



Gestire lo storage con il software Element

Element Software

NetApp
January 15, 2024

Sommario

Gestire lo storage con il software Element	1
Trova ulteriori informazioni	1
Accedere all'interfaccia utente del software Element	1
Configurare le opzioni del sistema SolidFire dopo l'implementazione	2
Utilizzare le opzioni di base nell'interfaccia utente del software Element	9
Gestire gli account	11
Gestire il sistema	25
Gestire volumi e volumi virtuali	53
Proteggi i tuoi dati	80
Risolvere i problemi del sistema	125

Gestire lo storage con il software Element

Utilizza il software Element per configurare lo storage SolidFire, monitorare la capacità e le performance del cluster e gestire l'attività dello storage in un'infrastruttura multi-tenant.

Element è il sistema operativo per lo storage 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 singolo sistema storage ai client esterni. Il software Element è responsabile di tutto il coordinamento, la scalabilità e la gestione del cluster nel suo complesso.

L'interfaccia software si basa sull'API Element.

- ["Accedere all'interfaccia utente del software Element"](#)
- ["Configurare le opzioni del sistema SolidFire dopo l'implementazione"](#)
- ["Aggiornare i componenti del sistema storage"](#)
- ["Utilizzare le opzioni di base nell'interfaccia utente del software Element"](#)
- ["Gestire gli account"](#)
- ["Gestire il sistema"](#)
- ["Gestire volumi e volumi virtuali"](#)
- ["Proteggi i tuoi dati"](#)
- ["Risolvere i problemi del sistema"](#)

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Accedere all'interfaccia utente del software Element

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

Assicurarsi che i blocchi dei popup e le impostazioni NoScript siano disattivati nel browser.

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

1. Scegliere una delle seguenti opzioni:

- IPv6: Inserire `https://[IPv6 MVIP address]` ad esempio:

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

- IPv4: Inserire `https://[IPv4 MVIP address]` ad esempio:

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

2. Per DNS, immettere il nome host.
3. Fare clic sui messaggi dei certificati di autenticazione.

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Configurare le opzioni del sistema SolidFire dopo l'implementazione

Dopo aver configurato il sistema SolidFire, è possibile eseguire alcune attività facoltative.

Se si modificano le credenziali nel sistema, potrebbe essere necessario conoscere l'impatto su altri componenti.

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

Trova ulteriori informazioni

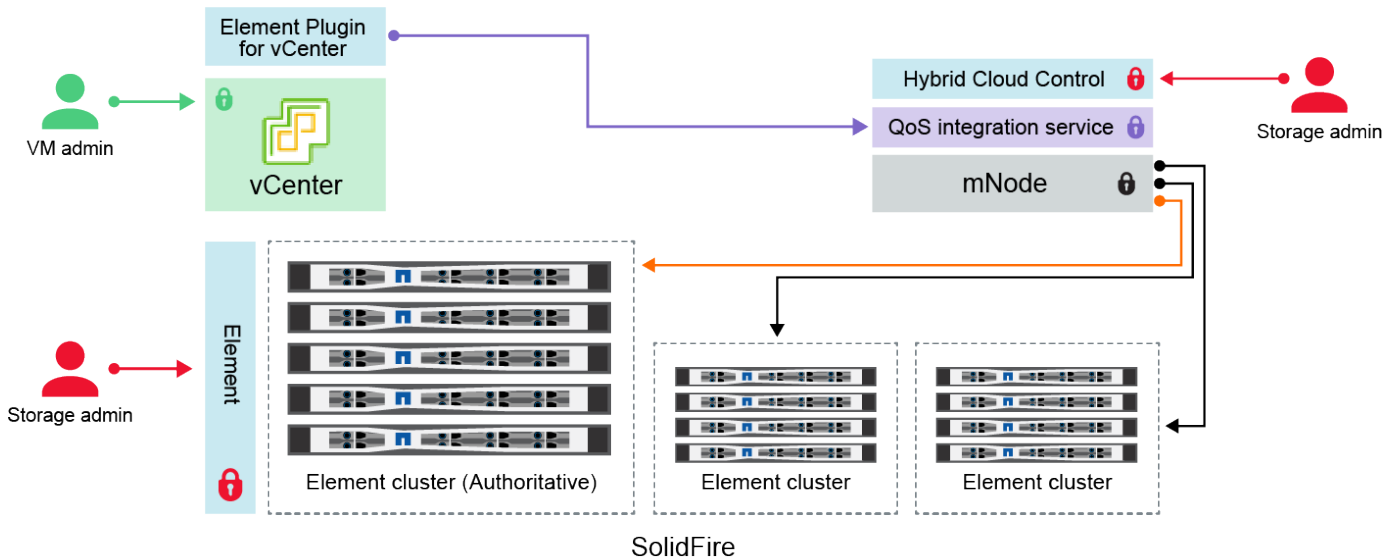
- ["Modificare le credenziali in NetApp HCI e NetApp SolidFire"](#)
- ["Modificare il certificato SSL predefinito del software Element"](#)
- ["Modificare la password IPMI per i nodi"](#)
- ["Abilitare l'autenticazione a più fattori"](#)
- ["Inizia a utilizzare la gestione esterna delle chiavi"](#)
- ["Creare un cluster che supporti i dischi 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 è generalmente parte delle procedure di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nell'implementazione.



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



Interazioni dei componenti NetApp
SolidFire:





- Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control
- Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode
- mNode and services use Element certificates to communicate with authoritative storage cluster
- mNode and services use Element administrative credentials for additional storage clusters
- Administrators use VMware vSphere Single Sign-on credentials to log into vCenter

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali dell'elemento 	<p>Applicabile a: NetApp HCI e SolidFire</p> <p>Gli amministratori utilizzano queste credenziali per accedere a:</p> <ul style="list-style-type: none"> • Interfaccia utente Element sul cluster di storage Element • Controllo del cloud ibrido sul nodo di gestione (mnode) <p>Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noto come <i>cluster autorevole</i> per cui è stato inizialmente configurato mnode. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se le credenziali per i cluster di storage aggiunti successivamente vengono modificate, le credenziali devono essere aggiornate anche in mnode utilizzando l'API mnode.</p>	<ul style="list-style-type: none"> • "Aggiornare le password di amministrazione del cluster di storage." • Aggiornare le credenziali di amministratore del cluster di storage in mnode utilizzando "API modifyclusteradmin".

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali vSphere Single Sign-on 	<p>Applicabile a: Solo NetApp HCI</p> <p>Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI, le credenziali vengono configurate nel motore di implementazione NetApp come segue:</p> <ul style="list-style-type: none"> • username@vsphere.local con la password specificata, e. • administrator@vsphere.local con la password specificata. <p>Quando si utilizza un vCenter esistente per implementare NetApp HCI, le credenziali di accesso singolo vSphere vengono gestite dagli amministratori IT VMware.</p>	<p>"Aggiornare le credenziali vCenter ed ESXi".</p>
Credenziali BMC (Baseboard Management Controller) 	<p>Applicabile a: Solo NetApp HCI</p> <p>Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di calcolo NetApp in un'implementazione NetApp HCI. BMC offre funzioni di base per il monitoraggio dell'hardware e la console virtuale.</p> <p>Le credenziali BMC (a volte denominate <i>IPMI</i>) per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con BMC nei nodi di calcolo durante gli aggiornamenti del firmware del nodo di calcolo.</p> <p>Quando le credenziali BMC vengono modificate, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate anche su mnode per mantenere tutte le funzionalità di controllo del cloud ibrido.</p>	<ul style="list-style-type: none"> • "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C, "Modificare la password IPMI predefinita". • Per i nodi H410S e H610S, "Modificare la password IPM predefinita". • "Modificare le credenziali BMC sul nodo di gestione".

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
<p>Credenziali ESXi</p> 	<p>Applicabile a: Solo NetApp HCI</p> <p>Gli amministratori possono accedere agli host ESXi utilizzando SSH o DCUI locale con un account root locale. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp.</p> <p>Le credenziali radice ESXi per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni 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 calcolo e i controlli dello stato.</p> <p>Quando le credenziali root di ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate su mnode per mantenere la funzionalità di controllo del cloud ibrido.</p>	<p>"Aggiorna le credenziali per gli host vCenter e ESXi".</p>
<p>Password di integrazione QoS</p> 	<p>Applicabile a: NetApp HCI e opzionale in SolidFire</p> <p>Non utilizzato dagli amministratori per gli accessi interattivi.</p> <p>L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite:</p> <ul style="list-style-type: none"> • Plug-in Element per vCenter Server e. • Servizio QoS su mnode. <p>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 o generata automaticamente durante l'implementazione di NetApp HCI.</p> <p>Nessun impatto su altri componenti.</p>	<p>"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server".</p> <p>Il plug-in NetApp Element per la password SIOC del server vCenter è noto anche come <i>password QoSSIOC</i>.</p> <p>Consulta l'articolo Element Plug-in for vCenter Server KB article.</p>

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali di vCenter Service Appliance 	<p>Applicabile a: NetApp HCI solo se configurato dal motore di implementazione NetApp</p> <p>Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. A seconda della versione di VMware vSphere implementata, alcuni amministratori del dominio di Single Sign-on di vSphere possono anche accedere all'appliance.</p> <p>Nessun impatto su altri componenti.</p>	Non sono necessarie modifiche.
Credenziali amministratore di NetApp Management Node 	<p>Applicabile a: NetApp HCI e opzionale in SolidFire</p> <p>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 attivato per impostazione predefinita.</p> <p>Nelle implementazioni NetApp HCI, il nome utente e la password sono stati specificati dall'utente durante l'installazione iniziale di tale nodo di calcolo nel motore di implementazione NetApp.</p> <p>Nessun impatto su altri componenti.</p>	Non sono necessarie modifiche.

Trova ulteriori informazioni

- ["Modificare il certificato SSL predefinito del software Element"](#)
- ["Modificare la password IPMI per i nodi"](#)
- ["Abilitare l'autenticazione a più fattori"](#)
- ["Inizia a utilizzare la gestione esterna delle chiavi"](#)
- ["Creare un cluster che supporti i dischi FIPS"](#)

Modificare il certificato SSL predefinito del software Element

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

Quando viene creato un cluster software NetApp Element, il cluster crea un certificato SSL (Secure Sockets Layer) con firma automatica e una chiave privata univoci 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 i certificati autofirmati e quelli emessi e verificati da un'autorità di certificazione (CA) attendibile.

È possibile utilizzare i seguenti metodi API per ottenere ulteriori informazioni sul certificato SSL predefinito e apportare modifiche.

- **GetSSLCertificate**

È possibile utilizzare ["Metodo GetSSLCertificate"](#) Per recuperare informazioni sul certificato SSL attualmente installato, inclusi tutti i dettagli del certificato.

- **SetSSLCertificate**

È possibile utilizzare ["Metodo SetSSLCertificate"](#) Per impostare i certificati SSL del cluster e per nodo in base al certificato e alla chiave privata fornita. Il sistema convalida il certificato e la chiave privata per impedire l'applicazione di un certificato non valido.

- **RemoveSSLCertificate**

Il ["Metodo RemoveSSLCertificate"](#) Rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una nuova chiave privata.



Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Tutti i nodi rimossi dal cluster tornano a un certificato autofirmato e tutte le informazioni di certificato e chiave definite dall'utente vengono rimosse dal nodo.

Trova ulteriori informazioni

- ["Modificare il certificato SSL predefinito del nodo di gestione"](#)
- ["Quali sono i requisiti relativi all'impostazione di certificati SSL personalizzati in Element Software?"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Modificare la password IPMI predefinita per i nodi

È possibile modificare la password di amministratore predefinita di Intelligent Platform Management Interface (IPMI) non appena si dispone dell'accesso remoto IPMI al nodo. Questa operazione potrebbe essere utile se sono stati rilevati aggiornamenti per l'installazione.

Per ulteriori informazioni sulla configurazione dell'accesso IPM per i nodi, vedere ["Configurare IPMI per ciascun 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 storage non appena si configura la porta di rete IPMI.

Di cosa hai bisogno

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Immettere il nome utente `ADMIN` e password `ADMIN` al prompt di login.
3. Una volta effettuato l'accesso, fare clic sulla scheda **Configuration** (Configurazione).
4. Fare clic su **utenti**.
5. Selezionare `ADMIN` e fare clic su **Modify User** (Modifica utente).
6. Selezionare la casella di controllo **Change Password** (Modifica password).
7. Immettere una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modify**, 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 storage non appena si configura la porta di rete IPMI.

Di cosa hai bisogno

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Immettere il nome utente `root` e password `calvin` al prompt di login.
3. Una volta effettuato l'accesso, fare clic 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 **Administrator** dall'elenco.
7. Attivare la casella di controllo **Change Password** (Modifica password).
8. Immettere una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Save** (Salva) nella parte inferiore della pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

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 il feedback.

- ["Visualizzare l'attività API"](#)
- ["Icone nell'interfaccia degli elementi"](#)
- ["Fornire un feedback"](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Visualizzare l'attività API

Il sistema Element utilizza l'API NetApp Element come base per le sue funzionalità e funzionalità. L'interfaccia utente di Element consente di visualizzare vari tipi di attività API in tempo reale sul sistema durante l'utilizzo dell'interfaccia. Con il log API, è possibile visualizzare l'attività API di sistema avviata dall'utente e in background, nonché le chiamate API effettuate nella pagina visualizzata.

È possibile utilizzare il log API per identificare i metodi API 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 di Element, fare clic su **API Log**.
2. Per modificare il tipo di attività API visualizzata nella finestra API Log (Registro API), attenersi alla seguente procedura:
 - a. Selezionare **Requests** per visualizzare il traffico delle richieste API.
 - b. Selezionare **Responses** per visualizzare il traffico di risposta API.
 - c. Filtrare i tipi di traffico API selezionando una delle seguenti opzioni:
 - **Avviato dall'utente**: Traffico API dalle attività durante questa sessione dell'interfaccia utente Web.
 - **Background polling**: Traffico API generato dall'attività di sistema in background.
 - **Pagina corrente**: Traffico API generato dalle attività sulla pagina che si sta visualizzando.

Trova ulteriori informazioni

- ["Gestione dello storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Frequenza di refresh dell'interfaccia influenzata dal carico del cluster

A seconda dei tempi di risposta delle API, il cluster potrebbe regolare automaticamente l'intervallo di aggiornamento dei dati per alcune parti della pagina del software NetApp Element che si sta visualizzando.








L'intervallo di refresh viene ripristinato ai valori predefiniti quando si ricarica la pagina nel browser. Per visualizzare l'intervallo di aggiornamento corrente, fare clic sul nome del cluster nell'angolo superiore destro della pagina. Si noti che l'intervallo controlla la frequenza con cui vengono effettuate le richieste API, non la velocità con cui i dati vengono ripristinati dal server.





Quando un cluster è sottoposto a un carico pesante, potrebbe mettere in coda le richieste API dall'interfaccia utente di Element. In rari casi, quando la risposta del sistema viene ritardata in modo significativo, ad esempio una connessione di rete lenta combinata con un cluster occupato, è possibile che l'utente venga disconnesso dall'interfaccia utente di Element se il sistema non risponde alle richieste API in coda in modo sufficientemente rapido. Se si viene reindirizzati alla schermata di disconnessione, è possibile effettuare nuovamente l'accesso dopo aver disperso qualsiasi richiesta iniziale di autenticazione del browser. Quando si torna alla pagina di panoramica, potrebbe essere richiesto di inserire le credenziali del cluster se non vengono salvate dal browser.

Icone nell'interfaccia degli elementi

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 riferimento rapido:

Icona	Descrizione
	Azioni
	Backup in
	Clonare o copiare
	Eliminare o eliminare
	Modifica
	Filtro
	Abbinare

	Aggiornare
	Ripristinare
	Ripristina da
	Eseguire il rollback
	Snapshot

Fornire un feedback

È possibile migliorare l'interfaccia utente Web del software Element e risolvere eventuali problemi dell'interfaccia utente utilizzando il modulo di feedback accessibile dall'interfaccia utente.

1. Da qualsiasi pagina dell'interfaccia utente di Element, fare clic sul pulsante **Feedback**.
2. Inserire le informazioni pertinenti nei campi Summary (Riepilogo) e Description (Descrizione).
3. Allegare eventuali screenshot utili.
4. Immettere un nome e un indirizzo e-mail.
5. Selezionare la casella di controllo per includere i dati relativi all'ambiente corrente.
6. Fare clic su **Invia**.

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire gli account

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai clienti di connettersi ai volumi di un cluster. Quando si crea un volume, questo viene assegnato a un account specifico. È inoltre possibile gestire gli account amministratore del cluster per un sistema storage SolidFire.

- ["Utilizzare gli account con CHAP"](#)
- ["Gestire gli account utente degli amministratori del cluster"](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Utilizzare gli account con CHAP

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi di un cluster. Un account contiene l'autenticazione CHAP (Challenge-Handshake Authentication Protocol) richiesta per accedere ai volumi 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.

Creare un account

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

Ogni nome account nel sistema deve essere univoco.

1. Selezionare **Gestione > account**.
2. Fare clic su **Create account** (Crea account).
3. Immettere 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.

- **Initiator Secret** per l'autenticazione della sessione del nodo CHAP.
 - **Target Secret** per l'autenticazione della sessione del nodo CHAP.
5. Fare clic su **Create account** (Crea account).

Visualizza i dettagli dell'account

È possibile visualizzare l'attività delle performance per i singoli account in un formato grafico.

Le informazioni del grafico forniscono informazioni di i/o e throughput per l'account. I livelli di attività medi e di picco sono indicati in incrementi di periodi di reporting 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 di un account.
3. Fare clic su **View Details** (Visualizza dettagli).

Di seguito sono riportati alcuni dettagli:

- **Status:** Lo stato dell'account. Valori possibili:
 - Attivo: Un account attivo.

- **Locked (bloccato):** Un account bloccato.
- **Rimosso:** Un account che è stato eliminato e rimosso.
- **Active Volumes** (volumi attivi): Il numero di volumi attivi assegnati all'account.
- **Compressione:** Il punteggio di efficienza della compressione per i volumi assegnati all'account.
- **Deduplica:** Il punteggio di efficienza della deduplica per i volumi assegnati all'account.
- **Thin Provisioning:** Il punteggio di efficienza del thin provisioning per i volumi assegnati all'account.
- **Efficienza complessiva:** Il punteggio di efficienza globale per i volumi assegnati all'account.

Modificare un account

È possibile modificare un account per modificare lo stato, i segreti CHAP o 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 improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettersi sempre dalle sessioni iSCSI che saranno interessate dalla modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato modifiche alle impostazioni dell'inziatore 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 di un account.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. **Opzionale:** modificare il **Nome utente**.
5. **Opzionale:** fare clic sull'elenco a discesa **Stato** e selezionare un altro stato.



Se si modifica lo stato su **Locked**, tutte le connessioni iSCSI all'account vengono terminate e l'account non è più accessibile. I volumi associati all'account vengono mantenuti; tuttavia, i volumi non sono rilevabili tramite iSCSI.

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



Se non si modificano le credenziali **CHAP Settings**, queste rimangono invariate. Se i campi delle credenziali vengono vuoti, il sistema genera nuove password.

7. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un account

È possibile eliminare un account quando non è più necessario.

Eliminare e rimuovere 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 dell'account che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire gli account utente degli amministratori del cluster

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

Tipi di account amministratore del cluster di storage

Esistono due tipi di account amministratore in un cluster di storage che esegue il software NetApp Element: l'account primario dell'amministratore del cluster e un account dell'amministratore del cluster.

- **Account primario amministratore del cluster**

Questo account amministratore viene creato al momento della creazione del cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo a un utente root in un sistema Linux. È possibile modificare la password per questo account amministratore.

- **Account amministratore del cluster**

È possibile assegnare a un account amministratore del cluster un intervallo limitato di accesso amministrativo 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 ed Element UI all'interno del sistema di storage.



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

Visualizzare i dettagli dell'amministratore del cluster

1. Per creare un account di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
 - a. Fare clic su **utenti > amministratori cluster**.

2. Nella pagina Cluster Admins della scheda Users (utenti), è possibile visualizzare le seguenti informazioni.

- **ID:** Numero sequenziale assegnato all'account dell'amministratore del cluster.
- **Username:** Il nome assegnato all'account dell'amministratore del cluster al momento della creazione.
- **Access:** Le autorizzazioni utente assegnate all'account utente. Valori possibili:
 - leggi
 - creazione di report
 - nodi
 - dischi
 - volumi
 - account
 - ClusterAdmins
 - amministratore



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

- **Type:** Il tipo di amministratore del cluster. Valori possibili:
 - Cluster
 - LDAP
- **Attributes:** Se l'account 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 software NetApp Element](#)".

Creare un account amministratore del cluster

È possibile creare nuovi account amministratore del cluster con autorizzazioni per consentire o limitare l'accesso a specifiche aree del sistema di storage. Quando si impostano le autorizzazioni dell'account amministratore del cluster, il sistema concede i diritti di sola lettura per 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.

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

In seguito, è possibile modificare i privilegi degli account amministratore del cluster per report, nodi, dischi, volumi, account, e 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.

È inoltre possibile rimuovere in seguito 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 di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
 - a. Fare clic su **utenti > amministratori cluster**.

- b. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
 - c. Selezionare il tipo di utente **Cluster**.
 - d. Immettere un nome utente e una password per l'account e confermare la password.
 - e. Selezionare 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 **Create Cluster Admin** (Crea amministratore cluster).
2. Per creare un account amministratore del cluster nella directory LDAP, eseguire le seguenti operazioni:
- a. Fare clic su **Cluster > LDAP**.
 - b. Assicurarsi che l'autenticazione LDAP sia attivata.
 - c. Fare clic su **Test User Authentication** (verifica 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 un secondo momento.
 - d. Fare clic su **utenti > amministratori cluster**.
 - e. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
 - f. Selezionare il tipo di utente LDAP.
 - g. Nel campo Distinguished Name (Nome distinto), seguire l'esempio nella casella di testo per immettere un nome distinto completo per l'utente o il gruppo. In alternativa, incollarlo dal nome distinto precedentemente copiato.

Se il nome distinto fa parte di un gruppo, tutti gli utenti che fanno parte di tale gruppo sul server LDAP disporranno delle autorizzazioni per questo account admin.

Per aggiungere utenti o gruppi amministratori cluster LDAP, il formato generale del nome utente è "LDAP:<Full Distinguished Name>".

- a. Selezionare 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 **Create Cluster Admin** (Crea amministratore cluster).

Modificare le autorizzazioni di amministratore del cluster

È possibile modificare i privilegi dell'account amministratore del cluster per report, nodi, dischi, volumi, account, e 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 Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Selezionare le autorizzazioni utente da applicare all'account.
5. Fare clic su **Save Changes** (Salva modifiche).

Modificare le password per gli account amministratore del cluster

È possibile utilizzare l'interfaccia utente Element per modificare le password dell'amministratore del cluster.

1. Fare clic su **utenti > amministratori cluster**.
2. Fare clic sull'icona Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Nel campo Change Password (Modifica password), immettere una nuova password e confermarla.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- ["Abilitare l'autenticazione LDAP con l'interfaccia utente Element"](#)
- ["Disattiva LDAP"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire LDAP

È possibile impostare il protocollo LDAP (Lightweight Directory Access Protocol) per abilitare la funzionalità di accesso sicura e 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 indirizzi IPv4 e IPv6.

L'abilitazione di LDAP prevede le seguenti procedure di alto livello, descritte in dettaglio:

1. **Completare la procedura di preconfigurazione per il supporto LDAP.** Verificare di disporre di tutti i dettagli necessari per configurare l'autenticazione LDAP.
2. **Attiva 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 GetLdapConfiguration API o controllando la configurazione LDAP utilizzando l'interfaccia utente Element.
4. **Verificare l'autenticazione LDAP** (con il `readonly` utente). Verificare che la configurazione LDAP sia corretta eseguendo il metodo TestLdapAuthentication API o utilizzando l'interfaccia utente Element. Per questo test iniziale, utilizzare il nome utente "sAMAccountName" di `readonly` utente. In questo modo, il cluster viene convalidato per verificare che sia configurato correttamente per l'autenticazione LDAP `readonly` le credenziali e l'accesso sono corretti. Se questo passaggio non riesce, ripetere i passi da 1 a 3.
5. **Verificare l'autenticazione LDAP** (con un account utente che si desidera aggiungere). Ripetere il setp 4 con un account utente che si desidera aggiungere come amministratore del cluster di elementi. Copiare il `distinguished` Nome (DN) o l'utente (o il gruppo). Questo DN verrà utilizzato nella fase 6.
6. **Aggiungere l'amministratore del cluster LDAP** (copiare e incollare il DN dalla fase 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, incollare il DN completo copiato al punto 5. In questo modo si garantisce che il DN sia formattato correttamente.
7. **Verificare l'accesso dell'amministratore del cluster.** Accedere al cluster utilizzando l'utente amministratore del cluster LDAP appena creato. Se è stato aggiunto un gruppo LDAP, è possibile

effettuare l'accesso come qualsiasi utente del gruppo.

Completare la procedura di preconfigurazione per il supporto LDAP

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

Fasi

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

Abilitare l'autenticazione LDAP con l'interfaccia utente Element

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

È possibile configurare LDAP con l'interfaccia utente Element o 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 in uso `SearchAndBind` come tipo di autenticazione. Nell'esempio viene utilizzato un singolo Windows Server 2012 R2 Active Directory Server.

Fasi

1. Fare clic su **Cluster > LDAP**.
2. Fare clic su **Si** per attivare l'autenticazione LDAP.
3. Fare clic su **Aggiungi un server**.
4. Inserire il campo **host Name/IP Address** (Nome host/Indirizzo IP).



È inoltre possibile inserire un numero di porta personalizzato opzionale.

Ad esempio, per aggiungere un numero di porta personalizzato, immettere <host name or ip address>:<port number>

5. **Opzionale:** selezionare **Usa protocollo LDAPS**.
6. Inserire le informazioni richieste in **Impostazioni generali**.

LDAP Servers

Host Name/IP Address	<input type="text" value="192.168.9.99"/>	Remove
	<input type="checkbox"/> Use LDAPS Protocol	

[Add a Server](#)

General Settings

Auth Type	<input type="text" value="Search and Bind"/>	▼
Search Bind DN	<input type="text" value="msmyth@thesmyths.ca"/>	
Search Bind Password	<input type="text" value="e.g. password"/>	<input type="checkbox"/> Show password
User Search Base DN	<input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/>	
User Search Filter	<input type="text" value="(&(objectClass=person)((sAMAccountName=%USER"/>	
Group Search Type	<input type="text" value="Active Directory"/>	▼
Group Search Base DN	<input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/>	

[Save Changes](#)

7. Fare clic su **Enable LDAP** (attiva LDAP).
8. Fare clic su **Test User Authentication** (verifica autenticazione utente) per verificare l'accesso al server per un utente.
9. Copiare il nome distinto e le informazioni del gruppo di utenti che verranno visualizzate in seguito per la creazione degli amministratori del cluster.
10. Fare clic su **Save Changes** (Salva modifiche) per salvare le nuove impostazioni.
11. Per creare un utente in questo gruppo in modo che chiunque possa effettuare l'accesso, attenersi alla seguente procedura:
 - a. Fare clic su **utente** > **Visualizza**.

Create a New Cluster Admin

Select User Type

Cluster LDAP

Enter User Details

Distinguished Name

CN=StorageAdmins,OU=Home
users,DC=thesmyths,DC=ca

Select User Permissions

- | | |
|------------------------------------|--|
| <input type="checkbox"/> Reporting | <input type="checkbox"/> Volumes |
| <input type="checkbox"/> Nodes | <input type="checkbox"/> Accounts |
| <input type="checkbox"/> Drives | <input type="checkbox"/> Cluster Admin |

Accept the Following End User License Agreement

- Per il nuovo utente, fare clic su **LDAP** per tipo utente e incollare il gruppo copiato nel campo Nome distinto.
- Selezionare le autorizzazioni, in genere tutte le autorizzazioni.
- Scorrere verso il basso fino al Contratto di licenza con l'utente finale e fare clic su **Accetto**.
- Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

Ora si dispone di un utente con il valore di un gruppo Active Directory.

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Abilitare l'autenticazione LDAP con l'API Element

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

È possibile configurare LDAP con l'interfaccia utente Element o l'API Element. Questa procedura descrive

come configurare LDAP utilizzando l'API Element.

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

Fasi

1. Attivare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.
2. Inserire 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	Indica che il cluster utilizzerà l'account di servizio di sola lettura per cercare prima l'utente autenticato e successivamente associare tale utente, se trovato e autenticato.
GroupSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca dei gruppi. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.

Parametri utilizzati	Descrizione
UserSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca degli utenti. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.
GroupSearchType: ActiveDirectory	Utilizza il server Windows Active Directory come server LDAP.
<pre>userSearchFilter: " (&(objectClass=person) (sAMAccountName=%USERNAME%)) "</pre> <p>Per utilizzare userPrincipalName (indirizzo e-mail per l'accesso), è possibile modificare userSearchFilter in:</p> <pre>" (&(objectClass=person) (userPrincipalName=%USERNAME%)) "</pre> <p>In alternativa, per eseguire ricerche in userPrincipalName e sAMAccountName, è possibile utilizzare il seguente userSearchFilter:</p> <pre>" (&(objectClass=person) (</pre>	(SAMAccountName=%NOME UTENTE%)(userPrincipalName=%NOME UTENTE%)" ----
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
Si tratta del nome distinto dell'utente di sola lettura che verrà utilizzato per cercare nella directory LDAP. Per Active directory è generalmente più semplice utilizzare userPrincipalName (formato indirizzo email) per l'utente.	SearchBindPassword

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Visualizza i dettagli LDAP

Visualizzare le informazioni LDAP nella pagina LDAP della scheda Cluster.



Per visualizzare queste impostazioni di configurazione LDAP, è necessario attivare LDAP.

1. Per visualizzare i dettagli LDAP con l'interfaccia utente Element, fare clic su **Cluster > LDAP**.

- **Host Name/IP Address** (Nome host/Indirizzo IP): Indirizzo di un server di directory LDAP o LDAPS.
- **Auth Type**: Il metodo di autenticazione dell'utente. Valori possibili:
 - Binding diretto
 - Ricerca e binding
- **Search Bind DN**: DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP dell'utente (richiede l'accesso a livello di bind alla directory LDAP).
- **Search Bind Password**: Password utilizzata per autenticare l'accesso al server LDAP.
- **User Search base DN** (DN base ricerca utente): Il DN di base della struttura utilizzata per avviare la ricerca dell'utente. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
- **User Search Filter** (filtro di ricerca utente): Immettere quanto segue utilizzando il nome di dominio:

```
(&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERN  
AME%)))
```
- **Group Search Type** (tipo ricerca gruppo): Tipo di ricerca che controlla il filtro di ricerca gruppo predefinito utilizzato. Valori possibili:
 - Active Directory: Appartenenza nidificata a tutti i gruppi LDAP di un utente.
 - No Groups (Nessun gruppo): Nessun supporto di gruppo.
 - DN membro: Gruppi di membri in stile DN (livello singolo).
- **Group Search base DN**: Il DN di base della struttura utilizzata per avviare la ricerca di gruppo. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
- **Test User Authentication** (verifica autenticazione utente): Una volta configurato LDAP, utilizzare questa opzione per verificare l'autenticazione del nome utente e della password per il server LDAP. Immettere un account già esistente per eseguire il test. Vengono visualizzate le informazioni distinte relative al nome e al gruppo di utenti, che è possibile copiare per l'utilizzo successivo durante la creazione degli amministratori del cluster.

Verificare la configurazione LDAP

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

Fasi

1. Per verificare la configurazione LDAP con l'interfaccia utente Element, procedere come segue:
 - a. Fare clic su **Cluster > LDAP**.
 - b. Fare clic su **Test autenticazione LDAP**.
 - c. Risolvere eventuali problemi utilizzando le informazioni riportate nella tabella seguente:

Messaggio di errore	Descrizione
xLDAPUserNotFound	<ul style="list-style-type: none"> L'utente sottoposto a test non è stato trovato nella configurazione <code>userSearchBaseDN</code> sottostruttura. Il <code>userSearchFilter</code> non è configurato correttamente.
xLDAPBindFailed (Error: Invalid credentials)	<ul style="list-style-type: none"> Il nome utente sottoposto a test è un utente LDAP valido, ma la password fornita non è corretta. Il nome utente sottoposto a test è un utente LDAP valido, ma l'account è attualmente disattivato.
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 <code>userSearchBaseDN</code> Non è una posizione valida all'interno della struttura LDAP.
xLDAPSearchFailed (Error: Referral)	<ul style="list-style-type: none"> Il <code>userSearchBaseDN</code> Non è una posizione valida all'interno della struttura LDAP. Il <code>userSearchBaseDN</code> e <code>groupSearchBaseDN</code> Si trovano in un'unità organizzativa nidificata. Ciò può causare problemi di autorizzazione. La soluzione è includere l'unità organizzativa nelle voci DN di base dell'utente e del gruppo, ad esempio: <code>ou=storage, cn=company, cn=com</code>

2. Per verificare la configurazione LDAP con l'API Element, procedere come indicato di seguito:

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 di gruppi a 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"
  }
}

```

Disattiva LDAP

È possibile disattivare l'integrazione LDAP utilizzando l'interfaccia utente Element.

Prima di iniziare, prendere nota di tutte le impostazioni di configurazione, poiché la disattivazione di LDAP cancella tutte le impostazioni.

Fasi

1. Fare clic su **Cluster > LDAP**.
2. Fare clic su **No**.
3. Fare clic su **Disable LDAP** (Disattiva LDAP).

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire il sistema

È possibile gestire il sistema nell'interfaccia utente di Element. Ciò include l'abilitazione dell'autenticazione a più fattori, la gestione delle impostazioni del cluster, il supporto degli

standard FIPS (Federal Information Processing Standards) e l'utilizzo della gestione esterna delle chiavi.

- ["Abilitare l'autenticazione a più fattori"](#)
- ["Configurare le impostazioni del cluster"](#)
- ["Creare un cluster che supporti i dischi FIPS"](#)
- ["Inizia a utilizzare la gestione esterna delle chiavi"](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Abilitare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) utilizza un provider di identità (IdP) di terze parti tramite il linguaggio SAML (Security Assertion Markup Language) per gestire le sessioni utente. MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, come password e SMS, password e messaggi di posta elettronica.

Impostare l'autenticazione a più fattori

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 sono disponibili nella ["Riferimento API dell'elemento"](#).

1. Creare una nuova configurazione IdP (Identity Provider) 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 da IdP di terze parti. Questi metadati devono essere validati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni del formatter JSON, ad esempio: <https://freeformatter.com/json-escape.html>.

2. Recuperare i metadati del cluster, tramite `spMetadataUrl`, da copiare 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 IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull'IdP di terze parti in modo che includa l'attributo "NameID" per identificare in modo univoco un utente per la registrazione dell'audit e per il corretto funzionamento della disconnessione singola.
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 attributo SAML per l'effetto desiderato, come mostrato negli esempi seguenti:

- Email=[bob@company.com](#) — dove IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
- Group=cluster-Administrator - dove IdP è configurato per rilasciare una proprietà di gruppo in cui tutti gli utenti devono avere accesso. Tenere presente che l'associazione nome attributo/valore SAML è sensibile alla distinzione tra maiuscole e minuscole per motivi di sicurezza.

5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Ulteriori informazioni per l'autenticazione a più fattori

È necessario conoscere le seguenti avvertenze relative all'autenticazione a più fattori.

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



Se il cluster utilizza un certificato precedente all'aggiornamento a meno di 2048 bit, il certificato del cluster deve essere aggiornato con un certificato a 2048 bit o superiore dopo l'aggiornamento all'elemento 12.0 o successivo.

- 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). Aggiungere utenti amministratori cluster LDAP o utenti amministratori cluster locali se si desidera creare utenti con queste funzionalità.

Trova ulteriori informazioni

- ["Gestione dello storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Configurare le impostazioni del cluster

È possibile visualizzare e modificare le impostazioni a livello di cluster ed eseguire attività specifiche del cluster dalla scheda Cluster dell'interfaccia utente di Element.

È possibile configurare impostazioni come la soglia di fullness del cluster, l'accesso al supporto, la crittografia a riposo, i volumi virtuali, SnapMirror, E NTP broadcast client.

Opzioni

- [Lavorare con volumi virtuali](#)
- [Utilizzare la replica SnapMirror tra cluster Element e ONTAP](#)
- [Impostare la soglia completa del cluster](#)

- [Abilitare e disabilitare l'accesso al supporto](#)
- ["Come vengono calcolate le soglie blockSpace per l'elemento"](#)
- [Attivare e disattivare la crittografia per un cluster](#)
- [Gestire il banner Termini di utilizzo](#)
- [Configurare i server Network Time Protocol per il cluster da interrogare](#)
- [Gestire SNMP](#)
- [Gestire i dischi](#)
- [Gestire i nodi](#)
- [Gestire le reti virtuali](#)
- [Visualizza i dettagli delle porte Fibre Channel](#)

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Attivare e disattivare la crittografia a riposo per un cluster

Con i cluster SolidFire, è possibile crittografare tutti i dati inattivi memorizzati sui dischi del cluster. È possibile abilitare la protezione a livello di cluster dei dischi con crittografia automatica (SED) utilizzando entrambi ["crittografia basata su hardware o software a riposo"](#).

È possibile attivare la crittografia hardware a riposo utilizzando l'interfaccia utente o l'API Element. L'attivazione della funzione di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile attivare la crittografia software a riposo utilizzando solo l'API Element.

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



Per i cluster di storage all-flash SolidFire, la crittografia software a riposo deve essere attivata durante la creazione del cluster e non può essere disattivata dopo la creazione del cluster.

Di cosa hai bisogno

- Si dispone dei privilegi di amministratore del cluster per attivare o modificare le impostazioni di crittografia.
- Per la crittografia basata su hardware a riposo, è stato garantito che il cluster sia in buono stato prima di modificare le impostazioni di crittografia.
- Se si disattiva la crittografia, due nodi devono partecipare a un cluster per accedere alla chiave e disattivare la crittografia su un disco.

Controllare la crittografia nello stato di riposo

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare ["GetClusterInfo"](#) metodo. È possibile utilizzare ["GetSoftwareEncryptionAtRestInfo"](#) metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi.



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

Opzioni

- [Abilitare la crittografia basata su hardware a riposo](#)
- [Abilitare la crittografia basata su software a riposo](#)
- [Disattiva la crittografia basata su hardware a riposo](#)

Abilitare la crittografia basata su hardware a riposo



Per attivare la crittografia a riposo utilizzando una configurazione di gestione delle chiavi esterna, è necessario attivare la crittografia a riposo tramite "API". L'abilitazione mediante il pulsante Element UI esistente tornerà a utilizzare chiavi generate internamente.

1. Dall'interfaccia utente di Element, selezionare **Cluster > Settings**.
2. Selezionare **Enable Encryption at REST (attiva crittografia a riposo)**.

Abilitare la crittografia basata su software a riposo



La crittografia software a riposo non può essere disattivata dopo che è stata attivata sul cluster.

1. Durante la creazione del cluster, eseguire "[creare il metodo del cluster](#)" con `enableSoftwareEncryptionAtRest` impostare su `true`.

Disattiva la crittografia basata su hardware a riposo

1. Dall'interfaccia utente di Element, selezionare **Cluster > Settings**.
2. Selezionare **Disattiva crittografia a riposo**.

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

Impostare la soglia completa del cluster

È possibile modificare il livello con cui il sistema genera un avviso di riempimento del cluster a blocchi seguendo la procedura riportata di seguito. Inoltre, è possibile utilizzare il metodo dell'API `ModifyClusterFullThreshold` per modificare il livello con cui il sistema genera un avviso di blocco o metadati.

Di cosa hai bisogno

È necessario disporre dei privilegi di amministratore del cluster.

Fasi

1. Fare clic su **Cluster > Settings**.
2. Nella sezione Cluster Full Settings (Impostazioni cluster complete), inserire una percentuale in **Raise a warning alert when `_`% Capacity remains before Helix not recovery from a node failure** (Invia un avviso quando la capacità del `_`% rimane prima che Helix non possa

3. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

["Come vengono calcolate le soglie blockSpace per l'elemento"](#)

Abilitare e disabilitare 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 > Settings**.
2. Nella sezione Enable / Disable Support Access (attiva/Disattiva accesso al supporto), immettere la durata (in ore) per la quale si desidera consentire l'accesso al supporto.
3. Fare clic su **Enable Support Access** (attiva accesso supporto).
4. **Opzionale:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestire il banner Termini di utilizzo

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

Opzioni

[Attivare il banner Termini di utilizzo](#) [Modificare il banner Termini di utilizzo](#) [Disattiva il banner Termini di utilizzo](#)

Attivare il banner Termini di utilizzo

È possibile attivare un banner Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente fa clic sul banner, viene visualizzata una finestra di dialogo contenente il messaggio configurato per il cluster. Il banner può essere ignorato in qualsiasi momento.

Per attivare 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**, inserire il testo da visualizzare nella finestra di dialogo Termini di utilizzo.



Non superare i 4096 caratteri.

3. Fare clic su **Enable** (attiva).

Modificare il banner Termini di utilizzo

Puoi modificare il testo visualizzato dall'utente quando seleziona il banner di accesso Termini di utilizzo.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.
- Assicurarsi che la funzione Termini di utilizzo sia attivata.

Fasi

1. Fare clic su **utenti > Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modificare il testo che si desidera visualizzare.



Non superare i 4096 caratteri.

3. Fare clic su **Save Changes** (Salva modifiche).

Disattiva il banner Termini di utilizzo

È possibile disattivare il banner Termini di utilizzo. Con il banner disattivato, non viene più richiesto all'utente di accettare i termini di utilizzo quando si utilizza l'interfaccia utente di Element.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.
- Assicurarsi che le condizioni d'uso siano attivate.

Fasi

1. Fare clic su **utenti > Termini di utilizzo**.
2. Fare clic su **Disable** (Disattiva).

Impostare Network Time Protocol

L'impostazione del protocollo NTP (Network Time Protocol) può essere eseguita in due modi: Istruire ciascun nodo di un cluster a rimanere in attesa delle trasmissioni o richiedere a ciascun nodo di eseguire una query su un server NTP per gli aggiornamenti.

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

Configurare i server Network Time Protocol per il cluster da interrogare

È possibile richiedere a ciascun nodo di un cluster di eseguire query su un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede informazioni NTP.

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, non è sempre possibile stabilire una connessione a questo sito a seconda della posizione fisica del cluster SolidFire.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di storage siano state configurate e operative. A tale scopo, configurare i server DNS su ogni nodo di storage e assicurarsi che le porte siano aperte consultando la pagina requisiti della porta di rete.

È possibile inserire fino a cinque server NTP diversi.



È possibile utilizzare indirizzi IPv4 e IPv6.

Di cosa hai bisogno

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

Fasi

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 > Settings**.
4. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **No**, che utilizza la configurazione NTP standard.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Configurare il cluster in modo che sia in attesa di trasmissioni NTP

Utilizzando la modalità di trasmissione, è possibile impostare ciascun nodo di un cluster in modo che ascolti sulla rete i messaggi di trasmissione NTP (Network Time Protocol) provenienti da un determinato server.

Di cosa hai bisogno

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

Fasi

1. Fare clic su **Cluster > Settings**.
2. Inserire il server NTP o i server che utilizzano la modalità di trasmissione nell'elenco dei server.
3. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **Yes** (Sì) per utilizzare un client di trasmissione.
4. Per impostare il client di trasmissione, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire 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 del modello di protezione basato sull'utente SNMP e configurare i trap per monitorare il cluster SolidFire. È inoltre possibile visualizzare e accedere ai file della base di informazioni di gestione.



È possibile utilizzare indirizzi IPv4 e 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 attivare o disattivare SNMP. Dopo aver attivato SNMP, è possibile scegliere la versione da utilizzare. Se si utilizza la versione 2, è possibile aggiungere i requestori e, se si utilizza la versione 3, è possibile configurare gli utenti USM.

- **SNMP Trap Settings** (Impostazioni trap SNMP)

È possibile identificare le trap che si desidera acquisire. È possibile impostare l'host, la porta e la stringa di comunità per ciascun destinatario del trap.

Configurare un richiedente SNMP

Quando SNMP versione 2 è attivato, è possibile attivare o disattivare un richiedente e configurare i requestori per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster > SNMP**.
2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 2** (versione 2).
4. Nella sezione **Requestori**, inserire le informazioni **stringa di comunità e rete**.



Per impostazione predefinita, la stringa di comunità è pubblica e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Opzionale:** per aggiungere un altro richiedente, fare clic su **Aggiungi richiedente** e immettere le informazioni **stringa di comunità e rete**.
6. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- [Configurare i trap SNMP](#)
- [Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione](#)

Configurare un utente SNMP USM

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

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

2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 3** (versione 3).
4. Nella sezione **utenti USM**, immettere il nome, la password e la passphrase.
5. **Opzionale:** per aggiungere un altro utente USM, fare clic su **Aggiungi utente USM** e inserire il nome, la password e la passphrase.
6. Fare clic su **Save Changes** (Salva modifiche).

Configurare i trap SNMP

Gli amministratori di sistema possono utilizzare i trap SNMP, definiti anche notifiche, per monitorare lo stato del cluster SolidFire.

Quando i trap SNMP sono attivati, il cluster SolidFire genera trap associati alle voci del registro eventi e agli avvisi di sistema. Per ricevere notifiche SNMP, è necessario scegliere i trap da generare e identificare i destinatari delle informazioni trap. Per impostazione predefinita, non viene generato alcun trap.

1. Fare clic su **Cluster > SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
 - Trap di guasti del cluster
 - Trap di guasti risolti nel cluster
 - Trap di eventi del cluster
3. Nella sezione **destinatari trap**, immettere le informazioni relative a host, porta e community string per un destinatario.
4. **Opzionale:** Per aggiungere un altro destinatario trap, fare clic su **Aggiungi destinatario trap** e immettere le informazioni relative a host, porta e stringa di comunità.
5. Fare clic su **Save Changes** (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 dei volumi
- Volumi per statistiche account
- Statistiche dei nodi
- Altri dati, ad esempio report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente gli access point di livello superiore (OID) per i prodotti SF-Series.

Fasi

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

2. In **MIB SNMP**, fare clic sul file MIB che si desidera scaricare.
3. Nella finestra di download risultante, aprire o salvare il file MIB.

Gestire i dischi

Ogni nodo contiene uno o più dischi fisici utilizzati per memorizzare una parte dei dati per il cluster. Il cluster utilizza la capacità e le prestazioni del disco dopo che il disco è stato aggiunto correttamente a un cluster. È possibile utilizzare l'interfaccia utente Element per gestire i dischi.

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Dettagli sui dischi

La pagina Drives (unità) della scheda Cluster (cluster) fornisce un elenco dei dischi attivi nel cluster. È possibile filtrare la pagina selezionando dalle 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 dischi non assegnati a un cluster ed elencati nella scheda Available (disponibili) dopo la creazione di un nuovo cluster SolidFire.

I seguenti elementi vengono visualizzati nell'elenco dei dischi attivi.

- **ID unità**

Il numero sequenziale assegnato al disco.

- **ID nodo**

Il numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

Il nome del nodo che ospita l'unità.

- **Slot**

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

- **Capacità**

Le dimensioni del disco, in GB.

- **Seriale**

Il numero di serie del disco.

- **Usura residua**

L'indicatore del livello di usura.

Il sistema storage indica la quantità approssimativa di usura disponibile su ogni disco a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un disco che ha consumato il 5% dei cicli di scrittura e cancellazione progettati riporta il 95% di usura rimanente. Il sistema non aggiorna automaticamente le informazioni sull'usura del disco; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

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

Gestire i nodi

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

Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato un guasto appropriato del cluster.

Trova ulteriori informazioni

[Aggiungere un nodo a un cluster](#)

Aggiungere un nodo a un cluster

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

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

È possibile aggiungere nodi di capacità inferiore o superiore 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 spostare i dati in modo da lasciare spazio sufficiente in caso di guasto di uno dei nodi più grandi. È possibile aggiungere capacità di nodo inferiori a un cluster di nodi più grande per migliorare le performance.



Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato l'errore del cluster strandedCapacity.

["Video di NetApp: Scalabilità in base ai termini: Espansione di un cluster SolidFire"](#)

È possibile aggiungere nodi alle appliance NetApp HCI.

Fasi

1. Selezionare **Cluster > Nodes**.
2. Fare clic su **Pending** (in sospeso) per visualizzare l'elenco dei nodi in sospeso.

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 Pending Active (attivo in sospeso).

SolidFire installa la versione software Element del cluster sui nodi in sospeso quando vengono aggiunti a un cluster. L'operazione potrebbe richiedere alcuni minuti.

3. Effettuare una delle seguenti operazioni:
 - Per aggiungere singoli nodi, fare clic sull'icona **azioni** del nodo che si desidera aggiungere.
 - Per aggiungere più nodi, selezionare la casella di controllo dei nodi da aggiungere, quindi **azioni in blocco**. **Nota:** se il nodo che si sta 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. Una volta aggiornato, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo si trova in uno stato Active pendingActive.
4. Fare clic su **Aggiungi**.

Il nodo viene visualizzato nell'elenco dei nodi attivi.

Trova ulteriori informazioni

[Versione e compatibilità dei nodi](#)

Versione e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione software di Element installata su un nodo. I cluster di storage basati su software Element imbasano automaticamente un'immagine di un nodo alla versione software Element sul cluster se il nodo e il cluster non sono compatibili.

Il seguente elenco descrive i livelli di importanza delle release software che compongono il numero di versione del software Element:

- **Maggiore**

Il primo numero indica una versione 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 può essere creato un cluster con nodi con versioni principali miste.

- **Minore**

Il secondo numero indica funzionalità software più piccole o miglioramenti alle funzionalità software esistenti che sono state aggiunte a una release principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa release incrementale non è compatibile con altre release incrementali di software elemento con un componente minore 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 software dell'elemento rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0 e 11.0.2 con 11.0.3.

I numeri di versione principali e secondari devono corrispondere per la compatibilità. I micro numeri non devono corrispondere per la compatibilità.

Capacità del cluster in un ambiente a nodi misti

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

La serie H è composta da nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi sono entrambi compatibili con 10 GbE e 25 GbE.

Si consiglia di non mischiare nodi non crittografati e crittografati. In un cluster a nodi misti, nessun nodo può superare il 33% 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 SF-Series 9605. La soglia di capacità del cluster viene calcolata in base alla potenziale perdita del nodo più grande in questa situazione.

A partire da Element 12.0, i seguenti nodi storage della serie SF non sono supportati:

- SF3010
- SF6010
- SF9010

Se si aggiorna uno di questi nodi di storage all'elemento 12.0, viene visualizzato un errore che indica che questo nodo non è supportato dall'elemento 12.0.

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio i tag di servizio, i dettagli dei dischi e la grafica per l'utilizzo e le statistiche dei dischi. La pagina nodi della scheda Cluster fornisce la colonna Version (versione) in cui è possibile visualizzare la versione software di ciascun nodo.

Fasi

1. Fare clic su **Cluster > Nodes**.
2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **azioni** di un nodo.
3. Fare clic su **View Details** (Visualizza dettagli).
4. Esaminare i dettagli del nodo:
 - **Node ID**: L'ID generato dal sistema per il nodo.
 - **Node Name** (Nome nodo): Il nome host del nodo.
 - **IOPS 4k disponibili**: Gli IOPS configurati per il nodo.
 - **Node role**: Ruolo del nodo nel cluster. Valori possibili:
 - Cluster Master: Nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
 - Ensemble Node: Nodo che partecipa al cluster. Esistono 3 o 5 nodi di ensemble a seconda delle

dimensioni del cluster.

- Fibre Channel: Un nodo nel cluster.
- **Node Type:** Il tipo di modello del nodo.
- **Active Drives:** Il numero di dischi attivi nel nodo.
- **IP di gestione:** L'indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione della rete da 1 GbE o 10 GbE.
- **Cluster IP:** L'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi dello stesso cluster.
- **Storage IP:** L'indirizzo IP (SIP) dello storage assegnato al nodo utilizzato per il rilevamento della rete iSCSI e per tutto il traffico della rete dati.
- **Management VLAN ID** (ID VLAN di gestione): L'ID virtuale per la rete locale di gestione.
- **Storage VLAN ID:** L'ID virtuale per la rete locale di storage.
- **Version:** La versione del software in esecuzione su ciascun nodo.
- **Replication Port** (porta di replica): La porta utilizzata sui nodi per la replica remota.
- **Service Tag:** Numero di service tag univoco assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

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

Consente di visualizzare informazioni sulle porte Fibre Channel collegate al cluster.

Fasi

1. Fare clic su **Cluster > FC Ports**.
2. Per filtrare le informazioni in questa pagina, fare clic su **Filter** (filtro).
3. Leggi i dettagli:
 - **Node ID:** Il nodo che ospita la sessione per la connessione.
 - **Node Name:** Nome del nodo generato dal sistema.
 - **Slot:** Numero dello slot in cui si trova la porta Fibre Channel.
 - **HBA Port:** Porta fisica sull'HBA (host bus adapter) Fibre Channel.
 - **WWNN:** Il nome del nodo mondiale.
 - **WWPN:** Il nome della porta universale di destinazione.
 - **Switch WWN:** Nome mondiale dello switch Fibre Channel.
 - **Port state** (Stato porta): Stato corrente della porta.
 - **NID porta:** L'ID della porta del nodo sul fabric Fibre Channel.
 - **Speed:** La velocità negoziata di Fibre Channel. I valori possibili sono i seguenti:
 - 4 Gbps
 - 8 Gbps
 - 16 Gbps

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire le reti virtuali

Il networking virtuale nello storage SolidFire consente di connettere il traffico tra più client su reti logiche separate a un cluster. Le connessioni al cluster vengono separate nello stack di rete attraverso l'utilizzo del tagging VLAN.

Trova ulteriori informazioni

- [Aggiungere una rete virtuale](#)
- [Abilitare il routing e l'inoltro virtuale](#)
- [Modificare una rete virtuale](#)
- [Modificare le VLAN VRF](#)
- [Eliminare una rete virtuale](#)

Aggiungere una rete virtuale

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

Di cosa hai bisogno

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



Per questa configurazione, è necessario prendere in considerazione i seguenti criteri:

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

Quando viene aggiunta una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascun nodo richiede un indirizzo IP della rete virtuale. Il numero di indirizzi IP specificati durante la creazione di una nuova rete virtuale deve essere uguale o superiore al numero di nodi nel cluster. Gli indirizzi delle reti virtuali vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi nel cluster.

Fasi

1. Fare clic su **Cluster > Network**.
2. Fare clic su **Create VLAN** (Crea VLAN).
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:

- **Nome VLAN**
 - **Tag VLAN**
 - **SVIP**
 - **Netmask**
 - (Facoltativo) **Descrizione**
4. Inserire l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **blocchi di indirizzi IP**.
 5. Inserire **Size** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
 6. Fare clic su **Add a block** (Aggiungi un blocco) per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
 7. Fare clic su **Create VLAN** (Crea VLAN).

Visualizza i dettagli della rete virtuale

Fasi

1. Fare clic su **Cluster > Network**.
2. Esaminare i dettagli.
 - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
 - **Name**: Nome univoco assegnato dall'utente per la rete VLAN.
 - **VLAN Tag**: Tag VLAN assegnato al momento della creazione della rete virtuale.
 - **SVIP**: Indirizzo IP virtuale dello storage assegnato alla rete virtuale.
 - **Netmask**: Netmask per questa rete virtuale.
 - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere attivato.
 - **VRF Enabled**: Indicazione dell'attivazione o meno del routing e dell'inoltro virtuale.
 - **IP utilizzati**: Intervallo di indirizzi IP della rete virtuale utilizzati per la rete virtuale.

Abilitare il routing e l'inoltro virtuale

È possibile attivare il routing e l'inoltro virtuale (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di lavorare contemporaneamente. Questa funzionalità è disponibile solo per le reti di storage.

È possibile attivare 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 > Network**.
2. Per attivare VRF su una nuova VLAN, selezionare **Create VLAN** (Crea VLAN).
 - a. Inserire le informazioni pertinenti per la nuova VRF/VLAN. Vedere aggiunta di una rete virtuale.
 - b. Selezionare la casella di controllo **Enable VRF** (attiva VRF*).
 - c. **Opzionale**: Inserire un gateway.
3. Fare clic su **Create VLAN** (Crea VLAN).

Trova ulteriori informazioni

[Aggiungere una rete virtuale](#)

Modificare una rete virtuale

È possibile modificare gli attributi della VLAN, ad esempio il nome della 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 iSCSI, replica remota o altre sessioni di rete, la modifica potrebbe non riuscire.

Quando si gestiscono le dimensioni degli intervalli di indirizzi IP della VLAN, 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 gli indirizzi IP, dall'intervallo di indirizzi IP iniziale o in un blocco IP, utilizzati dai nodi nel cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare indirizzi IP in uso specifici ad altri nodi nel cluster.

È possibile aggiungere un blocco di indirizzi IP seguendo la procedura riportata di seguito:

1. Selezionare **Cluster > Network**.
2. Selezionare l'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **Edit VLAN** (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 **Save Changes** (Salva modifiche).

Collegamento agli articoli della Knowledge base per la 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 IP duplicato dopo l'aggiunta di un nodo di storage nella VLAN sul cluster di elementi"](#)
- ["Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati in Element"](#)

Modificare le VLAN VRF

È possibile modificare gli attributi della VLAN VRF, ad esempio nome VLAN, netmask, gateway e blocchi di indirizzi IP.

1. Fare clic su **Cluster > Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Fare clic su **Edit** (Modifica).

4. Inserire i nuovi attributi per la VLAN VRF nella finestra di dialogo **Edit VLAN** (Modifica VLAN).
5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare una rete virtuale

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

1. Fare clic su **Cluster > Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Trova ulteriori informazioni

[Modificare una rete virtuale](#)

Creare un cluster che supporti i dischi FIPS

La sicurezza sta diventando sempre più critica per l'implementazione di soluzioni in molti ambienti dei clienti. Gli standard FIPS (Federal Information Processing Standards) sono standard per la sicurezza e l'interoperabilità dei computer. La crittografia certificata FIPS 140-2 per i dati inattivi è un componente della soluzione di sicurezza globale.

- ["Evitare la combinazione di nodi per i dischi FIPS"](#)
- ["Abilitare la crittografia a riposo"](#)
- ["Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS"](#)
- ["Attivare la funzione dischi FIPS"](#)
- ["Controllare lo stato del disco FIPS"](#)
- ["Risolvere i problemi relativi alla funzione del disco FIPS"](#)

Evitare la combinazione di nodi per i dischi FIPS

Per prepararsi all'attivazione della funzione dischi FIPS, evitare di combinare nodi in cui alcuni sono in grado di supportare dischi FIPS e altri no.

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

- Tutti i dischi sono certificati come dischi FIPS.
- Tutti i nodi sono nodi di dischi FIPS.
- La crittografia a riposo (EAR) è attivata.
- La funzione dischi FIPS è attivata. Tutti i dischi e i nodi devono essere compatibili con FIPS e la crittografia a riposo deve essere attivata per abilitare la funzione disco FIPS.

Abilitare la crittografia a riposo

È possibile attivare e disattivare la crittografia a livello di cluster a riposo. Questa funzione

non è attivata per impostazione predefinita. Per supportare le unità FIPS, è necessario attivare la crittografia a riposo.

1. Nell'interfaccia utente del software NetApp Element, fare clic su **cluster > Impostazioni**.
2. Fare clic su *Enable Encryption at REST (attiva crittografia a riposo)

Trova ulteriori informazioni

- [Attivare e disattivare la crittografia per un cluster](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS

Verificare se tutti i nodi del 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:

- None (Nessuna): Il nodo non è in grado di supportare la funzione dei dischi FIPS.
- Parziale: Il nodo è compatibile con FIPS, ma non tutti i dischi sono dischi FIPS.
- Pronto: Il nodo è compatibile con FIPS e tutti i dischi sono dischi FIPS o non sono presenti dischi.

Fasi

1. Utilizzando l'API Element, verificare se i nodi e i dischi nel cluster di storage sono in grado di utilizzare dischi FIPS immettendo:

```
GetFipsReport
```

2. Esaminare i risultati, prendendo nota di eventuali nodi che non hanno visualizzato lo stato Ready (Pronto).
3. Per i nodi che non hanno visualizzato lo stato Ready, verificare se il disco è in grado di supportare la funzione dei dischi FIPS:
 - Utilizzando l'API Element, immettere: `GetHardwareList`
 - Annotare il valore di **DriveEncryptionCapabilityType**. Se si tratta di "fips", l'hardware può supportare la funzione dei dischi FIPS.

Vedere i dettagli su `GetFipsReport` oppure `ListDriveHardware` in ["Riferimento API dell'elemento"](#).

4. Se il disco non supporta la funzione dischi FIPS, sostituire l'hardware con hardware FIPS (nodo o dischi).

Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Attivare la funzione dischi FIPS

È possibile attivare la funzione dischi FIPS utilizzando il software NetApp Element

EnableFeature Metodo API.

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

Fase

1. Utilizzando l'API Element, abilitare FIPS su tutti i dischi immettendo:

```
EnableFeature params: FipsDrives
```

Trova ulteriori informazioni

- ["Gestire lo storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Controllare lo stato del disco FIPS

È possibile verificare se la funzione delle unità FIPS è attivata sul cluster utilizzando il software NetApp Element GetFeatureStatus Metodo API, che indica se lo stato FIPS Drives Enabled (dischi FIPS abilitati) è true (vero) o false.

1. Utilizzando l'API Element, verificare la funzione dei dischi FIPS nel cluster immettendo:

```
GetFeatureStatus
```

2. Esaminare i risultati di GetFeatureStatus Chiamata API. Se il valore FIPS Drives Enabled (dischi FIPS attivati) è True (vero), la funzione FIPS Drives (dischi FIPS) è attivata.

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

Trova ulteriori informazioni

- ["Gestire lo storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Risolvere i problemi relativi alla funzione del disco FIPS

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

1. Utilizzando l'interfaccia utente di Element, selezionare **Reporting > Alerts**.
2. Individuare eventuali guasti del cluster, tra cui:

- Dischi FIPS non corrispondenti
- FIPS non rispetta la conformità

3. Per suggerimenti sulla risoluzione, vedere informazioni sul codice di errore del cluster.

Trova ulteriori informazioni

- [Codici di guasto del cluster](#)
- ["Gestire lo storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Abilitare FIPS 140-2 per HTTPS sul cluster

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

Con il software NetApp Element, è possibile attivare la modalità operativa FIPS (Federal Information Processing Standards) 140-2 sul cluster. L'attivazione di questa modalità attiva il modulo di sicurezza crittografica NetApp (NCSM) e sfrutta la crittografia certificata FIPS 140-2 livello 1 per tutte le comunicazioni via HTTPS all'interfaccia utente e all'API NetApp Element.



Una volta attivata la modalità FIPS 140-2, non è possibile disattivarla. Quando la modalità FIPS 140-2 è attivata, ciascun nodo del cluster si riavvia ed esegue un autotest che garantisce che NCSM sia abilitato e funzioni correttamente nella modalità certificata FIPS 140-2. Ciò causa un'interruzione delle connessioni di gestione e di storage sul cluster. È necessario pianificare attentamente e attivare questa modalità solo se l'ambiente richiede il meccanismo di crittografia che offre.

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

Di seguito viene riportato un esempio della richiesta API per attivare FIPS:

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

Una volta attivata questa modalità operativa, tutte le comunicazioni HTTPS utilizzano la crittografia approvata da FIPS 140-2.

Trova ulteriori informazioni

- [Crittografie SSL](#)
- ["Gestire lo storage con l'API Element"](#)

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Crittografie SSL

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

I seguenti elenchi forniscono le crittografie standard SSL (Secure Socket Layer) supportate dal software Element e le crittografie SSL supportate quando la modalità FIPS 140-2 è attivata:

- **FIPS 140-2 disattivato**

- 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 ulteriori informazioni

[Abilitare FIPS 140-2 per HTTPS sul cluster](#)

Inizia a utilizzare la gestione esterna delle chiavi

EKM (External Key Management) offre una gestione sicura delle chiavi di autenticazione (AK) insieme a un server esterno delle chiavi (EKS) off-cluster. Gli AKS vengono utilizzati per bloccare e sbloccare i dischi con crittografia automatica (SED) quando "crittografia a riposo" è attivato sul cluster. EKS fornisce generazione e storage sicuri di AKS. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito DA OASIS, per comunicare con EKS.

- ["Configurare la gestione esterna"](#)
- ["Ridigita la chiave master di crittografia software a riposo"](#)
- ["Ripristino di chiavi di autenticazione inaccessibili o non valide"](#)
- ["Comandi API esterni per la gestione delle chiavi"](#)

Trova ulteriori informazioni

- ["API CreateCluster che può essere utilizzata per attivare la crittografia software a riposo"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

Impostare la gestione esterna delle chiavi

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

Di cosa hai bisogno

- Se si imposta la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, è stata attivata la crittografia software a riposo utilizzando ["CreateCluster"](#) metodo su un nuovo cluster che non contiene volumi.

Fasi

1. Stabilire una relazione di trust con EKS (External Key Server).
 - a. Creare una coppia di chiavi pubbliche/private per il cluster di elementi che viene utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API: ["CreatePublicPrivateKeyPair"](#)
 - b. Ottenere la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. La CSR consente al server delle chiavi di verificare che il cluster di elementi che accederà alle chiavi sia autenticato come cluster di elementi. Chiamare il seguente metodo API: ["GetClientCertificateSignRequest"](#)
 - c. Utilizzare EKS/Certificate Authority per firmare la CSR recuperata. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un provider di chiavi definisce dove ottenere una chiave e un server definisce gli attributi specifici di EKS con cui verrà comunicata.
 - a. Creare un provider di chiavi in cui risiedono i dettagli del server di chiavi chiamando il seguente metodo API: ["CreateKeyProviderKmp"](#)
 - b. Creare un server chiavi che fornisce il certificato firmato e il certificato della chiave pubblica dell'autorità di certificazione chiamando i seguenti metodi API: ["CreateKeyServerKmp"](#) ["TestKeyServerKmp"](#)

Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.
 - c. Aggiungere il server delle chiavi nel contenitore del provider di chiavi chiamando i seguenti metodi API: ["AddKeyServerToProviderKmp"](#) ["TestKeyProviderKmp"](#)

Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.
3. Eseguire una delle seguenti operazioni come fase successiva per la crittografia a riposo:
 - a. (Per la crittografia hardware a riposo) Enable (attiva) ["crittografia hardware a riposo"](#) Fornendo l'ID del

provider di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il ["EnableEncryptionAtRest"](#) Metodo API.



È necessario attivare la crittografia a riposo tramite ["API"](#). Attivando la crittografia a riposo utilizzando il pulsante dell'interfaccia utente Element esistente, la funzione torna a utilizzare le chiavi generate internamente.

- b. (Per la crittografia software a riposo) per ["crittografia software a riposo"](#) Per utilizzare il provider di chiavi appena creato, passare l'ID del provider di chiavi a ["RekeySoftwareEncryptionAtRestMasterKey"](#) Metodo API.

Trova ulteriori informazioni

- ["Attivare e disattivare la crittografia per un cluster"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

Ridigita la chiave master di crittografia software a riposo

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

Potrebbe essere necessario eseguire una nuova chiave nell'ambito di una delle seguenti procedure:

- Creare una nuova chiave come parte di un cambiamento dalla gestione interna delle chiavi alla gestione esterna delle chiavi.
- Creare una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.



Questo processo è asincrono e restituisce una risposta prima del completamento dell'operazione di rekey. È possibile utilizzare ["GetAsyncResult"](#) metodo per eseguire il polling del sistema per verificare il completamento del processo.

Di cosa hai bisogno

- È stata attivata la crittografia software a riposo utilizzando ["CreateCluster"](#) Metodo su un nuovo cluster che non contiene volumi e non dispone di i/O. Utilizzare il `GetSoftwareEncryptionatRestInfo` per confermare che lo stato è `enabled` prima di procedere.
- Lo hai fatto ["instaurazione di una relazione di fiducia"](#) Tra il cluster SolidFire e un server di chiavi esterne (EKS). Eseguire ["TestKeyProviderKmip"](#) metodo per verificare che sia stabilita una connessione con il provider di chiavi.

Fasi

1. Eseguire ["ListKeyProvidersKmip"](#) Comando e copia dell'ID del provider di chiavi (`keyProviderID`).
2. Eseguire ["RekeySoftwareEncryptionAtRestMasterKey"](#) con `keyManagementType` parametro as `external` e `keyProviderID` Come numero ID del provider di chiavi del passaggio precedente:

```

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

```

3. Copiare il `asyncHandle` valore di `RekeySoftwareEncryptionAtRestMasterKey` risposta del comando.
4. Eseguire `GetAsyncResult` con il `asyncHandle` valore del passaggio precedente per confermare la modifica della configurazione. Dalla risposta del comando, dovresti vedere che la configurazione della vecchia chiave master è stata aggiornata con le nuove informazioni sulla chiave. Copiare il nuovo ID del provider 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. Eseguire `GetSoftwareEncryptionatRestInfo` per confermare i dettagli della nuova 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 ulteriori informazioni

- ["Gestire lo storage con l'API Element"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

Ripristino di chiavi di autenticazione inaccessibili o non valide

Occasionalmente, può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, viene generato un guasto del cluster (indicato come codice di guasto del cluster). I due casi più probabili sono descritti qui.

Il cluster non è in grado di sbloccare i dischi a causa di un errore del cluster KmipServerFault.

Questo 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 le fasi di ripristino riportate nei codici di guasto del cluster (se presenti).

Un errore sliceServiceUnhealthy potrebbe essere impostato perché i dischi metadati sono stati contrassegnati come guasti e posizionati nello stato "Available" (disponibile).

Procedura per la cancellazione:

1. Aggiungere di nuovo i dischi.
2. Dopo 3-4 minuti, controllare che il sliceServiceUnhealthy il guasto è stato cancellato.

Vedere ["codici di guasto del cluster"](#) per ulteriori informazioni.

Comandi API esterni per la gestione delle chiavi

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

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

- [CreatePublicPrivateKeyPair](#)
- [GetClientCertificateSignRequest](#)

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

- [CreateKeyServerKmip](#)
- [ModifyKeyServerKmip](#)
- [DeleteKeyServerKmip](#)
- [GetKeyServerKmip](#)
- [ListKeyServerKmip](#)
- [TestKeyServerKmip](#)

Utilizzato per la creazione e la manutenzione di provider di chiavi che gestiscono server di chiavi esterni:

- [CreateKeyProviderKmip](#)
- [DeleteKeyProviderKmip](#)
- [AddKeyServerToProviderKmip](#)
- [RemoveKeyServerFromProviderKmip](#)
- [GetKeyProviderKmip](#)
- [ListKeyProvidersKmip](#)
- [RekeySoftwareEncryptionAtRestMasterKey](#)
- [TestKeyProviderKmip](#)

Per informazioni sui metodi API, vedere ["Informazioni di riferimento API"](#).

Gestire volumi e volumi virtuali

È possibile gestire i dati in un cluster che esegue il software Element dalla scheda Management (Gestione) dell'interfaccia utente 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 policy di qualità del servizio (QoS).

- ["Lavorare con i volumi"](#)
- ["Lavorare con volumi virtuali"](#)
- ["Lavorare con gli iniziatori e i gruppi di accesso ai volumi"](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Lavorare con i volumi

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel. Dalla pagina Volumes (volumi) della scheda Management (Gestione), è possibile creare, modificare, clonare ed eliminare volumi su un nodo. È inoltre possibile visualizzare le statistiche relative alla larghezza di banda del volume e all'utilizzo di i/O.

Trova ulteriori informazioni

- ["Gestire le policy di qualità del servizio"](#)
- ["Creare un volume"](#)
- ["Visualizza i dettagli delle performance dei singoli volumi"](#)
- ["Modificare i volumi attivi"](#)
- ["Eliminare un volume"](#)
- ["Ripristinare un volume cancellato"](#)
- ["Eliminare un volume"](#)
- ["Clonare un volume"](#)
- ["Assegnare LUN a volumi Fibre Channel"](#)
- ["Applicare una policy di QoS ai volumi"](#)
- ["Rimuovere l'associazione dei criteri QoS di un volume"](#)

Gestire le policy di qualità del servizio

Una policy 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 QoS Policies (Criteri QoS) nella scheda Management (Gestione).



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

["Video NetApp: Policy di qualità del servizio SolidFire"](#)

Vedere ["Performance e qualità del servizio"](#).

- Creare una policy QoS
- Modificare un criterio QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare policy QoS e applicarle durante la creazione di volumi.

1. Selezionare **Management > QoS Policies**.
2. Fare clic su **Crea policy QoS**.

3. Inserire il nome * Policy Name*.
4. Inserire i valori **min IOPS**, **Max IOPS** e **Burst IOPS**.
5. Fare clic su **Crea policy QoS**.

Modificare un criterio QoS

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

1. Selezionare **Management > QoS Policies**.
2. Fare clic sull'icona Actions (azioni) per il criterio QoS che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. Nella finestra di dialogo **Edit QoS Policy** (Modifica policy QoS), modificare le seguenti proprietà come richiesto:
 - Nome policy
 - IOPS minimi
 - IOPS max
 - IOPS burst
5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare una policy QoS

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



Se invece si tenta di disassociare un volume da un criterio QoS, è possibile modificare le impostazioni QoS per quel volume su customizzato.

1. Selezionare **Management > QoS Policies**.
2. Fare clic sull'icona Actions (azioni) per il criterio QoS che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Trova ulteriori informazioni

- ["Rimuovere l'associazione dei criteri QoS di un volume"](#)
- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Gestire i volumi

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel.

Dalla pagina Volumes (volumi) della scheda Management (Gestione), è possibile creare, modificare, clonare ed eliminare volumi su un nodo.

Creare 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 **Management > Volumes**.
2. Fare clic su **Create Volume** (Crea volume).
3. Nella finestra di dialogo **Create a New Volume** (Crea un nuovo volume), immettere il nome del volume.
4. Inserire le dimensioni totali del volume.



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

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

5. Selezionare **Block Size** (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 **Create account** (Crea account), immettere un nuovo nome account e fare clic su **Create** (Crea). L'account viene creato e associato al nuovo volume.



Se sono presenti più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.

7. Per impostare la **qualità del servizio**, effettuare una delle seguenti operazioni:
 - a. In **Policy**, è possibile selezionare un criterio QoS esistente, se disponibile.
 - b. In **Custom Settings** (Impostazioni personalizzate), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.

I volumi con un valore massimo o burst IOPS superiore a 20,000 IOPS potrebbero richiedere una profondità di coda elevata o più sessioni per ottenere questo livello di IOPS su un singolo volume.

8. Fare clic su **Create Volume** (Crea volume).

Visualizzare i dettagli del volume

1. Selezionare **Management > Volumes**.
2. Esaminare i dettagli.
 - **ID**: L'ID generato dal sistema per il volume.
 - **Name** (Nome): Il nome assegnato al volume al momento della creazione.
 - **Account**: Il 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.
 - **Access**: Il tipo di accesso assegnato al volume al momento della creazione. Valori possibili:
 - Lettura/scrittura: Tutte le letture e le scritture sono accettate.

- Sola lettura: Tutte le attività di lettura sono consentite; non sono consentite scritture.
- Bloccato: È consentito solo l'accesso come amministratore.
- ReplicationTarget: Designato come volume di destinazione in una coppia di volumi replicati.
- **Utilizzato**: La percentuale di spazio utilizzato nel volume.
- **Size**: Dimensione totale (in GB) del volume.
- **Snapshot**: Il numero di snapshot creati per il volume.
- **QoS Policy**: Il nome e il collegamento alla policy QoS definita dall'utente.
- **IOPS min**: Il numero minimo di IOPS garantito per il volume.
- **IOPS max**: Il numero massimo di IOPS consentito per il volume.
- **Burst IOPS**: Il numero massimo di IOPS consentito per un breve periodo di tempo per il volume. Impostazione predefinita = 15,000.
- **Attributes**: Attributi assegnati al volume come coppia chiave/valore tramite un metodo API.
- **512e**: Indicazione dell'attivazione di 512e su un volume. Valori possibili:
 - Sì
 - No
- **Creato il**: La data e l'ora in cui è stato creato il volume.

Visualizzare i dettagli dei singoli volumi

È possibile visualizzare le statistiche delle performance per i singoli volumi.

1. Selezionare **Reporting > Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Actions (azioni) per un volume.
3. Fare clic su **View Details** (Visualizza dettagli).

Nella parte inferiore della pagina viene visualizzato un vassoio contenente informazioni generali sul volume.

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

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

Modificare i volumi attivi

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

È possibile ridimensionare un volume quando lo spazio disponibile sul cluster è sufficiente nelle seguenti condizioni:

- Condizioni di funzionamento normali.
- Vengono segnalati errori o errori del volume.
- Il volume è in fase di clonaggio.
- Il volume è in fase di risyncing.

Fasi

1. Selezionare **Management > Volumes**.
2. Nella finestra **Active**, fare clic sull'icona Actions (azioni) del volume che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. **Opzionale:** consente di modificare le dimensioni totali del volume.
 - È possibile aumentare, ma non diminuire, le dimensioni del volume. È possibile ridimensionare un solo volume in una singola operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.
 - Se si stanno regolando le dimensioni del volume per la replica, è necessario innanzitutto aumentare le dimensioni del volume assegnato come destinazione della replica. Quindi, è possibile ridimensionare il volume di origine. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

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

- 1 GB = 000 000 000 byte
 - 1GiB = 1 073 741 824 byte
5. **Opzionale:** selezionare un livello di accesso diverso per uno dei seguenti account:
 - Di sola lettura
 - Lettura/scrittura
 - Bloccato
 - Destinazione della replica
 6. **Opzionale:** selezionare l'account che deve avere accesso al volume.

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



Se sono presenti più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.

7. **Opzionale:** per modificare la selezione in **qualità del servizio**, effettuare una delle seguenti operazioni:
 - a. In **Policy**, è possibile selezionare un criterio QoS esistente, se disponibile.
 - b. In **Custom Settings** (Impostazioni personalizzate), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.



Se si utilizzano policy QoS su un volume, è possibile impostare una QoS personalizzata per rimuovere l'affiliazione della policy QoS con il volume. La QoS personalizzata sovrascrive e regola i valori dei criteri QoS per le impostazioni QoS del volume.



Quando si modificano i valori IOPS, è necessario aumentare 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 a blocchi di grandi dimensioni, limitando al contempo gli IOPS sostenuti per un volume.

8. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un volume

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

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

Se un volume utilizzato per creare uno snapshot viene cancellato, le relative snapshot associate diventano inattive. Quando i volumi di origine cancellati vengono rimossi, anche le snapshot inattive associate vengono rimosse 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.

Fasi

1. Selezionare **Management > Volumes**.
2. Per eliminare un singolo volume, attenersi alla seguente procedura:
 - a. Fare clic sull'icona Actions (azioni) per il volume che si desidera eliminare.
 - b. Nel menu visualizzato, fare clic su **Delete** (Elimina).
 - c. Confermare l'azione.

Il sistema sposta il volume nell'area **Deleted** della pagina **Volumes**.

3. Per eliminare più volumi, attenersi alla seguente procedura:
 - a. Nell'elenco dei volumi, selezionare la casella accanto ai volumi che si desidera eliminare.
 - b. Fare clic su **azioni in blocco**.
 - c. Nel menu visualizzato, fare clic su **Delete** (Elimina).
 - d. Confermare l'azione.

Il sistema sposta i volumi nell'area **Deleted** della pagina **Volumes**.

Ripristinare un volume cancellato

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

1. Selezionare **Management > Volumes**.
2. Fare clic sulla scheda **Deleted** per visualizzare l'elenco dei volumi eliminati.
3. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.

4. Nel menu visualizzato, fare clic su **Restore** (Ripristina).
5. Confermare l'azione.

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

Eliminare un volume

Quando un volume viene eliminato, viene rimosso in modo permanente dal sistema. Tutti i dati nel volume vengono persi.

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

1. Selezionare **Management > Volumes**.
2. Fare clic sul pulsante **Deleted**.
3. Eseguire la procedura per eliminare uno o più volumi.

Opzione	Fasi
Eliminare un singolo volume	<ol style="list-style-type: none"> a. Fare clic sull'icona Actions (azioni) per il volume che si desidera eliminare. b. Fare clic su Rimuovi. c. Confermare l'azione.
Eliminare più volumi	<ol style="list-style-type: none"> a. Selezionare i volumi che si desidera eliminare. b. Fare clic su azioni in blocco. c. Nel menu visualizzato, selezionare Rimuovi. d. Confermare l'azione.

Clonare un volume

È possibile creare un clone di uno o più volumi per creare una copia point-in-time dei dati. Quando si clonano un volume, il sistema crea uno snapshot del volume e quindi una copia dei dati a cui fa riferimento lo snapshot. Si tratta di un processo asincrono e la quantità di tempo richiesta dal processo dipende dalla dimensione del volume che si sta clonando e dal carico corrente del cluster.

Il cluster supporta fino a due richieste di cloni in esecuzione per volume alla volta e fino a otto operazioni di cloni dei volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per l'elaborazione successiva.



I sistemi operativi differiscono per il trattamento dei volumi clonati. VMware ESXi tratterà un volume clonato come una copia di volume o un volume di snapshot. Il volume sarà un dispositivo disponibile da utilizzare per creare un nuovo datastore. Per ulteriori informazioni sul montaggio di volumi cloni e sulla gestione delle LUN snapshot, consultare la documentazione VMware all'indirizzo "[Montaggio di una copia del datastore VMFS](#)" e "[Gestione di datastore VMFS duplicati](#)".



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

Fasi

1. Selezionare **Management > Volumes**.
2. Per clonare un singolo volume, attenersi alla seguente procedura:
 - a. Nell'elenco dei volumi nella pagina **Active**, fare clic sull'icona Actions (azioni) del volume che si desidera clonare.
 - b. Nel menu visualizzato, fare clic su **Clone**.
 - c. Nella finestra **Clone Volume**, immettere un nome di volume per il volume appena clonato.
 - d. Selezionare una dimensione e una misurazione per il volume utilizzando la casella di selezione **Volume Size** (dimensione volume) e l'elenco.



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

- 1 GB = 000 000 000 byte
- 1GiB = 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**.



Durante questa fase, è possibile creare un account facendo clic sul collegamento **Create account** (Crea account), immettendo un nome account e facendo clic su **Create** (Crea account). Il sistema aggiunge automaticamente l'account all'elenco **account** dopo averlo creato.

3. Per clonare più volumi, attenersi alla seguente procedura:
 - a. Nell'elenco dei volumi nella pagina **Active**, selezionare la casella accanto ai volumi che si desidera clonare.
 - b. Fare clic su **azioni in blocco**.
 - c. Nel menu visualizzato, selezionare **Clone**.
 - d. Nella finestra di dialogo **Clone Multiple Volumes** (Copia volumi multipli), inserire un prefisso per i volumi clonati nel campo **New Volume Name Prefix** (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**.



L'aumento delle dimensioni del volume di un clone comporta la creazione di un nuovo volume con ulteriore spazio libero alla fine del volume. A seconda dell'utilizzo del volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per utilizzarlo.

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Assegnare LUN a volumi Fibre Channel

È possibile modificare l'assegnazione del LUN per un volume Fibre Channel in un gruppo di accesso al volume. È inoltre possibile assegnare i LUN dei volumi Fibre Channel quando si crea un gruppo di accesso ai volumi.

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 rilevare il nuovo ID LUN.

1. Selezionare **Gestione > gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. In **Assign LUN ID** (Assegna ID LUN) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **LUN Assignments** (assegnazioni LUN).
5. Per ciascun volume dell'elenco a cui si desidera assegnare un LUN, immettere un nuovo valore nel campo **LUN** corrispondente.
6. Fare clic su **Save Changes** (Salva modifiche).

Applicare una policy di QoS ai volumi

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

Il criterio QoS che si desidera applicare in blocco deve esistere.

1. Selezionare **Management > Volumes**.
2. Nell'elenco dei volumi, selezionare la casella accanto ai volumi a cui si desidera applicare il criterio QoS.
3. Fare clic su **azioni in blocco**.
4. Nel menu visualizzato, fare clic su **Apply QoS Policy** (Applica policy QoS).
5. Selezionare il criterio QoS dall'elenco a discesa.
6. Fare clic su **Apply** (Applica).

Trova ulteriori informazioni

[Policy sulla qualità del servizio](#)

Rimuovere l'associazione dei criteri QoS di un volume

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

Il volume che si desidera modificare deve essere associato a un criterio QoS.

1. Selezionare **Management > Volumes**.
2. Fare clic sull'icona Actions (azioni) per un volume che contiene un criterio QoS che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Nel menu visualizzato sotto **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 **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

[Eliminare una policy QoS](#)

Lavorare con volumi virtuali

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

Il sistema di storage software NetApp Element viene fornito con la funzione volumi virtuali (VVol) disattivata. È necessario eseguire un'attività singola per attivare manualmente la funzionalità vSphere Vol tramite l'interfaccia utente di Element.

Dopo aver attivato la funzionalità Vol, nell'interfaccia utente viene visualizzata una scheda Vols che offre opzioni di monitoraggio correlate a Vols e di gestione limitate. Inoltre, un componente software lato storage noto come provider VASA funge da servizio di consapevolezza dello storage per vSphere. La maggior parte dei comandi VVol, come creazione, cloning e modifica di VVol, vengono avviati da un host vCenter Server o ESXi e tradotti dal provider VASA in API Element per il sistema storage software Element. I comandi per creare, eliminare e gestire i container di storage e eliminare i volumi virtuali possono essere avviati utilizzando l'interfaccia utente di Element.

La maggior parte delle configurazioni necessarie per l'utilizzo della funzionalità Virtual Volumes con i sistemi storage software Element è realizzata in vSphere. Consultare la *Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire* per registrare il provider VASA in vCenter, creare e gestire i datastore VVol e gestire lo storage in base alle policy.



Non registrare più di un provider VASA NetApp Element in una singola istanza di vCenter. Quando viene aggiunto un secondo provider VASA NetApp Element, questo rende inaccessibili tutti i datastore VVOL.



Il supporto DI VASA per più vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con vCenter. Per eseguire l'installazione, scaricare il file VASA39.tar.gz dal "[Download di software NetApp](#)" e seguire le indicazioni nel manifesto. Il provider VASA di NetApp Element 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.

Trova ulteriori informazioni

- [Abilitare i volumi virtuali](#)
- [Visualizzare i dettagli del volume virtuale](#)
- [Eliminare un volume virtuale](#)
- [Creare un container di storage](#)
- [Modificare un container di storage](#)
- [Eliminare un contenitore di storage](#)

- [Endpoint del protocollo](#)
- [Associazioni](#)
- [Dettagli host](#)

Abilitare i volumi virtuali

È necessario attivare manualmente la funzionalità vVol (vSphere Virtual Volumes) tramite il software NetApp Element. Il sistema software Element viene fornito con la funzionalità VVol disattivata per impostazione predefinita e non viene automaticamente attivata durante una nuova installazione o un aggiornamento. L'attivazione della funzione VVol è un'attività di configurazione unica.

Di cosa hai bisogno

- 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 VVol.
- Se si utilizza Element 11.3 o versione successiva, il cluster deve essere connesso a un ambiente ESXi 6.0 update 3 o versione successiva.



L'attivazione della funzionalità vSphere Virtual Volumes modifica in modo permanente la configurazione del software Element. La funzionalità VVol deve essere attivata solo se il cluster è connesso a un ambiente compatibile con VMware ESXi VVols. È possibile disattivare la funzione VVol e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster, che elimina tutti i dati presenti nel sistema.

Fasi

1. Selezionare **Clusters > Settings**.
2. Individuare le impostazioni specifiche del cluster per i volumi virtuali.
3. Fare clic su **Enable Virtual Volumes** (Abilita volumi virtuali)
4. Fare clic su **Si** per confermare la modifica della configurazione dei volumi virtuali.

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



Quando la funzionalità VVol è attivata, 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 **Clusters > Settings**. Questo URL verrà utilizzato per registrare il provider VASA in vCenter.
6. Creare un contenitore di storage in **VVol > Storage Containers**.



È necessario creare almeno un container di storage in modo che le VM possano essere fornite a un datastore Vol.

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



VSphere richiede ulteriori attività di configurazione. Consultare la *Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire* per registrare il provider VASA in vCenter, creare e gestire i datastore VVol e gestire lo storage in base alle policy.

Trova ulteriori informazioni

["Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire"](#)

Visualizzare i dettagli del volume virtuale

È possibile rivedere 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 performance per ogni volume virtuale, inclusi input, output, throughput, latenza, profondità della coda e informazioni sul volume.

Di cosa hai bisogno

- La funzionalità VVol dovrebbe essere stata attivata nell'interfaccia utente Element per il cluster.
- È necessario aver creato un container di storage associato.
- Il cluster vSphere dovrebbe essere stato configurato per utilizzare la funzionalità VVol del software Element.
- È necessario aver creato almeno una macchina virtuale in vSphere.

Fasi

1. Fare clic su **VVol > volumi virtuali**.

Vengono visualizzate le informazioni relative a tutti i volumi virtuali attivi.

2. Fare clic sull'icona **Actions** del volume virtuale che si desidera esaminare.
3. Nel menu visualizzato, selezionare **Visualizza dettagli**.

Dettagli

La pagina Virtual Volumes (volumi virtuali) della scheda VVols (volumi virtuali) fornisce informazioni su ciascun volume virtuale attivo nel cluster, ad esempio l'ID del volume, lo snapshot ID, l'ID del volume virtuale padre e l'ID del volume virtuale.

- **Volume ID:** L'ID del volume sottostante.
- **Snapshot ID:** L'ID dello snapshot del volume sottostante. Il valore è 0 se il volume virtuale non rappresenta uno snapshot SolidFire.
- **Parent Virtual Volume ID:** L'ID del volume virtuale del volume virtuale padre. Se l'ID è pari a zero, il volume virtuale è indipendente senza alcun collegamento a un elemento padre.
- **Virtual Volume ID:** UUID del volume virtuale.
- **Name (Nome):** Il nome assegnato al volume virtuale.
- **Storage Container:** Il container di storage proprietario del volume virtuale.
- **Guest OS Type:** Sistema operativo associato al volume virtuale.
- **Virtual Volume Type:** Il tipo di volume virtuale: Config, Data, Memory, Swap o Other.

- **Access:** Le autorizzazioni di lettura/scrittura assegnate al volume virtuale.
- **Size:** Dimensione del volume virtuale in GB o GiB.
- **Snapshot:** Il numero di snapshot associati. Fare clic sul numero per il collegamento ai dettagli dell'istantanea.
- **Min IOPS:** Impostazione minima di QoS IOPS del volume virtuale.
- **Massimo IOPS:** Impostazione massima di QoS IOPS del volume virtuale.
- **Burst IOPS:** Impostazione massima di qualità del burst del volume virtuale.
- **VMW_VMID:** Le informazioni nei campi che precedono "VMW_" sono definite da VMware.
- **Create Time** (ora di creazione): L'ora in cui è stata completata l'attività di creazione del volume virtuale.

Dettagli dei singoli volumi virtuali

La pagina Virtual Volumes (volumi virtuali) della scheda Vols (volumi virtuali) fornisce le seguenti informazioni sul volume virtuale quando si seleziona un singolo volume virtuale e ne visualizza i dettagli.

- **VMW_XXX:** Le informazioni nei campi con la dicitura "VMW_" sono definite da VMware.
- **Parent Virtual Volume ID:** L'ID del volume virtuale del volume virtuale padre. Se l'ID è pari a zero, il volume virtuale è indipendente senza alcun collegamento a un elemento padre.
- **Virtual Volume ID:** UUID del volume virtuale.
- **Virtual Volume Type:** Il tipo di volume virtuale: Config, Data, Memory, Swap o Other.
- **Volume ID:** L'ID del volume sottostante.
- **Access:** Le 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.
- **Total Volume Size:** 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 Blocks:** Numero totale di blocchi da 4 KiB senza dati dopo il completamento dell'ultimo round dell'operazione di garbage collection.
- **Snapshot:** Il numero di snapshot associati. Fare clic sul numero per il collegamento ai dettagli dell'istantanea.
- **Min IOPS:** Impostazione minima di QoS IOPS del volume virtuale.
- **Massimo IOPS:** Impostazione massima di QoS IOPS del volume virtuale.
- **Burst IOPS:** Impostazione massima di qualità del burst del volume virtuale.
- **Enable 512:** Poiché i volumi virtuali utilizzano sempre l'emulazione delle dimensioni dei blocchi da 512 byte, il valore è sempre sì.
- **Volumes paired** (volumi associati): Indica se un volume è associato.
- **Create Time** (ora di creazione): L'ora in cui è stata completata l'attività di creazione del volume virtuale.
- **Dimensione blocchi:** Dimensione dei blocchi sul volume.
- **Unaligned Scrittura:** Per i volumi 512e, il numero di operazioni di scrittura che non si trovavano su un confine di settore 4k. Un numero elevato di scritture non allineate potrebbe indicare un allineamento errato 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 errato 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 in formato NAA IEEE Registered Extended.
- **Attributes:** Elenco delle coppie nome-valore nel formato oggetto JSON.

Eliminare un volume virtuale

Sebbene i volumi virtuali debbano essere sempre cancellati dal VMware Management Layer, la funzionalità di eliminazione dei volumi virtuali è attivata dall'interfaccia utente di Element. Eliminare un volume virtuale dall'interfaccia utente di Element solo quando è assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire.

1. Selezionare **VVol > volumi virtuali**.
2. Fare clic sull'icona Actions (azioni) per il volume virtuale che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).



È necessario eliminare un volume virtuale dal livello di gestione VMware per assicurarsi che il volume virtuale sia correttamente slegato prima dell'eliminazione. Eliminare un volume virtuale dall'interfaccia utente di Element solo quando è 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 viene eliminato immediatamente.

4. Confermare l'azione.
5. Aggiornare l'elenco dei volumi virtuali per confermare che il volume virtuale è stato rimosso.
6. **Opzionale:** Selezionare **Reporting > Event Log** per confermare che l'eliminazione è stata eseguita correttamente.

Gestire i container di storage

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

I container di storage vengono creati e legati agli account NetApp Element. Un container di storage creato sullo storage Element viene visualizzato come datastore vSphere in vCenter ed ESXi. I container di storage non allocano spazio nello storage degli elementi. Vengono semplicemente utilizzati per associare logicamente i volumi virtuali.

È supportato un massimo di quattro container di storage per cluster. Per abilitare la funzionalità VVol, è necessario almeno un container di storage.

Creare un container di storage

È possibile creare contenitori di storage nell'interfaccia utente di Element e rilevarli in vCenter. È necessario

creare almeno un container di storage per iniziare il provisioning delle macchine virtuali con supporto Vol.

Prima di iniziare, attivare la funzionalità VVol nell'interfaccia utente Element per il cluster.

Fasi

1. Selezionare **VVol > Storage Containers**.
2. Fare clic sul pulsante **Create Storage Containers** (Crea container di storage).
3. Inserire le informazioni sul contenitore di storage nella finestra di dialogo **Crea un nuovo contenitore di storage**:
 - a. Immettere un nome per il contenitore di storage.
 - b. Configurare i segreti di initiator e target per CHAP.



Lasciare vuoti i campi CHAP Settings (Impostazioni CHAP) per generare automaticamente i segreti.

- c. Fare clic sul pulsante **Create Storage Container** (Crea contenitore di storage).
4. Verificare che il nuovo contenitore di storage venga visualizzato nell'elenco nella sottoscheda **Storage Containers**.



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

Visualizzare i dettagli del container di storage

Nella pagina Storage Containers della scheda VVol, è possibile visualizzare le informazioni relative a tutti i container di storage attivi nel cluster.

- **Account ID**: L'ID dell'account NetApp Element associato al container di storage.
- **Name**: Il nome del contenitore di storage.
- **Status**: Lo stato del contenitore di storage. Valori possibili:
 - Attivo: Il contenitore di storage è in uso.
 - Bloccato: Il contenitore di storage è bloccato.
- **PE Type**: Il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile per il software Element).
- **Storage Container ID**: UUID del container di storage del volume virtuale.
- **Active Virtual Volumes** (volumi virtuali attivi): Il numero di volumi virtuali attivi associati al container di storage.

Visualizzare i dettagli dei singoli container di storage

È possibile visualizzare le informazioni sul contenitore di storage per un singolo contenitore selezionandole dalla pagina Storage Containers nella scheda VVols.

- **Account ID**: L'ID dell'account NetApp Element associato al container di storage.
- **Name**: Il nome del contenitore di storage.
- **Status**: Lo stato del contenitore di storage. Valori possibili:
 - Attivo: Il contenitore di storage è in uso.

- **Bloccato:** Il contenitore di storage è bloccato.
- **CHAP Initiator Secret:** Il segreto CHAP unico per l'iniziatore.
- **CHAP Target Secret:** Il segreto CHAP unico per il target.
- **Storage Container ID:** UUID del container di storage del volume virtuale.
- **Protocol Endpoint Type** (tipo endpoint protocollo): Indica il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile).

Modificare un container di storage

È possibile modificare l'autenticazione CHAP del container di storage nell'interfaccia utente di Element.

1. Selezionare **VVol > Storage Containers**.
2. Fare clic sull'icona **azioni** del contenitore di storage che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. In Impostazioni CHAP, modificare le credenziali Initiator Secret e Target Secret utilizzate per l'autenticazione.



Se non si modificano le credenziali CHAP Settings, queste rimangono invariate. Se i campi delle credenziali vengono vuoti, il sistema genera automaticamente nuovi segreti.

5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un contenitore di storage

È possibile eliminare i contenitori di storage dall'interfaccia utente di Element.

Di cosa hai bisogno

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

Fasi

1. Selezionare **VVol > Storage Containers**.
2. Fare clic sull'icona **azioni** del contenitore di storage che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.
5. Aggiornare l'elenco dei contenitori di storage nella sottoscheda **Storage Containers** per confermare che il contenitore di storage è stato rimosso.

Endpoint del protocollo

Gli endpoint del protocollo sono access point utilizzati da un host per gestire lo storage in un cluster che esegue il software NetApp Element. Gli endpoint del protocollo non possono essere cancellati 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 con software Element crea automaticamente un endpoint di protocollo per nodo di storage nel cluster. Ad esempio, un cluster di storage a sei nodi dispone di sei endpoint di protocollo mappati a ciascun host ESXi. Gli endpoint del protocollo sono gestiti dinamicamente dal software Element e vengono creati, spostati o rimossi in base alle necessità senza alcun intervento. Gli endpoint del protocollo sono la

destinazione per il multi-pathing e fungono da proxy i/o per le LUN sussidiarie. Ogni endpoint del protocollo utilizza un indirizzo SCSI disponibile, proprio come un target iSCSI standard. Gli endpoint del protocollo appaiono come un dispositivo di storage a blocco singolo (512 byte) nel client vSphere, ma questo dispositivo di storage non è disponibile per la formattazione o l'utilizzo come storage.

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

Dettagli degli endpoint del protocollo

La pagina Protocol Endpoints (endpoint del protocollo) nella scheda VVols (VVols) fornisce informazioni sull'endpoint del protocollo.

- **ID provider primario**

L'ID del provider dell'endpoint del protocollo primario.

- **ID provider secondario**

L'ID del provider dell'endpoint del protocollo secondario.

- **ID endpoint del protocollo**

UUID dell'endpoint del protocollo.

- **Protocol Endpoint state (Stato endpoint protocollo)**

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

- Attivo: L'endpoint del protocollo è in uso.
- Start: L'endpoint del protocollo è in fase di avvio.
- Failover: Si è verificato un failover dell'endpoint del protocollo.
- Riservato: L'endpoint del protocollo è riservato.

- **Tipo di provider**

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

- Primario
- Secondario

- **SCSI NAA DEVICE ID (ID DISPOSITIVO NAA SCSI)**

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

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 del protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint del protocollo e restituisce il binding all'host ESXi. Una volta eseguito il bound, l'host ESXi può eseguire operazioni di i/o con il volume virtuale associato.

Dettagli sui binding

La pagina binding della scheda VVol fornisce informazioni di binding su ciascun volume virtuale.

Vengono visualizzate le seguenti informazioni:

- **ID host**

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

- **ID endpoint del protocollo**

ID endpoint del protocollo corrispondenti a ciascun nodo del cluster SolidFire.

- **Protocol Endpoint in Band ID**

L'ID del dispositivo NAA SCSI dell'endpoint del protocollo.

- **Protocol Endpoint Type** (tipo di endpoint del protocollo)

Il tipo di endpoint del protocollo.

- **VVol Binding ID**

UUID di binding del volume virtuale.

- **ID volume**

UUID (Universally Unique Identifier) del volume virtuale.

- **VVol ID secondario**

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

Dettagli host

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

Vengono visualizzate le seguenti informazioni:

- **ID host**

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

- **Indirizzo host**

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

- *** Binding***

ID di binding per tutti i volumi virtuali associati all'host ESXi.

- **ID cluster ESX**

L'ID del cluster host vSphere o il GUID vCenter.

- **IQN iniziatore**

IQN iniziatore per l'host del volume virtuale.

- **ID endpoint del protocollo SolidFire**

Endpoint del protocollo attualmente visibili all'host ESXi.

Lavorare con gli iniziatori e i gruppi di accesso ai volumi

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 degli iniziatori iSCSI o le WWPN Fibre Channel in un insieme 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 per l'account.
- Autenticazione CHAP a livello di iniziatore: È possibile assegnare una destinazione CHAP univoca e segreti per iniziatori specifici senza essere associati a un singolo CHAP in un singolo account. Questa autenticazione CHAP a livello di iniziatore sostituisce le credenziali a livello di account.

Facoltativamente, con il CHAP per-initiator, è possibile applicare l'autorizzazione per initiator e l'autenticazione CHAP per-initiator. Queste opzioni possono essere definite in base all'iniziatore e un gruppo di accesso può contenere una combinazione di iniziatori con diverse opzioni.

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



I gruppi di accesso ai volumi hanno i seguenti limiti:

- In un gruppo di accesso è consentito un massimo di 64 IQN o WWPN.
- Un gruppo di accesso può essere costituito 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.

Trova ulteriori informazioni

- [Creare un gruppo di accesso al volume](#)
- [Aggiungere volumi a un gruppo di accesso](#)
- [Rimuovere i volumi da un gruppo di accesso](#)
- [Creare un iniziatore](#)
- [Modificare un iniziatore](#)
- [Aggiungere un singolo iniziatore a un gruppo di accesso al volume](#)

- [Aggiungere più iniziatori a un gruppo di accesso al volume](#)
- [Rimuovere gli iniziatori da un gruppo di accesso](#)
- [Eliminare un gruppo di accesso](#)
- [Eliminare un iniziatore](#)


Creare un gruppo di accesso al volume


È possibile creare gruppi di accesso ai volumi associando gli iniziatori a un insieme di volumi per un accesso protetto. È quindi possibile concedere l'accesso ai volumi del gruppo con un account CHAP Initiator secret e un account CHAP Secret.

Se si utilizza CHAP basato su iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso a volume, fornendo una maggiore sicurezza. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

Fasi

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic su **Create Access Group** (Crea gruppo di accesso).
3. Inserire 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	<p>a. Nella sezione Add Initiator (Aggiungi iniziatori), selezionare un iniziatore Fibre Channel esistente dall'elenco Unbound Fibre Channel Initiator (iniziatori Fibre Channel non associati).</p> <p>b. Fare clic su Aggiungi iniziatore FC.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> È possibile creare un iniziatore durante questa fase facendo clic sul collegamento Create Initiator (Crea iniziatore), immettendo un nome iniziatore e facendo clic su Create (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco degli iniziatori dopo averlo creato.</p> </div> <p>Un esempio del formato è il seguente:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0; background-color: #f0f0f0;"> <p>5f:47:ac:c0:5c:74:d4:02</p> </div>

Opzione	Descrizione
Aggiunta di un iniziatore iSCSI	<p>Nella sezione Add Initiator (Aggiungi iniziatori), selezionare un iniziatore esistente dall'elenco Initiator (iniziatori). Nota: è possibile creare un iniziatore durante questa fase facendo clic sul collegamento Create Initiator (Crea iniziatore), immettendo il nome di un iniziatore e facendo clic su Create (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco degli iniziatori dopo averlo creato.</p> <p>Un esempio del formato è il seguente:</p> <pre>iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b</pre> <p> È possibile trovare l'IQN iniziatore per ciascun volume selezionando View Details (Visualizza dettagli) nel menu Actions (azioni) del volume nell'elenco Management > Volumes > Active (Gestione* > volumi > attivo).</p> <p>Quando si modifica un iniziatore, è possibile impostare l'attributo requiredCHAP su True, che consente di impostare il segreto dell'iniziatore di destinazione. Per ulteriori informazioni, vedere informazioni API sul metodo ModifyInitiator API.</p> <p>"Gestire lo storage con l'API Element"</p>

5. **Opzionale:** aggiungere altri iniziatori secondo necessità.
6. In Add Volumes (Aggiungi volumi), selezionare un volume dall'elenco **Volumes** (volumi).
Il volume viene visualizzato nell'elenco **Attached Volumes** (volumi collegati).
7. **Opzionale:** aggiungere altri volumi in base alle esigenze.
8. Fare clic su **Create Access Group** (Crea gruppo di accesso).

Trova ulteriori informazioni

[Aggiungere volumi a un gruppo di accesso](#)

Visualizzare i dettagli dei singoli gruppi di accesso

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

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per un gruppo di accesso.
3. Fare clic su **View Details** (Visualizza dettagli).

Dettagli del gruppo di accesso al volume

La pagina gruppi di accesso nella scheda Gestione fornisce informazioni sui gruppi di accesso ai volumi.

Vengono visualizzate le seguenti informazioni:

- **ID**: L'ID generato dal sistema per il gruppo di accesso.
- **Name** (Nome): Il nome assegnato al gruppo di accesso al momento della creazione.
- **Active Volumes** (volumi attivi): Il numero di volumi attivi nel gruppo di accesso.
- **Compressione**: Il punteggio di efficienza della compressione per il gruppo di accesso.
- **Deduplica**: Il punteggio di efficienza della deduplica per il gruppo di accesso.
- **Thin Provisioning**: Il punteggio di efficienza del thin provisioning per il gruppo di accesso.
- **Efficienza complessiva**: Il punteggio di efficienza globale per il gruppo di accesso.
- **Initiator**: Numero di iniziatori connessi al gruppo di accesso.

Aggiungere volumi a un gruppo di accesso

È possibile aggiungere volumi a un gruppo di accesso al volume. Ciascun volume può appartenere a più di un gruppo di accesso al volume; è possibile visualizzare i gruppi a cui appartiene ciascun volume nella pagina **Active Volumes**.

È inoltre possibile utilizzare questa procedura per aggiungere volumi a un gruppo di accesso ai volumi Fibre Channel.

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso a cui si desidera aggiungere volumi.
3. Fare clic sul pulsante **Edit** (Modifica).
4. In Add Volumes (Aggiungi volumi), selezionare un volume dall'elenco **Volumes** (volumi).

È possibile aggiungere altri volumi ripetendo questo passaggio.

5. Fare clic su **Save Changes** (Salva modifiche).

Rimuovere i volumi da un gruppo di accesso

Quando si rimuove un volume da un gruppo di accesso, il gruppo non ha più accesso a tale 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 improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato qualsiasi modifica alle impostazioni dell'iniziatore e del cluster.

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso da cui si desidera rimuovere i volumi.
3. Fare clic su **Edit** (Modifica).
4. In Add Volumes (Aggiungi volumi) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **Attached Volumes** (volumi collegati).
5. Selezionare il volume che si desidera rimuovere dall'elenco e fare clic sull'icona **x** per rimuoverlo dall'elenco.

È possibile rimuovere più volumi ripetendo questo passaggio.

6. Fare clic su **Save Changes** (Salva modifiche).

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnarli alias.

È inoltre possibile assegnare attributi CHAP basati su initiator utilizzando una chiamata API. Per aggiungere un nome account CHAP e le credenziali per ogni iniziatore, è necessario utilizzare `CreateInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP. L'accesso initiator 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 ulteriori informazioni, vedere le informazioni di riferimento API. "[Gestire lo storage con l'API Element](#)"

Fasi

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

Opzione	Fasi
Creare un singolo iniziatore	<ol style="list-style-type: none">a. Fare clic su Crea un singolo iniziatore.b. Immettere l'IQN o il WWPN dell'iniziatore nel campo IQN/WWPN.c. Immettere un nome descrittivo per l'iniziatore nel campo Alias.d. Fare clic su Crea iniziatore.
Creare più iniziatori	<ol style="list-style-type: none">a. Fare clic su creazione di iniziatori in blocco.b. Inserire un elenco di IQN o WWPN nella casella di testo.c. Fare clic su Aggiungi iniziatori.d. Scegliere 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 Create initiator (Crea iniziatori).

Modificare un iniziatore

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

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

Vedere "[Gestire lo storage con l'API Element](#)".

Fasi

1. Fare clic su **Gestione > iniziatori**.
2. Fare clic sull'icona Actions (azioni) per l'inziatore che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Inserire un nuovo alias per l'inziatore nel campo **Alias**.
5. Fare clic su **Save Changes** (Salva modifiche).

Aggiungere un singolo iniziatore a un gruppo di accesso al volume

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

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



È possibile trovare l'inziatore per ciascun volume facendo clic sull'icona Actions (azioni) e selezionando **View Details** (Visualizza dettagli) per il volume nell'elenco Active Volumes (volumi attivi).

Se si utilizza CHAP basato su iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso a volume, fornendo una maggiore sicurezza. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

Fasi

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Per aggiungere un iniziatore Fibre Channel al gruppo di accesso al volume, attenersi alla seguente procedura:
 - a. In Add Initiator (Aggiungi iniziatori), selezionare un iniziatore Fibre Channel esistente dall'elenco **Unbound Fibre Channel Initiator** (iniziatori Fibre Channel non associati).
 - b. Fare clic su **Aggiungi iniziatore FC**.



È possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo un nome iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'inziatore all'elenco **initiator** dopo averlo creato.

Un esempio del formato è il seguente:

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

5. Per aggiungere un iSCSI Initiator al gruppo di accesso al volume, in Add Initiator (Aggiungi iniziatori), selezionare un iniziatore esistente dall'elenco **Initiator** (iniziatori).



È possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo un nome iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'inziatore all'elenco **initiator** dopo averlo creato.

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

Un esempio del formato è il seguente:

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



È possibile trovare l'IQN iniziatore per ciascun volume dalla pagina **Management > Volumes Active Volumes** facendo clic sull'icona **Actions** (azioni) e selezionando **View Details** (Visualizza dettagli) per il volume.

6. Fare clic su **Save Changes** (Salva modifiche).

Aggiungere più iniziatori a un gruppo di accesso al volume

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

Quando si aggiungono gli 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 **Actions** (azioni), quindi su **View Details** (Visualizza dettagli) per il volume nell'elenco **Active Volumes** (volumi attivi).

È possibile aggiungere più iniziatori a un gruppo di accesso a un volume esistente per consentire l'accesso ai volumi e assegnare credenziali CHAP univoche per ciascun iniziatore all'interno di tale gruppo di accesso a un volume. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

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

Per ulteriori informazioni, vedere ["Gestire lo storage con l'API Element"](#).

Fasi

1. Fare clic su **Gestione > iniziatori**.
2. Selezionare gli iniziatori che si desidera aggiungere a un gruppo di accesso.
3. Fare clic sul pulsante **azioni in blocco**.
4. Fare clic su **Add to Volume Access Group** (Aggiungi a gruppo di accesso volume).
5. Nella finestra di dialogo **Add to Volume Access Group** (Aggiungi a gruppo di accesso al volume), selezionare un gruppo di accesso dall'elenco **Volume Access Group** (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 sarà più possibile accedere ai volumi di tale gruppo di accesso al volume. Il normale accesso 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 improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato qualsiasi modifica alle impostazioni dell'inziatore e del cluster.

Fasi

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera rimuovere.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. In Add Initiator (Aggiungi iniziatori) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **Initiators** (iniziatori).
5. Selezionare l'icona x per ciascun iniziatore che si desidera rimuovere dal gruppo di accesso.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminare 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. Una volta eliminato il gruppo di accesso, l'accesso di gruppo ai volumi viene interrotto.

1. Fare clic su **Gestione > gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera eliminare.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Per eliminare anche gli iniziatori associati a questo gruppo di accesso, selezionare la casella di controllo **Delete initiator in this access group** (Elimina iniziatori in questo gruppo di accesso).
5. Confermare l'azione.

Eliminare un iniziatore

È possibile eliminare un iniziatore una volta che non è più necessario. Quando si elimina un iniziatore, il sistema lo rimuove da qualsiasi gruppo di accesso al volume associato. Tutte le connessioni che utilizzano l'inziatore rimangono valide fino al ripristino della connessione.

Fasi

1. Fare clic su **Gestione > iniziatori**.
2. Eseguire la procedura per eliminare un singolo iniziatore o più iniziatori:

Opzione	Fasi
Eliminare un singolo iniziatore	<ol style="list-style-type: none"> Fare clic sull'icona azioni dell'iniziatore che si desidera eliminare. Fare clic su Delete (Elimina). Confermare l'azione.
Eliminare più iniziatori	<ol style="list-style-type: none"> Selezionare le caselle di controllo accanto agli iniziatori che si desidera eliminare. Fare clic sul pulsante azioni in blocco. Nel menu visualizzato, selezionare Delete (Elimina). Confermare l'azione.

Proteggi i tuoi dati

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

- **Istantanee**

La protezione dei dati solo Snapshot replica i dati modificati in specifici punti di tempo in un cluster remoto. Vengono replicati solo gli snapshot creati nel cluster di origine. Le scritture attive dal volume di origine non lo sono.

[Utilizzare le snapshot dei volumi per la protezione dei dati](#)

- **Replica remota tra cluster e volumi eseguiti su Element**

È possibile replicare i dati del volume in modo sincrono o asincrono da uno dei cluster di 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 con tecnologia SnapMirror**

Con la tecnologia NetApp SnapMirror, è possibile replicare le snapshot acquisite utilizzando Element to ONTAP per scopi di disaster recovery. In una relazione SnapMirror, Element è un endpoint e ONTAP è l'altro.

[Utilizzare la replica SnapMirror tra cluster Element e ONTAP](#)

- **Eseguire 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 in archivi a oggetti SolidFire, S3 o Swift](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

Utilizzare le snapshot dei volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume. È possibile creare un'istantanea di un volume e utilizzarla in un secondo momento se è necessario riportare un volume nello stato in cui si trovava al momento della creazione dell'istantanea.

Gli snapshot sono simili ai cloni dei volumi. Tuttavia, le snapshot sono semplicemente repliche dei metadati del volume, pertanto non è possibile montarle o scriverle. La creazione di uno snapshot di volume richiede anche solo una piccola quantità di risorse e spazio di sistema, rendendo la creazione dello snapshot più rapida rispetto alla clonazione.

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

Facoltativamente, replicare gli snapshot in un cluster remoto e utilizzarli come copia di backup del volume. In questo modo, è possibile eseguire il rollback di un volume a un punto specifico utilizzando lo snapshot replicato. In alternativa, è possibile creare un clone di un volume da uno snapshot replicato.

Trova ulteriori informazioni

- [Utilizzare snapshot di singoli volumi per la protezione dei dati](#)
- [Utilizzo di snapshot di gruppo per attività di protezione dei dati](#)
- [Pianificazione di uno snapshot](#)

Utilizzare snapshot di singoli volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume. È possibile utilizzare un singolo volume anziché un gruppo di volumi per lo snapshot.

Trova ulteriori informazioni

- [Creare un'istantanea del volume](#)
- [Modifica la conservazione delle snapshot](#)
- [Eliminazione di uno snapshot](#)
- [Clonare un volume da uno snapshot](#)
- [Eseguire il rollback di un volume in uno snapshot](#)
- [Backup di uno snapshot di volume in un archivio di oggetti Amazon S3](#)
- [Backup di uno snapshot di volume in un archivio di oggetti OpenStack Swift](#)
- [Backup di uno snapshot di volume in un cluster SolidFire](#)

Creare un'istantanea del volume

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

volume.

1. Fare clic su **Management > Volumes**.
2. Fare clic sull'icona **Actions** del volume che si desidera utilizzare per lo snapshot.
3. Nel menu visualizzato, selezionare **Snapshot**.
4. Nella finestra di dialogo **Create Snapshot of Volume** (Crea snapshot del volume), inserire il nuovo nome dello snapshot.
5. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per assicurarsi che lo snapshot venga acquisito in replica quando il volume padre viene associato.
6. Per impostare la conservazione dello snapshot, selezionare una delle seguenti opzioni:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
7. Per eseguire una singola istantanea, attenersi alla seguente procedura:
 - a. Fare clic su **scatta istantanea ora**.
 - b. Fare clic su **Create Snapshot** (Crea istantanea).
8. Per pianificare l'esecuzione dello snapshot in un momento successivo, attenersi alla seguente procedura:
 - a. Fare clic su **Crea pianificazione snapshot**.
 - b. Immettere un **nuovo nome pianificazione**.
 - c. Scegliere un **tipo di pianificazione** dall'elenco.
 - d. **Opzionale:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
 - e. Fare clic su **Crea pianificazione**.

Trova ulteriori informazioni

[Pianifica un'istantanea](#)

Modifica la conservazione delle snapshot

È possibile modificare il periodo di conservazione di uno snapshot per controllare quando o se il sistema elimina gli snapshot. Il periodo di conservazione specificato inizia quando si inserisce 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 dall'ora di creazione dello snapshot). È possibile specificare intervalli in minuti, ore e giorni.

Fasi

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea che si desidera modificare.
3. Nel menu visualizzato, fare clic su **Edit** (Modifica).
4. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per assicurarsi che lo snapshot venga acquisito nella replica quando il volume padre viene associato.

5. **Opzionale:** selezionare un'opzione di conservazione per lo snapshot:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per selezionare il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminare uno snapshot

È possibile eliminare uno snapshot di volume da un cluster di storage 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 viene sincronizzato con il cluster di destinazione quando lo si elimina, la replica di sincronizzazione viene completata e lo snapshot viene cancellato dal cluster di origine. Lo snapshot non viene cancellato dal cluster di destinazione.

È inoltre possibile eliminare dal cluster di destinazione le snapshot replicate nella destinazione. Lo snapshot cancellato viene conservato in un elenco di snapshot cancellati sulla destinazione fino a quando il sistema non rileva l'eliminazione dello snapshot sul cluster di origine. Quando la destinazione rileva l'eliminazione dello snapshot di origine, la destinazione interrompe la replica dello snapshot.

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

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **azioni** per lo snapshot che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Clonare un volume da uno snapshot

È possibile creare un nuovo volume da uno snapshot di un volume. In questo modo, il sistema utilizza le informazioni di snapshot per clonare un nuovo volume utilizzando i dati contenuti nel volume al momento della creazione dello snapshot. Questo processo memorizza le informazioni relative ad altri snapshot del volume nel volume appena creato.

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot che si desidera utilizzare per il clone del volume.
3. Nel menu visualizzato, fare clic su **Clone Volume from Snapshot** (Clona volume da snapshot).
4. Inserire un **Nome volume** nella finestra di dialogo **Clone Volume from Snapshot** (Copia volume da snapshot).
5. Selezionare **Total Size** (dimensione totale) e le unità di misura per il nuovo volume.
6. Selezionare un tipo **Access** per il volume.
7. Selezionare un **account** dall'elenco da associare al nuovo volume.
8. Fare clic su **Avvia clonazione**.

Eseguire il rollback di un volume in uno snapshot

È possibile eseguire il rollback di un volume a uno snapshot precedente in qualsiasi momento. In questo modo vengono ripristinate le modifiche apportate al volume dalla creazione dello snapshot.

Fasi

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, selezionare **Rollback Volume to Snapshot** (Ripristina volume in snapshot).
4. **Opzionale:** per salvare lo stato corrente del volume prima di eseguire il rollback allo snapshot:
 - a. Nella finestra di dialogo **Rollback to Snapshot**, selezionare **Save the current state as a snapshot** (Salva stato corrente del volume come snapshot).
 - b. Immettere un nome per il nuovo snapshot.
5. Fare clic su **Rollback Snapshot**.

Eseguire il backup di uno snapshot di un volume

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

- ["Eseguire il backup di uno snapshot di volume in un archivio di oggetti Amazon S3"](#)
- ["Eseguire il backup di uno snapshot di volume in un archivio di oggetti OpenStack Swift"](#)
- ["Eseguire il backup di uno snapshot di volume in un cluster SolidFire"](#)

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

Puoi eseguire il backup delle istantanee di SolidFire in archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Integrated Backup** sotto **Backup in**, selezionare **S3**.
5. Selezionare un'opzione in **formato dati**:
 - **Nativo:** Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso:** Un formato non compresso compatibile con altri sistemi.
6. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
7. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
8. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).

9. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
10. **Opzionale:** Inserire un nametag da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

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

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

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup in**, selezionare **Swift**.
5. Selezionare un'opzione in **formato dati**:
 - **Nativo:** Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso:** Un formato non compresso compatibile con altri sistemi.
6. Inserire un **URL** da utilizzare per accedere all'archivio di oggetti.
7. Inserire un **Nome utente** per l'account.
8. Inserire la **Authentication Key** dell'account.
9. Inserire il **container** in cui memorizzare il backup.
10. **Opzionale:** Inserire un **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di uno snapshot di volume in un cluster SolidFire

È possibile eseguire il backup delle snapshot dei volumi che risiedono su un cluster SolidFire in un cluster SolidFire remoto.

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

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Management > Volumes**.
2. Fare clic sull'icona **Actions** del volume di destinazione.
3. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
4. Nella finestra di dialogo **Ripristino integrato** sotto **Ripristina da**, selezionare **SolidFire**.
5. Selezionare un formato dati in **formato dati**:
 - **Nativo:** Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso:** Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).

7. Copiare la chiave dalla casella **Bulk Volume Write Key** negli Appunti.
8. Nel cluster di origine, fare clic su **Data Protection > Snapshot**.
9. Fare clic sull'icona Actions (azioni) per lo snapshot che si desidera utilizzare per il backup.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo **Backup integrato** sotto **Backup in**, selezionare **SolidFire**.
12. Selezionare lo stesso formato di dati selezionato in precedenza nel campo **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Nel campo **Bulk Volume Write Key** (chiave di scrittura volume in blocco), incollare la chiave generata in precedenza nel cluster di destinazione.
17. Fare clic su **Avvia lettura**.

Utilizzo di snapshot di gruppo per attività di protezione dei dati

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

Trova ulteriori informazioni

- [Creare un'istantanea di gruppo](#)
- [Modificare le snapshot di gruppo](#)
- [Modificare i membri dell'istantanea del gruppo](#)
- [Eliminare uno snapshot di gruppo](#)
- [Eseguire il rollback dei volumi in uno snapshot di gruppo](#)
- [Clonare più volumi](#)
- [Clonare più volumi da uno snapshot di gruppo](#)

Dettagli snapshot di gruppo

La pagina Group Snapshots (istantanee gruppo) della scheda Data Protection (protezione dati) fornisce informazioni sulle istantanee del gruppo.

- **ID**

L'ID generato dal sistema per lo snapshot di gruppo.

- **UUID**

L'ID univoco dello snapshot di gruppo.

- **Nome**

Nome definito dall'utente per lo snapshot di gruppo.

- **Ora di creazione**

L'ora in cui è stata creata l'istantanea del gruppo.

- **Stato**

Lo stato corrente dello snapshot. Valori possibili:

- Preparazione: Lo snapshot è in fase di preparazione e non è ancora scrivibile.
- Fatto: Questo snapshot ha terminato la preparazione ed è ora utilizzabile.
- Attivo: Lo snapshot è il ramo attivo.

- *** N. volumi***

Il numero di volumi nel gruppo.

- **Conservare fino al**

Il giorno e l'ora in cui lo snapshot viene cancellato.

- **Replica remota**

Indicazione dell'attivazione o meno dello snapshot per la replica su un cluster SolidFire remoto. Valori possibili:

- Enabled (attivato): Lo snapshot è abilitato per la replica remota.
- Disabled (Disattivato): Lo snapshot non è abilitato per la replica remota.

Creazione di uno snapshot di gruppo

È possibile creare un'istantanea di un gruppo di volumi e una pianificazione snapshot di gruppo per automatizzare le snapshot di gruppo. Un singolo snapshot di gruppo può creare costantemente snapshot di fino a 32 volumi alla volta.

Fasi

1. Fare clic su **Management > Volumes**.
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 **Group Snapshot** (istantanea gruppo).
5. Inserire un nuovo nome di snapshot di gruppo nella finestra di dialogo Crea snapshot di gruppo dei volumi.
6. **Opzionale:** selezionare la casella di controllo **Includi ogni membro Snapshot di gruppo nella replica quando accoppiato** per assicurarsi che ogni snapshot venga acquisito nella replica quando il volume padre viene associato.
7. Selezionare un'opzione di conservazione per lo snapshot di gruppo:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.

8. Per eseguire una singola istantanea, attenersi alla seguente procedura:
 - a. Fare clic su **scatta snapshot di gruppo ora**.
 - b. Fare clic su **Create Group Snapshot** (Crea istantanea gruppo).
9. Per pianificare l'esecuzione dello snapshot in un momento successivo, attenersi alla seguente procedura:
 - a. Fare clic su **Crea pianificazione snapshot di gruppo**.
 - b. Immettere un **nuovo nome pianificazione**.
 - c. Selezionare un **tipo di pianificazione** dall'elenco.
 - d. **Opzionale:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
 - e. Fare clic su **Crea pianificazione**.

Modifica delle snapshot di gruppo

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

1. Fare clic su **Data Protection > Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. **Opzionale:** per modificare l'impostazione di replica per lo snapshot di gruppo:
 - a. Fare clic su **Edit** (Modifica) accanto a **Current Replication** (replica corrente).
 - b. Selezionare la casella di controllo **include each Group Snapshot Member in Replication when paired** (Includi ogni membro Snapshot di gruppo nella replica quando viene associato) per assicurarsi che ogni snapshot venga acquisito in replica quando viene associato il volume padre.
5. **Opzionale:** per modificare l'impostazione di conservazione per lo snapshot di gruppo, selezionare una delle seguenti opzioni:
 - a. Fare clic su **Edit** (Modifica) accanto a **Current retention** (conservazione corrente).
 - b. Selezionare un'opzione di conservazione per lo snapshot di gruppo:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminazione di uno snapshot di gruppo

È possibile eliminare un'istantanea di gruppo dal sistema. Quando si elimina lo snapshot di gruppo, è possibile scegliere se tutte le snapshot associate al gruppo vengono eliminate o conservate come singole istantanee.

Se si elimina un volume o uno snapshot membro di uno snapshot di gruppo, non è più possibile eseguire il rollback allo snapshot di gruppo. Tuttavia, è possibile eseguire il rollback di ciascun volume singolarmente.

1. Fare clic su **Data Protection > Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot che si desidera eliminare.

3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Selezionare una delle seguenti opzioni nella finestra di dialogo di conferma:
 - Fare clic su **Delete group snapshot AND all group snapshot members** (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 membri snapshot di gruppo come singole snapshot** per eliminare lo snapshot di gruppo ma conservare tutti gli snapshot dei membri.
5. Confermare l'azione.

Eeguire il rollback dei volumi in uno snapshot di gruppo

È possibile eseguire il rollback di un gruppo di volumi in qualsiasi momento 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 di gruppo. Il rollback ripristina anche le dimensioni del volume alle dimensioni registrate nello snapshot originale. Se il sistema ha eliminato un volume, anche tutte le snapshot di quel volume sono state eliminate al momento della rimozione; il sistema non ripristina le snapshot del volume eliminate.

1. Fare clic su **Data Protection > Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera utilizzare per il rollback del volume.
3. Nel menu risultante, selezionare **Rollback Volumes to Group Snapshot** (Esegui il rollback dei volumi in Group Snapshot).
4. **Opzionale:** Per salvare lo stato corrente dei volumi prima di eseguire il rollback allo snapshot:
 - a. Nella finestra di dialogo **Rollback to Snapshot**, selezionare **Save Volumes' Current state as a group snapshot** (Salva stato corrente dei volumi come snapshot di gruppo).
 - b. Immettere un nome per il nuovo snapshot.
5. Fare clic su **Rollback Group Snapshot**.

Modifica dei membri dello snapshot di gruppo

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

1. Fare clic su **Data Protection > Snapshot**.
2. Fare clic sulla scheda **membri**.
3. Fare clic sull'icona Actions (azioni) per il membro dello snapshot di gruppo che si desidera modificare.
4. Nel menu visualizzato, selezionare **Edit** (Modifica).
5. Per modificare l'impostazione di replica per lo snapshot, selezionare una delle seguenti opzioni:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Clonare più volumi

È possibile creare più cloni di volume in una singola operazione per creare una copia point-in-time dei dati su un gruppo di volumi.

Quando si clonano un volume, il sistema crea uno snapshot del volume e 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 un tempo variabile in base alle dimensioni e al numero dei volumi clonati.

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

Fasi

1. Fare clic su **Management > Volumes**.
2. Fare clic sulla scheda **Active**.
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 **Clone** nel menu visualizzato.
6. Inserire un **nuovo prefisso nome volume** nella finestra di dialogo **Clone multiple Volumes** (Copia volumi multipli).

Il prefisso viene applicato a tutti i volumi del gruppo.

7. **Opzionale:** selezionare un account diverso a cui appartiene il clone.

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

8. **Opzionale:** 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 point-in-time. 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 del sistema.

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

1. Fare clic su **Data Protection > Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera utilizzare per i cloni del volume.
3. Nel menu risultante, selezionare **Clone Volumes from Group Snapshot** (Clona volumi da snapshot di gruppo).
4. Inserire un **nuovo prefisso nome volume** nella finestra di dialogo **Clone Volumes from Group Snapshot** (Copia volumi da snapshot gruppo).

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

5. **Opzionale:** selezionare un account diverso a cui appartiene il clone.

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

6. **Opzionale:** 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 un'istantanea

È possibile proteggere i dati di un volume o di un gruppo di volumi programmando che le snapshot dei volumi vengano eseguite a intervalli specificati. È possibile pianificare l'esecuzione automatica di snapshot di singoli volumi o di gruppi.

Quando si configura una pianificazione snapshot, è possibile scegliere tra intervalli di tempo in base ai giorni della settimana o dei giorni del mese. È inoltre possibile specificare i giorni, le ore e i minuti prima che si verifichi l'istantanea successiva. Se il volume viene replicato, è possibile memorizzare le snapshot risultanti su un sistema di storage remoto.

Trova ulteriori informazioni

- [Creare una pianificazione di snapshot](#)
- [Modificare una pianificazione di snapshot](#)
- [Eliminare una pianificazione di snapshot](#)
- [Copiare una pianificazione di snapshot](#)

Dettagli della pianificazione di Snapshot

Nella pagina Data Protection > Schedules (protezione dati > programmi), è possibile visualizzare le seguenti informazioni nell'elenco delle pianificazioni di snapshot.

- **ID**

L'ID generato dal sistema per lo snapshot.

- **Tipo**

Il tipo di pianificazione. Snapshot è attualmente l'unico tipo supportato.

- **Nome**

Il nome assegnato alla pianificazione al momento della sua creazione. I nomi delle pianificazioni di Snapshot possono contenere fino a 223 caratteri e contengono caratteri a-z, 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**

Indicazione se il programma deve essere eseguito una sola volta o a intervalli regolari.

- **Pausa manuale**

Indicazione se la pianificazione è stata messa in pausa manualmente.

- **ID volume**

L'ID del volume utilizzato dalla pianificazione quando viene eseguita la pianificazione.

- **Ultima esecuzione**

L'ultima volta in cui è stato eseguito il programma.

- **Stato ultima esecuzione**

Il risultato dell'ultima esecuzione del programma. Valori possibili:

- Successo
- Guasto

Creare una pianificazione di snapshot

È possibile pianificare un'istantanea di uno o più volumi in modo che venga eseguita automaticamente a intervalli specificati.

Quando si configura una pianificazione snapshot, è possibile scegliere tra intervalli di tempo in base ai giorni della settimana o dei giorni del mese. È inoltre possibile creare una pianificazione ricorrente e specificare i giorni, le ore e i minuti prima che si verifichi l'istantanea successiva.

Se si pianifica l'esecuzione di uno snapshot in un periodo di tempo non divisibile di 5 minuti, lo snapshot verrà eseguito nel periodo di tempo successivo, divisibile di 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.

Fasi

1. Fare clic su **Data Protection > Schedules**.
2. Fare clic su **Crea pianificazione**.
3. Nel campo **Volume IDS CSV**, immettere un singolo ID volume o un elenco separato da virgole di ID volume da includere nell'operazione di snapshot.
4. Immettere un nuovo nome per la pianificazione.
5. Selezionare un tipo di pianificazione e impostarla dalle opzioni fornite.
6. **Opzionale:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione dello snapshot a tempo indeterminato.
7. **Opzionale:** inserire un nome per la nuova istantanea nel campo **New Snapshot Name** (Nome nuova istantanea).

Se si lascia il campo vuoto, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.

8. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiate** per assicurarsi che le snapshot vengano acquisite nella replica quando il volume padre viene associato.
9. Per impostare la conservazione dello snapshot, selezionare una delle seguenti opzioni:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
10. Fare clic su **Crea pianificazione**.

Modificare una pianificazione di snapshot

È possibile modificare le pianificazioni di snapshot esistenti. Dopo la modifica, la prossima volta che la pianificazione viene eseguita, utilizza gli attributi aggiornati. Tutte le snapshot create dalla pianificazione originale rimangono nel sistema di storage.

Fasi

1. Fare clic su **Data Protection > Schedules**.
2. Fare clic sull'icona **azioni** relativa alla pianificazione che si desidera modificare.
3. Nel menu visualizzato, fare clic su **Edit** (Modifica).
4. Nel campo **Volume IDS CSV**, modificare l'ID di un singolo volume o l'elenco separato da virgole degli ID di volume attualmente inclusi nell'operazione di snapshot.
5. Per sospendere o riprendere la pianificazione, selezionare una delle seguenti opzioni:
 - Per mettere in pausa un programma attivo, selezionare **Sì** dall'elenco **Pausa manualmente programma**.
 - Per riprendere un programma in pausa, selezionare **No** dall'elenco **Manually Pause Schedule** (programma di pausa manuale).
6. Immettere un nome diverso per la pianificazione nel campo **New Schedule Name** (Nome nuova pianificazione), se si desidera.
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. **Opzionale:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione dello snapshot a tempo indeterminato.
9. **Opzionale:** inserire o modificare il nome del nuovo snapshot nel campo **New Snapshot Name** (Nome nuovo snapshot).

Se si lascia il campo vuoto, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.
10. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiate** per assicurarsi che le snapshot vengano acquisite nella replica quando il volume padre viene associato.
11. Per modificare l'impostazione di conservazione, selezionare una delle seguenti opzioni:
 - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
 - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per selezionare il periodo di tempo in cui il sistema conserva lo snapshot.
12. Fare clic su **Save Changes** (Salva modifiche).

Copiare una pianificazione di snapshot

È possibile copiare una pianificazione e mantenerne gli attributi correnti.

1. Fare clic su **Data Protection > Schedules**.
2. Fare clic sull'icona Actions (azioni) per il programma che si desidera copiare.
3. Nel menu visualizzato, fare clic su **Crea copia**.

Viene visualizzata la finestra di dialogo **Create Schedule** (Crea pianificazione), contenente gli attributi correnti della pianificazione.

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

Eliminare una pianificazione di snapshot

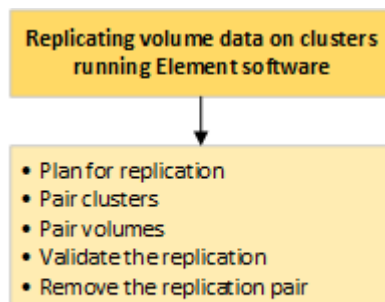
È possibile eliminare una pianificazione di snapshot. Una volta eliminata la pianificazione, non vengono eseguite snapshot pianificate in futuro. Tutte le snapshot create dalla pianificazione rimangono nel sistema di storage.

1. Fare clic su **Data Protection > Schedules**.
2. Fare clic sull'icona **azioni** del programma che si desidera eliminare.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Confermare l'azione.

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 creazione rapida di copie remote dei dati dei volumi. È possibile associare un cluster di storage a un massimo di quattro altri cluster di storage. È possibile replicare i dati del volume in modo sincrono o asincrono da uno dei cluster di una coppia di cluster per scenari di failover e failback.

Il processo di replica include i seguenti passaggi:



- ["Pianificare l'associazione di cluster e volumi per la replica in tempo reale"](#)
- ["Associare i cluster per la replica"](#)

- ["Associare i volumi"](#)
- ["Convalidare la replica del volume"](#)
- ["Eliminare una relazione di volume dopo la replica"](#)
- ["Gestire le relazioni dei volumi"](#)

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

La replica remota in tempo reale richiede l'associazione di due cluster di storage che eseguono il software Element, l'associazione di volumi su ciascun cluster e la convalida della replica. Una volta completata la replica, è necessario eliminare la relazione del volume.

Di cosa hai bisogno

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.
- Tutti gli indirizzi IP dei nodi delle reti di gestione e storage per i cluster accoppiati vengono instradati l'uno all'altro.
- La MTU di tutti i nodi accoppiati deve essere la stessa e deve essere supportata end-to-end tra i cluster.
- Entrambi i cluster di storage devono avere nomi di cluster univoci, MVIP, SVIP e tutti gli indirizzi IP dei nodi.
- La differenza tra le versioni software degli elementi sui cluster non è superiore a una versione principale. Se la differenza è maggiore, uno dei cluster deve essere aggiornato per eseguire la replica dei dati.



Le appliance WAN Accelerator non sono state qualificate da NetApp per l'utilizzo durante la replica dei dati. Queste appliance possono interferire con la compressione e la deduplica se implementate tra due cluster che stanno replicando i dati. Assicurarsi di qualificare completamente gli effetti di qualsiasi appliance WAN Accelerator prima di implementarla in un ambiente di produzione.

Trova ulteriori informazioni

- [Associare i cluster per la replica](#)
- [Associare i volumi](#)
- [Assegnare un'origine e una destinazione di replica ai volumi accoppiati](#)

Associare i cluster per la replica

Per utilizzare la funzionalità di replica in tempo reale, è necessario associare due cluster come primo passo. Dopo aver associato e connesso due cluster, è possibile configurare i volumi attivi su un cluster per la replica continua su un secondo cluster, fornendo una protezione continua dei dati (CDP).

Di cosa hai bisogno

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.
- Tutti i MIPS e i SIPS 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 univoci, MVIP, SVIP e tutti gli indirizzi IP dei

nodi.

- La differenza tra le versioni software degli elementi sui cluster non è superiore a una versione principale. Se la differenza è maggiore, uno dei cluster deve essere aggiornato per eseguire la replica dei dati.



L'associazione dei cluster richiede una connettività completa tra i nodi della rete di gestione. La replica richiede la connettività tra i singoli nodi sulla rete del cluster di storage.

È possibile associare un cluster a un massimo di quattro altri cluster per la replica dei volumi. È inoltre possibile associare tra loro i cluster all'interno del gruppo di cluster.

Trova ulteriori informazioni

[Requisiti delle porte di rete](#)

Associare i cluster utilizzando MVIP o una chiave di accoppiamento

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

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

Trova ulteriori informazioni

- [Associare i cluster utilizzando MVIP](#)
- [Associare i cluster utilizzando una chiave di accoppiamento](#)

Associare i cluster utilizzando 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 disporre dell'accesso dell'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 di poter associare i cluster.

1. Nel cluster locale, selezionare **Data Protection > Cluster Pairs**.
2. Fare clic su **Pair Cluster**.
3. Fare clic su **Start Pairing** (Avvia associazione) e fare clic su **Yes** (Sì) per indicare che si dispone dell'accesso al cluster remoto.
4. Inserire l'indirizzo MVIP del cluster remoto.

5. Fare clic su **complete pairing on remote cluster**.

Nella finestra **Authentication Required** (autenticazione richiesta), immettere il nome utente e la password dell'amministratore del cluster remoto.

6. Sul cluster remoto, selezionare **Data Protection > Cluster Pairs**.

7. Fare clic su **Pair Cluster**.

8. Fare clic su **completa associazione**.

9. Fare clic sul pulsante **complete Pairing** (completa associazione).

Trova ulteriori informazioni

- [Associare i cluster utilizzando una chiave di accoppiamento](#)
- ["Associazione di cluster mediante MVIP \(video\)"](#)

Associare i cluster utilizzando una chiave di accoppiamento

Se si dispone dell'accesso di un amministratore del cluster a un cluster locale ma non a un cluster remoto, è possibile associare i cluster utilizzando una chiave di accoppiamento. Una chiave di accoppiamento viene generata su un cluster locale e quindi inviata in modo sicuro a un amministratore del cluster presso un sito remoto per stabilire una connessione e completare l'accoppiamento del cluster per la replica in tempo reale.

1. Nel cluster locale, selezionare **Data Protection > Cluster Pairs**.
2. Fare clic su **Pair Cluster**.
3. Fare clic su **Start Pairing** (Avvia associazione) e fare clic su **No** per indicare che non si dispone dell'accesso al cluster remoto.
4. Fare clic su **generate Key** (genera chiave).



Questa azione genera una chiave di testo per l'associazione e crea una coppia di cluster non configurata sul cluster locale. Se la procedura non viene completata, è necessario eliminare manualmente la coppia di cluster.

5. Copiare la chiave di accoppiamento del cluster negli Appunti.
6. Rendere la chiave di accoppiamento accessibile all'amministratore del cluster nel sito del cluster remoto.



La chiave di accoppiamento del cluster contiene una versione di MVIP, nome utente, password e informazioni sul database per consentire le connessioni dei volumi per la replica remota. Questa chiave deve essere trattata in modo sicuro e non memorizzata in modo da consentire l'accesso accidentale o non sicuro al nome utente o alla password.



Non modificare i caratteri della chiave di accoppiamento. La chiave diventa non valida se viene modificata.

7. Sul cluster remoto, selezionare **Data Protection > Cluster Pairs**.
8. Fare clic su **Pair Cluster**.

9. Fare clic su **complete Pairing** (completa associazione) e inserire la chiave di associazione nel campo **Pairing Key** (chiave di associazione) (il metodo consigliato è incollare).
10. Fare clic su **completa associazione**.

Trova ulteriori informazioni

- [Associare i cluster utilizzando MVIP](#)
- ["Associazione dei cluster mediante una chiave di accoppiamento dei cluster \(video\)"](#)

Convalidare la connessione della coppia di cluster

Una volta completata l'associazione del cluster, è possibile verificare la connessione della coppia di cluster per garantire la riuscita della replica.

1. Nel cluster locale, selezionare **Data Protection > Cluster Pairs**.
2. Nella finestra **Cluster Pairs**, verificare che la coppia di cluster sia connessa.
3. **Opzionale:** tornare al cluster locale e alla finestra **Cluster Pairs** e verificare che la coppia di cluster sia connessa.

Associare i volumi

Dopo aver stabilito una connessione tra i cluster di una coppia di cluster, è possibile associare un volume di un cluster a un volume dell'altro cluster della coppia. Quando viene stabilita una relazione di accoppiamento dei volumi, è necessario identificare quale volume è la destinazione della replica.

È possibile associare due volumi per la replica in tempo reale memorizzati in diversi cluster di storage in una coppia di cluster connessi. Dopo aver associato due cluster, è possibile configurare i volumi attivi su un cluster per la replica continua su un secondo cluster, fornendo una protezione continua dei dati (CDP). È inoltre possibile assegnare un volume come origine o destinazione della replica.

I volumi sono sempre uno a uno. Dopo che un volume fa parte di un'associazione con un volume su un altro cluster, non è possibile associarlo nuovamente con altri volumi.

Di cosa hai bisogno

- È stata stabilita una connessione tra i cluster di una coppia di cluster.
- Si dispone dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.

Fasi

1. [Creare 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 replica ai volumi accoppiati](#)

Creare un volume di destinazione con accesso in lettura o scrittura

Il processo di replica 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 **Management > Volumes**.
2. Fare clic su **Create Volume** (Crea volume).
3. Nella finestra di dialogo Create a New Volume (Crea un nuovo volume), immettere il nome del volume.
4. Inserire le dimensioni totali del volume, selezionare una dimensione di blocco per il volume e selezionare l'account che deve avere accesso al volume.
5. Fare clic su **Create Volume** (Crea volume).
6. Nella finestra Active (attivo), fare clic sull'icona Actions (azioni) per il volume.
7. Fare clic su **Edit** (Modifica).
8. Impostare il livello di accesso dell'account su destinazione della replica.
9. Fare clic su **Save Changes** (Salva modifiche).

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

Il processo di associazione prevede l'associazione di due volumi utilizzando un ID volume o una chiave di associazione.

1. Associare i volumi selezionando uno dei seguenti metodi:
 - Utilizzo di un ID volume: Utilizzare questo metodo se si dispone dell'accesso dell'amministratore del cluster a entrambi i cluster sui quali devono essere associati i volumi. Questo metodo utilizza l'ID del volume sul cluster remoto per avviare una connessione.
 - Utilizzo di una chiave di accoppiamento: Utilizzare questo metodo se si dispone dell'accesso dell'amministratore del cluster solo al cluster di origine. Questo metodo genera una chiave di accoppiamento che può essere utilizzata sul cluster remoto per completare la coppia di volumi.



La chiave di accoppiamento del volume contiene una versione crittografata delle informazioni del volume e potrebbe contenere informazioni riservate. Condividere questa chiave solo in modo sicuro.

Trova ulteriori informazioni

- [Associare i volumi utilizzando un ID volume](#)
- [Associare i volumi utilizzando una chiave di accoppiamento](#)

Associare i volumi utilizzando un ID volume

È possibile associare un volume a un altro volume su un cluster remoto se si dispone delle credenziali di amministratore del cluster per il cluster remoto.

Di cosa hai bisogno

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



È possibile assegnare un'origine e una destinazione di replica dopo il processo di associazione. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione delle dimensioni del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

- Conoscere l'ID del volume di destinazione.

Fasi

1. Selezionare **Management > Volumes**.
2. Fare clic sull'icona **azioni** del volume che si desidera associare.
3. Fare clic su **Pair** (abbina).
4. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **Start Pairing** (Avvia associazione).
5. Selezionare **do** per indicare che si dispone dell'accesso al cluster remoto.
6. Selezionare una **Replication Mode** dall'elenco:
 - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.
 - **Real-time (Synchronous)**: Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
 - **Solo istantanee**: Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Selezionare un cluster remoto dall'elenco.
8. Scegliere un ID volume remoto.
9. Fare clic su **Start Pairing** (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 Element del cluster remoto, selezionare **complete Pairing** (completa associazione).
11. Confermare i dettagli in **Confirm Volume Pairing** (Conferma associazione volume).
12. Fare clic su **completa associazione**.

Dopo aver confermato l'associazione, i due cluster iniziano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Volume Status** (Stato volume) della finestra **Volume Pairs** (coppie di volumi). Viene visualizzata la coppia di volumi `PausedMisconfigured` fino a quando non vengono assegnate l'origine e la destinazione della coppia di volumi.

Una volta completata l'associazione, aggiornare la tabella Volumes (volumi) per rimuovere l'opzione **Pair** dall'elenco **Actions** (azioni) per il volume associato. Se non si aggiorna la tabella, l'opzione **Pair** rimane disponibile per la selezione. Se si seleziona di nuovo l'opzione **Pair**, viene visualizzata una nuova scheda e, poiché il volume è già associato, il sistema riporta un `StartVolumePairing Failed: xVolumeAlreadyPaired` Messaggio di errore nella finestra **Pair Volume** della pagina dell'interfaccia utente dell'elemento.

Trova ulteriori informazioni

- [Messaggi di associazione del volume](#)
- [Avvisi di associazione del volume](#)
- [Assegnare un'origine e una destinazione di replica ai volumi accoppiati](#)

Associare i volumi utilizzando una chiave di accoppiamento

Se non si dispone delle credenziali di amministratore del cluster per un cluster remoto, è possibile associare un volume a un altro volume di un cluster remoto utilizzando una chiave di accoppiamento.

Di cosa hai bisogno

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



È possibile assegnare un'origine e una destinazione di replica dopo il processo di associazione. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione delle dimensioni del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

Fasi

1. Selezionare **Management > Volumes**.
2. Fare clic sull'icona **azioni** del volume che si desidera associare.
3. Fare clic su **Pair** (abbina).
4. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **Start Pairing** (Avvia associazione).
5. Selezionare **i do not** per indicare che non si dispone dell'accesso al cluster remoto.
6. Selezionare una **Replication Mode** dall'elenco:
 - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.
 - **Real-time (Synchronous)**: Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
 - **Solo istantanee**: Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Fare clic su **generate Key** (genera chiave).



Questa azione genera una chiave di testo per l'associazione e crea una coppia di volumi non configurata sul cluster locale. Se la procedura non viene completata, è necessario eliminare manualmente la coppia di volumi.

8. Copiare la chiave di accoppiamento nella clipboard del computer.
9. Rendere la chiave di accoppiamento accessibile all'amministratore del cluster nel sito del cluster remoto.



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



Non modificare i caratteri della chiave di accoppiamento. La chiave diventa non valida se viene modificata.

10. Nell'interfaccia utente degli elementi del cluster remoto, selezionare **Management > Volumes**.
11. Fare clic sull'icona Actions (azioni) per il volume che si desidera associare.
12. Fare clic su **Pair** (abbina).
13. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **complete Pairing** (completa associazione).
14. Incollare la chiave di accoppiamento dall'altro cluster nella casella **Pairing Key** (chiave di associazione).
15. Fare clic su **completa associazione**.

Dopo aver confermato l'associazione, i due cluster iniziano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Volume Status** (Stato volume) della finestra **Volume Pairs** (coppie di volumi). Viene visualizzata la coppia di volumi `PausedMisconfigured` fino a quando non vengono assegnate l'origine e la destinazione della coppia di volumi.

Una volta completata l'associazione, aggiornare la tabella Volumes (volumi) per rimuovere l'opzione **Pair** dall'elenco **Actions** (azioni) per il volume associato. Se non si aggiorna la tabella, l'opzione **Pair** rimane disponibile per la selezione. Se si seleziona di nuovo l'opzione **Pair**, viene visualizzata una nuova scheda e, poiché il volume è già associato, il sistema riporta un `StartVolumePairing Failed: xVolumeAlreadyPaired` Messaggio di errore nella finestra **Pair Volume** della pagina dell'interfaccia utente dell'elemento.

Trova ulteriori informazioni

- [Messaggi di associazione del volume](#)
- [Avvisi di associazione del volume](#)
- [Assegnare un'origine e una destinazione di replica ai volumi accoppiati](#)

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

Una volta associati i volumi, è necessario assegnare un volume di origine e il relativo volume di destinazione della replica. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È inoltre possibile utilizzare questa procedura 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 fosse disponibile.

Di cosa hai bisogno

È possibile accedere ai cluster contenenti i volumi di origine e di destinazione.

Fasi

1. Preparare il volume di origine:
 - a. Dal cluster che contiene il volume che si desidera assegnare come origine, selezionare **Management**

> Volumes.

- b. Fare clic sull'icona **azioni** del volume che si desidera assegnare come origine e fare clic su **Modifica**.
- c. Nell'elenco a discesa **Access**, selezionare **Read/Write** (lettura/scrittura).



Se si sta annullando l'assegnazione di origine e destinazione, questa azione fa sì che la coppia di volumi visualizzi il seguente messaggio fino a quando non viene assegnata una nuova destinazione di replica: PausedMisconfigured

La modifica dell'accesso interrompe la replica del volume e interrompe la trasmissione dei dati. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

- a. Fare clic su **Save Changes** (Salva modifiche).

2. Preparare il volume di destinazione:

- a. Dal cluster che contiene il volume che si desidera assegnare come destinazione, selezionare **Management > Volumes**.
- b. Fare clic sull'icona Actions (azioni) per il volume che si desidera assegnare come destinazione e fare clic su **Edit** (Modifica).
- c. Nell'elenco a discesa **Access**, selezionare **Replication Target**.



Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. È necessario utilizzare un nuovo volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione 512e e configurazione QoS. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

- d. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- [Associare i volumi utilizzando un ID volume](#)
- [Associare i volumi utilizzando una chiave di accoppiamento](#)

Convalidare la replica del volume

Una volta replicato un volume, assicurarsi che i volumi di origine e di destinazione siano attivi. Quando si trova in uno stato attivo, i volumi vengono associati, i dati vengono inviati dall'origine al volume di destinazione e i dati sono sincronizzati.

1. Da entrambi i cluster, selezionare **Data Protection > Volume Pairs**.
2. Verificare che lo stato del volume sia attivo.

Trova ulteriori informazioni

[Avvisi di associazione del volume](#)

Eliminare una relazione di volume dopo la replica

Una volta completata la replica e non è più necessaria la relazione della coppia di volumi,

è possibile eliminare la relazione del volume.

1. Selezionare **Data Protection > Volume Pairs**.
2. Fare clic sull'icona **Actions** della coppia di volumi che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Gestire le relazioni dei volumi

È possibile gestire le relazioni dei volumi in molti modi, ad esempio mettendo in pausa la replica, invertendo l'accoppiamento dei volumi, modificando la modalità di replica, eliminando una coppia di volumi o eliminando una coppia di cluster.

Trova ulteriori informazioni

- [Mettere in pausa la replica](#)
- [Modificare la modalità di replica](#)
- [Eliminare le coppie di volumi](#)

Mettere in pausa la replica

È possibile sospendere manualmente la replica se è necessario interrompere l'elaborazione i/o per un breve periodo di tempo. È possibile sospendere la replica se si verifica un aumento nell'elaborazione i/o e si desidera ridurre il carico di elaborazione.

1. Selezionare **Data Protection > Volume Pairs**.
2. Fare clic sull'icona **Actions** (azioni) per la coppia di volumi.
3. Fare clic su **Edit** (Modifica).
4. Nel riquadro **Edit Volume Pair** (Modifica coppia di volumi), sospendere manualmente il processo di replica.



La sospensione o la ripresa manuale della replica del volume causa la cessazione o la ripresa della trasmissione dei dati. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Save Changes** (Salva modifiche).

Modificare la modalità di replica

È possibile modificare le proprietà della coppia di volumi per modificare la modalità di replica della relazione della coppia di volumi.

1. Selezionare **Data Protection > Volume Pairs**.
2. Fare clic sull'icona **Actions** (azioni) per la coppia di volumi.
3. Fare clic su **Edit** (Modifica).
4. Nel riquadro **Edit Volume Pair** (Modifica coppia di volumi), selezionare una nuova modalità di replica:
 - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.

- **Real-time (Synchronous):** Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
- **Solo istantanee:** Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate. **Attenzione:** la modifica della modalità di replica modifica immediatamente la modalità. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare le coppie di volumi

È possibile eliminare una coppia di volumi se si desidera rimuovere un'associazione di coppia tra due volumi.

1. Selezionare **Data Protection > Volume Pairs**.
2. Fare clic sull'icona Actions (azioni) per la coppia di volumi che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Eliminare una coppia di cluster

È possibile eliminare una coppia di cluster dall'interfaccia utente degli elementi di uno dei cluster della coppia.

1. Fare clic su **Data Protection > Cluster Pairs**.
2. Fare clic sull'icona Actions (azioni) per una coppia di cluster.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Confermare l'azione.
5. Eseguire nuovamente i passaggi dal secondo cluster nell'associazione del cluster.

Dettagli della coppia di cluster

La pagina Cluster Pairs della scheda Data Protection (protezione dati) fornisce informazioni sui cluster che sono stati associati o che sono in fase di associazione. Il sistema visualizza i messaggi di associazione e di avanzamento nella colonna Status (Stato).

- **ID**

ID generato dal sistema assegnato a ciascuna coppia di cluster.

- **Nome cluster remoto**

Il nome dell'altro cluster della coppia.

- **MVIP remoto**

L'indirizzo IP virtuale di gestione dell'altro cluster della coppia.

- **Stato**

Stato della replica del cluster remoto

- **Replica dei volumi**

Il numero di volumi contenuti nel cluster che sono accoppiati per la replica.

- **UUID**

Un ID univoco assegnato a ciascun cluster della coppia.

Dettagli della coppia di volumi

La pagina Volume Pairs (coppie di volumi) nella scheda Data Protection (protezione dati) fornisce informazioni sui volumi che sono stati associati o che sono in fase di associazione. Il sistema visualizza i messaggi di associazione e di avanzamento nella colonna Volume Status (Stato volume).

- **ID**

ID generato dal sistema per il volume.

- **Nome**

Il nome assegnato al volume al momento della creazione. I nomi dei volumi possono contenere fino a 223 caratteri e contengono a-z, 0-9 e trattino (-).

- **Account**

Nome dell'account assegnato al volume.

- **Volume Status** (Stato volume)

Stato di replica del volume

- **Stato snapshot**

Stato del volume di snapshot.

- **Modalità**

Il metodo di replica in scrittura del client. I valori possibili sono i seguenti:

- Asincrono
- Solo Snapshot
- Sincronizza

- **Direzione**

La direzione dei dati del volume:

- Icona del volume di origine (➔) indica che i dati vengono scritti in una destinazione esterna al cluster.
- Icona del volume di destinazione (➔) indica che i dati vengono scritti nel volume locale da un'origine esterna.

- **Ritardo asincrono**

Periodo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è associato, 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 volume remoto**

Nome assegnato al volume remoto al momento della creazione.

Messaggi di associazione del volume

È possibile visualizzare i messaggi di associazione dei volumi durante il processo di associazione iniziale dalla pagina Volume Pairs (coppie di volumi) nella scheda Data Protection (protezione dati). Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia nella vista elenco Replica volumi.

- **PausedDisconnected**

Replica di origine o sincronizzazione RPC scaduta. La connessione al cluster remoto è stata persa. Controllare le connessioni di rete al cluster.

- **RisumingConnected**

La sincronizzazione della replica remota è ora attiva. Avvio del processo di sincronizzazione e attesa dei dati.

- **RisumingRRSync**

Una singola copia helix dei metadati del volume viene eseguita sul cluster associato.

- **RisumingLocalSync**

Viene eseguita una copia a doppia elica dei metadati del volume nel cluster associato.

- **RisumingDataTransfer**

Il trasferimento dei dati è ripreso.

- **Attivo**

I volumi vengono associati e i dati vengono inviati dall'origine al volume di destinazione e i dati sono sincronizzati.

- **Inattivo**

Nessuna attività di replica in corso.

Avvisi di associazione del volume

La pagina Thevolume Pairs della scheda Data Protection (protezione dati) fornisce questi messaggi dopo l'accoppiamento dei volumi. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia (se non diversamente indicato) nella vista elenco Replica volumi.

- **PausedClusterFull**

Poiché il cluster di destinazione è pieno, la replica di origine e il trasferimento di dati in blocco non possono procedere. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedExceedMaxSnapshotCount**

Il volume di destinazione dispone già del numero massimo di snapshot e non può replicare snapshot aggiuntivi.

- **PausedManual**

Il volume locale è stato messo in pausa manualmente. Prima di riprendere la replica, è necessario che la replica sia sospesa.

- **PausedManualRemote**

Il volume remoto è in modalità di pausa manuale. È richiesto l'intervento manuale per riattivare il volume remoto prima che la replica venga ripresa.

- **PausedMisconfigured**

In attesa di un'origine e di una destinazione attive. È richiesto l'intervento manuale per riprendere la replica.

- **QoS Paused**

QoS di destinazione non è riuscito a sostenere i/o in entrata. La replica riprende automaticamente. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedSlowLink**

Collegamento lento rilevato e replica interrotta. La replica riprende automaticamente. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedVolumeSizeMismatch**

Il volume di destinazione non ha le stesse dimensioni del volume di origine.

- **PausedXCOPY**

Viene inviato un comando SCSI XCOPY a un volume di origine. Il comando deve essere completato prima che la replica possa riprendere. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **StoppedMisconfigured**

È stato rilevato un errore di configurazione permanente. Il volume remoto è stato disaccoppiato o disaccoppiato. Non è possibile eseguire alcuna azione correttiva; è necessario stabilire una nuova associazione.

Utilizzare la replica SnapMirror tra cluster Element e ONTAP

È possibile creare relazioni SnapMirror dalla scheda protezione dati dell'interfaccia utente di NetApp Element. La funzionalità di SnapMirror deve essere attivata per visualizzarla nell'interfaccia utente.

IPv6 non è supportato per la replica di SnapMirror tra il software NetApp Element e i cluster ONTAP.

["Video NetApp: SnapMirror per NetApp HCI ed Element Software"](#)

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare le copie Snapshot con i sistemi NetApp ONTAP. Il motivo principale dell'utilizzo di questa tecnologia è il disaster recovery di NetApp HCI in ONTAP. Gli endpoint includono ONTAP, ONTAP Select e Cloud Volumes ONTAP. Consulta la protezione dei dati TR-4641 NetApp HCI.

["Report tecnico NetApp 4641: Protezione dei dati NetApp HCI"](#)

Trova ulteriori informazioni

- ["Creazione del data fabric con NetApp HCI, ONTAP e infrastruttura convergente"](#)
- ["Replica tra il software NetApp Element e ONTAP"](#)

Panoramica di SnapMirror

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare le snapshot con i sistemi NetApp ONTAP.

I sistemi che eseguono Element possono comunicare direttamente con SnapMirror su sistemi ONTAP 9.3 o superiori. L'API di 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 di SnapMirror tra il software Element e i sistemi ONTAP.

È possibile replicare i volumi originati da ONTAP in volumi Element in casi di utilizzo specifici con funzionalità limitate. Per ulteriori informazioni, consultare la documentazione di ONTAP.

Trova ulteriori informazioni

["Replica tra software Element e ONTAP"](#)

Attivare SnapMirror sul cluster

È necessario attivare manualmente la funzionalità SnapMirror a livello di cluster tramite l'interfaccia utente di NetApp Element. Il sistema viene fornito con la funzionalità SnapMirror disattivata per impostazione predefinita e non viene attivata automaticamente durante una nuova installazione o un aggiornamento. L'attivazione della funzione SnapMirror è un'attività di configurazione unica.

SnapMirror può essere abilitato solo per i cluster che eseguono il software Element utilizzato insieme ai volumi su un sistema NetApp ONTAP. È necessario attivare la funzionalità SnapMirror solo se il cluster è connesso per l'utilizzo con i volumi NetApp ONTAP.

Di cosa hai bisogno

Il cluster di storage deve eseguire il software NetApp Element.

Fasi

1. Fare clic su **Clusters > Impostazioni**.
2. Individuare le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Enable SnapMirror** (attiva SnapMirror)



L'attivazione della funzionalità SnapMirror modifica in modo permanente la configurazione del software Element. È possibile disattivare la funzione SnapMirror e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster.

4. Fare clic su **Si** per confermare la modifica della configurazione di SnapMirror.

Attivare SnapMirror sul volume

È necessario attivare SnapMirror sul volume nell'interfaccia utente di Element. Ciò consente la replica dei dati in volumi ONTAP specificati. Questa è l'autorizzazione dell'amministratore del cluster che esegue il software NetApp Element per SnapMirror per controllare un volume.

Di cosa hai bisogno

- SnapMirror è stato attivato nell'interfaccia utente Element per il cluster.
- È disponibile un endpoint SnapMirror.
- Il volume deve essere di dimensioni di blocco 512e.
- Il volume non partecipa alla replica remota.
- Il tipo di accesso al volume non è destinazione della replica.



È inoltre possibile impostare questa proprietà durante la creazione o la clonazione di un volume.

Fasi

1. Fare clic su **Management > Volumes**.
2. Fare clic sull'icona **Actions** del volume per il quale si desidera attivare SnapMirror.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. Nella finestra di dialogo **Edit Volume** (Modifica volume), selezionare la casella di controllo **Enable SnapMirror** (attiva SnapMirror).
5. Fare clic su **Save Changes** (Salva modifiche).

Creare un endpoint SnapMirror

Prima di creare una relazione, è necessario creare un endpoint SnapMirror nell'interfaccia utente di NetApp Element.

Un endpoint SnapMirror è un cluster ONTAP che funge da destinazione di replica per un cluster che esegue software Element. Prima di creare una relazione SnapMirror, creare un endpoint SnapMirror.

È possibile creare e gestire fino a quattro endpoint SnapMirror in un cluster di storage 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 utilizzando l'API Element.

Per ulteriori informazioni sui metodi API, vedere "[Gestire lo storage con l'API Element](#)".

Di cosa hai bisogno

- È necessario aver attivato SnapMirror nell'interfaccia utente Element per il cluster di storage.
- Conosci le credenziali ONTAP per l'endpoint.

Fasi

1. Fare clic su **Data Protection > SnapMirror Endpoints**.
2. Fare clic su **Create Endpoint** (Crea endpoint).
3. Nella finestra di dialogo **Crea nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster del sistema ONTAP.
4. Immettere le credenziali di amministratore di ONTAP associate all'endpoint.
5. Leggi ulteriori dettagli:
 - LIF: Elenca le interfacce logiche dell'intercluster ONTAP utilizzate per comunicare con Element.
 - Status (Stato): Mostra lo stato corrente dell'endpoint SnapMirror. I valori possibili sono: Connesso, disconnesso e non gestito.
6. Fare clic su **Create Endpoint** (Crea endpoint).

Creare una relazione SnapMirror

È necessario creare una relazione SnapMirror nell'interfaccia utente di NetApp Element.



Quando un volume non è ancora abilitato per SnapMirror e si sceglie di creare una relazione dall'interfaccia utente di Element, SnapMirror viene attivato automaticamente su tale volume.

Di cosa hai bisogno

SnapMirror è attivato sul volume.

Fasi

1. Fare clic su **Management > Volumes**.
2. Fare clic sull'icona **azioni** del volume che deve essere parte della relazione.
3. Fare clic su **Crea una relazione SnapMirror**.
4. Nella finestra di dialogo **Crea una relazione SnapMirror**, selezionare 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 **Storage Virtual Machine** per questa relazione.
 - b. Selezionare **aggregato** dall'elenco a discesa.
 - c. Nel campo **Volume Name Suffix** (suffisso nome volume), immettere un suffisso.



Il sistema rileva il nome del volume di origine e lo copia nel campo **Volume Name** (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 **Use existing volume** (Usa volume esistente).
 - a. Selezionare **Storage Virtual Machine** per questa relazione.
 - b. Selezionare il volume di destinazione per questa nuova relazione.
8. Nella sezione **Dettagli relazione**, selezionare un criterio. Se il criterio selezionato dispone di regole di conservazione, nella tabella regole vengono visualizzate le regole e le etichette associate.
9. **Opzionale**: Selezionare un programma.

In questo modo si determina la frequenza con cui la relazione crea le copie.

10. **Opzionale**: Nel campo **limita larghezza di banda a**, immettere la quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
11. Leggi ulteriori dettagli:
 - **State**: Stato di relazione corrente del volume di destinazione. I valori possibili sono:
 - uninitialized (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 di SnapMirror.
 - Interrotto: Il volume di destinazione è in lettura/scrittura e sono presenti snapshot.
 - **Status**: Stato corrente della relazione. I valori possibili sono idle, trasferimento, controllo, sospensione, quiesced, in coda, preparazione, finalizzazione, interruzione e interruzione.
 - **Lag Time** (tempo di ritardo): La quantità di tempo in secondi che il sistema di destinazione rimane indietro rispetto al sistema di origine. Il tempo di ritardo non deve superare l'intervallo di pianificazione del trasferimento.
 - **Bandwidth limit** (limite larghezza di banda): La quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
 - **Ultimo trasferimento**: Data e ora dell'ultimo snapshot trasferito. Fare clic per ulteriori informazioni.
 - **Nome policy**: Il nome del criterio SnapMirror di ONTAP per la relazione.
 - **Tipo di policy**: Tipo di policy SnapMirror di ONTAP selezionata per la relazione. I valori possibili sono:
 - mirror_asincrono
 - vault_mirror
 - **Nome pianificazione**: Nome della pianificazione preesistente sul sistema ONTAP selezionato per questa relazione.

12. Per non eseguire l'inizializzazione in questo momento, assicurarsi che la casella di controllo **Inizializza** non sia selezionata.



L'inizializzazione può richiedere molto tempo. Potrebbe essere necessario eseguire questa operazione durante le ore di lavoro fuori dalle ore di punta. L'inizializzazione esegue un trasferimento baseline; crea una copia snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. È possibile eseguire l'inizializzazione manualmente o utilizzare un programma per avviare il processo di inizializzazione (e gli aggiornamenti successivi) in base alla pianificazione.

13. Fare clic su **Crea relazione**.
14. Fare clic su **Data Protection > SnapMirror Relationship** per visualizzare questa nuova relazione SnapMirror.

Azioni di relazione di SnapMirror

È possibile configurare una relazione dalla pagina delle relazioni di SnapMirror della scheda protezione dati. Di seguito sono descritte le opzioni dell'icona azioni.

- **Edit**: Modifica la policy utilizzata o la pianificazione della relazione.
- **Delete**: Elimina la relazione SnapMirror. Questa funzione non elimina il volume di destinazione.
- **Inizializza**: Esegue il primo trasferimento iniziale dei dati di riferimento per stabilire una nuova relazione.
- **Update**: Esegue un aggiornamento on-demand della relazione, replicando i nuovi dati e le copie Snapshot incluse dall'ultimo aggiornamento alla destinazione.
- **Quiesce**: Impedisce ulteriori aggiornamenti per una relazione.
- **Resume**: Riprende una relazione che è stata rinunciata.
- **Break**: Consente di eseguire la lettura/scrittura del volume di destinazione e di interrompere tutti i trasferimenti correnti e futuri. Determinare che i client non utilizzano il volume di origine originale, poiché l'operazione di risincronizzazione inversa rende il volume di origine di sola lettura.
- **Resync**: Stabilisce una relazione interrotta nella stessa direzione prima che si verificasse l'interruzione.
- **Reverse Resync**: Automatizza i passaggi necessari per creare e inizializzare una nuova relazione nella direzione opposta. Questa operazione può essere eseguita solo se la relazione esistente si trova in uno stato interrotto. Questa operazione non elimina la relazione corrente. Il volume di origine torna alla copia Snapshot più recente e viene risincronizzato con la destinazione. Tutte le modifiche apportate al volume di origine dall'ultimo aggiornamento di SnapMirror sono perse. Tutte le modifiche apportate o i nuovi dati scritti nel volume di destinazione corrente vengono inviati nuovamente al volume di origine originale.
- **Interrompi**: Annulla un trasferimento in corso. Se viene emesso un aggiornamento di SnapMirror per una relazione interrotta, la relazione continua con l'ultimo trasferimento dall'ultimo checkpoint di riavvio creato prima dell'interruzione.

Etichette SnapMirror

Un'etichetta SnapMirror funge da indicatore 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 di SnapMirror. Il ruolo della relazione è quello di applicare le regole al momento del trasferimento dei dati selezionando lo snapshot etichettato corrispondente, copiandolo nel volume di destinazione e garantendo che venga conservato il numero corretto di copie. Si riferisce alla policy per determinare il numero di conservazione e il periodo di conservazione. Il criterio 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 applicare per lo snapshot, lo snapshot di gruppo o la pianificazione selezionati.

Aggiungere le etichette SnapMirror alle snapshot

Le etichette SnapMirror specificano il criterio di conservazione delle snapshot sull'endpoint SnapMirror. È possibile aggiungere etichette alle istantanee e raggruppare le istantanee.

È possibile visualizzare le etichette disponibili da una finestra di dialogo relazione SnapMirror esistente o da Gestore di sistema NetApp ONTAP.



Quando si aggiunge un'etichetta a uno snapshot di gruppo, le etichette esistenti alle singole istantanee vengono sovrascritte.

Di cosa hai bisogno

- SnapMirror è attivato sul cluster.
- L'etichetta che si desidera aggiungere esiste già in ONTAP.

Fasi

1. Fare clic su **Data Protection > Snapshot** o sulla pagina **Group Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot o lo snapshot di gruppo a cui si desidera aggiungere un'etichetta SnapMirror.
3. Nella finestra di dialogo **Edit Snapshot** (Modifica snapshot), inserire il testo nel campo **SnapMirror Label** (etichetta SnapMirror). L'etichetta deve corrispondere all'etichetta di una regola nel criterio applicato alla relazione SnapMirror.
4. Fare clic su **Save Changes** (Salva modifiche).

Aggiunta di etichette SnapMirror alle pianificazioni di snapshot

È possibile aggiungere etichette SnapMirror alle pianificazioni di snapshot per garantire l'applicazione di un criterio SnapMirror. È possibile visualizzare le etichette disponibili da una finestra di dialogo relazione SnapMirror esistente o da NetAppONTAP System Manager.

Di cosa hai bisogno

- SnapMirror deve essere attivato a livello di cluster.
- L'etichetta che si desidera aggiungere esiste già in ONTAP.

Fasi

1. Fare clic su **Data Protection > Schedules**.
2. Aggiungere un'etichetta SnapMirror a una pianificazione in uno dei seguenti modi:

Opzione	Fasi
Creazione di una nuova pianificazione	a. Selezionare Crea pianificazione . b. Inserire tutti gli altri dettagli pertinenti. c. Selezionare Crea pianificazione .
Modifica della pianificazione esistente	a. Fare clic sull'icona azioni del programma a cui si desidera aggiungere un'etichetta e selezionare Modifica . b. Nella finestra di dialogo visualizzata, inserire il testo nel campo etichetta SnapMirror . c. Selezionare Save Changes (Salva modifiche).

Trova ulteriori informazioni

[Creare una pianificazione di snapshot](#)

Disaster recovery con 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 e il failover verso il volume di destinazione.



Se il cluster originale è completamente guasto o non esiste, contattare il supporto NetApp per ulteriore assistenza.

Eseguire un failover da un cluster di elementi

È possibile eseguire un failover dal cluster di elementi per rendere il volume di destinazione di lettura/scrittura e accessibile agli host sul lato di destinazione. Prima di eseguire un failover dal cluster di elementi, è necessario interrompere la relazione SnapMirror.

Utilizzare l'interfaccia utente di NetApp Element per eseguire il failover. Se l'interfaccia utente di Element non è disponibile, è possibile utilizzare anche Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP per eseguire il comando break relationship.

Di cosa hai bisogno

- Esiste una relazione SnapMirror che contiene almeno uno snapshot valido nel volume di destinazione.
- È necessario eseguire il failover sul volume di destinazione a causa di un'interruzione non pianificata o di un evento pianificato nel sito primario.

Fasi

1. Nell'interfaccia utente di Element, fare clic su **Data Protection > SnapMirror Relanes**.
2. Individuare la relazione con il volume di origine che si desidera eseguire il failover.
3. Fare clic sull'icona **azioni**.
4. Fare clic su **Interrompi**.

5. Confermare l'azione.

Il volume sul cluster di destinazione dispone ora dell'accesso in lettura/scrittura e può essere montato sugli host delle applicazioni per riprendere i carichi di lavoro di produzione. Tutta la replica di SnapMirror viene interrotta in seguito a questa azione. La relazione mostra uno stato di interrotto.

Eeguire un failback a Element

Una volta mitigato il problema sul lato primario, è necessario risincronizzare il volume di origine originale e ripristinare il software NetApp Element. I passaggi da eseguire variano a seconda che il volume di origine sia ancora esistente o che sia necessario eseguire il failback a un volume appena creato.

Trova ulteriori informazioni

- [Eeguire un failback quando il volume di origine esiste ancora](#)
- [Eeguire un failback quando il volume di origine non esiste più](#)
- [Scenari di failback di SnapMirror](#)

Scenari di failback di SnapMirror

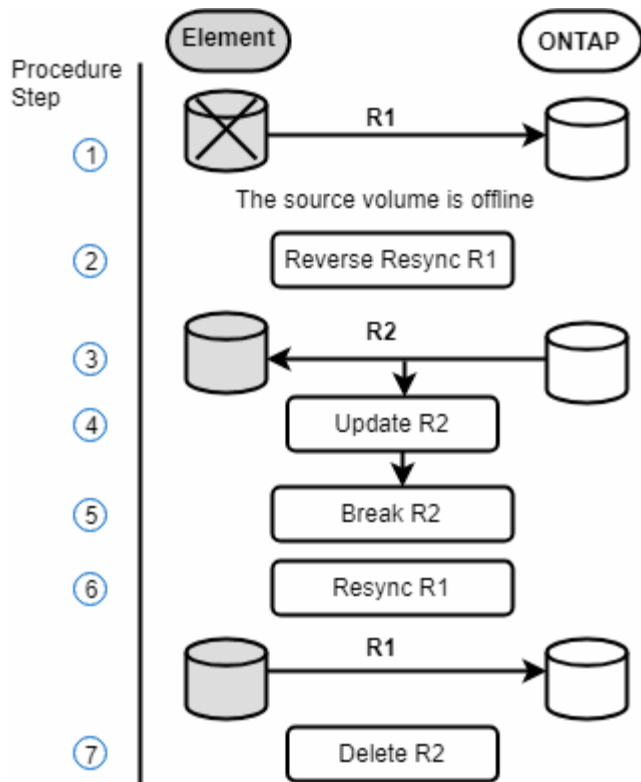
La funzionalità di disaster recovery di SnapMirror è illustrata in due scenari di failback. Questi presuppongono che la relazione originale sia stata interrotta.

Le fasi delle procedure corrispondenti vengono aggiunte come riferimento.

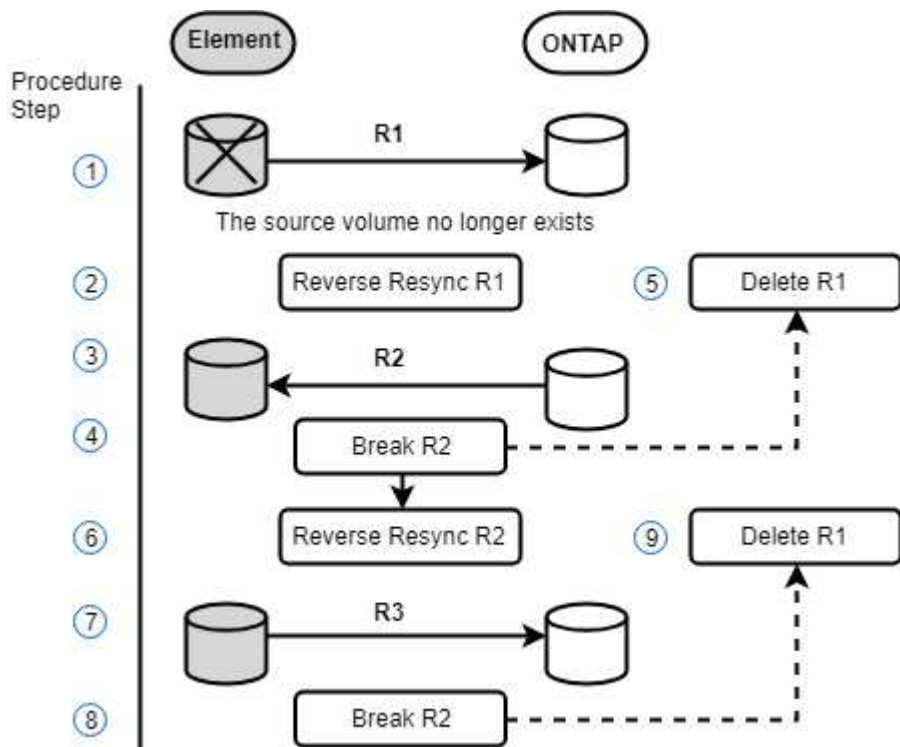


Negli esempi qui riportati, R1 = relazione originale in cui il cluster che esegue il software NetApp Element è il volume di origine (elemento) originale e ONTAP è il volume di destinazione originale (ONTAP). R2 e R3 rappresentano le relazioni inverse create attraverso l'operazione di risincronizzazione inversa.

La seguente immagine mostra lo scenario di failback quando il volume di origine è ancora presente:



L'immagine seguente mostra lo scenario di failback quando il volume di origine non esiste più:



Trova ulteriori informazioni

- [Eseguire un failback quando il volume di origine esiste ancora](#)
- [Eseguire un failback quando il volume di origine non esiste più](#)

Eseguire un failback quando il volume di origine esiste ancora

È possibile risincronizzare il volume di origine originale e eseguire un failback utilizzando l'interfaccia utente di NetApp Element. Questa procedura si applica agli scenari in cui il volume di origine originale esiste ancora.

1. Nell'interfaccia utente di Element, individuare la relazione che si è spezzata per eseguire il failover.
2. Fare clic sull'icona delle azioni e fare clic su **Reverse Resync** (risincronizzazione inversa).
3. Confermare l'azione.



L'operazione Reverse Resync crea una nuova relazione in cui i ruoli dei volumi di origine e di destinazione originali vengono invertiti (questo comporta due relazioni quando la relazione originale persiste). Tutti i nuovi dati del volume di destinazione originale vengono trasferiti al volume di origine come parte dell'operazione di risincronizzazione inversa. È possibile continuare ad accedere e scrivere i dati nel volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host nel volume di origine ed eseguire un aggiornamento di SnapMirror prima di reindirizzare nuovamente al volume primario originale.

4. Fare clic sull'icona Actions (azioni) della relazione inversa appena creata e fare clic su **Update** (Aggiorna).

Una volta completata la risincronizzazione inversa, assicurarsi 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, per completare il failback e riattivare il volume primario originale, procedere come segue:

5. Fare clic sull'icona Actions (azioni) della relazione inversa e fare clic su **Break** (Interrompi).
6. Fare clic sull'icona Actions (azioni) della relazione originale e fare clic su **Resync**.



Il volume primario originale può ora essere montato per riprendere i carichi di lavoro di produzione sul volume primario originale. La replica di SnapMirror originale riprende in base al criterio e alla pianificazione configurati per la relazione.

7. Dopo aver confermato che lo stato della relazione originale è "snapmirrored", fare clic sull'icona Actions (azioni) della relazione inversa e fare clic su **Delete** (Elimina).

Trova ulteriori informazioni

[Scenari di failback di SnapMirror](#)

Eseguire un failback quando il volume di origine non esiste più

È possibile risincronizzare il volume di origine originale e eseguire un failback utilizzando l'interfaccia utente di NetApp Element. Questa sezione si applica agli scenari in cui il volume di origine originale è stato perso ma il cluster originale è ancora intatto. Per istruzioni su come eseguire il ripristino in un nuovo cluster, consultare la documentazione sul sito del supporto NetApp.

Di cosa hai bisogno

- Si dispone di una relazione di replica interrotta tra i volumi Element e ONTAP.
- Il volume dell'elemento viene irrimediabilmente perso.

- Il nome del volume originale viene visualizzato come NON TROVATO.

Fasi

1. Nell'interfaccia utente di Element, individuare la relazione che si è spezzata per eseguire il failover.

Best practice: prendere nota della policy di SnapMirror e dei dettagli di pianificazione della relazione interrotta originale. Queste informazioni saranno necessarie quando si ricrea la relazione.

2. Fare clic sull'icona **azioni** e fare clic su **Reverse Resync** (risincronizzazione inversa).
3. Confermare 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 (questo comporta due relazioni quando la relazione originale persiste). Poiché il volume originale non esiste più, il sistema crea un nuovo volume elemento con lo stesso nome e le stesse dimensioni del volume di origine. Al nuovo volume viene assegnata una policy QoS predefinita chiamata SM-recovery ed è associato a un account predefinito chiamato SM-recovery. Si desidera modificare manualmente l'account e la policy QoS per tutti i volumi creati da SnapMirror per sostituire i volumi di origine 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 i dati nel volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host nel volume attivo ed eseguire un aggiornamento di 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 seguenti passaggi 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 **interruzione**.
5. Fare clic sull'icona **azioni** della relazione originale, in cui il volume di origine non esiste, quindi fare clic su **Elimina**.
6. Fare clic sull'icona **Actions** della relazione inversa, che si è spezzata al punto 4, quindi fare clic su **Reverse Resync** (risincronizzazione inversa).
7. In questo modo vengono invertiti l'origine e la destinazione e si ottiene una relazione con la stessa origine e destinazione del volume della relazione originale.
8. Fare clic sull'icona **azioni** e su **Modifica** per aggiornare questa relazione con le impostazioni di pianificazione e policy QoS originali di cui si è preso nota.
9. Ora è possibile eliminare in modo sicuro la relazione inversa risynced al punto 6.

Trova ulteriori informazioni

[Scenari di failback di 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 storage ONTAP può

fungere da origine ed elemento come destinazione.

- Esistono due scenari:
 - Nessuna relazione precedente di disaster recovery. Seguire tutte le fasi di questa procedura.
 - Esiste una relazione di disaster recovery precedente, ma non tra i volumi utilizzati per questa mitigazione. In questo caso, seguire solo i passaggi 3 e 4 riportati di seguito.

Di cosa hai bisogno

- Il nodo di destinazione dell'elemento deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.

Specificare il percorso di destinazione dell'elemento nel formato `hostip:/lun/<id_number>`, dove `lun` è la stringa corrente "lun" e `id_number` è l'ID del volume dell'elemento.

Fasi

1. Utilizzando ONTAP, creare la relazione con il cluster di elementi:

```
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 `show` di ONTAP `snapmirror`.

Vedere le informazioni sulla creazione di una relazione di replica nella documentazione di ONTAP e per la sintassi completa dei comandi, vedere la pagina `man` di ONTAP.

3. Utilizzando il `ElementCreateVolume` API, creare il volume di destinazione e impostare la modalità di accesso al volume di destinazione su SnapMirror:

Creare 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 replica utilizzando ONTAP `snapmirror initialize` comando:

```

snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume

```

Backup e 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 ripristini i volumi da OpenStack Swift o Amazon S3, hai bisogno di informazioni manifeste dal processo di backup originale. Se si sta ripristinando un volume di cui è stato eseguito il backup su un sistema di storage SolidFire, non sono necessarie informazioni sul manifesto.

Trova ulteriori informazioni

- [Eseguire il backup di un volume in un archivio di oggetti Amazon S3](#)
- [Eseguire il backup di un volume in un archivio di oggetti OpenStack Swift](#)
- [Eseguire il backup di un volume in un cluster di storage SolidFire](#)
- [Ripristinare un volume dal backup in un archivio di oggetti Amazon S3](#)
- [Ripristinare un volume dal backup in un archivio di oggetti OpenStack Swift](#)
- [Ripristinare un volume dal backup su un cluster di storage SolidFire](#)

Eseguire il backup di un volume in un archivio di oggetti Amazon S3

Puoi eseguire il backup dei volumi in archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Management > Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume di cui si desidera eseguire il backup.

3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Integrated Backup** sotto **Backup in**, selezionare **S3**.
5. Selezionare un'opzione in **formato dati**:
 - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
7. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
8. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).
9. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
10. Inserire un nametag da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di un volume in un archivio di oggetti OpenStack Swift

È possibile eseguire il backup dei volumi in archivi di oggetti esterni compatibili con OpenStack Swift.

1. Fare clic su **Management > Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume di cui eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Backup integrato** sotto **Backup in**, selezionare **Swift**.
5. Selezionare un formato dati in **formato dati**:
 - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un URL da utilizzare per accedere all'archivio di oggetti nel campo **URL**.
7. Immettere un nome utente per l'account nel campo **Nome utente**.
8. Inserire la chiave di autenticazione per l'account nel campo **Authentication Key** (chiave di autenticazione).
9. Inserire il contenitore in cui memorizzare il backup nel campo **container**.
10. **Opzionale**: Inserire un tag nome da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di un volume in un cluster di storage SolidFire

È possibile eseguire il backup dei volumi che risiedono su un cluster remoto per i cluster di storage che eseguono il software Element.

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

Vedere ["Associare i cluster per la replica"](#).

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come

autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, **Gestione > volumi**.
2. Fare clic sull'icona Actions (azioni) per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **Restore from** (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 storage SolidFire.
 - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).
7. Copiare la chiave dalla casella **Bulk Volume Write Key** negli Appunti.
8. Nel cluster di origine, andare a **Management > Volumes**.
9. Fare clic sull'icona Actions (azioni) per il volume di cui eseguire il backup.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo **Backup integrato** sotto **Backup in**, selezionare **SolidFire**.
12. Selezionare la stessa opzione selezionata in precedenza nel campo **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Nel campo **Bulk Volume Write Key** (chiave di scrittura volume in blocco), incollare la chiave generata in precedenza nel cluster di destinazione.
17. Fare clic su **Avvia lettura**.

Ripristinare un volume dal backup in un archivio di oggetti Amazon S3

Puoi ripristinare un volume da un backup su un archivio di oggetti Amazon S3.

1. Fare clic su **Reporting > Event Log**.
2. Individuare l'evento di backup che ha creato il backup da ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copiare le informazioni del manifesto negli Appunti.
5. Fare clic su **Management > Volumes**.
6. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
8. Nella finestra di dialogo **Integrated Restore** sotto **Restore from** (Ripristina da), selezionare **S3**.
9. Selezionare l'opzione corrispondente al backup in **formato dati**:
 - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.

- **Non compresso**: Un formato non compresso compatibile con altri sistemi.
10. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
 11. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
 12. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).
 13. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
 14. Incollare le informazioni del manifesto nel campo **manifesto**.
 15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup in un archivio di oggetti OpenStack Swift

È possibile ripristinare un volume da un backup su un archivio di oggetti OpenStack Swift.

1. Fare clic su **Reporting > Event Log**.
2. Individuare l'evento di backup che ha creato il backup da ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copiare le informazioni del manifesto negli Appunti.
5. Fare clic su **Management > Volumes**.
6. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
8. Nella finestra di dialogo **Integrated Restore** sotto **Restore from**, selezionare **Swift**.
9. Selezionare l'opzione corrispondente al backup in **formato dati**:
 - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
 - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
10. Inserire un URL da utilizzare per accedere all'archivio di oggetti nel campo **URL**.
11. Immettere un nome utente per l'account nel campo **Nome utente**.
12. Inserire la chiave di autenticazione per l'account nel campo **Authentication Key** (chiave di autenticazione).
13. Inserire il nome del contenitore in cui è memorizzato il backup nel campo **container**.
14. Incollare le informazioni del manifesto nel campo **manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup su un cluster di storage SolidFire

È possibile ripristinare un volume da un backup su un cluster di storage SolidFire.

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Management > Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
3. Nel menu visualizzato, fare clic su **Restore from** (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 storage SolidFire.
 - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).
7. Copiare le informazioni **Volume Write Key** negli Appunti.
8. Nel cluster di origine, fare clic su **Management > Volumes**.
9. Fare clic sull'icona Actions (azioni) del volume che si desidera utilizzare per il ripristino.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo **Backup integrato**, selezionare **SolidFire** in **Backup su**.
12. Selezionare l'opzione corrispondente al backup in **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Incollare la chiave dagli appunti nel campo **Volume Write Key**.
17. Fare clic su **Avvia lettura**.

Risolvere i problemi del sistema

È necessario monitorare il sistema a scopo diagnostico e ottenere informazioni sulle tendenze delle performance e sugli stati delle varie operazioni del sistema. Potrebbe essere necessario sostituire nodi o SSD per scopi di manutenzione.

- ["Visualizza informazioni sugli eventi di sistema"](#)
- ["Visualizzare lo stato delle attività in esecuzione"](#)
- ["Visualizzare gli avvisi di sistema"](#)
- ["Visualizzare l'attività delle performance dei nodi"](#)
- ["Visualizza le performance dei volumi"](#)
- ["Visualizzare le sessioni iSCSI"](#)
- ["Visualizzare le sessioni Fibre Channel"](#)
- ["Risolvere i problemi relativi ai dischi"](#)
- ["Risolvere i problemi dei nodi"](#)
- ["Utilizzo di utility per nodo per nodi di storage"](#)
- ["Lavorare con il nodo di gestione"](#)

- ["Comprendere i livelli di completezza del cluster"](#)

Per ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per server vCenter"](#)

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 per il cluster.

1. Nell'interfaccia utente di Element, selezionare **Reporting > Event Log**.

Per ogni evento, vengono visualizzate le seguenti informazioni:

Elemento	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 servizio	Il servizio che ha segnalato l'evento (se applicabile).
Nodo	Il nodo che ha riportato l'evento (se applicabile).
ID disco	L'unità che ha segnalato l'evento (se applicabile).
Ora dell'evento	L'ora in cui si è verificato l'evento.

Trova ulteriori informazioni

[Tipi di evento](#)

Tipi di evento

Il sistema riporta diversi tipi di eventi; ogni evento è un'operazione che il sistema ha completato. 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 vengono visualizzati nel registro eventi:

- **ApiEvent**

Eventi avviati da un utente attraverso un'API o un'interfaccia utente Web che modificano le impostazioni.

- **BinAssignmentsEvent**

Eventi correlati all'assegnazione dei bin di dati. I bin sono essenzialmente container 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 a blocchi.

- **BsKillEvent**

Eventi di sistema correlati alle interruzioni del servizio di blocco.

- **BulkOpEvent**

Eventi correlati alle operazioni eseguite su un intero volume, ad esempio backup, ripristino, snapshot o clone.

- **CloneEvent**

Eventi correlati alla clonazione del volume.

- **ClusterMasterEvent**

Eventi visualizzati all'inizializzazione del cluster o in seguito a modifiche della configurazione del cluster, ad esempio l'aggiunta o la rimozione di nodi.

- **CsumEvent**

Eventi relativi a checksum di dati non validi sul disco.

- **DataEvent**

Eventi relativi alla lettura e alla scrittura dei dati.

- **DbEvent**

Eventi correlati al database globale gestito dai nodi dell'ensemble nel cluster.

- **DriveEvent**

Eventi relativi alle operazioni del disco.

- **EncryptionAtRestEvent**

Eventi correlati al processo di crittografia su un cluster.

- **EnsembleEvent**

Eventi correlati all'aumento o alla diminuzione del numero di nodi in un ensemble.

- **FiberChannelEvent**

Eventi relativi alla configurazione e alle connessioni ai nodi.

- **GcEvent**

Gli eventi relativi ai processi vengono eseguiti ogni 60 minuti per recuperare lo storage su dischi a blocchi. Questo processo è noto anche come garbage collection.

- **leEvent**

Errore di sistema interno.

- **InstallEvent**

Eventi di installazione automatica del software. Il software viene installato automaticamente su un nodo in sospenso.

- **ISCSIEvent**

Eventi relativi a problemi iSCSI nel sistema.

- **LimitEvent**

Eventi correlati al numero di volumi o volumi virtuali in un account o nel cluster che si avvicina al numero massimo consentito.

- **MaintenanceModeEvent**

Eventi correlati alla modalità di manutenzione del nodo, ad esempio la disattivazione del nodo.

- **NetworkEvent**

Eventi relativi allo stato della rete virtuale.

- **PlatformHardwareEvent**

Eventi relativi a problemi rilevati sui dispositivi hardware.

- **RemoteClusterEvent**

Eventi relativi all'associazione remota del cluster.

- **SchedulerEvent**

Eventi correlati agli snapshot pianificati.

- **ServiceEvent**

Eventi relativi allo stato del servizio di sistema.

- **SliceEvent**

Eventi correlati al server Slice, come la rimozione di un disco o di un volume di metadati.

Esistono tre tipi di eventi di riassegnazione delle sezioni, che includono informazioni sul servizio a cui viene assegnato un volume:

- flipping: passaggio del servizio primario a un nuovo servizio primario

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

- spostamento: passaggio del servizio secondario a un nuovo servizio secondario

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

- eliminazione: rimozione di un volume da un set di servizi

```
sliceID {oldSecondaryServiceID(s)}
```

- **SnmpTrapEvent**

Eventi relativi ai trap SNMP.

- **StatEvent**

Eventi relativi alle statistiche di sistema.

- **TsEvent**

Eventi relativi al servizio di trasporto del sistema.

- ***Exception ***

Eventi correlati a eccezioni di sistema impreviste.

- **UreEvent**

Eventi correlati a errori di lettura non ripristinabili che si verificano durante la lettura dal dispositivo di storage.

- **VasaProviderEvent**

Eventi relativi a un provider VASA (vSphere API for Storage Awareness).

Visualizzare lo stato delle attività in esecuzione

È possibile visualizzare lo stato di avanzamento e completamento delle attività in

esecuzione nell'interfaccia utente Web che vengono segnalate dai metodi API ListSyncJobs e ListBulkVolumeJobs. È possibile accedere alla pagina delle attività in esecuzione dalla scheda Reporting dell'interfaccia utente di Element.

Se sono presenti numerose attività, il sistema potrebbe metterle in coda ed eseguirle in batch. La pagina operazioni in esecuzione visualizza i servizi attualmente sincronizzati. Una volta completato, un'attività viene sostituita dalla successiva attività di sincronizzazione in coda. Le attività di sincronizzazione potrebbero continuare a essere visualizzate nella pagina delle attività in esecuzione fino a quando non sono più necessarie.



È possibile visualizzare i dati di sincronizzazione delle repliche per i volumi sottoposti a replica nella pagina delle attività in esecuzione del cluster contenente il volume di destinazione.

Visualizzare gli avvisi di sistema

È possibile visualizzare gli avvisi per informazioni sugli errori o sugli errori del cluster nel sistema. Gli avvisi possono essere informazioni, avvisi o errori e rappresentano un buon indicatore della corretta esecuzione del cluster. La maggior parte degli errori si risolve automaticamente.

È possibile utilizzare il metodo API ListClusterFaults per automatizzare il monitoraggio degli avvisi. Ciò consente di ricevere una notifica di tutti gli avvisi che si verificano.

1. Nell'interfaccia utente di Element, selezionare **Reporting > Alerts**.

Il sistema aggiorna gli avvisi sulla pagina ogni 30 secondi.

Per ogni evento, vengono visualizzate le seguenti informazioni:

Elemento	Descrizione
ID	ID univoco associato a un avviso del cluster.

Severità	<p>Il grado di importanza dell'avviso. Valori possibili:</p> <ul style="list-style-type: none"> • Attenzione: Un problema di lieve entità che potrebbe richiedere presto l'intervento dell'utente. Gli aggiornamenti del sistema sono ancora consentiti. • Errore: Un errore che potrebbe causare il peggioramento delle performance o la perdita di alta disponibilità (ha). Gli errori in genere non devono influire altrimenti sul servizio. • Critico: Un guasto grave che influisce sul servizio. Il sistema non è in grado di fornire richieste di i/o API o client. Il funzionamento in questo stato potrebbe causare la potenziale perdita di dati. • BestPractice: Non viene utilizzata una procedura consigliata per la configurazione del sistema.
Tipo	L'elemento interessato dal guasto. Può essere un nodo, un disco, un cluster, un servizio o un volume.
Nodo	ID nodo per il nodo a cui si riferisce questo guasto. Incluso per i guasti al nodo e al disco, altrimenti impostato su - (DASH).
ID disco	ID del disco a cui si riferisce questo guasto. Incluso per i guasti del disco, altrimenti impostato su - (DASH).
Codice di errore	Un codice descrittivo che indica la causa del guasto.
Dettagli	Una descrizione del guasto con ulteriori dettagli.
Data	La data e l'ora in cui è stato registrato il guasto.

2. Fare clic su **Show Details** (Mostra dettagli) per visualizzare le informazioni relative all'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 relative all'avviso, inclusa la data in cui è stato risolto, vengono spostate nell'area Resolved (risolto).

Trova ulteriori informazioni

- [Codici di guasto del cluster](#)
- ["Gestire lo storage con l'API Element"](#)

Codici di guasto del cluster

Il sistema segnala un errore o uno stato che potrebbe essere interessante generando un codice di errore, elencato nella pagina Avvisi. Questi codici consentono di determinare quale componente del sistema ha rilevato l'avviso e perché è stato generato.

L'elenco seguente descrive i diversi tipi di codici:

- **AuthenticationServiceFault**

Il servizio di autenticazione su uno o più nodi del cluster non funziona come previsto.

Contattare il supporto NetApp per assistenza.

- **AvailableVirtualNetworkIPAddressesLow**

Il numero di indirizzi della rete virtuale nel blocco di indirizzi IP è basso.

Per risolvere questo guasto, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuale.

- **BlockClusterFull**

Lo spazio di storage a blocchi disponibile non è sufficiente per supportare una perdita di un singolo nodo. Per informazioni dettagliate sui livelli di completezza del cluster, vedere il metodo API `GetClusterFullThreshold`. Questo guasto del cluster indica una delle seguenti condizioni:

- `Stage3Low` (Avvertenza): Soglia definita dall'utente superata. Regolare le impostazioni di Cluster Full o aggiungere altri nodi.
- `Stage4critical` (errore): Spazio insufficiente per il ripristino in caso di guasto a 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
- `Stage5CompletelyConsumed` (critico)¹; non sono consentite operazioni di scrittura o nuove connessioni iSCSI. Verranno mantenute le attuali connessioni iSCSI. Le operazioni di scrittura non vengono eseguite fino a quando non viene aggiunta una maggiore capacità al cluster. Per risolvere questo errore, eliminare o eliminare volumi o aggiungere un altro nodo di storage al cluster di storage.

- **BlocksDegraded**

I dati del blocco non vengono più replicati completamente a causa di un errore.

Severità	Descrizione
Attenzione	Sono accessibili solo due copie complete dei dati del blocco.
Errore	È possibile accedere a una sola copia completa dei dati del blocco.
Critico	Non è possibile accedere a copie complete dei dati del blocco.

Nota: lo stato di avviso può verificarsi solo su un sistema Triple Helix.

Per risolvere questo guasto, ripristinare i nodi offline o i servizi di blocco oppure contattare il supporto

NetApp per assistenza.

- **BlockServiceToFull**

Un servizio a blocchi sta utilizzando troppo spazio.

Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **BlockServiceUnhealthy**

Un servizio a blocchi è stato rilevato come non integro:

- Severità = Avvertenza: Non viene intrapresa alcuna azione. Questo periodo di avviso scade tra `cTimeUntilBSIsKilledMsec=330000` millisecondi.
- Severità = errore: Il sistema sta discommissionando automaticamente i dati e replicando i dati su altri dischi integri.
- Severità = critico: Ci sono servizi di blocco guasti su diversi nodi maggiori o uguali al numero di repliche (2 per doppia elica). I dati non sono disponibili e la sincronizzazione bin non verrà completata. Verificare la presenza di problemi di connettività di rete ed errori hardware. In caso di guasto di componenti hardware specifici, si verificheranno altri guasti. Il guasto viene disattivato quando il servizio a blocchi è accessibile o quando il servizio è stato disattivato.

- **ClockSkewExceedsFaultThreshold**

L'inclinazione temporale tra il master del cluster e il nodo che presenta un token supera la soglia consigliata. Il cluster di storage non è in grado di correggere automaticamente l'inclinazione temporale tra i nodi.

Per risolvere questo errore, utilizzare server NTP interni alla rete, anziché i valori predefiniti per l'installazione. Se si utilizza un server NTP interno, contattare il supporto NetApp per assistenza.

- **ClusterCannotSync**

Esiste una condizione di spazio insufficiente e i dati sulle unità di storage a blocchi offline non possono essere sincronizzati con le unità ancora attive.

Per risolvere questo guasto, aggiungere ulteriore storage.

- **ClusterFull**

Non c'è più spazio di storage libero nel cluster di storage.

Per risolvere questo guasto, aggiungere ulteriore storage.

- **ClusterIOPSAreOverProvised**

Il provisioning degli IOPS del cluster è eccessivo. La somma di tutti gli IOPS QoS minimi è maggiore degli IOPS previsti del cluster. La QoS minima non può essere mantenuta per tutti i volumi contemporaneamente.

Per risolvere questo problema, ridurre le impostazioni minime di QoS IOPS per i volumi.

- **DisableDriveSecurityFailed**

Il cluster non è configurato per abilitare la sicurezza del disco (crittografia a riposo), ma almeno un disco ha

attivato la sicurezza del disco, il che significa che la disattivazione della sicurezza del disco su tali dischi ha avuto esito negativo. Questo guasto viene registrato con la severità "Warning".

Per risolvere questo guasto, controllare i dettagli del guasto per individuare il motivo per cui non è stato possibile disattivare la protezione del disco. I motivi possibili sono:

- Impossibile acquisire la chiave di crittografia. Esaminare il problema di accesso alla chiave o al server delle chiavi esterno.
- L'operazione di disattivazione non è riuscita sul disco, determinare se potrebbe essere stata acquisita la chiave errata. Se nessuna di queste è la causa del guasto, potrebbe essere necessario sostituire il disco.

È possibile tentare di ripristinare un disco che non disattiva correttamente la protezione anche se viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere i dischi dal sistema spostandoli su Available (disponibile), eseguire una cancellazione sicura sul disco e riportarli su Active (attivo).

• **DisconnectedClusterPair**

Una coppia di cluster è disconnessa o configurata in modo errato. Controllare la connettività di rete tra i cluster.

• **DisconnectedRemoteNode**

Un nodo remoto è disconnesso o configurato in modo non corretto. Verificare la connettività di rete tra i nodi.

• **DisconnctedSnapMirrorEndpoint**

Un endpoint SnapMirror remoto è disconnesso o configurato in modo errato. Controllare la connettività di rete tra il cluster e SnapMirrorEndpoint remoto.

• **DriveAvailable**

Uno o più dischi sono disponibili nel cluster. In generale, tutti i cluster devono avere tutti i dischi aggiunti e nessuno nello stato disponibile. Se il guasto si verifica in modo imprevisto, contattare il supporto NetApp.

Per risolvere questo guasto, aggiungere eventuali dischi disponibili al cluster di storage.

• **DriveFailed**

Il cluster restituisce questo errore quando uno o più dischi si sono guastati, indicando una delle seguenti condizioni:

- Drive Manager non può accedere al disco.
- Il servizio slice o block ha avuto un errore troppe volte, presumibilmente a causa di errori di lettura o scrittura del disco e non può essere riavviato.
- Disco mancante.
- Il servizio master per il nodo non è accessibile (tutti i dischi nel nodo sono considerati mancanti/guasti).
- L'unità è bloccata e non è possibile acquisire la chiave di autenticazione dell'unità.
- L'unità è bloccata e l'operazione di sblocco non riesce. Per risolvere questo problema:
- Verificare la connettività di rete del nodo.

- Sostituire l'unità.
- Assicurarsi che la chiave di autenticazione sia disponibile.

• **DriveHealthFault**

Un disco non ha superato il controllo dello stato DI salute SMART e di conseguenza le funzioni del disco sono ridotte. Per questo guasto è presente un livello di gravità critico:

- Disco con seriale: <serial number> nello slot: <node slot> <drive slot> non ha superato IL controllo dello stato DI salute generale SMART. Per risolvere il problema, sostituire il disco.

• **DriveWearFault**

La durata rimanente di un disco è scesa al di sotto delle soglie, ma è ancora in funzione. Esistono due livelli di gravità possibili per questo guasto: Critico e Avviso:

- Disco con seriale: <serial number> nello slot: <node slot> <drive slot> ha livelli di usura critici.
- Disco con seriale: <serial number> nello slot: <node slot> <drive slot> ha basse riserve di usura. Per risolvere il problema, sostituire il disco al più presto.

• **DuplicateClusterMasterCandidate**

È stato rilevato più di un candidato master del cluster di storage. Contattare il supporto NetApp per assistenza.

• **EnableDriveSecurityFailed**

Il cluster è configurato per richiedere la protezione del disco (crittografia a riposo), ma non è stato possibile attivare la protezione del disco su almeno un disco. Questo guasto viene registrato con la severità "Warning".

Per risolvere questo guasto, controllare i dettagli del guasto per individuare il motivo per cui non è stato possibile attivare la protezione del disco. I motivi possibili sono:

- Impossibile acquisire la chiave di crittografia. Esaminare il problema di accesso alla chiave o al server delle chiavi esterno.
- L'operazione di abilitazione non è riuscita sul disco, determinare se potrebbe essere stata acquisita la chiave errata. Se nessuna di queste è la causa del guasto, potrebbe essere necessario sostituire il disco.

È possibile tentare di ripristinare un disco che non abilita correttamente la protezione anche se viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere i dischi dal sistema spostandoli su Available (disponibile), eseguire una cancellazione sicura sul disco e riportarli su Active (attivo).

• **EnsembleDegraded**

La connettività di rete o l'alimentazione di uno o più nodi dell'ensemble sono state perse.

Per risolvere questo errore, ripristinare la connettività di rete o l'alimentazione.

• **eccezione**

Un guasto segnalato che non è un guasto di routine. Questi guasti non vengono cancellati automaticamente dalla coda degli errori. Contattare il supporto NetApp per assistenza.

- **FailedSpaceTooFull**

Un servizio a blocchi non risponde alle richieste di scrittura dei dati. In questo modo il servizio slice esaurisce lo spazio necessario per memorizzare le scritture non riuscite.

Per risolvere questo errore, ripristinare la funzionalità dei servizi a blocchi per consentire la normale continuazione delle operazioni di scrittura e l'archiviazione dello spazio non riuscito dal servizio slice.

- **FanSensor**

Un sensore della ventola è guasto o mancante.

Per risolvere questo guasto, sostituire l'hardware guasto.

- **FiberChannelAccessDebraded**

Un nodo Fibre Channel non risponde ad altri nodi nel cluster di storage sul proprio IP di storage per un certo periodo di tempo. In questo stato, il nodo viene quindi considerato non reattivo e genera un errore del cluster. Controllare la connettività di rete.

- **FiberChannelAccessUnavailable**

Tutti i nodi Fibre Channel non rispondono. Vengono visualizzati gli ID del nodo. Controllare la connettività di rete.

- **FiberChannelActiveIxl**

Il numero di Nexus IXL si sta avvicinando al limite supportato di 8000 sessioni attive per nodo Fibre Channel.

- Il limite delle Best practice è 5500.
- Il limite di avviso è 7500.
- Il limite massimo (non applicato) è 8192. Per risolvere questo guasto, ridurre il numero di Nexus IXL al di sotto del limite di Best practice di 5500.

- **FiberChannelConfig**

Questo guasto del cluster indica una delle seguenti condizioni:

- Sullo slot PCI è presente una porta Fibre Channel imprevista.
- Esiste un modello HBA Fibre Channel imprevisto.
- Si è verificato un problema con il firmware di un HBA Fibre Channel.
- Una porta Fibre Channel non è in linea.
- Si è verificato un problema persistente nella configurazione del pass-through Fibre Channel. Contattare il supporto NetApp per assistenza.

- **FiberChannelIOPS**

Il numero totale di IOPS si sta avvicinando al limite di IOPS per i nodi Fibre Channel nel cluster. I limiti sono:

- FC0025: Limite DI 450.000 IOPS con dimensione del blocco 4K per nodo Fibre Channel.
- FCN001: Limite OPS di 625 K con dimensione del blocco 4K per nodo Fibre Channel. Per risolvere

questo guasto, bilanciare il carico su tutti i nodi Fibre Channel disponibili.

- **FiberChannelStaticIXL**

Il numero di Nexus IXL si sta avvicinando al limite supportato di 16000 sessioni statiche per nodo Fibre Channel.

- Il limite delle Best practice è 11000.
- Il limite di avviso è 15000.
- Il limite massimo (imposto) è 16384. Per risolvere questo guasto, ridurre il numero di Nexus IXL al di sotto del limite di Best practice di 11000.

- **FileSystemCapacityLow**

Spazio insufficiente su uno dei filesystem.

Per risolvere questo errore, aggiungere più capacità al file system.

- **FipsDrivesMismatch**

Un'unità non FIPS è stata fisicamente inserita in un nodo di storage FIPS o un'unità FIPS è stata fisicamente inserita in un nodo di storage non FIPS. Viene generato un singolo guasto per nodo ed elenca tutti i dischi interessati.

Per risolvere questo guasto, rimuovere o sostituire il disco o i dischi non corrispondenti in questione.

- **FipsDrivesOutOfCompliance**

Il sistema ha rilevato che la crittografia a riposo è stata disattivata dopo l'attivazione della funzione dischi FIPS. Questo errore viene generato anche quando la funzione FIPS Drives (dischi FIPS) è attivata e nel cluster di storage è presente un disco o un nodo non FIPS.

Per risolvere questo errore, attivare la crittografia a riposo o rimuovere l'hardware non FIPS dal cluster di storage.

- **FipsSelfTestFailure**

Il sottosistema FIPS ha rilevato un errore durante l'autotest.

Contattare il supporto NetApp per assistenza.

- **HardwareConfigMismatch**

Questo guasto del cluster indica una delle seguenti condizioni:

- La configurazione non corrisponde alla definizione del nodo.
- Le dimensioni del disco non sono corrette per questo tipo di nodo.
- È stato rilevato un disco non supportato. Una possibile ragione è che la versione dell'elemento installata non riconosce questo disco. Si consiglia di aggiornare il software Element su questo nodo.
- Il firmware del disco non corrisponde.
- Lo stato che supporta la crittografia del disco non corrisponde al nodo. Contattare il supporto NetApp per assistenza.

- **IdPCertificateExpiration**

Il certificato SSL del provider di servizi del cluster da utilizzare con un provider di identità di terze parti (IdP) è in fase di scadenza o è già scaduto. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione
Attenzione	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, aggiornare il certificato SSL prima della scadenza. Utilizzare il metodo `UpdateIdpConfiguration` API con `refreshCertificateExpirationTime=true` Per fornire il certificato SSL aggiornato.

- **InconsistentBondModes**

Mancano le modalità bond sul dispositivo VLAN. Questo guasto visualizza la modalità bond prevista e la modalità bond attualmente in uso.

- **InconsistentInterfaceConfiguration**

La configurazione dell'interfaccia non è coerente.

Per risolvere questo errore, assicurarsi che le interfacce dei nodi nel cluster di storage siano configurate in modo coerente.

- **InconsistentMentus**

Questo guasto del cluster indica una delle seguenti condizioni:

- Mancata corrispondenza Bond1G: MTU non coerenti rilevate sulle interfacce Bond1G.
- Mancata corrispondenza Bond10G: MTU non coerenti rilevate 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.

- **InconsistentSubnetMasks**

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 bond non è corretto.

- **InvalidConfiguredFiberChannelNodeCount**

Una delle due connessioni di nodo Fibre Channel previste è degradata. Questo errore viene visualizzato quando è collegato un solo nodo Fibre Channel.

Per risolvere questo guasto, controllare la connettività di rete del cluster e il cablaggio di rete e verificare la presenza di servizi non riusciti. Se non ci sono problemi di rete o di servizio, contattare il supporto NetApp per la sostituzione di un nodo Fibre Channel.

- **IrqBalanceFailed**

Si è verificata un'eccezione durante il tentativo di bilanciare gli interrupt.

Contattare il supporto NetApp per assistenza.

- **KmipCertificateFault**

- Il certificato dell'autorità di certificazione principale (CA) sta per scadere.

Per risolvere questo errore, acquisire un nuovo certificato dalla CA principale con una data di scadenza di almeno 30 giorni e utilizzare `ModifyKeyServerKmip` per fornire il certificato CA principale aggiornato.

- Il certificato client è in scadenza.

Per risolvere questo errore, creare una nuova CSR utilizzando `GetClientCertificateSigningRequest`, fare in modo che la nuova data di scadenza sia di almeno 30 giorni e utilizzare `ModifyKeyServerKmip` per sostituire il certificato del client KMIP in scadenza con il nuovo certificato.

- Il certificato dell'autorità di certificazione principale (CA) è scaduto.

Per risolvere questo errore, acquisire un nuovo certificato dalla CA principale con una data di scadenza di almeno 30 giorni e utilizzare `ModifyKeyServerKmip` per fornire il certificato CA principale aggiornato.

- Certificato client scaduto.

Per risolvere questo errore, creare una nuova CSR utilizzando `GetClientCertificateSigningRequest`, fare in modo 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 nel certificato dell'autorità di certificazione principale (CA).

Per risolvere questo errore, verificare che sia stato fornito il certificato corretto e, se necessario, riacquisire il certificato dalla CA principale. Utilizzare `ModifyKeyServerKmip` per installare il certificato client KMIP corretto.

- Errore nel certificato del client.

Per risolvere questo errore, verificare che sia installato il certificato client KMIP corretto. La CA principale del certificato client deve essere installata su EKS. Utilizzare `ModifyKeyServerKmip` per installare il certificato client KMIP corretto.

- **KmipServerFault**

- Errore di connessione

Per risolvere questo guasto, verificare che il server delle chiavi esterne sia attivo e raggiungibile tramite la rete. Utilizzare `TestKeyServerKimp` e `TestKeyProviderKmip` per verificare la connessione.

- Errore di autenticazione

Per risolvere questo errore, verificare che vengano utilizzati i certificati CA root e client KMIP corretti e che la chiave privata e il certificato del client KMIP corrispondano.

- Errore del server

Per risolvere questo guasto, controllare i dettagli dell'errore. In base all'errore restituito, potrebbe essere necessario eseguire la risoluzione dei problemi sul server chiavi esterno.

• MemoriaEccThreshold

Sono stati rilevati numerosi errori ECC correggibili o non correggibili. Questo guasto utilizza le seguenti severità in base all'urgenza:

Evento	Severità	Descrizione
Un singolo cErrorCount DIMM raggiunge cDimmCorrectableErrWarrThreshold.	Attenzione	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM Slot>
Un singolo cErrorCount DIMM rimane al di sopra di cDimmCorrectableErrWarrThreshold fino alla scadenza di cErrorFaultTimer per il DIMM.	Errore	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM>
Un controller di memoria riporta cErrorCount al di sopra di cMemCttrCorrectableErrWarrThreshold e cMemCttrCorrectableErrWarrWarrDuration è specificato.	Attenzione	Errori di memoria ECC correggibili superiori alla soglia sul controller di memoria: <Processor> <Memory Controller>
Un controller di memoria segnala cErrorCount al di sopra di cMemCttrCorrectableErrWarnThreshold fino alla scadenza di cErrorFaultTimer per il controller di memoria.	Errore	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM>
Un singolo DIMM riporta un uErrorCount superiore a zero, ma inferiore a cDimmUncorrectableErrFaultThreshold.	Attenzione	Errori di memoria ECC non correggibili rilevati su DIMM: <Processor> <DIMM Slot>
Un singolo DIMM riporta un uErrorCount di almeno cDimmUncorrectableErrFaultThreshold.	Errore	Errori di memoria ECC non correggibili rilevati su DIMM: <Processor> <DIMM Slot>

Un controller di memoria segnala un valore uErrorCount superiore a zero, ma inferiore a cMemCtrlUncorrectableErrFaultThreshold.	Attenzione	Errori di memoria ECC non correggibili rilevati sul controller di memoria: <Processor> <Memory Controller>
Un controller di memoria segnala un uErrorCount di almeno cMemCtrlUncorrectableErrFaultThreshold.	Errore	Errori di memoria ECC non correggibili rilevati sul controller di memoria: <Processor> <Memory Controller>

Per risolvere questo guasto, contattare il supporto NetApp per assistenza.

• MemoriaUsageThreshold

L'utilizzo della memoria è superiore al normale. Questo guasto utilizza le seguenti severità in base all'urgenza:



Per informazioni più dettagliate sul tipo di guasto, vedere l'intestazione **Dettagli** nell'errore.

Severità	Descrizione
Attenzione	Memoria di sistema insufficiente.
Errore	Memoria di sistema molto bassa.
Critico	La memoria di sistema è completamente consumata.

Per risolvere questo guasto, contattare il supporto NetApp per assistenza.

• MetadataClusterFull

Lo spazio di storage dei metadati non è sufficiente per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di completezza del cluster, vedere il metodo API GetClusterFullThreshold. Questo guasto del cluster indica una delle seguenti condizioni:

- Stage3Low (Avvertenza): Soglia definita dall'utente superata. Regolare le impostazioni di Cluster Full o aggiungere altri nodi.
- Stage4critical (errore): Spazio insufficiente per il ripristino in caso di guasto a 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
- Stage5CompletelyConsumed (critico)¹; non sono consentite operazioni di scrittura o nuove connessioni iSCSI. Verranno mantenute le attuali connessioni iSCSI. Le operazioni di scrittura non vengono eseguite fino a quando non viene aggiunta una maggiore capacità al cluster. Eliminare o eliminare i dati o aggiungere altri nodi. Per risolvere questo errore, eliminare o eliminare volumi o aggiungere un altro nodo di storage al cluster di storage.

• MtuCheckFailure

Un dispositivo di rete non è configurato per le dimensioni MTU corrette.

Per risolvere questo guasto, assicurarsi che tutte le interfacce di rete e le porte dello switch siano configurate per i frame jumbo (MTU fino a 9000 byte).

- **NetworkConfig**

Questo guasto del cluster indica una delle seguenti condizioni:

- Non è presente un'interfaccia prevista.
- È presente un'interfaccia duplicata.
- Un'interfaccia configurata non è disponibile.
- È necessario riavviare la rete. Contattare il supporto NetApp per assistenza.

- **NoAvailableVirtualNetworkIPAddresses**

Nessun indirizzo di rete virtuale disponibile nel blocco di indirizzi IP.

- Il TAG virtualNetworkID n. (n. n.) non ha indirizzi IP di storage disponibili. Non è possibile aggiungere nodi aggiuntivi al cluster. Per risolvere questo guasto, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuale.

- **NodeHardwareFault (<name> interfaccia di rete non attivo o cavo scollegato)**

Un'interfaccia di rete è inattiva o il cavo è scollegato.

Per risolvere questo guasto, controllare la connettività di rete per il nodo o i nodi.

- **NodeHardwareFault (lo stato in grado di supportare la crittografia del disco non corrisponde allo stato in grado di supportare la crittografia del nodo per il disco nello slot <node slot> <drive slot>)**

Un disco non corrisponde alle funzionalità di crittografia con il nodo di storage in cui è installato.

- **NodeHardwareFault (<actual size> delle dimensioni del disco <drive type> non corretto per il disco nello slot <node slot> <drive slot> per questo tipo di nodo - <expected size> previsto)**

Un nodo di storage contiene un disco di dimensioni non corrette per questo nodo.

- **NodeHardwareFault (disco non supportato rilevato nello slot <node slot> <drive slot>; le statistiche e le informazioni sullo stato dei dischi non saranno disponibili)**

Un nodo di storage contiene un disco non supportato.

- **NodeHardwareFault (l'unità nello slot <node slot> <drive slot> deve utilizzare la versione del firmware <expected version>, ma la versione <actual version> non è supportata)**

Un nodo di storage contiene un disco con una versione del firmware non supportata.

- **NodeMaintenanceMode**

Un nodo è stato posto in modalità di manutenzione. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione
----------	-------------

Attenzione	Indica che il nodo è ancora in modalità di manutenzione.
Errore	Indica che la modalità di manutenzione non è riuscita a disattivarsi, probabilmente a causa di uno standby guasto o attivo.

Per risolvere questo guasto, disattivare la modalità di manutenzione al termine della manutenzione. Se l'errore di livello di errore persiste, contattare il supporto NetApp per assistenza.

- **NodeOffline**

Il software Element non è in grado di 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 l'implementazione dei nodi di storage; i client potrebbero riscontrare problemi di performance se LACP non è attivato e configurato correttamente.

- **NtpServerUnreachable**

Il cluster di storage non è in grado di 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 il tempo del cluster di storage e il tempo del server NTP specificato è eccessiva. Il cluster di storage non è in grado di correggere automaticamente la differenza.

Per risolvere questo errore, utilizzare server NTP interni alla rete, anziché i valori predefiniti per l'installazione. Se si utilizzano server NTP interni e il problema persiste, contattare il supporto NetApp per assistenza.

- **NvramDeviceStatus**

Si è verificato un errore, un errore o un errore di un dispositivo NVRAM. Questo guasto ha le seguenti severità:

Severità	Descrizione
----------	-------------

Attenzione	<p>L'hardware ha rilevato un avviso. Questa condizione può essere transitoria, ad esempio un avviso di temperatura.</p> <ul style="list-style-type: none"> • NvmLifetimeError • NvmLifetimeStatus • EnergySourceLifetimeStatus • EnergySourceTemperatureStatus • WarningThresholdExceed
Errore	<p>L'hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere il disco slice dall'operazione (questo genera un evento di rimozione del disco). Se i servizi di slice secondaria non sono disponibili, il disco non verrà rimosso. Errori restituiti oltre agli errori di livello di avviso:</p> <ul style="list-style-type: none"> • 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	<p>L'hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere il disco slice dall'operazione (questo genera un evento di rimozione del disco). Se i servizi di slice secondaria non sono disponibili, il disco non verrà rimosso.</p> <ul style="list-style-type: none"> • PersistenzaLost • ArmStatusSaveNArmed • CsaveStatusError

Sostituire l'hardware guasto nel nodo. Se questo non risolve il problema, contattare il supporto NetApp per assistenza.

- **PowerSupplyError**

Questo guasto del cluster indica una delle seguenti condizioni:

- Non è presente alcun alimentatore.
- Si è verificato un guasto nell'alimentatore.
- Un ingresso di alimentazione è mancante o fuori portata. Per risolvere questo guasto, verificare che l'alimentazione ridondante sia fornita a tutti i nodi. Contattare il supporto NetApp per assistenza.

- **ProvisionedSpaceTooFull**

La capacità complessiva fornita dal cluster è troppo piena.

Per risolvere questo errore, aggiungere ulteriore spazio fornito o eliminare e rimuovere volumi.

- **RemoteRepAsyncDelayExced**

Il ritardo asincrono configurato per la replica è stato superato. Controllare la connettività di rete tra i cluster.

- **RemoteRepClusterFull**

I volumi hanno messo in pausa la replica remota perché il cluster di storage di destinazione è troppo pieno.

Per risolvere questo guasto, liberare spazio sul cluster di storage di destinazione.

- **RemoteRepSnapshotClusterFull**

I volumi hanno messo in pausa la replica remota degli snapshot perché il cluster di storage di destinazione è troppo pieno.

Per risolvere questo guasto, liberare spazio sul cluster di storage di destinazione.

- **RemoteRepSnapshotsExceeddedededLimit**

I volumi hanno messo in pausa la replica remota degli snapshot perché il volume del cluster di storage di destinazione ha superato il limite di snapshot.

Per risolvere questo guasto, aumentare il limite di snapshot sul cluster di storage di destinazione.

- **ScheduleActionError**

Una o più attività pianificate sono eseguite, ma non sono riuscite.

L'errore viene cancellato se l'attività pianificata viene eseguita di nuovo e ha esito positivo, se l'attività pianificata viene eliminata o se l'attività viene messa in pausa e ripresa.

- **SensorReadingFailed**

L'autotest del Baseboard Management Controller (BMC) non è riuscito o un sensore non è in grado di comunicare con il BMC.

Contattare il supporto NetApp per assistenza.

- **ServiceNotRunning**

Un servizio richiesto non è in esecuzione.

Contattare il supporto NetApp per assistenza.

- **SliceServiceTooFull**

A un servizio slice è assegnata una capacità di provisioning troppo bassa.

Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **SliceServiceUnhealthy**

Il sistema ha rilevato che un servizio slice non è integro e lo sta automaticamente smantellando.

- Severità = Avvertenza: Non viene intrapresa alcuna azione. Questo periodo di avviso scadrà tra 6 minuti.
- Severità = errore: Il sistema sta discommissionando automaticamente i dati e replicando i dati su altri dischi integri. Verificare la presenza di problemi di connettività di rete ed errori hardware. In caso di guasto di componenti hardware specifici, si verificheranno altri guasti. Il guasto viene disattivato quando il servizio slice è accessibile o quando il servizio è stato disattivato.

• SshEnabled

Il servizio SSH è attivato su uno o più nodi nel cluster di storage.

Per risolvere questo guasto, disattivare il servizio SSH sul nodo o sui nodi appropriati o contattare il supporto NetApp per assistenza.

• SslCertificateExpiration

Il certificato SSL associato a questo nodo è in fase di scadenza o è scaduto. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione
Attenzione	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 guasto, rinnovare il certificato SSL. Se necessario, contattare il supporto NetApp per assistenza.

• StrandedCapacity

Un singolo nodo rappresenta oltre la metà della capacità del cluster di storage.

Per mantenere la ridondanza dei dati, il sistema riduce la capacità del nodo più grande in modo che parte della sua capacità a blocchi sia bloccata (non utilizzata).

Per risolvere questo guasto, aggiungere più dischi ai nodi di storage esistenti o aggiungere nodi di storage al cluster.

• TempSensor

Un sensore di temperatura segnala temperature superiori al normale. Questo guasto può essere attivato in combinazione con guasti powerSupplyError o fanSensor.

Per risolvere questo guasto, verificare l'eventuale presenza di ostruzioni nel flusso d'aria in prossimità del cluster di storage. Se necessario, contattare il supporto NetApp per assistenza.

• upgrade

Un aggiornamento è in corso da oltre 24 ore.

Per risolvere questo guasto, riprendere l'aggiornamento o contattare il supporto NetApp per assistenza.

- **UnresponsiveService**

Un servizio non risponde.

Contattare il supporto NetApp per assistenza.

- **VirtualNetworkConfig**

Questo guasto del cluster indica una delle seguenti condizioni:

- Non è presente un'interfaccia.
- Esiste uno spazio dei nomi non corretto su un'interfaccia.
- La netmask non è corretta.
- Indirizzo IP errato.
- Un'interfaccia non è attiva e in esecuzione.
- Esiste un'interfaccia superflua su un nodo. Contattare il supporto NetApp per assistenza.

- **VolumesDegraded**

I volumi secondari non hanno terminato la replica e la sincronizzazione. Il messaggio viene cancellato al termine della sincronizzazione.

- **VolumesOffline**

Uno o più volumi nel cluster di storage sono offline. Sarà presente anche il guasto **volumeDegraded**.

Contattare il supporto NetApp per assistenza.

Visualizzare l'attività delle performance dei nodi

È possibile visualizzare l'attività delle performance per ciascun nodo in un formato grafico. Queste informazioni forniscono statistiche in tempo reale per CPU e IOPS (Read/write i/o Operations per second) per ogni disco del nodo. Il grafico di utilizzo viene aggiornato ogni cinque secondi e il grafico delle statistiche del disco viene aggiornato ogni dieci secondi.

1. Fare clic su **Cluster > Nodes**.
2. Fare clic su **azioni** per il nodo che si desidera visualizzare.
3. Fare clic su **View Details** (Visualizza dettagli).



È possibile visualizzare punti specifici nel tempo sulla linea e sui grafici a barre posizionando il cursore sulla linea o sulla barra.

Visualizza le performance dei volumi

È possibile visualizzare informazioni dettagliate sulle performance per tutti i volumi nel cluster. È possibile ordinare le informazioni in base all'ID del volume o a una delle colonne delle prestazioni. È inoltre possibile utilizzare il filtro per 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 **Refresh Every** (Aggiorna ogni) e scegliendo un valore diverso. L'intervallo di refresh predefinito è 10 secondi se il cluster ha meno di 1000 volumi; in caso contrario, l'intervallo predefinito è 60 secondi. Se si sceglie il valore mai, l'aggiornamento automatico della pagina viene disattivato.

È possibile riattivare l'aggiornamento automatico facendo clic su **attiva l'aggiornamento automatico**.

1. Nell'interfaccia utente di Element, selezionare **Reporting > Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Actions (azioni) per un volume.
3. Fare clic su **View Details** (Visualizza dettagli).

Nella parte inferiore della pagina viene visualizzato un vassoio contenente informazioni generali sul volume.

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

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

Trova ulteriori informazioni

[Dettagli sulle performance dei volumi](#)

Dettagli sulle performance dei volumi

È possibile visualizzare le statistiche delle performance dei volumi dalla pagina Volume Performance (prestazioni volume) della scheda Reporting (rapporti) nell'interfaccia utente di Element.

L'elenco seguente descrive i dettagli disponibili:

- **ID**

L'ID generato dal sistema per il volume.

- **Nome**

Il nome assegnato al volume al momento della creazione.

- **Account**

Il 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.

- **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 valore massimo
- >100 = il client sta utilizzando il burst

- **IOPS totali**

Il numero totale di IOPS (lettura e scrittura) attualmente eseguiti sul volume.

- **Lettura IOPS**

Il numero totale di IOPS di lettura attualmente in esecuzione sul volume.

- **IOPS di scrittura**

Il numero totale di IOPS di scrittura attualmente in esecuzione sul volume.

- **Throughput totale**

La quantità totale di throughput (lettura e scrittura) attualmente eseguita sul volume.

- **Throughput in lettura**

La quantità totale di throughput in lettura attualmente eseguita rispetto al volume.

- **Throughput in scrittura**

La quantità totale di throughput di scrittura attualmente eseguita sul volume.

- **Latenza totale**

Il tempo medio, in microsecondi, per completare le operazioni di lettura e scrittura su un volume.

- **Latenza di lettura**

Il tempo medio, in microsecondi, per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.

- **Latenza di scrittura**

Il tempo medio, in microsecondi, per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.

- **Profondità coda**

Il numero di operazioni di lettura e scrittura in sospeso nel volume.

- **Dimensione media io**

Dimensione media in byte di i/o recente nel volume negli ultimi 500 millisecondi.

Visualizzare 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 > iSCSI Sessions**.
2. Per visualizzare i campi relativi ai criteri di filtro, fare clic su **Filter** (filtro).

Trova ulteriori informazioni

[Dettagli della sessione iSCSI](#)

Dettagli della sessione iSCSI

È possibile visualizzare informazioni sulle sessioni iSCSI connesse al cluster.

Il seguente elenco descrive le informazioni che è possibile trovare sulle sessioni iSCSI:

- **Nodo ***

Nodo che ospita la partizione dei metadati primaria per il volume.

- **Account**

Il nome dell'account proprietario del volume. Se il valore è vuoto, viene visualizzato un trattino (-).

- **Volume**

Il nome del volume identificato nel nodo.

- **ID volume**

ID del volume associato all'IQN di destinazione.

- **ID iniziatore**

ID generato dal sistema per l'iniziatore.

- **Alias iniziatore**

Un nome opzionale per l'iniziatore che semplifica la ricerca dell'iniziatore in un elenco lungo.

- **IP Initiator**

L'indirizzo IP dell'endpoint che avvia la sessione.

- **Initiator IQN**

L'IQN dell'endpoint che avvia la sessione.

- **IP di destinazione**

L'indirizzo IP del nodo che ospita il volume.

- **IQN di destinazione**

L'IQN del volume.

- **Creato il**

Data in cui è stata stabilita la sessione.

Visualizzare le sessioni Fibre Channel

È possibile visualizzare le sessioni Fibre Channel (FC) collegate al cluster. È possibile filtrare le informazioni per includere solo le connessioni che si desidera visualizzare nella finestra.

1. Nell'interfaccia utente di Element, selezionare **Reporting > FC Sessions**.
2. Per visualizzare i campi relativi ai criteri di filtro, fare clic su **Filter** (filtro).

Trova ulteriori informazioni

[Dettagli della sessione Fibre Channel](#)

Dettagli della sessione Fibre Channel

Sono disponibili informazioni sulle sessioni Fibre Channel (FC) attive collegate al cluster.

Il seguente elenco descrive le informazioni disponibili 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**

ID generato dal sistema per l'iniziatore.

- **WWPN iniziatore**

Il nome della porta internazionale di inizio.

- **Alias iniziatore**

Un nome opzionale per l'iniziatore che semplifica la ricerca dell'iniziatore in un elenco lungo.

- **WWPN di destinazione**

Il nome della porta globale di destinazione.

- **Volume Access Group**

Nome del gruppo di accesso al volume a cui appartiene la sessione.

- **ID gruppo di accesso volume**

ID generato dal sistema per il gruppo di accesso.

Risolvere i problemi relativi ai dischi

È possibile sostituire un disco a stato solido (SSD) guasto con un disco sostitutivo. Gli SSD per i nodi di storage SolidFire sono sostituibili a caldo. Se si sospetta un guasto a un SSD, contattare il supporto NetApp per verificare il guasto e seguire la procedura di risoluzione corretta. NetApp Support collabora inoltre con te per ottenere un disco sostitutivo in base al tuo contratto di servizio.

Come sostituire in questo caso significa che è possibile rimuovere un disco guasto da un nodo attivo e sostituirlo con un nuovo disco SSD di NetApp. Si sconsiglia di rimuovere i dischi non guasti su un cluster attivo.

È necessario mantenere le parti di ricambio on-site suggerite dal supporto NetApp per consentire la sostituzione immediata del disco in caso di guasto.



A scopo di test, se si simula un guasto del disco estraendo un disco da un nodo, è necessario attendere 30 secondi prima di inserirlo nuovamente nello slot del disco.

Se un disco si guasta, Double Helix ridistribuisce i dati sul disco tra i nodi rimanenti nel cluster. I guasti di più dischi sullo stesso nodo non sono un problema, poiché il software Element protegge da due copie di dati che risiedono sullo stesso nodo. Un disco guasto provoca i seguenti eventi:

- I dati vengono migrati dal disco.
- La capacità complessiva del cluster è ridotta dalla capacità del disco.
- La protezione dei dati Double Helix garantisce la presenza di due copie valide dei dati.



I sistemi storage SolidFire non supportano la rimozione di un disco se la quantità di storage necessaria per la migrazione dei dati risulta insufficiente.

Per ulteriori informazioni

- [Rimuovere i dischi guasti dal cluster](#)
- [Risoluzione dei problemi di base dei dischi MDSS](#)
- [Rimuovere i dischi MDSS](#)
- ["Sostituzione delle unità per i nodi di storage SolidFire"](#)
- ["Sostituzione delle unità per i nodi storage della serie H600S"](#)
- ["Informazioni sull'hardware H410S e H610S"](#)
- ["Informazioni sull'hardware della serie SF"](#)

Rimuovere i dischi guasti dal cluster

Il sistema SolidFire mette un disco in uno stato di errore se l'autodiagnosi del disco indica al nodo che si è verificato un errore o se la comunicazione con il disco si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco dei dischi guasti. È necessario rimuovere un disco guasto dall'elenco dei dischi guasti nel software NetApp Element.

I dischi nell'elenco **Alerts** vengono visualizzati come **blockServiceUnhealthy** quando un nodo è offline. Al

riavvio del nodo, se il nodo e i relativi dischi tornano online entro cinque minuti e mezzo, i dischi si aggiornano automaticamente e continuano come dischi attivi nel cluster.

1. Nell'interfaccia utente di Element, selezionare **Cluster > Drives**.
2. Fare clic su **Failed** (guasto) per visualizzare l'elenco dei dischi guasti.
3. Annotare il numero di slot del disco guasto.

Queste informazioni sono necessarie per individuare il disco guasto nello chassis.

4. Rimuovere i dischi guasti utilizzando uno dei seguenti metodi:

Opzione	Fasi
Per rimuovere singoli dischi	<ol style="list-style-type: none">a. Fare clic su azioni per l'unità che si desidera rimuovere.b. Fare clic su Rimuovi.
Per rimuovere più dischi	<ol style="list-style-type: none">a. Selezionare tutte le unità che si desidera rimuovere e fare clic su azioni in blocco.b. Fare clic su Rimuovi.

Risoluzione dei problemi di base dei dischi MDSS

È possibile ripristinare i dischi di metadati (o slice) aggiungendoli di nuovo al cluster nel caso in cui uno o entrambi i dischi di metadati si guastino. È possibile eseguire l'operazione di ripristino nell'interfaccia utente di NetApp Element se la funzione MDSS è già attivata sul nodo.

Se uno o entrambi i dischi di metadati in un nodo presentano un guasto, il servizio slice viene arrestato e i dati di entrambi i dischi vengono sottoposti a backup su dischi diversi nel nodo.

I seguenti scenari delineano possibili scenari di guasto e forniscono consigli di base per correggere il problema:

Errore del disco slice del sistema

- In questo scenario, lo slot 2 viene verificato e riportato a uno stato disponibile.
- Il disco slice del sistema deve essere ripopolato prima che il servizio slice possa essere riportato online.
- Sostituire il disco slice di sistema, quando il disco slice di sistema diventa disponibile, aggiungere il disco e il disco slot 2 contemporaneamente.



Non è possibile aggiungere l'unità nello slot 2 da sola come unità di metadati. È necessario aggiungere entrambe le unità al nodo contemporaneamente.

Lo slot 2 non funziona

- In questo scenario, il disco slice del sistema viene verificato e riportato a uno stato disponibile.
- Sostituire lo slot 2 con uno spare, quando lo slot 2 diventa disponibile, aggiungere contemporaneamente il disco slice di sistema e il disco slot 2.

Errore del disco slice di sistema e dello slot 2

- È necessario sostituire sia l'unità slice di sistema che lo slot 2 con un disco libero. Quando entrambi i dischi diventano disponibili, aggiungere contemporaneamente l'unità slice di sistema e l'unità slot 2.

Ordine delle operazioni

- Sostituire il disco hardware guasto con un disco libero (sostituire entrambi i dischi se sono guasti).
- Aggiungere nuovamente i dischi al cluster una volta ripopolati e che si trovano in uno stato disponibile.

Verificare le operazioni

- Verificare che i dischi nello slot 0 (o interno) e nello slot 2 siano identificati come dischi metadati nell'elenco Active Drives (dischi attivi).
- Verificare che il bilanciamento di tutte le sezioni sia stato completato (nel registro eventi non sono presenti ulteriori messaggi di spostamento delle sezioni per almeno 30 minuti).

Per ulteriori informazioni

[Aggiungere dischi MDSS](#)

Aggiungere dischi MDSS

È possibile aggiungere una seconda unità di metadati su un nodo SolidFire convertendo l'unità di blocco nello slot 2 in un'unità slice. Ciò si ottiene attivando la funzione multi-drive slice service (MDSS). Per attivare questa funzione, è necessario contattare il supporto NetApp.

Per portare un disco slice in uno stato disponibile potrebbe essere necessario sostituire un disco guasto con un disco nuovo o libero. È necessario aggiungere il disco slice di sistema contemporaneamente all'aggiunta del disco per lo slot 2. Se si tenta di aggiungere il disco slot 2 slice da solo o prima di aggiungere il disco slice di sistema, il sistema genera un errore.

1. Fare clic su **Cluster > Drives**.
2. Fare clic su **Available** (disponibile) per visualizzare l'elenco dei dischi disponibili.
3. Selezionare le unità slice da aggiungere.
4. Fare clic su **azioni in blocco**.
5. Fare clic su **Aggiungi**.
6. Verificare dalla scheda **Active Drives** che le unità siano state aggiunte.

Rimuovere i dischi MDSS

È possibile rimuovere i dischi multi-drive slice service (MDSS). Questa procedura si applica solo se il nodo ha più dischi slice.



Se il disco slice del sistema e il disco slot 2 si guastano, il sistema arresta i servizi slice e rimuove i dischi. Se non si verifica alcun guasto e si rimuovono i dischi, entrambi devono essere rimossi contemporaneamente.

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

2. Dalla scheda **Available** drives (dischi disponibili), fare clic sulla casella di controllo relativa ai dischi slice da rimuovere.
3. Fare clic su **azioni in blocco**.
4. Fare clic su **Rimuovi**.
5. Confermare l'azione.

Risolvere i problemi dei nodi

È possibile rimuovere i nodi da un cluster per la manutenzione o la sostituzione. È necessario utilizzare l'interfaccia utente o l'API NetApp Element per rimuovere i nodi prima di portarli fuori linea.

Di seguito è riportata una panoramica della procedura per la rimozione dei nodi di storage:

- Assicurarsi che il cluster disponga di 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 la migrazione dei dati dal sistema ai dischi del nodo ad altri dischi nel cluster. Il tempo necessario per questo processo dipende dalla quantità di dati da migrare.

- Rimuovere il nodo dal cluster.

Tenere presenti le seguenti considerazioni prima di spegnere o accendere un nodo:

- Spegnere nodi e cluster comporta rischi se non viene eseguita correttamente.

Lo spegnimento di un nodo deve essere eseguito sotto la direzione del supporto NetApp.

- Se un nodo è rimasto inattivo per più di 5.5 minuti in qualsiasi condizione di arresto, la protezione dei dati Double Helix inizia l'attività di scrittura di singoli blocchi replicati in un altro nodo per replicare i dati. In questo caso, contattare il supporto NetApp per assistenza nell'analisi del nodo guasto.
- Per riavviare o spegnere un nodo in modo sicuro, è possibile utilizzare il comando Shutdown API.
- Se un nodo si trova in uno stato inattivo o spento, è necessario contattare il supporto NetApp prima di riportarlo online.
- Dopo aver riportato un nodo online, è necessario aggiungerne di nuovo i dischi al cluster, a seconda del periodo di tempo in cui è rimasto fuori servizio.

Per ulteriori informazioni

["Sostituzione di uno chassis SolidFire guasto"](#)

["Sostituzione di un nodo della serie H600S guasto"](#)

Spegnere un cluster

Per spegnere un intero cluster, attenersi alla seguente procedura.

Fasi

1. (Facoltativo) contattare il supporto NetApp per assistenza nel completamento delle fasi preliminari.
2. Verificare che tutti i/o siano interrotti.

3. Disconnettere tutte le sessioni iSCSI:

- a. Accedere all'indirizzo IP virtuale di gestione (MVIP) sul cluster per aprire l'interfaccia utente Element.
- b. Annotare i nodi elencati nell'elenco nodi.
- c. Eseguire il metodo Shutdown API con l'opzione halt specificata su ciascun ID nodo del cluster.

Quando si riavvia il cluster, è necessario seguire alcuni passaggi per verificare che tutti i nodi siano in linea:



1. Verificare che tutti i livelli critici di severità e. `volumesOffline` i guasti del cluster sono stati risolti.
2. Attendere da 10 a 15 minuti per consentire al cluster di stabilizzarsi.
3. Avviare la creazione degli host per accedere ai dati.

Se si desidera dedicare più tempo all'accensione dei nodi e alla verifica dell'integrità dei nodi dopo la manutenzione, contattare il supporto tecnico per ricevere assistenza con il ritardo della sincronizzazione dei dati per evitare una sincronizzazione bin non necessaria.

Trova ulteriori informazioni

["Come spegnere e accendere correttamente un cluster di storage NetApp Solidfire/HCI"](#)

Utilizzo di utility per nodo per nodi di storage

È possibile utilizzare le utility 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 utility per nodo forniscono informazioni e strumenti specifici che consentono di risolvere i problemi di rete tra nodi o con il nodo di gestione.

Trova ulteriori informazioni

- [Accedere alle impostazioni per nodo utilizzando 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 utility di sistema utilizzando l'interfaccia utente per nodo](#)

Accedere alle impostazioni per nodo utilizzando l'interfaccia utente per nodo

È possibile accedere alle impostazioni di rete, alle impostazioni del cluster, ai test e alle utility di sistema nell'interfaccia utente per nodo dopo aver inserito l'IP del nodo di gestione e autenticato.

Se si desidera modificare le impostazioni di un nodo in uno stato attivo che fa parte di un cluster, è necessario accedere come utente amministratore del cluster.



Configurare o modificare un nodo alla volta. Prima di apportare modifiche a un altro nodo, assicurarsi che le impostazioni di rete specificate abbiano l'effetto previsto e che la rete sia stabile e in grado di garantire prestazioni ottimali.

1. Aprire l'interfaccia utente per nodo utilizzando uno dei seguenti metodi:

- Inserire l'indirizzo IP di gestione seguito da :442 in una finestra del browser e accedere utilizzando un nome utente e una password admin.
- Nell'interfaccia utente di Element, selezionare **Cluster > Nodes**, quindi fare clic sul collegamento dell'indirizzo IP di gestione per il nodo che si desidera configurare o modificare. Nella finestra del browser visualizzata, è possibile modificare le impostazioni del nodo.

The screenshot displays the NetApp Hybrid Cloud Control interface for Node01. The left sidebar shows the NetApp logo and 'Hybrid Cloud Control' at the top, with 'Node01' selected below. The main content area is titled 'Node01' and features a navigation bar with 'NETWORK SETTINGS' (highlighted), 'CLUSTER SETTINGS', 'SYSTEM TESTS', and 'SYSTEM UTILITIES'. The 'Network Settings' page includes a 'Bond1G' / 'Bond10G' selector and a 'Reset Changes' link. The settings are organized into two columns:

Method	Link Speed
static	1000
IPv4 Address	IPv4 Subnet Mask
[Redacted]	255.255.255.0
IPv4 Gateway Address	IPv6 Address
[Redacted]	[Redacted]
IPv6 Gateway Address	MTU
[Redacted]	1500
DNS Servers	
[Redacted]	
Search Domains	
[Redacted]	
Bond Mode	Status

Dettagli delle impostazioni di rete dall'interfaccia utente per nodo

È possibile modificare le impostazioni di rete del nodo di storage per assegnare al nodo un nuovo set di attributi di rete.

Le impostazioni di rete per un nodo di storage sono visualizzate nella pagina **Impostazioni di rete** quando si effettua l'accesso al nodo (<https://<node IP>:442/hcc/Node/network-settings>). È possibile selezionare le impostazioni **Bond1G** (gestione) o **Bond10G** (storage). L'elenco seguente descrive le impostazioni che è possibile modificare quando un nodo di storage si trova nello stato Available (disponibile), Pending (in sospeso) o Active (attivo):

- **Metodo**

Il metodo utilizzato per configurare l'interfaccia. Metodi possibili:

- Loopback: Consente di definire l'interfaccia di loopback IPv4.
- Manual (Manuale): Consente di definire le interfacce per le quali non viene eseguita alcuna configurazione per impostazione predefinita.
- dhcp: Utilizzato per ottenere un indirizzo IP tramite DHCP.
- Static (statico): Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.

- **Velocità di collegamento**

La velocità negoziata dalla NIC virtuale.

- **Indirizzo IPv4**

L'indirizzo IPv4 per la rete eth0.

- **IPv4 Subnet Mask**

Suddivisioni di indirizzi della rete IPv4.

- **Indirizzo gateway IPv4**

Router network address (Indirizzo di rete del router) per l'invio dei pacchetti dalla rete locale.

- **Indirizzo IPv6**

L'indirizzo IPv6 per la rete eth0.

- **IPv6 Gateway Address**

Router network address (Indirizzo di rete del router) per l'invio dei pacchetti dalla rete locale.

- **MTU**

Dimensione massima dei pacchetti che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete per lo storage, il valore deve essere 9000.

- **Server DNS**

Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Cerca domini**

Cercare ulteriori indirizzi MAC disponibili per il sistema.

- **Modalità Bond**

Può essere una delle seguenti modalità:

- ActivePassive (predefinito)
- ALB
- LACP

- **Stato**

Valori possibili:

- UpandRunning
- Giù
- Su

- **Virtual Network Tag**

Tag assegnato al momento della creazione della rete virtuale.

- **Percorsi**

Route statiche verso host o reti specifici attraverso l'interfaccia associata che i route sono configurati per l'utilizzo.

Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo

È possibile verificare le impostazioni del cluster per un nodo di storage dopo la configurazione del cluster e modificare il nome host del nodo.

Il seguente elenco descrive le impostazioni del cluster per un nodo di storage indicate nella pagina **Cluster Settings** dell'interfaccia utente per nodo (<https://<node IP>:442/hcc/Node/cluster-settings>).

- **Ruolo**

Ruolo del nodo nel cluster. Valori possibili:

- Storage: Nodo storage o Fibre Channel.
- Gestione: Il nodo è un nodo di gestione.

- **Nome host**

Nome del nodo.

- **Cluster**

Nome del cluster.

- **Appartenenza al cluster**

Stato del nodo. Valori possibili:

- Disponibile: Il nodo non ha un nome di cluster associato e non fa ancora parte di un cluster.
- In sospenso: 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 software compatibile sul nodo. Al termine, il nodo passa allo stato attivo.
- Attivo: Il nodo partecipa a un cluster. L'autenticazione è necessaria per modificare il nodo.

• **Versione**

Versione del software Element in esecuzione sul nodo.

• **Ensemble**

Nodi che fanno parte dell'insieme di 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. Questo valore predefinito è Bond1G, ma può anche utilizzare Bond10G.

• **Interfaccia storage**

Interfaccia di rete dello storage con Bond10G.

• **Crittografia abilitata**

Indica se il nodo supporta o meno la crittografia del disco.

Eseguire test di sistema utilizzando l'interfaccia utente per nodo

È possibile verificare le modifiche alle impostazioni di rete dopo averle salvate nella configurazione di rete. È possibile eseguire i test per assicurarsi che il nodo di storage sia stabile e possa essere portato online senza problemi.

Si è effettuato l'accesso all'interfaccia utente per nodo per il nodo di storage.

1. Fare clic su **Test di sistema**.
2. Fare clic su **Esegui test** accanto al test che si desidera eseguire oppure selezionare **Esegui tutti test**.



L'esecuzione di tutte le operazioni di test può richiedere molto tempo e deve essere eseguita solo sotto la direzione del supporto NetApp.

- **Test Connected Ensemble**

Verifica e verifica la connettività a un insieme di database. Per impostazione predefinita, il test utilizza l'insieme per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un gruppo diverso per testare la connettività.

- **Test Connect MVIP**

Esegue il ping dell'indirizzo IP virtuale di gestione (MVIP) specificato ed esegue una semplice chiamata API a 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**

Ping dell'indirizzo IP virtuale dello storage (SVIP) specificato utilizzando pacchetti ICMP (Internet Control message Protocol) che corrispondono alle dimensioni massime dell'unità di trasmissione (MTU) impostate sulla scheda di rete. Quindi si connette a SVIP come iniziatore iSCSI. Per impostazione predefinita, il test utilizza l'SVIP per il cluster a cui è associato il nodo.

- **Test hardware Config**

Verifica che tutte le configurazioni hardware siano corrette, verifica la correttezza delle versioni del firmware e verifica che tutti i dischi siano installati e funzionino correttamente. Si tratta della stessa procedura utilizzata per i test di fabbrica.



Questo test richiede un elevato numero di risorse e deve essere eseguito solo se richiesto dal supporto NetApp.

- **Verifica della connettività locale**

Verifica la connettività a tutti gli altri nodi del cluster eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test viene visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

- **Eeguire il test per individuare il cluster**

Convalida che il nodo sia in grado di individuare il cluster specificato nella configurazione del cluster.

- **Test Network Config**

Verifica che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate nel sistema. Questo test non è destinato a rilevare guasti hardware quando un nodo partecipa attivamente a un cluster.

- **Test Ping**

Ping un elenco specifico di host o, se non ne viene specificato alcuno, crea dinamicamente un elenco di tutti i nodi registrati nel cluster e esegue il ping ciascuno per una semplice connettività.

- **Verifica della connettività remota**

Verifica la connettività a tutti i nodi dei cluster associati in remoto eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test viene visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

Eseguire le utility di sistema utilizzando l'interfaccia utente per nodo

È possibile utilizzare l'interfaccia utente per nodo per il nodo di storage per creare o eliminare pacchetti di supporto, reimpostare le impostazioni di configurazione per i dischi e riavviare i servizi di rete o cluster.

Si è effettuato l'accesso all'interfaccia utente per nodo per il nodo di storage.

1. Fare clic su **Utilità di sistema**.
2. Fare clic sul pulsante dell'utilità di sistema che si desidera eseguire.

- **Alimentazione di controllo**

Riavvia, spegne e riaccende il nodo.



Questa operazione causa la perdita temporanea della connettività di rete.

Specificare i seguenti parametri:

- Azione: Le opzioni includono Restart (Riavvia) e Halt (arresta) (Spegni).
- Wakeup Delay (ritardo di attivazione): Qualsiasi tempo aggiuntivo prima che il nodo ripresenti online.

- **Collect Node Logs**

Crea un bundle di supporto nella directory /tmp/bundle del nodo.

Specificare i seguenti parametri:

- Bundle Name (Nome bundle): Nome univoco per ciascun bundle di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
- Args extra: Questo parametro viene inviato allo script sf_make_support_bundle. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp.
- Timeout sec (sec timeout): Specificare il numero di secondi di attesa per ogni singola risposta ping.

- **Elimina registri nodi**

Elimina tutti i bundle di supporto correnti sul nodo creati utilizzando **Create Cluster Support Bundle** o il metodo API CreateSupportBundle.

- **Ripristina unità**

Inizializza i dischi e rimuove tutti i dati attualmente presenti sul disco. 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 ripristinare.

- **Reset Network Config** (Ripristina 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.

◦ Ripristina nodo

Consente di ripristinare le impostazioni predefinite di un nodo. Tutti i dati vengono rimossi, ma le impostazioni di rete del nodo vengono conservate durante questa operazione. I nodi possono essere ripristinati solo se non assegnati a un cluster e in stato disponibile.



Quando si utilizza questa opzione, tutti i dati, i pacchetti (aggiornamenti software), le configurazioni e i file di log vengono cancellati dal nodo.

◦ Riavvia rete

Riavvia tutti i servizi di rete su un nodo.



Questa operazione può causare la perdita temporanea della connettività di rete.

◦ Riavviare i servizi

Riavvia i servizi software Element su un nodo.



Questa operazione può causare un'interruzione temporanea del servizio del nodo. Questa operazione deve essere eseguita solo sotto la direzione 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 utility 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 di VMware vCenter ed evitare di definire le stesse risorse di storage e calcolo o istanze di vCenter in più nodi di gestione.

Vedere "[documentazione del nodo di gestione](#)" per ulteriori informazioni.

Comprendere i livelli di completezza del cluster

Il software cluster running Element genera errori del cluster per avvisare l'amministratore dello storage quando il cluster sta esaurendo la capacità. Sono disponibili tre livelli di riempimento del cluster, tutti visualizzati nell'interfaccia utente di NetApp Element: Avviso, errore e critico.

Il sistema utilizza il codice di errore BlockClusterFull per avvisare della completezza dello storage a blocchi del cluster. È possibile visualizzare i livelli di severità di pienezza del cluster dalla scheda Avvisi dell'interfaccia utente di Element.

Il seguente elenco include informazioni sui livelli di severità di BlockClusterFull:

- **Attenzione**

Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità dei blocchi del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al 3% sotto il livello di errore e può essere regolato tramite l'interfaccia utente e l'API Element. È necessario aggiungere più capacità o liberare capacità il prima possibile.

- **Errore**

Quando il cluster si trova in questo stato, in caso di perdita di un nodo, la capacità del cluster non sarà sufficiente per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot vengono bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per qualsiasi cluster. È necessario aggiungere ulteriore capacità o liberare immediatamente capacità.

- **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 effettuare nuove connessioni iSCSI al cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente ulteriore capacità.

Il sistema utilizza il codice di errore MetadataClusterFull per avvisare sulla completezza dello storage dei metadati del cluster. È possibile visualizzare la completezza dello storage dei metadati del cluster dalla sezione Cluster Capacity (capacità cluster) nella pagina Overview (Panoramica) della scheda Reporting (rapporti) nell'interfaccia utente di Element.

Il seguente elenco include informazioni sui livelli di severità MetadataClusterFull:

- **Attenzione**

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 3% sotto il livello di errore e può essere regolato tramite l'API Element. È necessario aggiungere più capacità o liberare capacità il prima possibile.

- **Errore**

Quando il cluster si trova in questo stato, in caso di perdita di un nodo, la capacità del cluster non sarà sufficiente per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot vengono bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per qualsiasi cluster. È necessario aggiungere ulteriore capacità o liberare immediatamente capacità.

- **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 effettuare nuove connessioni iSCSI al cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente ulteriore capacità.



Quanto segue si applica alle soglie del cluster a due nodi:

- L'errore di fullness dei metadati è inferiore del 20% al livello critico.

- L'errore di fullness del blocco è un disco a 1 blocco (inclusa la capacità inutilizzata) inferiore al livello critico, il che significa che due dischi a blocchi hanno una capacità inferiore al livello critico.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.