trattino).
ID unità	ID dell'unità a cui si riferisce questo errore. Incluso per guasti dell'unità, altrimenti impostato su - (trattino).

Codice di errore	Un codice descrittivo che indica la causa del guasto.
Dettagli	Una descrizione del guasto con dettagli aggiuntivi.
Data	Data e ora in cui è stato registrato l'errore.

2. Fare clic su **Mostra dettagli** per visualizzare le informazioni relative a un singolo avviso.
3. Per visualizzare i dettagli di tutti gli avvisi nella pagina, fare clic sulla colonna Dettagli.

   Dopo che il sistema ha risolto un avviso, tutte le informazioni sull'avviso, inclusa la data in cui è stato risolto, vengono spostate nell'area Risolti.

Trova maggiori informazioni

- Codici di errore del cluster
- "Gestisci l'archiviazione con l'API Element"

Codici di errore del cluster

Il sistema segnala un errore o uno stato che potrebbe essere di interesse generando un codice di errore, che viene elencato nella pagina Avvisi. Questi codici aiutano a determinare quale componente del sistema ha ricevuto l'avviso e perché è stato generato.

L'elenco seguente descrive i diversi tipi di codici:

- **errore di servizio di autenticazione**

  Il servizio di autenticazione su uno o più nodi del cluster non funziona come previsto.

  Per ricevere assistenza, contattare il supporto NetApp .

- **disponibileIndirizzi IP di rete virtualeBasso**

  Il numero di indirizzi di rete virtuali nel blocco di indirizzi IP è basso.

  Per risolvere questo errore, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuali.

- **blockClusterFull**

  Non c'è abbastanza spazio di archiviazione a blocchi libero per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di riempimento del cluster, vedere il metodo API GetClusterFullThreshold. Questo errore del cluster indica una delle seguenti condizioni:

  - stage3Low (Avviso): è stata superata la soglia definita dall'utente. Regola le impostazioni del Cluster completo o aggiungi altri nodi.
  - stage4Critical (Errore): non c'è abbastanza spazio per il ripristino da un errore di 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
  - stage5CompletelyConsumed (Critical)1; Non sono consentite scritture o nuove connessioni iSCSI. Le

attuali connessioni iSCSI saranno mantenute. Le scritture non riusciranno finché non verrà aggiunta ulteriore capacità al cluster.

Per risolvere questo errore, eliminare o ripulire i volumi oppure aggiungere un altro nodo di archiviazione al cluster di archiviazione.

- **blocchiDegradato**

  I dati del blocco non vengono più replicati completamente a causa di un errore.

Gravità	Descrizione
Avvertimento	Sono accessibili solo due copie complete dei dati del blocco.
Errore	È accessibile solo una singola copia completa dei dati del blocco.
Critico	Non sono accessibili copie complete dei dati del blocco.

  Nota: lo stato di avviso può verificarsi solo su un sistema Triple Helix.

  Per risolvere questo errore, ripristinare tutti i nodi offline o bloccare i servizi oppure contattare il supporto NetApp per ricevere assistenza.

- **blockServiceTooFull**

  Un servizio di blocco sta utilizzando troppo spazio.

  Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **blockServiceNon integro**

  È stato rilevato un servizio di blocco non funzionante:

  - Gravità = Avvertenza: non viene intrapresa alcuna azione. Questo periodo di avviso scadrà tra cTimeUntilBSIsKilledMSec=330000 millisecondi.
  - Gravità = Errore: il sistema sta automaticamente dismettendo i dati e replicandoli nuovamente su altre unità funzionanti.
  - Gravità = Critica: sono presenti servizi di blocco non riusciti su diversi nodi, superiori o uguali al conteggio delle repliche (2 per la doppia elica). I dati non sono disponibili e la sincronizzazione del cestino non verrà completata.

    Verificare la presenza di problemi di connettività di rete ed errori hardware. Si verificheranno altri guasti se specifici componenti hardware non funzionano. L'errore verrà risolto quando il servizio di blocco sarà accessibile o quando il servizio sarà stato dismesso.

- **BmcSelfTestFailed**

  Il Baseboard Management Controller (BMC) non ha superato l'autotest.

  Per ricevere assistenza, contattare l'assistenza NetApp .

Durante un aggiornamento a Element 12.5 o versione successiva, il `BmcSelfTestFailed` l'errore non viene generato per un nodo che ha un BMC preesistente non riuscito o quando il BMC di un nodo non funziona durante l'aggiornamento. I BMC che non superano gli autotest durante l'aggiornamento emetteranno un `BmcSelfTestFailed` avviso di errore dopo che l'intero cluster ha completato l'aggiornamento.

- **clockSkewExceedsFaultThreshold**

  Lo sfasamento temporale tra il master del cluster e il nodo che presenta un token supera la soglia consigliata. Il cluster di archiviazione non è in grado di correggere automaticamente lo sfasamento temporale tra i nodi.

  Per risolvere questo errore, utilizzare i server NTP interni alla rete anziché quelli predefiniti di installazione. Se si utilizza un server NTP interno, contattare il supporto NetApp per ricevere assistenza.

- **clusterNonPuòSincronizzarsi**

  Si è verificata una condizione di spazio insufficiente e i dati sulle unità di archiviazione a blocchi offline non possono essere sincronizzati con le unità ancora attive.

  Per risolvere questo problema, aggiungere altro spazio di archiviazione.

- **clusterFull**

  Non c'è più spazio di archiviazione libero nel cluster di archiviazione.

  Per risolvere questo problema, aggiungere altro spazio di archiviazione.

- **clusterIOPSAreOverProvisioned**

  Gli IOPS del cluster sono sovradimensionati. La somma di tutti gli IOPS QoS minimi è maggiore degli IOPS previsti del cluster. Non è possibile mantenere la QoS minima per tutti i volumi contemporaneamente.

  Per risolvere questo problema, ridurre le impostazioni minime QoS IOPS per i volumi.

- **SogliaEventoTermicoCpu**

  Il numero di eventi termici della CPU su una o più CPU supera la soglia configurata.

  Se non vengono rilevati nuovi eventi termici della CPU entro dieci minuti, l'avviso si risolverà automaticamente.

- **disableDriveSecurityFailed**

  Il cluster non è configurato per abilitare la sicurezza dell'unità (crittografia a riposo), ma almeno un'unità ha la sicurezza abilitata, il che significa che la disabilitazione della sicurezza dell'unità su tali unità non è riuscita. Questo errore viene registrato con gravità "Warning".

  Per risolvere questo errore, controllare i dettagli dell'errore per scoprire il motivo per cui non è stato possibile disattivare la sicurezza dell'unità. Le possibili ragioni sono:

  - Non è stato possibile acquisire la chiave di crittografia. Verificare il problema con l'accesso alla chiave o al server delle chiavi esterno.
  - L'operazione di disattivazione sull'unità non è riuscita. Verificare se è possibile che sia stata acquisita la chiave sbagliata.

Se nessuna di queste cause è la causa del guasto, potrebbe essere necessario sostituire l'unità.

È possibile tentare di ripristinare un'unità che non disattiva correttamente la sicurezza anche quando viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere l'unità/le unità dal sistema spostandola su Disponibile, eseguire una cancellazione sicura sull'unità e spostarla nuovamente su Attiva.

- **ClusterPair disconnesso**

  Una coppia di cluster è disconnessa o configurata in modo errato.

  Controllare la connettività di rete tra i cluster.

- **nodoremoto disconnesso**

  Un nodo remoto è disconnesso o configurato in modo errato.

  Controllare la connettività di rete tra i nodi.

- **disconnectedSnapMirrorEndpoint**

  Un endpoint remoto SnapMirror è disconnesso o configurato in modo errato.

  Verificare la connettività di rete tra il cluster e lo SnapMirrorEndpoint remoto.

- **unità disponibile**

  Nel cluster sono disponibili una o più unità. In generale, tutti i cluster dovrebbero avere tutte le unità aggiunte e nessuna nello stato disponibile. Se questo errore si verifica inaspettatamente, contattare l'assistenza NetApp .

  Per risolvere questo errore, aggiungere tutte le unità disponibili al cluster di archiviazione.

- **driveFailed**

  Il cluster restituisce questo errore quando una o più unità si guastano, indicando una delle seguenti condizioni:

  - Il gestore dell'unità non riesce ad accedere all'unità.
  - Il servizio slice o block ha avuto esito negativo troppe volte, presumibilmente a causa di errori di lettura o scrittura dell'unità, e non può essere riavviato.
  - L'unità è mancante.
  - Il servizio master per il nodo non è accessibile (tutte le unità nel nodo sono considerate mancanti/guaste).
  - L'unità è bloccata e non è possibile acquisire la chiave di autenticazione per l'unità.
  - L'unità è bloccata e l'operazione di sblocco non riesce.

    Per risolvere questo problema:

  - Controllare la connettività di rete per il nodo.
  - Sostituire l'unità.
  - Assicurarsi che la chiave di autenticazione sia disponibile.

- **driveHealthFault**

  Un'unità non ha superato il controllo di integrità SMART e, di conseguenza, le sue funzionalità risultano ridotte. Per questo errore esiste un livello di gravità critico:

  - L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> non ha superato il controllo di integrità generale SMART.

  Per risolvere questo errore, sostituire l'unità.

- **driveWearFault**

  La durata residua di un'unità è scesa al di sotto delle soglie, ma l'unità continua a funzionare. Esistono due possibili livelli di gravità per questo errore: Critico e Avvertenza:

  - L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> presenta livelli di usura critici.
  - L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> ha basse riserve di usura.

    Per risolvere questo problema, sostituire l'unità al più presto.

- **duplicateClusterMasterCandidates**

  È stato rilevato più di un candidato master del cluster di archiviazione.

  Per ricevere assistenza, contattare il supporto NetApp .

- **enableDriveSecurityFailed**

  Il cluster è configurato per richiedere la sicurezza dell'unità (crittografia a riposo), ma la sicurezza dell'unità non può essere abilitata su almeno un'unità. Questo errore viene registrato con gravità "Warning".

  Per risolvere questo errore, controllare i dettagli dell'errore per scoprire il motivo per cui non è stato possibile abilitare la sicurezza dell'unità. Le possibili ragioni sono:

  - Non è stato possibile acquisire la chiave di crittografia. Verificare il problema con l'accesso alla chiave o al server delle chiavi esterno.
  - L'operazione di abilitazione sull'unità non è riuscita. Verificare se è possibile che sia stata acquisita la chiave sbagliata. Se nessuna di queste cause è la causa del guasto, potrebbe essere necessario sostituire l'unità.

  È possibile tentare di ripristinare un'unità che non abilita correttamente la sicurezza anche quando viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere l'unità/le unità dal sistema spostandola su Disponibile, eseguire una cancellazione sicura sull'unità e spostarla nuovamente su Attiva.

- **ensembleDegraded**

  Si è verificata un'interruzione della connettività di rete o dell'alimentazione su uno o più nodi dell'ensemble.

  Per risolvere questo errore, ripristinare la connettività di rete o l'alimentazione.

- **eccezione**

  Un guasto segnalato che non è un guasto di routine. Questi errori non vengono cancellati

automaticamente dalla coda degli errori.

Per ricevere assistenza, contattare il supporto NetApp .

- **SpazioTroppoPienofallito**

  Un servizio a blocchi non risponde alle richieste di scrittura dei dati. Ciò fa sì che il servizio slice esaurisca lo spazio per archiviare le scritture non riuscite.

  Per risolvere questo errore, ripristinare la funzionalità dei servizi a blocchi per consentire alle scritture di continuare normalmente e allo spazio non riuscito di essere svuotato dal servizio slice.

- **sensore ventola**

  Un sensore della ventola è guasto o mancante.

  Per risolvere questo errore, sostituire l'hardware guasto.

- **fibreChannelAccessDegraded**

  Un nodo Fibre Channel non risponde agli altri nodi nel cluster di storage tramite il proprio IP di storage per un certo periodo di tempo. In questo stato, il nodo verrà considerato non reattivo e genererà un errore del cluster.

  Controllare la connettività di rete.

- **fibreChannelAccessUnavailable**

  Tutti i nodi Fibre Channel non rispondono. Vengono visualizzati gli ID dei nodi.

  Controllare la connettività di rete.

- **fibreChannelActiveIxL**

  Il conteggio di IxL Nexus si sta avvicinando al limite supportato di 8000 sessioni attive per nodo Fibre Channel.

  - Il limite ottimale è 5500.
  - Il limite di attenzione è 7500.
  - Il limite massimo (non applicato) è 8192.

  Per risolvere questo errore, ridurre il conteggio IxL Nexus al di sotto del limite ottimale di 5500.

- **fibreChannelConfig**

  Questo errore del cluster indica una delle seguenti condizioni:

  - C'è una porta Fibre Channel inaspettata su uno slot PCI.
  - Esiste un modello HBA Fibre Channel inaspettato.
  - Si è verificato un problema con il firmware di un HBA Fibre Channel.
  - Una porta Fibre Channel non è online.
  - Si verifica un problema persistente durante la configurazione del passthrough Fibre Channel.

  Per ricevere assistenza, contattare il supporto NetApp .

- **fibreChannelIOPS**

  Il conteggio totale degli IOPS si sta avvicinando al limite degli IOPS per i nodi Fibre Channel nel cluster. I limiti sono:

  - FC0025: limite di 450K IOPS con dimensione del blocco di 4K per nodo Fibre Channel.
  - FCN001: limite OPS di 625K con dimensione del blocco di 4K per nodo Fibre Channel.

  Per risolvere questo errore, bilanciare il carico su tutti i nodi Fibre Channel disponibili.

- **fibreChannelStaticIxL**

  Il conteggio IxL Nexus si sta avvicinando al limite supportato di 16.000 sessioni statiche per nodo Fibre Channel.

  - Il limite ottimale è 11000.
  - Il limite di attenzione è 15000.
  - Il limite massimo (applicato) è 16384.

  Per risolvere questo errore, ridurre il conteggio IxL Nexus al di sotto del limite ottimale di 11000.

- **fileSystemCapacityLow**

  Lo spazio su uno dei file system non è sufficiente.

  Per risolvere questo errore, aggiungere più capacità al file system.

- **fileSystemIsReadOnly**

  Un file system è passato alla modalità di sola lettura.

  Per ricevere assistenza, contattare il supporto NetApp .

- **fipsDrivesMismatch**

  Un'unità non FIPS è stata fisicamente inserita in un nodo di archiviazione compatibile con FIPS oppure un'unità FIPS è stata fisicamente inserita in un nodo di archiviazione non FIPS. Viene generato un singolo errore per nodo e vengono elencate tutte le unità interessate.

  Per risolvere questo errore, rimuovere o sostituire l'unità o le unità non corrispondenti in questione.

- **fipsDrivesOutOfCompliance**

  Il sistema ha rilevato che la crittografia a riposo è stata disabilitata dopo l'abilitazione della funzionalità Unità FIPS. Questo errore viene generato anche quando la funzionalità Unità FIPS è abilitata e nel cluster di archiviazione è presente un'unità o un nodo non FIPS.

  Per risolvere questo errore, abilitare la crittografia a riposo o rimuovere l'hardware non FIPS dal cluster di archiviazione.

- **fipsSelfTestFailure**

  Il sottosistema FIPS ha rilevato un errore durante l'autotest.

  Per ricevere assistenza, contattare il supporto NetApp .

- **hardwareConfigMismatch**

  Questo errore del cluster indica una delle seguenti condizioni:

  - La configurazione non corrisponde alla definizione del nodo.
  - La dimensione dell'unità per questo tipo di nodo non è corretta.
  - È stata rilevata un'unità non supportata. Un possibile motivo è che la versione Element installata non riconosce questa unità. Si consiglia di aggiornare il software Element su questo nodo.
  - C'è una mancata corrispondenza del firmware dell'unità.
  - Lo stato di capacità di crittografia dell'unità non corrisponde al nodo.

  Per ricevere assistenza, contattare il supporto NetApp .

- **idPCertificateExpiration**

  Il certificato SSL del fornitore di servizi del cluster per l'utilizzo con un fornitore di identità (IdP) di terze parti sta per scadere o è già scaduto. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	Il certificato scade entro 30 giorni.
Errore	Il certificato scade entro 7 giorni.
Critico	Il certificato scade entro 3 giorni o è già scaduto.

  Per risolvere questo errore, aggiorna il certificato SSL prima che scada. Utilizzare il metodo API UpdateIdpConfiguration con `refreshCertificateExpirationTime=true` per fornire il certificato SSL aggiornato.

- **inconsistentBondModes**

  Mancano le modalità di legame sul dispositivo VLAN. Questo errore visualizzerà la modalità di legame prevista e la modalità di legame attualmente in uso.

- **incoerenteMtus**

  Questo errore del cluster indica una delle seguenti condizioni:

  - Mancata corrispondenza Bond1G: sono state rilevate MTU incoerenti sulle interfacce Bond1G.
  - Mancata corrispondenza Bond10G: sono stati rilevati MTU incoerenti sulle interfacce Bond10G.

  Questo errore visualizza il nodo o i nodi in questione insieme al valore MTU associato.

- **inconsistentRoutingRules**

  Le regole di routing per questa interfaccia non sono coerenti.

- **SubnetMasks incoerenti**

  La maschera di rete sul dispositivo VLAN non corrisponde alla maschera di rete registrata internamente per la VLAN. Questo errore visualizza la maschera di rete prevista e la maschera di rete attualmente in

uso.

- **incorrectBondPortCount**

  Il numero di porte di collegamento non è corretto.

- **invalidConfiguredFibreChannelNodeCount**

  Una delle due connessioni previste del nodo Fibre Channel è degradata. Questo errore si verifica quando è connesso un solo nodo Fibre Channel.

  Per risolvere questo errore, controllare la connettività di rete del cluster e il cablaggio di rete, nonché verificare la presenza di servizi non funzionanti. Se non ci sono problemi di rete o di servizio, contattare l'assistenza NetApp per la sostituzione del nodo Fibre Channel.

- **irqBalanceFailed**

  Si è verificata un'eccezione durante il tentativo di bilanciare gli interrupt.

  Per ricevere assistenza, contattare il supporto NetApp .

- **kmipCertificateFault**
  - Il certificato della Root Certification Authority (CA) sta per scadere.

    Per risolvere questo errore, acquisire un nuovo certificato dalla CA radice con data di scadenza di almeno 30 giorni e utilizzare ModifyKeyServerKmip per fornire il certificato CA radice aggiornato.

  - Il certificato client sta per scadere.

    Per risolvere questo errore, creare un nuovo CSR utilizzando GetClientCertificateSigningRequest, farlo firmare assicurandosi che la nuova data di scadenza sia di almeno 30 giorni e utilizzare ModifyKeyServerKmip per sostituire il certificato client KMIP in scadenza con il nuovo certificato.

  - Il certificato dell'autorità di certificazione radice (CA) è scaduto.

    Per risolvere questo errore, acquisire un nuovo certificato dalla CA radice con data di scadenza di almeno 30 giorni e utilizzare ModifyKeyServerKmip per fornire il certificato CA radice aggiornato.

  - Il certificato client è scaduto.

    Per risolvere questo errore, creare un nuovo CSR utilizzando GetClientCertificateSigningRequest, farlo firmare assicurandosi che la nuova data di scadenza sia di almeno 30 giorni e utilizzare ModifyKeyServerKmip per sostituire il certificato client KMIP scaduto con il nuovo certificato.

  - Errore del certificato dell'autorità di certificazione radice (CA).

    Per risolvere questo errore, verificare che sia stato fornito il certificato corretto e, se necessario, riacquisire il certificato dalla CA radice. Utilizzare ModifyKeyServerKmip per installare il certificato client KMIP corretto.

  - Errore del certificato client.

    Per risolvere questo errore, verificare che sia installato il certificato client KMIP corretto. La CA radice del certificato client deve essere installata sull'EKS. Utilizzare ModifyKeyServerKmip per installare il certificato client KMIP corretto.

- **kmipServerFault**
  - Errore di connessione

    Per risolvere questo errore, verificare che il server delle chiavi esterne sia attivo e raggiungibile tramite la rete. Utilizza TestKeyServerKimp e TestKeyProviderKmip per testare la tua connessione.

  - Errore di autenticazione

    Per risolvere questo errore, verificare che vengano utilizzati i certificati client KMIP e CA radice corretti e che la chiave privata e il certificato client KMIP corrispondano.

  - Errore del server

    Per risolvere questo errore, controlla i dettagli dell'errore. Potrebbe essere necessario risolvere il problema sul server chiavi esterno in base all'errore restituito.

- **sogliaEccMemoria**

  Sono stati rilevati numerosi errori ECC correggibili o non correggibili. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Evento	Gravità	Descrizione
Un singolo DIMM cErrorCount raggiunge cDimmCorrectableErrWarnThreshold.	Avvertimento	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <Slot DIMM>
Un singolo DIMM cErrorCount rimane al di sopra di cDimmCorrectableErrWarnThreshold finché non scade cErrorFaultTimer per il DIMM.	Errore	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <DIMM>
Un controller di memoria segnala cErrorCount al di sopra di cMemCtlrCorrectableErrWarnThreshold e viene specificato cMemCtlrCorrectableErrWarnDuration.	Avvertimento	Errori di memoria ECC correggibili oltre la soglia sul controller di memoria: <Processore> <Controller di memoria>
Un controller di memoria segnala cErrorCount al di sopra di cMemCtlrCorrectableErrWarnThreshold finché non scade cErrorFaultTimer per il controller di memoria.	Errore	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <DIMM>

Un singolo DIMM segnala un uErrorCount superiore a zero, ma inferiore a cDimmUncorrectableErrFaultThreshold.	Avvertimento	Errore/i di memoria ECC non correggibile rilevato/i su DIMM: <Processore> <Slot DIMM>
Un singolo DIMM segnala un uErrorCount di almeno cDimmUncorrectableErrFaultThreshold.	Errore	Errore/i di memoria ECC non correggibile rilevato/i su DIMM: <Processore> <Slot DIMM>
Un controller di memoria segnala un uErrorCount superiore a zero, ma inferiore a cMemCtlrUncorrectableErrFaultThreshold.	Avvertimento	Errore/i di memoria ECC non correggibile/i rilevato/i sul controller di memoria: <Processore> <Controller di memoria>
Un controller di memoria segnala un uErrorCount di almeno cMemCtlrUncorrectableErrFaultThreshold.	Errore	Errore/i di memoria ECC non correggibile/i rilevato/i sul controller di memoria: <Processore> <Controller di memoria>

Per risolvere questo errore, contattare il supporto NetApp per ricevere assistenza.

- **soglia di utilizzo della memoria**

  L'utilizzo della memoria è superiore alla norma. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

  Per informazioni più dettagliate sul tipo di errore, consultare la sezione **Dettagli** nell'errore.

Gravità	Descrizione
Avvertimento	La memoria di sistema è insufficiente.
Errore	La memoria di sistema è molto bassa.
Critico	La memoria di sistema è completamente consumata.

  Per risolvere questo errore, contattare il supporto NetApp per ricevere assistenza.

- **metadataClusterFull**

  Non c'è abbastanza spazio libero per l'archiviazione dei metadati per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di riempimento del cluster, vedere il metodo API GetClusterFullThreshold. Questo errore del cluster indica una delle seguenti condizioni:

  - stage3Low (Avviso): è stata superata la soglia definita dall'utente. Regola le impostazioni del Cluster

completo o aggiungi altri nodi.

- stage4Critical (Errore): non c'è abbastanza spazio per il ripristino da un errore di 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
- stage5CompletelyConsumed (Critical)1; Non sono consentite scritture o nuove connessioni iSCSI. Le attuali connessioni iSCSI saranno mantenute. Le scritture non riusciranno finché non verrà aggiunta ulteriore capacità al cluster. Elimina o ripulisci i dati oppure aggiungi altri nodi.

Per risolvere questo errore, eliminare o ripulire i volumi oppure aggiungere un altro nodo di archiviazione al cluster di archiviazione.

- **mtuCheckFailure**

  Un dispositivo di rete non è configurato per la dimensione MTU corretta.

  Per risolvere questo errore, assicurarsi che tutte le interfacce di rete e le porte dello switch siano configurate per frame jumbo (MTU fino a 9000 byte di dimensione).

- **Configurazione di rete**

  Questo errore del cluster indica una delle seguenti condizioni:

  - Non è presente un'interfaccia prevista.
  - È presente un'interfaccia duplicata.
  - Un'interfaccia configurata non è attiva.
  - È necessario riavviare la rete.

  Per ricevere assistenza, contattare il supporto NetApp .

- **nessunIndirizzoIPdiReteVirtualeDisponibile**

  Non ci sono indirizzi di rete virtuali disponibili nel blocco di indirizzi IP.

  - virtualNetworkID # TAG(###) non ha indirizzi IP di archiviazione disponibili. Non è possibile aggiungere nodi aggiuntivi al cluster.

  Per risolvere questo errore, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuali.

- **nodeHardwareFault (l'interfaccia di rete <nome> è inattiva o il cavo è scollegato)**

  Un'interfaccia di rete è inattiva oppure il cavo è scollegato.

  Per risolvere questo errore, verificare la connettività di rete del nodo o dei nodi.

- **nodeHardwareFault (Lo stato di capacità di crittografia dell'unità non corrisponde allo stato di capacità di crittografia del nodo per l'unità nello slot <slot del nodo><slot dell'unità>)**

  Un'unità non corrisponde alle capacità di crittografia del nodo di archiviazione in cui è installata.

- **nodeHardwareFault (<tipo di unità> dimensione dell'unità <dimensione effettiva> errata per l'unità nello slot <slot del nodo><slot dell'unità> per questo tipo di nodo - prevista <dimensione prevista>)**

  Un nodo di archiviazione contiene un'unità di dimensioni errate per questo nodo.

- **nodeHardwareFault (Unità non supportata rilevata nello slot <slot nodo><slot unità>; le statistiche dell'unità e le informazioni sullo stato non saranno disponibili)**

Un nodo di archiviazione contiene un'unità che non supporta.

- **nodeHardwareFault (L'unità nello slot <slot nodo><slot unità> dovrebbe utilizzare la versione firmware <versione prevista>, ma utilizza la versione non supportata <versione effettiva>)**

  Un nodo di archiviazione contiene un'unità che esegue una versione del firmware non supportata.

- **nodeMaintenanceMode**

  Un nodo è stato messo in modalità manutenzione. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	Indica che il nodo è ancora in modalità di manutenzione.
Errore	Indica che la modalità di manutenzione non è riuscita a essere disattivata, molto probabilmente a causa di standby attivi o non riusciti.

  Per risolvere questo errore, disattivare la modalità di manutenzione una volta completata la manutenzione. Se l'errore persiste, contattare il supporto NetApp per ricevere assistenza.

- **nodoOffline**

  Il software Element non riesce a comunicare con il nodo specificato. Controllare la connettività di rete.

- **notUsingLACPBondMode**

  La modalità di bonding LACP non è configurata.

  Per risolvere questo errore, utilizzare il bonding LACP durante la distribuzione dei nodi di archiviazione; i client potrebbero riscontrare problemi di prestazioni se LACP non è abilitato e configurato correttamente.

- **ntpServerUnreachable**

  Il cluster di archiviazione non riesce a comunicare con il server o i server NTP specificati.

  Per risolvere questo errore, controllare la configurazione del server NTP, della rete e del firewall.

- **ntpTimeNotInSync**

  La differenza tra l'ora del cluster di archiviazione e l'ora specificata del server NTP è troppo grande. Il cluster di archiviazione non può correggere automaticamente la differenza.

  Per risolvere questo errore, utilizzare i server NTP interni alla rete anziché quelli predefiniti di installazione. Se si utilizzano server NTP interni e il problema persiste, contattare il supporto NetApp per ricevere assistenza.

- **nvramDeviceStatus**

  Un dispositivo NVRAM presenta un errore, è in errore o è guasto. Questo guasto ha le seguenti gravità:

Gravità	Descrizione
Avvertimento	È stato rilevato un avviso dall'hardware. Questa condizione può essere transitoria, come ad esempio un avviso di temperatura. • Errore di durata nvm • Stato di durata nvm • Stato della fonte energetica a vita • Stato della temperatura della fonte energetica • warningThresholdExceeded
Errore	L'hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere l'unità slice dal funzionamento (ciò genera un evento di rimozione dell'unità). Se i servizi di slice secondari non sono disponibili, l'unità non verrà rimossa. Errori restituiti oltre agli errori di livello Avviso: • Il punto di montaggio del dispositivo NVRAM non esiste. • La partizione del dispositivo NVRAM non esiste. • La partizione del dispositivo NVRAM esiste, ma non è montata.
Critico	L'hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere l'unità slice dal funzionamento (ciò genera un evento di rimozione dell'unità). Se i servizi di slice secondari non sono disponibili, l'unità non verrà rimossa. • persistenzapersa • armStatusSaveNArmed • csaveStatusError

Sostituire qualsiasi componente hardware guasto nel nodo. Se il problema persiste, contattare l'assistenza NetApp per ricevere assistenza.

- **ErroreAlimentazione**

  Questo errore del cluster indica una delle seguenti condizioni:

  - Non è presente un alimentatore.
  - Si è verificato un guasto all'alimentatore.
  - Un ingresso di alimentazione è mancante o fuori portata.

  Per risolvere questo errore, verificare che a tutti i nodi venga fornita alimentazione ridondante. Per ricevere assistenza, contattare il supporto NetApp .

- **Spaziotroppopieno**

  La capacità complessiva fornita dal cluster è troppo piena.

  Per risolvere questo errore, aggiungere altro spazio fornito oppure eliminare e ripulire i volumi.

- **remoteRepAsyncDelayExceeded**

  È stato superato il ritardo asincrono configurato per la replica. Controllare la connettività di rete tra i cluster.

- **remoteRepClusterFull**

  I volumi hanno sospeso la replica remota perché il cluster di archiviazione di destinazione è troppo pieno.

  Per risolvere questo errore, liberare spazio sul cluster di archiviazione di destinazione.

- **remoteRepSnapshotClusterFull**

  I volumi hanno sospeso la replica remota degli snapshot perché il cluster di archiviazione di destinazione è troppo pieno.

  Per risolvere questo errore, liberare spazio sul cluster di archiviazione di destinazione.

- **remoteRepSnapshotsExceededLimit**

  I volumi hanno sospeso la replica remota degli snapshot perché il volume del cluster di archiviazione di destinazione ha superato il limite di snapshot.

  Per risolvere questo errore, aumentare il limite degli snapshot sul cluster di archiviazione di destinazione.

- **scheduleActionError**

  Una o più attività programmate sono state eseguite, ma non sono riuscite.

  L'errore viene cancellato se l'attività pianificata viene eseguita nuovamente e ha esito positivo, se l'attività pianificata viene eliminata o se l'attività viene sospesa e ripresa.

- **sensorReadingFailed**

  Un sensore non è riuscito a comunicare con il Baseboard Management Controller (BMC).

  Per ricevere assistenza, contattare il supporto NetApp .

- **servizioNonInEsecuzione**

  Un servizio richiesto non è in esecuzione.

  Per ricevere assistenza, contattare il supporto NetApp .

- **sliceServiceTooFull**

  A un servizio slice è assegnata una capacità provisionata troppo bassa.

  Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **sliceServiceNon sano**

Il sistema ha rilevato che un servizio slice non è integro e lo sta disattivando automaticamente.

  - Gravità = Avvertenza: non viene intrapresa alcuna azione. Questo periodo di preavviso scadrà tra 6 minuti.
  - Gravità = Errore: il sistema sta automaticamente dismettendo i dati e replicandoli nuovamente su altre unità funzionanti.

Verificare la presenza di problemi di connettività di rete ed errori hardware. Si verificheranno altri guasti se specifici componenti hardware non funzionano. L'errore verrà risolto quando il servizio slice sarà accessibile o quando il servizio sarà stato dismesso.

- **sshAbilitato**

  Il servizio SSH è abilitato su uno o più nodi nel cluster di archiviazione.

  Per risolvere questo errore, disabilitare il servizio SSH sul nodo o sui nodi appropriati oppure contattare il supporto NetApp per ricevere assistenza.

- **ScadenzaCertificatoSsl**

  Il certificato SSL associato a questo nodo è prossimo alla scadenza o è scaduto. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	Il certificato scade entro 30 giorni.
Errore	Il certificato scade entro 7 giorni.
Critico	Il certificato scade entro 3 giorni o è già scaduto.

  Per risolvere questo errore, rinnovare il certificato SSL. Se necessario, contattare il supporto NetApp per ricevere assistenza.

- **capacità bloccata**

  Un singolo nodo rappresenta più della metà della capacità del cluster di archiviazione.

  Per mantenere la ridondanza dei dati, il sistema riduce la capacità del nodo più grande, in modo che parte della sua capacità di blocco rimanga bloccata (non utilizzata).

  Per risolvere questo errore, aggiungere più unità ai nodi di archiviazione esistenti oppure aggiungere nodi di archiviazione al cluster.

- **Sensore di temperatura**

  Un sensore di temperatura segnala temperature più alte del normale. Questo errore può essere attivato insieme agli errori powerSupplyError o fanSensor.

  Per risolvere questo problema, verificare che non vi siano ostruzioni al flusso d'aria in prossimità del cluster di archiviazione. Se necessario, contattare il supporto NetApp per ricevere assistenza.

- **aggiornamento**

È in corso un aggiornamento da più di 24 ore.

Per risolvere questo errore, riprendere l'aggiornamento o contattare il supporto NetApp per ricevere assistenza.

- **Servizio non responsivo**

  Un servizio non risponde più.

  Per ricevere assistenza, contattare il supporto NetApp .

- **virtualNetworkConfig**

  Questo errore del cluster indica una delle seguenti condizioni:

  - Non è presente alcuna interfaccia.
  - C'è uno spazio dei nomi errato su un'interfaccia.
  - La netmask è errata.
  - L'indirizzo IP è errato.
  - Un'interfaccia non è attiva e funzionante.
  - C'è un'interfaccia superflua su un nodo.

  Per ricevere assistenza, contattare il supporto NetApp .

- **volumiDegradati**

  I volumi secondari non hanno terminato la replicazione e la sincronizzazione. Il messaggio scompare al termine della sincronizzazione.

- **volumiOffline**

  Uno o più volumi nel cluster di archiviazione sono offline. Sarà presente anche l'errore **volumeDegraded**.

  Per ricevere assistenza, contattare il supporto NetApp .

Visualizza l'attività delle prestazioni del nodo

È possibile visualizzare l'attività prestazionale di ciascun nodo in formato grafico. Queste informazioni forniscono statistiche in tempo reale sulla CPU e sulle operazioni di I/O di lettura/scrittura al secondo (IOPS) per ogni unità del nodo. Il grafico di utilizzo viene aggiornato ogni cinque secondi, mentre il grafico delle statistiche dell'unità viene aggiornato ogni dieci secondi.

1. Fare clic su **Cluster** > **Nodi**.
2. Fare clic su **Azioni** per il nodo che si desidera visualizzare.
3. Fare clic su **Visualizza dettagli**.

> È possibile visualizzare punti specifici nel tempo sui grafici a linee e a barre posizionando il cursore sulla linea o sulla barra.

Prestazioni di volume

Visualizza le prestazioni del volume

È possibile visualizzare informazioni dettagliate sulle prestazioni di tutti i volumi nel cluster. È possibile ordinare le informazioni in base all'ID del volume o in base a una qualsiasi delle colonne relative alle prestazioni. È anche possibile filtrare le informazioni in base a determinati criteri.

È possibile modificare la frequenza con cui il sistema aggiorna le informazioni sulle prestazioni nella pagina facendo clic sull'elenco **Aggiorna ogni** e scegliendo un valore diverso. L'intervallo di aggiornamento predefinito è di 10 secondi se il cluster ha meno di 1000 volumi; in caso contrario, il valore predefinito è di 60 secondi. Se si sceglie il valore Mai, l'aggiornamento automatico della pagina è disabilitato.

Puoi riattivare l'aggiornamento automatico cliccando su **Attiva aggiornamento automatico**.

1. Nell'interfaccia utente di Element, seleziona **Reporting** > **Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Azioni per un volume.
3. Fare clic su **Visualizza dettagli**.

   Nella parte inferiore della pagina viene visualizzata una barra contenente informazioni generali sul volume.
4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi altri dettagli**.

   Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Trova maggiori informazioni

Dettagli sulle prestazioni del volume

Dettagli sulle prestazioni del volume

È possibile visualizzare le statistiche sulle prestazioni dei volumi dalla pagina Prestazioni volume della scheda Report nell'interfaccia utente dell'elemento.

L'elenco seguente descrive i dettagli a tua disposizione:

- **ID**

  ID generato dal sistema per il volume.
- **Nome**

  Nome dato al volume al momento della sua creazione.
- **Account**

  Nome dell'account assegnato al volume.
- **Gruppi di accesso**

  Nome del gruppo o dei gruppi di accesso al volume a cui appartiene il volume.

- **Utilizzo del volume**

  Un valore percentuale che descrive quanto il client sta utilizzando il volume.

  Valori possibili:

  - 0 = Il client non sta utilizzando il volume
  - 100 = Il client sta utilizzando il massimo
  - >100 = Il client sta utilizzando il burst
- **IOPS totali**

  Numero totale di IOPS (lettura e scrittura) attualmente eseguiti sul volume.
- **Leggi IOPS**

  Numero totale di IOPS di lettura attualmente eseguiti sul volume.
- **Scrivi IOPS**

  Numero totale di IOPS di scrittura attualmente eseguiti sul volume.
- **Rendimento totale**

  Quantità totale di throughput (lettura e scrittura) attualmente in esecuzione sul volume.
- **Velocità di lettura**

  Quantità totale di throughput di lettura attualmente in esecuzione sul volume.
- **Capacità di scrittura**

  Quantità totale di velocità di scrittura attualmente eseguita sul volume.
- **Latenza totale**

  Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura e scrittura su un volume.
- **Latenza di lettura**

  Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.
- **Latenza di scrittura**

  Tempo medio, in microsecondi, impiegato per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.
- **Profondità della coda**

  Numero di operazioni di lettura e scrittura in sospeso sul volume.
- **Dimensione media IO**

  Dimensione media in byte delle recenti operazioni di I/O sul volume negli ultimi 500 millisecondi.

sessioni iSCSI

Visualizza le sessioni iSCSI

È possibile visualizzare le sessioni iSCSI connesse al cluster. È possibile filtrare le informazioni per includere solo le sessioni desiderate.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **Sessioni iSCSI**.
2. Per visualizzare i campi dei criteri di filtro, fare clic su **Filtro**.

Trova maggiori informazioni

Dettagli della sessione iSCSI

Dettagli della sessione iSCSI

È possibile visualizzare informazioni sulle sessioni iSCSI connesse al cluster.

L'elenco seguente descrive le informazioni che è possibile trovare sulle sessioni iSCSI:

- **Nodo**

  Il nodo che ospita la partizione dei metadati primaria per il volume.

- **Account**

  Nome dell'account proprietario del volume. Se il valore è vuoto, viene visualizzato un trattino (-).

- **Volume**

  Il nome del volume identificato sul nodo.

- **ID volume**

  ID del volume associato al Target IQN.

- **ID iniziatore**

  Un ID generato dal sistema per l'iniziatore.

- **Alias dell'iniziatore**

  Un nome facoltativo per l'iniziatore che ne facilita la ricerca quando l'elenco è lungo.

- **IP Iniziatore**

  L'indirizzo IP dell'endpoint che avvia la sessione.

- **Iniziatore IQN**

  L'IQN dell'endpoint che avvia la sessione.

- **IP di destinazione**

  L'indirizzo IP del nodo che ospita il volume.

- **Obiettivo IQN**

  L'IQN del volume.

- **CAP**

  L'algoritmo CHAP per una sessione iSCSI. Se non viene utilizzato un algoritmo CHAP, viene visualizzato un trattino (-). Disponibile a partire da Element 12.8.

- **Creato il**

  Data in cui è stata istituita la sessione.

Sessioni Fibre Channel

Visualizza le sessioni Fibre Channel

È possibile visualizzare le sessioni Fibre Channel (FC) connesse al cluster. È possibile filtrare le informazioni per includere solo le connessioni che si desidera visualizzare nella finestra.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting** > **Sessioni FC**.
2. Per visualizzare i campi dei criteri di filtro, fare clic su **Filtro**.

Trova maggiori informazioni

Dettagli della sessione Fibre Channel

Dettagli della sessione Fibre Channel

È possibile trovare informazioni sulle sessioni Fibre Channel (FC) attive connesse al cluster.

L'elenco seguente descrive le informazioni che è possibile trovare sulle sessioni FC connesse al cluster:

- **ID nodo**

  Il nodo che ospita la sessione per la connessione.

- **Nome nodo**

  Nome del nodo generato dal sistema.

- **ID iniziatore**

  Un ID generato dal sistema per l'iniziatore.

- **Iniziatore WWPN**

  Nome della porta mondiale di avvio.

- **Alias dell'iniziatore**

Un nome facoltativo per l'iniziatore che ne facilita la ricerca quando l'elenco è lungo.

- **Obiettivo WWPN**

  Nome della porta di destinazione mondiale.

- **Gruppo di accesso al volume**

  Nome del gruppo di accesso al volume a cui appartiene la sessione.

- **ID gruppo di accesso al volume**

  ID generato dal sistema per il gruppo di accesso.

Risoluzione dei problemi delle unità

Risoluzione dei problemi delle unità

È possibile sostituire un'unità a stato solido (SSD) guasta con un'unità sostitutiva. Gli SSD per i nodi di archiviazione SolidFire sono sostituibili a caldo. Se sospetti che un SSD sia guasto, contatta l'assistenza NetApp per verificare il guasto e ricevere istruzioni sulla procedura di risoluzione corretta. Il supporto NetApp collabora anche con te per ottenere un'unità sostitutiva in base al tuo contratto di servizio.

In questo caso, "How-swappable" significa che è possibile rimuovere un'unità guasta da un nodo attivo e sostituirla con una nuova unità SSD di NetApp. Si sconsiglia di rimuovere unità non guaste da un cluster attivo.

È consigliabile tenere a disposizione in loco i pezzi di ricambio suggeriti dal supporto NetApp per consentire la sostituzione immediata dell'unità in caso di guasto.

> A scopo di test, se si simula un guasto dell'unità estraendo un'unità da un nodo, è necessario attendere 30 secondi prima di reinserire l'unità nello slot.

In caso di guasto di un'unità, Double Helix ridistribuisce i dati sull'unità tra i nodi rimanenti del cluster. I guasti di più unità sullo stesso nodo non rappresentano un problema, poiché il software Element protegge da due copie di dati residenti sullo stesso nodo. Un'unità guasta provoca i seguenti eventi:

- I dati vengono trasferiti dall'unità.
- La capacità complessiva del cluster è ridotta dalla capacità dell'unità.
- La protezione dei dati Double Helix garantisce che siano presenti due copie valide dei dati.

> I sistemi di archiviazione SolidFire non supportano la rimozione di un'unità se ciò comporta una quantità di spazio di archiviazione insufficiente per la migrazione dei dati.

Per maggiori informazioni

- Rimuovere le unità non riuscite dal cluster
- Risoluzione dei problemi di base dell'unità MDSS
- Rimuovere le unità MDSS
- "Sostituzione delle unità per i nodi di archiviazione SolidFire"

- "Sostituzione delle unità per i nodi di archiviazione della serie H600S"
- "Informazioni hardware H410S e H610S"
- "Informazioni sull'hardware della serie SF"

Rimuovere le unità non riuscite dal cluster

Il sistema SolidFire segnala un'unità in stato di errore se l'autodiagnosi dell'unità segnala al nodo un errore o se la comunicazione con l'unità si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco delle unità guaste. È necessario rimuovere un'unità guasta dall'elenco delle unità guaste nel software NetApp Element .

Le unità nell'elenco **Avvisi** vengono visualizzate come **blockServiceUnhealthy** quando un nodo è offline. Quando si riavvia il nodo, se il nodo e le sue unità tornano online entro cinque minuti e mezzo, le unità si aggiornano automaticamente e continuano a essere attive nel cluster.

1. Nell'interfaccia utente di Element, seleziona **Cluster** > **Unità**.
2. Fare clic su **Non riuscito** per visualizzare l'elenco delle unità non riuscite.
3. Annotare il numero di slot dell'unità guasta.

   Queste informazioni sono necessarie per individuare l'unità guasta nello chassis.

4. Rimuovere le unità danneggiate utilizzando uno dei seguenti metodi:

Opzione	Passi
Per rimuovere singole unità	a. Fare clic su **Azioni** per l'unità che si desidera rimuovere. b. Fare clic su **Rimuovi**.
Per rimuovere più unità	a. Seleziona tutte le unità che vuoi rimuovere e fai clic su **Azioni in blocco**. b. Fare clic su **Rimuovi**.

Risoluzione dei problemi di base dell'unità MDSS

È possibile ripristinare le unità metadati (o slice) aggiungendole nuovamente al cluster nel caso in cui una o entrambe le unità metadati si guastino. È possibile eseguire l'operazione di ripristino nell'interfaccia utente NetApp Element se la funzionalità MDSS è già abilitata sul nodo.

Se una o entrambe le unità di metadati in un nodo subiscono un errore, il servizio di suddivisione verrà arrestato e i dati di entrambe le unità verranno sottoposti a backup su unità diverse nel nodo.

Gli scenari seguenti delineano possibili scenari di errore e forniscono consigli di base per correggere il problema:

L’unità slice di sistema non funziona

- In questo scenario, lo slot 2 viene verificato e riportato allo stato disponibile.
- L’unità slice di sistema deve essere ripopolata prima che il servizio slice possa essere riattivato.
- È necessario sostituire l’unità slice di sistema; quando l’unità slice di sistema diventa disponibile, aggiungere contemporaneamente l’unità e l’unità slot 2.

> Non è possibile aggiungere l’unità nello slot 2 da sola come unità metadati. È necessario aggiungere entrambe le unità al nodo contemporaneamente.

Lo slot 2 non funziona

- In questo scenario, l’unità slice di sistema viene verificata e riportata allo stato disponibile.
- Dovresti sostituire lo slot 2 con uno di riserva; quando lo slot 2 diventa disponibile, aggiungi contemporaneamente l’unità slice di sistema e l’unità dello slot 2.

L’unità slice di sistema e lo slot 2 non funzionano

- Dovresti sostituire sia l’unità slice di sistema sia lo slot 2 con un’unità di riserva. Quando entrambe le unità diventano disponibili, aggiungere contemporaneamente l’unità slice di sistema e l’unità slot 2.

Ordine delle operazioni

- Sostituire l’unità hardware guasta con un’unità di riserva (sostituire entrambe le unità se entrambe sono guaste).
- Aggiungere nuovamente le unità al cluster quando sono state ripopolate e sono disponibili.

Verificare le operazioni

- Verificare che le unità nello slot 0 (o interno) e nello slot 2 siano identificate come unità metadati nell’elenco Unità attive.
- Verificare che il bilanciamento delle sezioni sia stato completato (non ci siano ulteriori messaggi di spostamento delle sezioni nel registro eventi per almeno 30 minuti).

Per maggiori informazioni

Aggiungi unità MDSS

Aggiungi unità MDSS

È possibile aggiungere una seconda unità metadati su un nodo SolidFire convertendo l’unità a blocchi nello slot 2 in un’unità slice. Ciò si ottiene abilitando la funzionalità Multi-Drive Slice Service (MDSS). Per abilitare questa funzionalità, è necessario contattare l’assistenza NetApp .

Per riportare un’unità slice in uno stato disponibile potrebbe essere necessario sostituire un’unità guasta con una nuova o di riserva. È necessario aggiungere l’unità slice di sistema contemporaneamente all’unità per lo slot 2. Se si tenta di aggiungere solo l’unità slice dello slot 2 o prima di aggiungere l’unità slice di sistema, il sistema genererà un errore.

1. Fare clic su **Cluster** > **Unità**.

2. Fare clic su **Disponibile** per visualizzare l'elenco delle unità disponibili.
3. Selezionare le unità slice da aggiungere.
4. Fare clic su **Azioni in blocco**.
5. Fare clic su **Aggiungi**.
6. Verificare nella scheda **Unità attive** che le unità siano state aggiunte.

Rimuovere le unità MDSS

È possibile rimuovere le unità MDSS (Multi-Drive Slice Service). Questa procedura si applica solo se il nodo ha più unità slice.

> Se l'unità slice di sistema e l'unità slot 2 si guastano, il sistema arresta i servizi slice e rimuove le unità. Se non si verificano guasti e si rimuovono le unità, è necessario rimuovere entrambe le unità contemporaneamente.

1. Fare clic su **Cluster** > **Unità**.
2. Nella scheda Unità **Disponibili**, fare clic sulla casella di controllo per le unità slice da rimuovere.
3. Fare clic su **Azioni in blocco**.
4. Fare clic su **Rimuovi**.
5. Conferma l'azione.

Risoluzione dei problemi dei nodi

Rimuovere i nodi da un cluster

È possibile rimuovere nodi da un cluster per manutenzione o sostituzione. È consigliabile utilizzare l'interfaccia utente o l'API NetApp Element per rimuovere i nodi prima di metterli offline.

Di seguito è riportata una panoramica della procedura per rimuovere i nodi di archiviazione:

- Assicurarsi che nel cluster vi sia capacità sufficiente per creare una copia dei dati sul nodo.
- Rimuovere le unità dal cluster utilizzando l'interfaccia utente o il metodo API RemoveDrives.

  Ciò comporta che il sistema migrerà i dati dalle unità del nodo ad altre unità nel cluster. Il tempo impiegato da questo processo dipende dalla quantità di dati da migrare.

- Rimuovere il nodo dal cluster.

Prima di spegnere o accendere un nodo, tenere a mente le seguenti considerazioni:

- Lo spegnimento di nodi e cluster comporta dei rischi se non eseguito correttamente.

  Lo spegnimento di un nodo deve essere effettuato sotto la supervisione del supporto NetApp .

- Se un nodo è rimasto inattivo per più di 5,5 minuti a causa di qualsiasi tipo di condizione di arresto, la protezione dei dati Double Helix avvia l'attività di scrittura di singoli blocchi replicati su un altro nodo per replicare i dati. In questo caso, contattare l'assistenza NetApp per ricevere assistenza nell'analisi del nodo non riuscito.

- Per riavviare o spegnere un nodo in modo sicuro, è possibile utilizzare il comando Shutdown API.
- Se un nodo è inattivo o spento, è necessario contattare l'assistenza NetApp prima di riportarlo online.
- Dopo che un nodo è stato riportato online, è necessario aggiungere nuovamente le unità al cluster, a seconda di quanto tempo è stato fuori servizio.

Per maggiori informazioni

"Sostituzione di uno chassis SolidFire guasto"

"Sostituzione di un nodo della serie H600S guasto"

Spegnere un cluster

Per spegnere un intero cluster, eseguire la seguente procedura.

Passi

1. (Facoltativo) Contattare l'assistenza NetApp per ricevere assistenza nel completamento dei passaggi preliminari.
2. Verificare che tutti gli I/O siano stati arrestati.
3. Disconnettere tutte le sessioni iSCSI:
   a. Passare all'indirizzo IP virtuale di gestione (MVIP) sul cluster per aprire l'interfaccia utente di Element.
   b. Notare i nodi elencati nell'elenco Nodi.
   c. Eseguire il metodo API Shutdown con l'opzione halt specificata su ciascun ID nodo nel cluster.

> Quando si riavvia il cluster, è necessario seguire alcuni passaggi per verificare che tutti i nodi siano online:
>
> 1. Verificare che tutti i livelli di gravità critica e `volumesOffline` gli errori del cluster sono stati risolti.
> 2. Attendere dai 10 ai 15 minuti affinché il cluster si depositi.
> 3. Iniziare a richiamare gli host per accedere ai dati.
>
> Se si desidera concedere più tempo per accendere i nodi e verificare che siano integri dopo la manutenzione, contattare l'assistenza tecnica per ricevere assistenza su come ritardare la sincronizzazione dei dati ed evitare una sincronizzazione bin non necessaria.

Trova maggiori informazioni

"Come arrestare e riaccendere correttamente un cluster di storage NetApp Solidfire/HCI"

Lavorare con utilità per nodo per nodi di archiviazione

Lavorare con utilità per nodo per nodi di archiviazione

È possibile utilizzare le utilità per nodo per risolvere i problemi di rete se gli strumenti di monitoraggio standard nell'interfaccia utente del software NetApp Element non forniscono informazioni sufficienti per la risoluzione dei problemi. Le utilità per nodo forniscono informazioni e strumenti specifici che possono aiutare a risolvere i problemi di

rete tra i nodi o con il nodo di gestione.

Trova maggiori informazioni

- Accedi alle impostazioni per nodo tramite l'interfaccia utente per nodo
- Dettagli delle impostazioni di rete dall'interfaccia utente per nodo
- Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo
- Eseguire test di sistema utilizzando l'interfaccia utente per nodo
- Eseguire le utilità di sistema utilizzando l'interfaccia utente per nodo

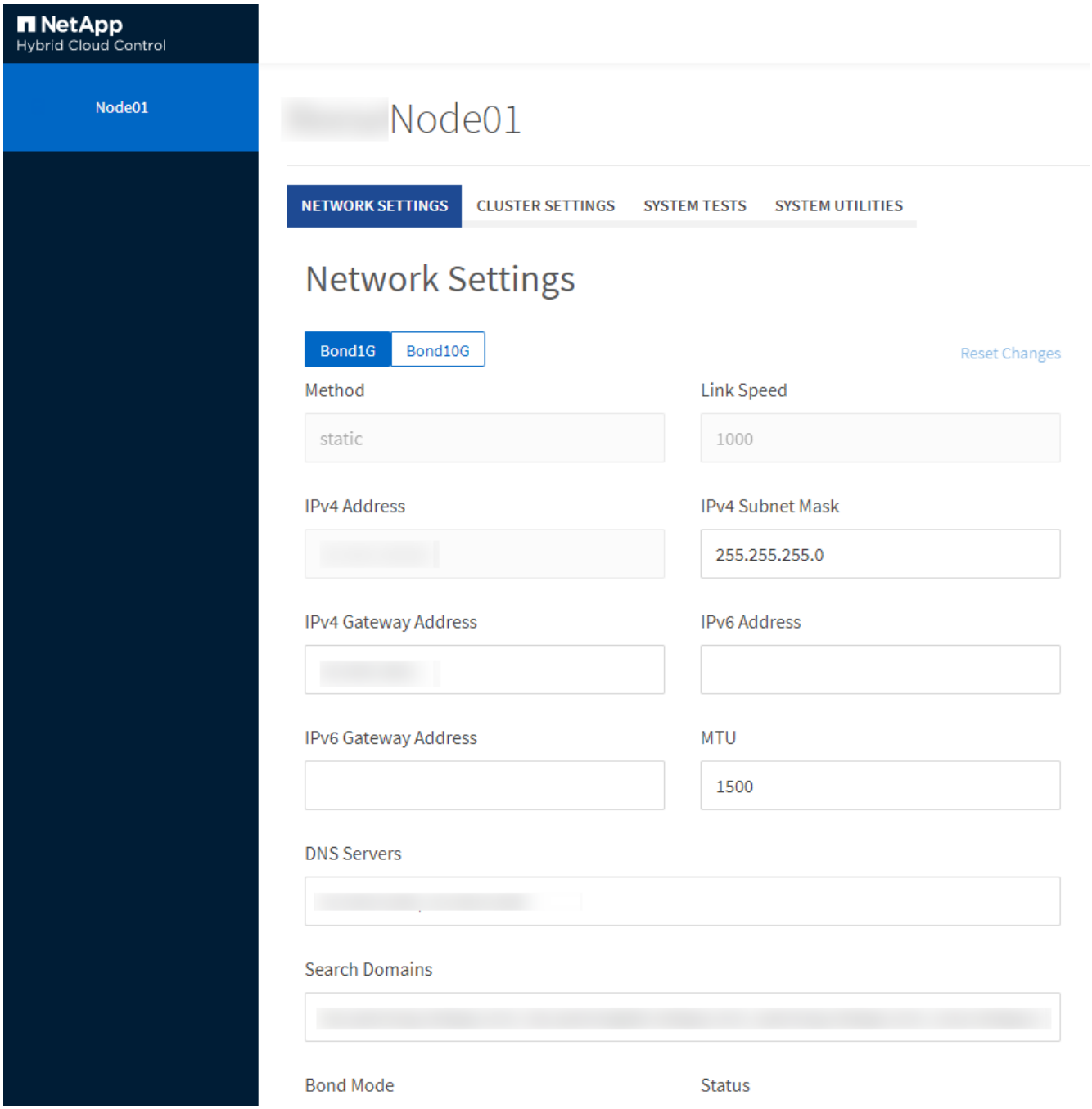
Accedi alle impostazioni per nodo tramite l'interfaccia utente per nodo

È possibile accedere alle impostazioni di rete, alle impostazioni del cluster, ai test e alle utilità di sistema nell'interfaccia utente per nodo dopo aver immesso l'IP del nodo di gestione ed eseguito l'autenticazione.

Se si desidera modificare le impostazioni di un nodo in stato Attivo che fa parte di un cluster, è necessario accedere come utente amministratore del cluster.

Dovresti configurare o modificare un nodo alla volta. Prima di apportare modifiche a un altro nodo, è necessario assicurarsi che le impostazioni di rete specificate abbiano l'effetto previsto e che la rete sia stabile e funzioni correttamente.

1. Aprire l'interfaccia utente per nodo utilizzando uno dei seguenti metodi:
   - Inserisci l'indirizzo IP di gestione seguito da :442 in una finestra del browser ed effettua l'accesso utilizzando un nome utente e una password amministratore.
   - Nell'interfaccia utente dell'elemento, seleziona **Cluster** > **Nodi** e fai clic sul collegamento all'indirizzo IP di gestione per il nodo che desideri configurare o modificare. Nella finestra del browser che si apre, puoi modificare le impostazioni del nodo.



Dettagli delle impostazioni di rete dall'interfaccia utente per nodo

È possibile modificare le impostazioni di rete del nodo di archiviazione per fornire al nodo un nuovo set di attributi di rete.

È possibile visualizzare le impostazioni di rete per un nodo di archiviazione nella pagina **Impostazioni di rete** quando si accede al nodo (`https://<node_IP>:442/hcc/node/network-settings`). È possibile selezionare le impostazioni **Bond1G** (gestione) o **Bond10G** (archiviazione). L'elenco seguente descrive le impostazioni che è possibile modificare quando un nodo di archiviazione è nello stato Disponibile, In sospeso o Attivo:

- **Metodo**

  Metodo utilizzato per configurare l'interfaccia. Metodi possibili:

    - loopback: utilizzato per definire l'interfaccia loopback IPv4.
    - manuale: utilizzato per definire le interfacce per le quali non viene effettuata alcuna configurazione di default.
    - dhcp: utilizzato per ottenere un indirizzo IP tramite DHCP.
    - statico: utilizzato per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.
- **Velocità di collegamento**

  La velocità negoziata dalla NIC virtuale.

- **Indirizzo IPv4**

  L'indirizzo IPv4 per la rete eth0.

- **Maschera di sottorete IPv4**

  Suddivisioni degli indirizzi della rete IPv4.

- **Indirizzo gateway IPv4**

  Indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.

- **Indirizzo IPv6**

  L'indirizzo IPv6 per la rete eth0.

- **Indirizzo gateway IPv6**

  Indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.

- **MTU**

  Dimensione massima del pacchetto che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete di archiviazione, il valore dovrebbe essere 9000.

- **Server DNS**

  Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Cerca domini**

  Cerca altri indirizzi MAC disponibili nel sistema.

- **Modalità legame**

  Può essere una delle seguenti modalità:

    - AttivoPassivo (predefinito)
    - CAMICE
    - LACP
- **Stato**

  Valori possibili:

- In funzione
- Giù
- Su

- **Tag Rete Virtuale**

  Tag assegnato al momento della creazione della rete virtuale.

- **Percorsi**

  Percorsi statici verso host o reti specifici tramite l'interfaccia associata per la quale i percorsi sono configurati.

Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo

È possibile verificare le impostazioni del cluster per un nodo di archiviazione dopo la configurazione del cluster e modificare il nome host del nodo.

L'elenco seguente descrive le impostazioni del cluster per un nodo di archiviazione indicato dalla pagina **Impostazioni cluster** dell'interfaccia utente per nodo (`https://<node_IP>:442/hcc/node/cluster-settings`).

- **Ruolo**

  Ruolo del nodo nel cluster. Valori possibili:

  - Archiviazione: nodo di archiviazione o Fibre Channel.
  - Gestione: il nodo è un nodo di gestione.

- **Nome host**

  Nome del nodo.

- **Grappolo**

  Nome del cluster.

- **Appartenenza al Cluster**

  Stato del nodo. Valori possibili:

  - Disponibile: il nodo non ha alcun nome di cluster associato e non fa ancora parte di un cluster.
  - In attesa: il nodo è configurato e può essere aggiunto a un cluster designato. Per accedere al nodo non è richiesta l'autenticazione.
  - PendingActive: il sistema sta installando un software compatibile sul nodo. Una volta completato, il nodo passerà allo stato Attivo.
  - Attivo: il nodo partecipa a un cluster. Per modificare il nodo è richiesta l'autenticazione.

- **Versione**

  Versione del software Element in esecuzione sul nodo.

- **Insieme**

Nodi che fanno parte dell'insieme del database.

- **ID nodo**

  ID assegnato quando un nodo viene aggiunto al cluster.

- **Interfaccia cluster**

  Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Interfaccia di gestione**

  Interfaccia di rete di gestione. L'impostazione predefinita è Bond1G, ma è possibile utilizzare anche Bond10G.

- **Interfaccia di archiviazione**

  Interfaccia di rete di archiviazione tramite Bond10G.

- **Capacità di crittografia**

  Indica se il nodo supporta o meno la crittografia dell'unità.

Eseguire test di sistema utilizzando l'interfaccia utente per nodo

È possibile testare le modifiche alle impostazioni di rete dopo averle inserite nella configurazione di rete. È possibile eseguire i test per verificare che il nodo di archiviazione sia stabile e possa essere messo online senza problemi.

Hai effettuato l'accesso all'interfaccia utente per nodo del nodo di archiviazione.

1. Fare clic su **Test di sistema**.
2. Fare clic su **Esegui test** accanto al test che si desidera eseguire oppure selezionare **Esegui tutti i test**.

   L'esecuzione di tutte le operazioni di test può richiedere molto tempo e dovrebbe essere effettuata solo su indicazione del supporto NetApp .

   - **Test Ensemble Connesso**

     Testa e verifica la connettività a un insieme di database. Per impostazione predefinita, il test utilizza l'ensemble per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un insieme diverso per testare la connettività.

   - **Test di connessione Mvip**

     Esegue il ping dell'indirizzo IP virtuale di gestione (MVIP) specificato e quindi esegue una semplice chiamata API all'MVIP per verificare la connettività. Per impostazione predefinita, il test utilizza l'MVIP per il cluster a cui è associato il nodo.

   - **Test Connect Svip**

     Esegue il ping dell'indirizzo IP virtuale di archiviazione specificato (SVIP) utilizzando pacchetti ICMP (Internet Control Message Protocol) che corrispondono alla dimensione MTU (Maximum Transmission

Unit) impostata sulla scheda di rete. Si connette quindi allo SVIP come iniziatore iSCSI. Per impostazione predefinita, il test utilizza l'SVIP per il cluster a cui è associato il nodo.

- **Test della configurazione hardware**

  Verifica che tutte le configurazioni hardware siano corrette, convalida che le versioni del firmware siano corrette e conferma che tutte le unità siano installate e funzionino correttamente. Si tratta dello stesso test di fabbrica.

  > Questo test richiede molte risorse e deve essere eseguito solo se richiesto dal supporto NetApp .

- **Test di connettività locale**

  Verifica la connettività con tutti gli altri nodi del cluster eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test verrà visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

- **Test Localizza Cluster**

  Convalida che il nodo possa individuare il cluster specificato nella configurazione del cluster.

- **Configurazione di rete di prova**

  Verifica che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate sul sistema. Questo test non è destinato a rilevare guasti hardware quando un nodo partecipa attivamente a un cluster.

- **Ping di prova**

  Esegue il ping di un elenco specificato di host oppure, se non ne viene specificato nessuno, crea dinamicamente un elenco di tutti i nodi registrati nel cluster ed esegue il ping di ciascuno per una semplice connettività.

- **Test di connettività remota**

  Verifica la connettività a tutti i nodi nei cluster accoppiati in remoto eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test verrà visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

Eseguire le utilità di sistema utilizzando l'interfaccia utente per nodo

È possibile utilizzare l'interfaccia utente per nodo del nodo di archiviazione per creare o eliminare bundle di supporto, reimpostare le impostazioni di configurazione per le unità e riavviare i servizi di rete o cluster.

Hai effettuato l'accesso all'interfaccia utente per nodo del nodo di archiviazione.

1. Fare clic su **Utilità di sistema**.
2. Fare clic sul pulsante relativo all'utilità di sistema che si desidera eseguire.
   - **Controllo del potere**

     Riavvia, spegne e riaccende il nodo o lo spegne.

Questa operazione provoca una perdita temporanea della connettività di rete.

Specificare i seguenti parametri:

- Azione: le opzioni includono Riavvia e Arresta (spegnimento).
- Ritardo di riattivazione: qualsiasi tempo aggiuntivo prima che il nodo torni online.

◦ **Raccogli i log dei nodi**

Crea un bundle di supporto nella directory /tmp/bundles del nodo.

Specificare i seguenti parametri:

- Nome bundle: nome univoco per ogni bundle di supporto creato. Se non viene specificato alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
- Argomenti aggiuntivi: questo parametro viene fornito allo script sf_make_support_bundle. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp .
- Timeout Sec: specifica il numero di secondi di attesa per ogni singola risposta ping.

◦ **Elimina i registri dei nodi**

Elimina tutti i bundle di supporto correnti sul nodo creati utilizzando **Create Cluster Support Bundle** o il metodo API CreateSupportBundle.

◦ **Reimposta unità**

Inizializza le unità e rimuove tutti i dati attualmente presenti sull'unità. È possibile riutilizzare l'unità in un nodo esistente o in un nodo aggiornato.

Specificare il seguente parametro:

- Unità: elenco dei nomi dei dispositivi (non degli ID unità) da reimpostare.

◦ **Reimposta configurazione di rete**

Aiuta a risolvere i problemi di configurazione di rete per un singolo nodo e ripristina la configurazione di rete di un singolo nodo alle impostazioni predefinite di fabbrica.

◦ **Reimposta nodo**

Ripristina le impostazioni di fabbrica di un nodo. Durante questa operazione tutti i dati vengono rimossi, ma le impostazioni di rete del nodo vengono conservate. I nodi possono essere reimpostati solo se non sono assegnati a un cluster e sono nello stato Disponibile.

Quando si utilizza questa opzione, tutti i dati, i pacchetti (aggiornamenti software), le configurazioni e i file di registro vengono eliminati dal nodo.

◦ **Riavvia la rete**

Riavvia tutti i servizi di rete su un nodo.

Questa operazione può causare la perdita temporanea della connettività di rete.

◦ **Riavvia i servizi**

Riavvia i servizi software Element su un nodo.

> Questa operazione può causare l'interruzione temporanea del servizio del nodo. Questa operazione deve essere eseguita solo su indicazione del supporto NetApp .

Specificare i seguenti parametri:

- Servizio: Nome del servizio da riavviare.
- Azione: azione da eseguire sul servizio. Le opzioni includono avvio, arresto e riavvio.

Lavorare con il nodo di gestione

È possibile utilizzare il nodo di gestione (mNode) per aggiornare i servizi di sistema, gestire le risorse e le impostazioni del cluster, eseguire test e utilità di sistema, configurare Active IQ per il monitoraggio del sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

> Come best practice, associare un solo nodo di gestione a un'istanza VMware vCenter ed evitare di definire le stesse risorse di archiviazione e di elaborazione o istanze vCenter in più nodi di gestione.

Vedere"documentazione del nodo di gestione" per maggiori informazioni.

Comprendere i livelli di pienezza del cluster

Il cluster che esegue il software Element genera errori del cluster per avvisare l'amministratore dello storage quando la capacità del cluster sta esaurendo. Esistono tre livelli di riempimento del cluster, tutti visualizzati nell'interfaccia utente NetApp Element : avviso, errore e critico.

Il sistema utilizza il codice di errore BlockClusterFull per avvisare che lo spazio di archiviazione dei blocchi del cluster è pieno. È possibile visualizzare i livelli di gravità del riempimento del cluster dalla scheda Avvisi dell'interfaccia utente dell'elemento.

L'elenco seguente include informazioni sui livelli di gravità di BlockClusterFull:

- **Avvertimento**

  Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità del blocco del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al tre percento al di sotto del livello di errore e può essere regolato tramite l'interfaccia utente e l'API di Element. È necessario aggiungere ulteriore capacità o liberarne altra il prima possibile.

- **Errore**

  Quando il cluster si trova in questo stato, se un nodo viene perso, non ci sarà capacità sufficiente nel cluster per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot sono tutti bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per nessun cluster. È necessario aggiungere ulteriore capacità o liberare capacità immediatamente.

- **Critico**

  Questo errore critico si è verificato perché il cluster è consumato al 100%. Si trova in uno stato di sola lettura e non è possibile stabilire nuove connessioni iSCSI con il cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente altra capacità.

Il sistema utilizza il codice di errore MetadataClusterFull per avvisare che lo spazio di archiviazione dei metadati del cluster è pieno. È possibile visualizzare la quantità di spazio disponibile per i metadati del cluster nella sezione Capacità del cluster nella pagina Panoramica della scheda Report nell'interfaccia utente dell'elemento.

L'elenco seguente include informazioni sui livelli di gravità MetadataClusterFull:

- **Avvertimento**

  Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità dei metadati del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al tre percento al di sotto del livello di errore e può essere regolato tramite l'API Element. È necessario aggiungere ulteriore capacità o liberarne altra il prima possibile.

- **Errore**

  Quando il cluster si trova in questo stato, se un nodo viene perso, non ci sarà capacità sufficiente nel cluster per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot sono tutti bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per nessun cluster. È necessario aggiungere ulteriore capacità o liberare capacità immediatamente.

- **Critico**

  Questo errore critico si è verificato perché il cluster è consumato al 100%. Si trova in uno stato di sola lettura e non è possibile stabilire nuove connessioni iSCSI con il cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente altra capacità.

Quanto segue si applica alle soglie dei cluster a due nodi:

- L'errore di completezza dei metadati è inferiore del 20% al livello critico.
- L'errore di riempimento del blocco è pari a 1 unità di blocco (inclusa la capacità bloccata) al di sotto del livello critico, ovvero la capacità è pari a due unità di blocco al di sotto del livello critico.

Informazioni sul copyright

Copyright © 2025 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.