# Concetti

## Element Software

NetApp
November 18, 2025

# Sommario

# Concetti

Apprendi i concetti di base relativi al software Element.

- "Panoramica del prodotto"
- Panoramica dell'architettura SolidFire
- Nodi
- Cluster
- "Sicurezza"
- Account e permessi
- "Volumi"
- Protezione dei dati
- Prestazioni e qualità del servizio

# Panoramica del prodotto

Un sistema di archiviazione all-flash SolidFire è composto da componenti hardware discreti (unità e nodi) combinati in un unico pool di risorse di archiviazione. Questo cluster unificato si presenta come un singolo sistema di archiviazione utilizzabile da client esterni ed è gestito tramite il software NetApp Element .

Utilizzando l'interfaccia Element, l'API o altri strumenti di gestione, è possibile monitorare la capacità e le prestazioni di archiviazione del cluster SolidFire e gestire l'attività di archiviazione in un'infrastruttura multi-tenant.

## Caratteristiche SolidFire

Un sistema Solidfire offre le seguenti caratteristiche:

- Offre storage ad alte prestazioni per la tua infrastruttura cloud privata su larga scala
- Fornisce una scala flessibile che consente di soddisfare le mutevoli esigenze di archiviazione
- Utilizza un'interfaccia software Element per la gestione dell'archiviazione basata su API
- Garantisce le prestazioni utilizzando le politiche di qualità del servizio
- Include il bilanciamento automatico del carico su tutti i nodi del cluster
- Riequilibra automaticamente i cluster quando vengono aggiunti o sottratti nodi

## Distribuzione di SolidFire

Utilizzare nodi di archiviazione forniti da NetApp e integrati con il software NetApp Element .

"Panoramica dell'architettura di archiviazione all-flash SolidFire"

## Trova maggiori informazioni

- "Plug-in NetApp Element per vCenter Server"

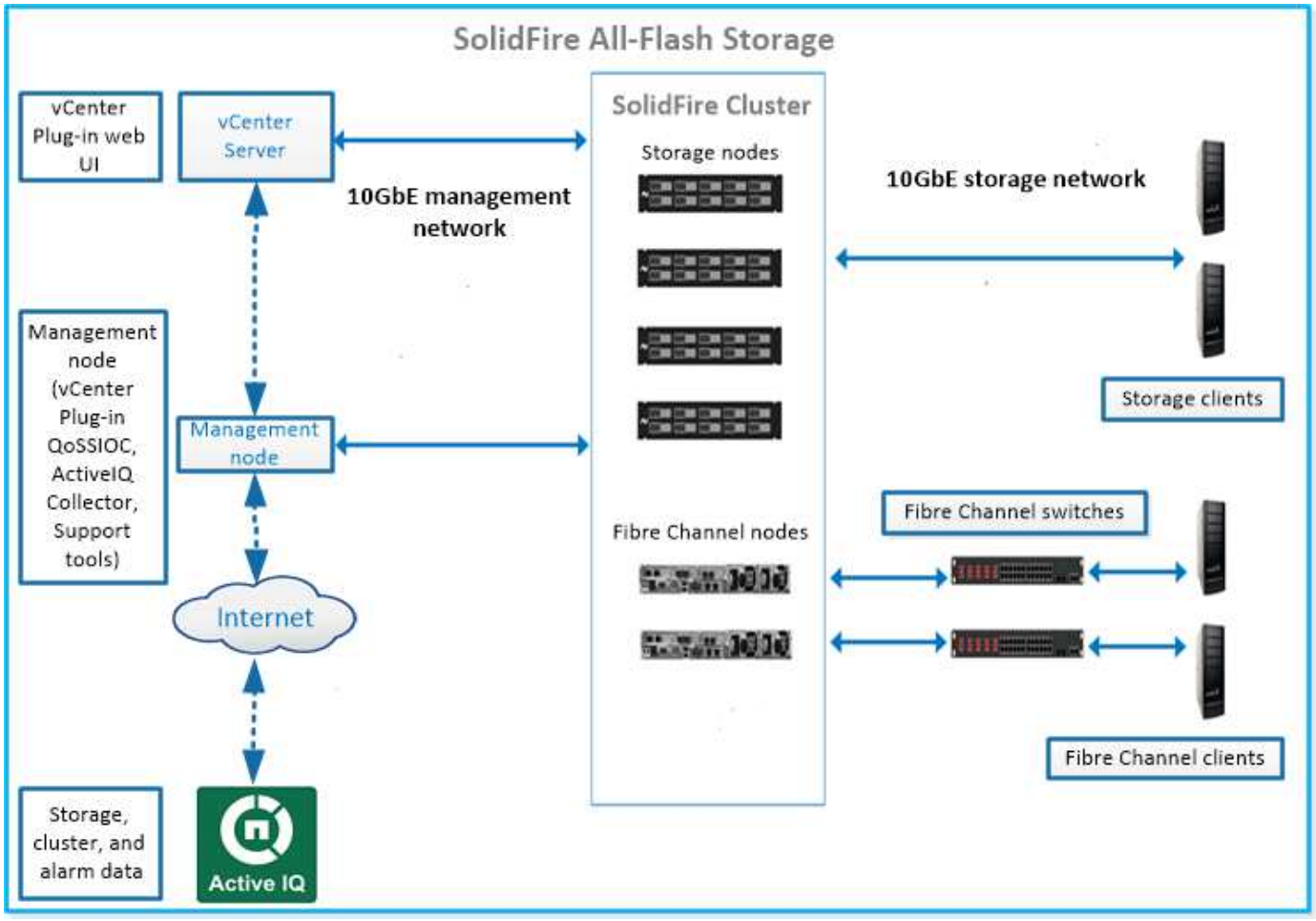
# Architettura e componenti

## Scopri di più sull'architettura SolidFire

Un sistema di storage all-flash SolidFire è composto da componenti hardware discreti (unità e nodi) che vengono combinati in un pool di risorse di storage con il software NetApp Element in esecuzione indipendente su ciascun nodo. Questo singolo sistema di archiviazione viene gestito come un'unica entità tramite l'interfaccia utente del software Element, l'API e altri strumenti di gestione.

Un sistema di archiviazione SolidFire include i seguenti componenti hardware:

- **Cluster**: l'hub del sistema di archiviazione SolidFire , ovvero un insieme di nodi.
- **Nodi**: i componenti hardware raggruppati in un cluster. Esistono due tipi di nodi:
  - Nodi di archiviazione, che sono server contenenti una raccolta di unità
  - Nodi Fibre Channel (FC), che utilizzi per connetterti ai client FC
- **Unità**: utilizzate nei nodi di archiviazione per archiviare i dati per il cluster. Un nodo di archiviazione contiene due tipi di unità:
  - Le unità metadati del volume archiviano informazioni che definiscono i volumi e altri oggetti all'interno di un cluster.
  - Le unità a blocchi memorizzano blocchi di dati per i volumi.



È possibile gestire, monitorare e aggiornare il sistema utilizzando l'interfaccia utente web di Element e altri strumenti compatibili:

- "Interfacce software SolidFire"
- "SolidFire Active IQ"
- "Nodo di gestione per il software Element"
- "Servizi di gestione"

### URL comuni

Ecco gli URL più comuni utilizzati con un sistema di archiviazione all-flash SolidFire :

| URL | Descrizione |
|---|---|
| `https://[storage cluster MVIP address]` | Accedi all'interfaccia utente del software NetApp Element . |
| `https://activeiq.solidfire.com` | Monitora i dati e ricevi avvisi su eventuali colli di bottiglia nelle prestazioni o potenziali problemi di sistema. |
| `https://[management node IP address]` | Accedi a NetApp Hybrid Cloud Control per aggiornare l'installazione dello storage e i servizi di gestione. |
| `https://[IP address]:442` | Dall'interfaccia utente per nodo, accedi alle impostazioni di rete e cluster e utilizza test e utilità di sistema."Saperne di più." |
| `https://[management node IP address]/mnode` | Utilizzare i servizi di gestione REST API e altre funzionalità dal nodo di gestione."Saperne di più." |
| `https://[management node IP address]:9443` | Registrare il pacchetto vCenter Plug-in in vSphere Web Client."Saperne di più." |

### Trova maggiori informazioni

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

## Interfacce software SolidFire

È possibile gestire un sistema di archiviazione SolidFire utilizzando diverse interfacce software e utilità di integrazione NetApp Element .

### Opzioni

- Interfaccia utente del software NetApp Element
- API del software NetApp Element
- Plug-in NetApp Element per vCenter Server
- Controllo del cloud ibrido NetApp
- Interfacce utente dei nodi di gestione
- Ulteriori utilità e strumenti di integrazione

### Interfaccia utente del software NetApp Element

Consente di configurare l'archiviazione Element, monitorare la capacità e le prestazioni del cluster e gestire l'attività di archiviazione in un'infrastruttura multi-tenant. Element è il sistema operativo di archiviazione al centro di un cluster SolidFire . Il software Element viene eseguito in modo indipendente su tutti i nodi del cluster e consente ai nodi del cluster di combinare risorse presentate come un unico sistema di archiviazione ai client esterni. Element Software è responsabile del coordinamento, della scalabilità e della gestione del cluster nel suo complesso. L'interfaccia software è basata sull'API Element.

"Gestisci lo storage con il software Element"

### API del software NetApp Element

Consente di utilizzare un set di oggetti, metodi e routine per gestire l'archiviazione degli elementi. L'API Element si basa sul protocollo JSON-RPC su HTTPS. È possibile monitorare le operazioni API nell'interfaccia utente dell'elemento abilitando il registro API; ciò consente di visualizzare i metodi che vengono inviati al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi emessi.

"Gestisci l'archiviazione con l'API Element"

### Plug-in NetApp Element per vCenter Server

Consente di configurare e gestire cluster di storage che eseguono il software Element utilizzando un'interfaccia alternativa per l'interfaccia utente di Element in VMware vSphere.

"Plug-in NetApp Element per vCenter Server"

### Controllo del cloud ibrido NetApp

Consente di aggiornare i servizi di archiviazione e gestione di Element e di gestire le risorse di archiviazione tramite l'interfaccia NetApp Hybrid Cloud Control.

"Gestisci e monitora lo storage con NetApp Hybrid Cloud Control"

### Interfacce utente dei nodi di gestione

Il nodo di gestione contiene due interfacce utente: un'interfaccia utente per la gestione dei servizi basati su REST e un'interfaccia utente per nodo per la gestione delle impostazioni di rete e cluster, nonché dei test e delle utilità del sistema operativo. Dall'interfaccia utente dell'API REST è possibile accedere a un menu di API correlate ai servizi che controllano le funzionalità del sistema basate sui servizi dal nodo di gestione.

### Ulteriori utilità e strumenti di integrazione

Sebbene in genere si gestisca l'archiviazione con NetApp Element, NetApp Element API e NetApp Element Plug-in per vCenter Server, è possibile utilizzare utilità e strumenti di integrazione aggiuntivi per accedere all'archiviazione.

#### Elemento CLI

"Elemento CLI"consente di controllare un sistema di archiviazione SolidFire tramite un'interfaccia a riga di comando senza dover ricorrere all'API Element.

#### Strumenti PowerShell per gli elementi

"Strumenti PowerShell per gli elementi"consentono di utilizzare una raccolta di funzioni di Microsoft Windows PowerShell che utilizzano l'API Element per gestire un sistema di archiviazione SolidFire .

#### SDK di elementi

"SDK di elementi"ti consentono di gestire il tuo cluster SolidFire utilizzando questi strumenti:

- Element Java SDK: consente ai programmatori di integrare l'API Element con il linguaggio di programmazione Java.
- Element .NET SDK: consente ai programmatori di integrare l'API Element con la piattaforma di programmazione .NET.
- Element Python SDK: consente ai programmatori di integrare l'API Element con il linguaggio di programmazione Python.

#### Suite di test API SolidFire Postman

Consente ai programmatori di utilizzare una raccolta di"Postino" funzioni che testano le chiamate API dell'elemento.

#### Adattatore di replicazione dello storage SolidFire

"Adattatore di replicazione dello storage SolidFire"si integra con VMware Site Recovery Manager (SRM) per abilitare la comunicazione con i cluster di storage SolidFire replicati ed eseguire i flussi di lavoro supportati.

#### SolidFire vRO

"SolidFire vRO"fornisce un modo pratico per utilizzare l'API Element per amministrare il sistema di archiviazione SolidFire con VMware vRealize Orchestrator.

#### Fornitore SolidFire VSS

"Fornitore SolidFire VSS"integra copie shadow VSS con snapshot e cloni di Element.

### Trova maggiori informazioni

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

## SolidFire Active IQ

"SolidFire Active IQ"è uno strumento basato sul Web che fornisce visualizzazioni storiche costantemente aggiornate dei dati dell'intero cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le prestazioni e la capacità del sistema, nonché di rimanere informati sullo stato di salute del cluster.

Puoi trovare le seguenti informazioni sul tuo sistema in SolidFire Active IQ:

- Numero di nodi e stato dei nodi: integri, offline o guasti
- Rappresentazione grafica dell'utilizzo della CPU, della memoria e della limitazione dei nodi

- Dettagli sul nodo, come numero di serie, posizione dello slot nello chassis, modello e versione del software NetApp Element in esecuzione sul nodo di storage
- Informazioni relative alla CPU e allo storage delle macchine virtuali

Per saperne di più su SolidFire Active IQ, vedere "Documentazione di SolidFire Active IQ" .

**Per maggiori informazioni**

- "Documentazione del software SolidFire ed Element"
- "Plug-in NetApp Element per vCenter Server"
- **Sito di supporto NetApp › Strumenti per Active IQ**

### Nodo di gestione per il software Element

IL"nodo di gestione (mNode)" è una macchina virtuale che viene eseguita in parallelo con uno o più cluster di archiviazione basati sul software Element. Viene utilizzato per aggiornare e fornire servizi di sistema, tra cui monitoraggio e telemetria, gestire le risorse e le impostazioni del cluster, eseguire test e utilità di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

Il nodo di gestione interagisce con un cluster di archiviazione per eseguire azioni di gestione, ma non è un membro del cluster di archiviazione. I nodi di gestione raccolgono periodicamente informazioni sul cluster tramite chiamate API e segnalano queste informazioni ad Active IQ per il monitoraggio remoto (se abilitato). I nodi di gestione sono anche responsabili del coordinamento degli aggiornamenti software dei nodi del cluster.

A partire dalla versione Element 11.3, il nodo di gestione funziona come host di microservizi, consentendo aggiornamenti più rapidi di servizi software selezionati al di fuori delle versioni principali. Questi microservizi o"servizi di gestione" vengono aggiornati frequentemente come pacchetti di servizi.

### Servizi di gestione per l'archiviazione all-flash SolidFire

A partire dalla versione Element 11.3, i **servizi di gestione** sono ospitati su"nodo di gestione" , consentendo aggiornamenti più rapidi di servizi software selezionati al di fuori delle versioni principali.

I servizi di gestione forniscono funzionalità di gestione centralizzata ed estesa per l'archiviazione all-flash SolidFire . Questi servizi includono"Controllo del cloud ibrido NetApp" , Telemetria del sistema Active IQ , registrazione e aggiornamenti del servizio, nonché il servizio QoSSIOC per Element Plug-in per vCenter.

Scopri di più su"rilasci di servizi di gestione" .

# Nodi

I nodi sono risorse hardware o virtuali raggruppate in un cluster per fornire capacità di elaborazione e di archiviazione a blocchi.

Il software NetApp Element definisce vari ruoli dei nodi per un cluster. I tipi di ruoli dei nodi sono i seguenti:

- Nodo di gestione

- Nodo di archiviazione
- Nodo Fibre Channel

Stati dei nodivariano a seconda dell'associazione del cluster.

## Nodo di gestione

Un nodo di gestione è una macchina virtuale utilizzata per aggiornare e fornire servizi di sistema, tra cui monitoraggio e telemetria, gestire risorse e impostazioni del cluster, eseguire test e utilità di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi."Saperne di più"

## Nodo di archiviazione

Un nodo di archiviazione SolidFire è un server contenente una raccolta di unità che comunicano tra loro tramite l'interfaccia di rete Bond10G. Le unità nel nodo contengono spazio di blocchi e metadati per l'archiviazione e la gestione dei dati. Ogni nodo contiene un'immagine di fabbrica del software NetApp Element .

I nodi di archiviazione presentano le seguenti caratteristiche:

- Ogni nodo ha un nome univoco. Se un nome di nodo non viene specificato da un amministratore, il valore predefinito è SF-XXXX, dove XXXX rappresenta quattro caratteri casuali generati dal sistema.
- Ogni nodo ha la propria cache di scrittura NVRAM(non-volatile random access memory) ad alte prestazioni per migliorare le prestazioni complessive del sistema e ridurre la latenza di scrittura.
- Ogni nodo è collegato a due reti, una di archiviazione e una di gestione, ciascuna con due collegamenti indipendenti per garantire ridondanza e prestazioni. Ogni nodo richiede un indirizzo IP su ogni rete.
- È possibile creare un cluster con nuovi nodi di archiviazione oppure aggiungere nodi di archiviazione a un cluster esistente per aumentare la capacità e le prestazioni di archiviazione.
- È possibile aggiungere o rimuovere nodi dal cluster in qualsiasi momento senza interrompere il servizio.

## Nodo Fibre Channel

I nodi SolidFire Fibre Channel forniscono connettività a uno switch Fibre Channel, al quale è possibile collegare i client Fibre Channel. I nodi Fibre Channel fungono da convertitore di protocollo tra i protocolli Fibre Channel e iSCSI; ciò consente di aggiungere la connettività Fibre Channel a qualsiasi cluster SolidFire nuovo o esistente.

I nodi Fibre Channel presentano le seguenti caratteristiche:

- Gli switch Fibre Channel gestiscono lo stato della struttura, garantendo interconnessioni ottimizzate.
- Il traffico tra due porte passa solo attraverso gli switch e non viene trasmesso ad altre porte.
- Il guasto di una porta è isolato e non influisce sul funzionamento delle altre porte.
- In una struttura possono comunicare simultaneamente più coppie di porte.

## Stati operativi del nodo

Un nodo può trovarsi in uno dei diversi stati, a seconda del livello di configurazione.

- **Disponibile**

Il nodo non ha alcun nome di cluster associato e non fa ancora parte di un cluster.

- **In attesa di**

  Il nodo è configurato e può essere aggiunto a un cluster designato.

  Per accedere al nodo non è richiesta l'autenticazione.

- **In attesa di attivazione**

  Il sistema sta installando il software Element compatibile sul nodo. Una volta completato, il nodo passerà allo stato Attivo.

- **Attivo**

  Il nodo partecipa a un cluster.

  Per modificare il nodo è richiesta l'autenticazione.

In ognuno di questi stati, alcuni campi sono di sola lettura.

### Trova maggiori informazioni

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

# Cluster

Un cluster è il fulcro di un sistema di archiviazione SolidFire ed è costituito da un insieme di nodi. Per realizzare l'efficienza di archiviazione SolidFire , è necessario disporre di almeno quattro nodi in un cluster. Un cluster appare sulla rete come un singolo gruppo logico e può quindi essere accessibile come storage a blocchi.

La creazione di un nuovo cluster inizializza un nodo come proprietario delle comunicazioni per un cluster e stabilisce le comunicazioni di rete per ciascun nodo nel cluster. Questo processo viene eseguito una sola volta per ogni nuovo cluster. È possibile creare un cluster utilizzando l'interfaccia utente Element o l'API.

È possibile ampliare un cluster aggiungendo nodi aggiuntivi. Quando si aggiunge un nuovo nodo, non si verifica alcuna interruzione del servizio e il cluster utilizza automaticamente le prestazioni e la capacità del nuovo nodo.

Gli amministratori e gli host possono accedere al cluster utilizzando indirizzi IP virtuali. Qualsiasi nodo del cluster può ospitare gli indirizzi IP virtuali. L'IP virtuale di gestione (MVIP) consente la gestione del cluster tramite una connessione 1GbE, mentre l'IP virtuale di archiviazione (SVIP) consente l'accesso dell'host all'archiviazione tramite una connessione 10GbE. Questi indirizzi IP virtuali consentono connessioni coerenti indipendentemente dalle dimensioni o dalla composizione di un cluster SolidFire . Se un nodo che ospita un indirizzo IP virtuale fallisce, un altro nodo nel cluster inizia a ospitare l'indirizzo IP virtuale.

A partire dalla versione 11.0 di Element, i nodi possono essere configurati con indirizzi IPv4, IPv6 o entrambi per la loro rete di gestione. Ciò vale sia per i nodi di archiviazione che per quelli di gestione, ad eccezione del nodo di gestione 11.3 e versioni successive che non supportano IPv6. Quando si crea un cluster, è possibile utilizzare un solo indirizzo IPv4 o IPv6 per MVIP e il tipo di indirizzo corrispondente deve essere configurato su tutti i nodi.

**Di più sui cluster**

- Cluster di archiviazione autorevoli
- Regola dei terzi
- Capacità bloccata
- Efficienza di archiviazione
- Quorum del cluster di archiviazione

## Cluster di archiviazione autorevoli

Il cluster di storage autorevole è il cluster di storage utilizzato da NetApp Hybrid Cloud Control per autenticare gli utenti.

Se il nodo di gestione ha un solo cluster di archiviazione, questo è il cluster autorevole. Se il nodo di gestione ha due o più cluster di storage, uno di questi cluster viene assegnato come cluster autorevole e solo gli utenti di quel cluster possono accedere a NetApp Hybrid Cloud Control. Per scoprire quale cluster è il cluster autorevole, è possibile utilizzare `GET /mnode/about` API. Nella risposta, l'indirizzo IP nel `token_url` campo è l'indirizzo IP virtuale di gestione (MVIP) del cluster di archiviazione autorevole. Se si tenta di accedere a NetApp Hybrid Cloud Control come utente che non si trova nel cluster autorevole, il tentativo di accesso non riuscirà.

Molte funzionalità di NetApp Hybrid Cloud Control sono progettate per funzionare con più cluster di storage, ma l'autenticazione e l'autorizzazione presentano delle limitazioni. La limitazione relativa all'autenticazione e all'autorizzazione è che l'utente del cluster autorevole può eseguire azioni su altri cluster collegati a NetApp Hybrid Cloud Control anche se non è un utente degli altri cluster di storage.

Prima di procedere con la gestione di più cluster di archiviazione, è necessario assicurarsi che gli utenti definiti sui cluster autorevoli siano definiti su tutti gli altri cluster di archiviazione con le stesse autorizzazioni. Puoi gestire gli utenti da"Interfaccia utente del software Element" .

Vedere"creare e gestire risorse di cluster di archiviazione" per ulteriori informazioni sull'utilizzo delle risorse del cluster di archiviazione del nodo di gestione.

## Regola dei terzi

Quando si combinano tipi di nodi di storage in un cluster di storage NetApp SolidFire , nessun singolo nodo di storage può contenere più del 33% della capacità totale del cluster di storage.

## Capacità bloccata

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

## Efficienza di archiviazione

I cluster di storage Netapp SolidFire sfruttano la deduplicazione, la compressione e il thin provisioning per ridurre la quantità di storage fisico necessaria per archiviare un volume.

- **Compressione**

  La compressione riduce la quantità di spazio di archiviazione fisico richiesto per un volume combinando i blocchi di dati in gruppi di compressione, ognuno dei quali viene archiviato come un singolo blocco.

- **Deduplicazione**

  La deduplicazione riduce la quantità di spazio di archiviazione fisico richiesto per un volume eliminando i blocchi di dati duplicati.

- **Provisioning sottile**

  Un volume con thin provisioning o LUN è un volume per il quale non è stato prenotato in anticipo alcuno spazio di archiviazione. Al contrario, lo spazio di archiviazione viene allocato dinamicamente, in base alle necessità. Lo spazio libero viene rilasciato nuovamente nel sistema di archiviazione quando i dati nel volume o LUN vengono eliminati

## Quorum del cluster di archiviazione

Il software Element crea un cluster di archiviazione dai nodi selezionati, che mantiene un database replicato della configurazione del cluster. Per mantenere il quorum necessario alla resilienza del cluster, è necessario che almeno tre nodi partecipino all'insieme del cluster.

# Sicurezza

Quando utilizzi il tuo sistema di archiviazione all-flash SolidFire , i tuoi dati sono protetti da protocolli di sicurezza standard del settore.

## Crittografia a riposo (hardware)

Tutte le unità nei nodi di archiviazione sono in grado di sfruttare la crittografia AES a 256 bit a livello di unità. Ogni unità ha la propria chiave di crittografia, che viene creata quando l'unità viene inizializzata per la prima volta. Quando si abilita la funzionalità di crittografia, viene creata una password per l'intero cluster e parti della password vengono poi distribuite a tutti i nodi del cluster. Nessun singolo nodo memorizza l'intera password. La password viene quindi utilizzata per proteggere con password tutti gli accessi alle unità. La password è necessaria per sbloccare l'unità e non è più necessaria a meno che non venga rimossa l'alimentazione dall'unità o quest'ultima non sia bloccata.

"Abilitazione della funzionalità di crittografia hardware a riposo"non influisce sulle prestazioni o sull'efficienza del cluster. Se un'unità o un nodo abilitato alla crittografia viene rimosso dalla configurazione del cluster tramite l'API Element o l'interfaccia utente Element, la crittografia a riposo verrà disabilitata sulle unità. Dopo aver rimosso l'unità, è possibile cancellarla in modo sicuro utilizzando `SecureEraseDrives` Metodo API. Se un'unità fisica o un nodo viene rimosso forzatamente, i dati rimangono protetti dalla password dell'intero cluster e dalle chiavi di crittografia individuali dell'unità.

## Crittografia a riposo (software)

Un altro tipo di crittografia a riposo, la crittografia software a riposo, consente di crittografare tutti i dati scritti su SSD in un cluster di archiviazione. "Quando abilitato" , crittografa automaticamente tutti i dati scritti e decrittografa tutti i dati letti nel software. La crittografia software a riposo rispecchia l'implementazione dell'unità auto-crittografante (SED) nell'hardware per garantire la sicurezza dei dati in assenza di SED.

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

Sia la crittografia a riposo basata su software che su hardware può essere utilizzata in modo indipendente o in combinazione tra loro.

## Gestione delle chiavi esterne

È possibile configurare il software Element in modo che utilizzi un servizio di gestione delle chiavi (KMS) di terze parti conforme a KMIP per gestire le chiavi di crittografia del cluster di archiviazione. Quando si abilita questa funzionalità, la chiave di crittografia della password di accesso all'unità a livello di cluster del cluster di archiviazione viene gestita da un KMS specificato dall'utente.

Element può utilizzare i seguenti servizi di gestione delle chiavi:

- Gemalto SafeNet KeySecure
- SafeNet AT KeySecure
- Controllo chiave HyTrust
- Responsabile della sicurezza dei dati Vormetric
- IBM Security Key Lifecycle Manager

Per ulteriori informazioni sulla configurazione della gestione delle chiavi esterne, vedere"per iniziare con la gestione delle chiavi esterne" documentazione.

## Autenticazione multifattoriale

L'autenticazione a più fattori (MFA) consente di richiedere agli utenti di presentare più tipi di prove per l'autenticazione con l'interfaccia utente Web NetApp Element o con l'interfaccia utente del nodo di storage al momento dell'accesso. È possibile configurare Element in modo che accetti solo l'autenticazione a più fattori per gli accessi che si integrano con il sistema di gestione utenti e il provider di identità esistenti. È possibile configurare Element per integrarlo con un provider di identità SAML 2.0 esistente, in grado di applicare più schemi di autenticazione, ad esempio password e messaggio di testo, password e messaggio di posta elettronica o altri metodi.

È possibile abbinare l'autenticazione a più fattori ai provider di identità (IdP) più comuni e compatibili con SAML 2.0, come Microsoft Active Directory Federation Services (ADFS) e Shibboleth.

Per configurare MFA, vedere "abilitare l'autenticazione a più fattori" documentazione.

## FIPS 140-2 per HTTPS e crittografia dei dati a riposo

I cluster di storage NetApp SolidFire supportano la crittografia conforme ai requisiti FIPS (Federal Information Processing Standard) 140-2 per i moduli crittografici. È possibile abilitare la conformità FIPS 140-2 sul cluster SolidFire sia per le comunicazioni HTTPS sia per la crittografia delle unità.

Quando si abilita la modalità operativa FIPS 140-2 sul cluster, il cluster attiva il NetApp Cryptographic Security Module (NCSM) e sfrutta la crittografia certificata FIPS 140-2 Livello 1 per tutte le comunicazioni tramite HTTPS all'interfaccia utente e all'API NetApp Element . Tu usi il `EnableFeature` API Element con `fips` parametro per abilitare la crittografia HTTPS FIPS 140-2. Nei cluster di archiviazione con hardware compatibile con FIPS, è anche possibile abilitare la crittografia delle unità FIPS per i dati inattivi utilizzando `EnableFeature` API Element con `FipsDrives` parametro.

Per ulteriori informazioni sulla preparazione di un nuovo cluster di archiviazione per la crittografia FIPS 140-2, vedere"Creare un cluster che supporti le unità FIPS" .

Per ulteriori informazioni sull'abilitazione di FIPS 140-2 su un cluster esistente e preparato, vedere"l'API dell'elemento EnableFeature" .

### Per maggiori informazioni

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

# Account e permessi

Per amministrare e fornire accesso alle risorse di archiviazione sul tuo sistema, dovrai configurare gli account per le risorse di sistema.

Utilizzando Element Storage puoi creare e gestire i seguenti tipi di account:

- Account utente amministratore per il cluster di archiviazione
- Account utente per l'accesso al volume di archiviazione
- Account utente cluster autorevoli per NetApp Hybrid Cloud Control

### Account amministratore del cluster di archiviazione

In un cluster di storage che esegue il software NetApp Element possono esistere due tipi di account amministratore:

- **Account amministratore del cluster primario**: questo account amministratore viene creato quando viene creato il cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo all'utente root in un sistema Linux. Puoi modificare la password per questo account amministratore.
- **Account amministratore del cluster**: è possibile concedere a un account amministratore del cluster un intervallo limitato di 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 e Element UI all'interno del sistema di archiviazione.

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

Puoi"gestire gli account degli amministratori del cluster" creando, eliminando e modificando gli account degli amministratori del cluster, cambiando la password degli amministratori del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

## Account utente

Gli account utente vengono utilizzati per controllare l'accesso alle risorse di storage su una rete basata sul software NetApp Element . È necessario almeno un account utente prima di poter creare un volume.

Quando si crea un volume, questo viene assegnato a un account. Se hai creato un volume virtuale, l'account è il contenitore di archiviazione.

Ecco alcune considerazioni aggiuntive:

- L'account contiene l'autenticazione CHAP necessaria per accedere ai volumi ad esso assegnati.
- A un account possono essere assegnati fino a 2000 volumi, ma un volume può appartenere a un solo account.
- Gli account utente possono essere gestiti dal punto di estensione NetApp Element Management.

## Account utente autorevoli del cluster

Gli account utente autorevoli del cluster possono eseguire l'autenticazione su qualsiasi risorsa di storage associata all'istanza di NetApp Hybrid Cloud Control di nodi e cluster. Con questo account puoi gestire volumi, account, gruppi di accesso e altro ancora su tutti i cluster.

Gli account utente autorevoli vengono gestiti tramite l'opzione Gestione utenti nel menu in alto a destra in NetApp Hybrid Cloud Control.

IL"cluster di archiviazione autorevole" è il cluster di storage utilizzato da NetApp Hybrid Cloud Control per autenticare gli utenti.

Tutti gli utenti creati sul cluster di storage autorevole possono accedere a NetApp Hybrid Cloud Control. Gli utenti creati su altri cluster di archiviazione *non* possono accedere a Hybrid Cloud Control.

- Se il nodo di gestione ha un solo cluster di archiviazione, questo è il cluster autorevole.
- Se il nodo di gestione ha due o più cluster di storage, uno di questi cluster viene assegnato come cluster autorevole e solo gli utenti di quel cluster possono accedere a NetApp Hybrid Cloud Control.

Sebbene molte funzionalità di NetApp Hybrid Cloud Control funzionino con più cluster di storage, l'autenticazione e l'autorizzazione presentano delle limitazioni necessarie. La limitazione relativa all'autenticazione e all'autorizzazione è che gli utenti del cluster autorevole possono eseguire azioni su altri cluster collegati a NetApp Hybrid Cloud Control anche se non sono utenti degli altri cluster di storage. Prima di procedere con la gestione di più cluster di archiviazione, è necessario assicurarsi che gli utenti definiti sui cluster autorevoli siano definiti su tutti gli altri cluster di archiviazione con le stesse autorizzazioni. È possibile gestire gli utenti da NetApp Hybrid Cloud Control.

## Conti di volume

Gli account specifici del volume sono specifici solo del cluster di archiviazione su cui sono stati creati. Questi account consentono di impostare autorizzazioni su volumi specifici nella rete, ma non hanno alcun effetto al di fuori di tali volumi.

Gli account dei volumi vengono gestiti all'interno della tabella NetApp Hybrid Cloud Control Volumes.

# Magazzinaggio

## Volumi

Il sistema di storage NetApp Element esegue il provisioning dello storage tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel.

Element Storage consente di creare, visualizzare, modificare, eliminare, clonare, eseguire il backup o ripristinare volumi per gli account utente. È inoltre possibile gestire ciascun volume su un cluster e aggiungere o rimuovere volumi nei gruppi di accesso ai volumi.

### Volumi persistenti

I volumi persistenti consentono di archiviare i dati di configurazione del nodo di gestione su un cluster di archiviazione specificato, anziché localmente con una macchina virtuale, in modo che i dati possano essere conservati in caso di perdita o rimozione del nodo di gestione. I volumi persistenti sono una configurazione del nodo di gestione facoltativa ma consigliata.

Un'opzione per abilitare i volumi persistenti è inclusa negli script di installazione e aggiornamento quando"distribuzione di un nuovo nodo di gestione" . I volumi persistenti sono volumi su un cluster di archiviazione basato sul software Element che contengono informazioni sulla configurazione del nodo di gestione per la VM del nodo di gestione host che persistono oltre la durata della VM. Se il nodo di gestione viene perso, una VM del nodo di gestione sostitutiva può riconnettersi e recuperare i dati di configurazione per la VM persa.

La funzionalità dei volumi persistenti, se abilitata durante l'installazione o l'aggiornamento, crea automaticamente più volumi. Questi volumi, come qualsiasi volume basato sul software Element, possono essere visualizzati tramite l'interfaccia utente Web del software Element, il plug-in NetApp Element per vCenter Server o l'API, a seconda delle preferenze e dell'installazione. I volumi persistenti devono essere attivi e funzionanti con una connessione iSCSI al nodo di gestione per mantenere i dati di configurazione correnti che possono essere utilizzati per il ripristino.

> 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

## Volumi virtuali (vVols)

vSphere Virtual Volumes è un paradigma di storage per VMware che sposta gran parte della gestione dello storage per vSphere dal sistema di storage a VMware vCenter. Con i volumi virtuali (vVols) è possibile allocare lo spazio di archiviazione in base ai requisiti delle singole macchine virtuali.

### Rilegature

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

### Endpoint del protocollo

Gli host VMware ESXi utilizzano proxy I/O logici noti come endpoint di protocollo per comunicare con i volumi virtuali. Gli host ESXi associano volumi virtuali agli endpoint del protocollo per eseguire operazioni di I/O. Quando una macchina virtuale sull'host esegue un'operazione di I/O, l'endpoint del protocollo associato indirizza l'I/O al volume virtuale a cui è associato.

Gli endpoint del protocollo in un cluster NetApp Element funzionano come unità logiche amministrative SCSI. Ogni endpoint del protocollo viene creato automaticamente dal cluster. Per ogni nodo di un cluster viene creato un endpoint di protocollo corrispondente. Ad esempio, un cluster a quattro nodi avrà quattro endpoint di protocollo.

iSCSI è l'unico protocollo supportato dal software NetApp Element . Il protocollo Fibre Channel non è supportato. Gli endpoint del protocollo non possono essere eliminati o modificati da un utente, non sono associati a un account e non possono essere aggiunti a un gruppo di accesso al volume.

### contenitori di stoccaggio

I contenitori di archiviazione sono strutture logiche che vengono mappate sugli account NetApp Element e vengono utilizzate per la creazione di report e l'allocazione delle risorse. Raggruppano la capacità di archiviazione grezza o aggregano le capacità di archiviazione che il sistema di archiviazione può fornire ai volumi virtuali. Un datastore VVol creato in vSphere viene mappato su un singolo contenitore di archiviazione. Per impostazione predefinita, un singolo contenitore di archiviazione dispone di tutte le risorse disponibili dal cluster NetApp Element . Se è necessaria una governance più granulare per il multi-tenancy, è possibile creare più contenitori di archiviazione.

I contenitori di archiviazione funzionano come account tradizionali e possono contenere sia volumi virtuali che volumi tradizionali. Sono supportati al massimo quattro contenitori di archiviazione per cluster. Per utilizzare la funzionalità VVols è necessario almeno un contenitore di archiviazione. È possibile individuare i contenitori di archiviazione in vCenter durante la creazione di VVol.

### Fornitore VASA

Per far sì che vSphere sia a conoscenza della funzionalità vVol sul cluster NetApp Element , l'amministratore di vSphere deve registrare il provider VASA NetApp Element con vCenter. Il provider VASA è il percorso di controllo fuori banda tra vSphere e il cluster Element. È responsabile dell'esecuzione delle richieste sul cluster Element per conto di vSphere, ad esempio la creazione di VM, la messa a disposizione di VM per vSphere e la pubblicità delle capacità di storage per vSphere.

Il provider VASA viene eseguito come parte del cluster master nel software Element. Il master del cluster è un servizio ad alta disponibilità che esegue il failover su qualsiasi nodo del cluster, se necessario. Se il master del cluster fallisce, il provider VASA si sposta di conseguenza, garantendo un'elevata disponibilità per il provider VASA. Tutte le attività di provisioning e gestione dell'archiviazione utilizzano il provider VASA, che gestisce tutte le modifiche necessarie sul cluster Element.

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

Il supporto VASA per un massimo di 10 vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con il tuo vCenter. Per installare, seguire le istruzioni nel manifesto VASA39 e scaricare il file .tar.gz da"Download del software NetApp" sito. Il provider NetApp Element VASA utilizza un certificato NetApp . Con questa patch, il certificato viene utilizzato senza modifiche da vCenter per supportare più vCenter per l'utilizzo di VASA e VVol. Non modificare il certificato. I certificati SSL personalizzati non sono supportati da VASA.

**Trova maggiori informazioni**

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

### Gruppi di accesso al volume

Creando e utilizzando gruppi di accesso al volume, è possibile controllare l'accesso a un set di volumi. Quando si associa un set di volumi e un set di iniziatori a un gruppo di accesso al volume, il gruppo di accesso concede a tali iniziatori l'accesso a quel set di volumi.

I gruppi di accesso ai volumi nello storage NetApp SolidFire consentono agli IQN dell'iniziatore iSCSI o ai WWPN Fibre Channel di accedere a una raccolta di volumi. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza utilizzare l'autenticazione CHAP. Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso alla rete Fibre Channel ai volumi nel gruppo di accesso.

I gruppi di accesso al volume hanno i seguenti limiti:

- Un massimo di 128 iniziatori per gruppo di accesso al volume.
- Massimo 64 gruppi di accesso per volume.
- Un gruppo di accesso può essere composto da un massimo di 2000 volumi.
- Un IQN o WWPN può appartenere a un solo gruppo di accesso al volume.
- Per i cluster Fibre Channel, un singolo volume può appartenere a un massimo di quattro gruppi di accesso.

### Iniziatori

Gli iniziatori consentono ai client esterni di accedere ai volumi in un cluster, fungendo da punto di ingresso per la comunicazione tra client e volumi. È possibile utilizzare gli iniziatori per l'accesso basato su CHAP anziché su account ai volumi di archiviazione. Un singolo iniziatore, se aggiunto a un gruppo di accesso al volume, consente ai membri del gruppo di accesso al volume di accedere a tutti i volumi di archiviazione aggiunti al gruppo senza richiedere l'autenticazione. Un iniziatore può appartenere a un solo gruppo di accesso.

# Protezione dei dati

Le funzionalità di protezione dei dati includono replica remota, snapshot dei volumi, clonazione dei volumi, domini di protezione e alta disponibilità con tecnologia Double Helix.

La protezione dei dati di archiviazione degli elementi include i seguenti concetti:

- Tipi di replicazione remota
- Snapshot del volume per la protezione dei dati
- Cloni di volume
- Panoramica del processo di backup e ripristino per Element Storage
- Domini di protezione
- Domini di protezione personalizzati
- Doppia elica ad alta disponibilità

## Tipi di replicazione remota

La replica remota dei dati può assumere le seguenti forme:

- Replica sincrona e asincrona tra cluster
- Replica solo snapshot
- Replica tra cluster Element e ONTAP tramite SnapMirror

Per maggiori informazioni, vedere "TR-4741: Replica remota del software NetApp Element" .

### Replica sincrona e asincrona tra cluster

Per i cluster che eseguono il software NetApp Element , la replica in tempo reale consente la rapida creazione di copie remote dei dati del volume.

È possibile associare un cluster di archiviazione a un massimo di altri quattro cluster di archiviazione. È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in una coppia di cluster per scenari di failover e failback.

#### Replica sincrona

La replica sincrona replica continuamente i dati dal cluster di origine al cluster di destinazione ed è influenzata da latenza, perdita di pacchetti, jitter e larghezza di banda.

La replica sincrona è adatta alle seguenti situazioni:

- Replicazione di più sistemi su breve distanza
- Un sito di ripristino di emergenza geograficamente locale rispetto alla fonte
- Applicazioni sensibili al fattore tempo e protezione dei database
- Applicazioni di continuità aziendale che richiedono che il sito secondario agisca come sito primario quando il sito primario è inattivo

#### Replica asincrona

La replica asincrona replica continuamente i dati da un cluster di origine a un cluster di destinazione senza attendere le conferme dal cluster di destinazione. Durante la replica asincrona, le scritture vengono riconosciute al client (applicazione) dopo essere state eseguite sul cluster di origine.

La replica asincrona è adatta alle seguenti situazioni:

- Il sito di disaster recovery è lontano dalla fonte e l'applicazione non tollera latenze indotte dalla rete.
- Esistono limitazioni di larghezza di banda sulla rete che collega i cluster di origine e di destinazione.

**Replica solo snapshot**

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

È possibile impostare la frequenza delle repliche degli snapshot.

La replica snapshot non influisce sulla replica asincrona o sincrona.

**Replica tra cluster Element e ONTAP tramite SnapMirror**

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

SnapMirror è una tecnologia di replicazione Snapshot NetApp che facilita il disaster recovery, progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. La tecnologia SnapMirror crea una replica, o mirror, dei dati di lavoro nell'archivio secondario, da cui è possibile continuare a fornire dati in caso di interruzione nel sito primario. I dati vengono rispecchiati a livello di volume.

La relazione tra il volume di origine nell'archiviazione primaria e il volume di destinazione nell'archiviazione secondaria è detta relazione di protezione dei dati. I cluster sono definiti endpoint in cui risiedono i volumi e i volumi che contengono i dati replicati devono essere sottoposti a peering. Una relazione peer consente ai cluster e ai volumi di scambiare dati in modo sicuro.

SnapMirror viene eseguito in modo nativo sui controller NetApp ONTAP ed è integrato in Element, che viene eseguito sui cluster NetApp HCI e SolidFire . La logica per controllare SnapMirror risiede nel software ONTAP ; pertanto, tutte le relazioni SnapMirror devono coinvolgere almeno un sistema ONTAP per eseguire il lavoro di coordinamento. Gli utenti gestiscono le relazioni tra Element e i cluster ONTAP principalmente tramite l'interfaccia utente di Element; tuttavia, alcune attività di gestione risiedono in NetApp ONTAP System Manager. Gli utenti possono gestire SnapMirror anche tramite CLI e API, entrambe disponibili in ONTAP ed Element.

Vedere "TR-4651: Architettura e configurazione NetApp SolidFire SnapMirror" (è richiesto l'accesso)

È necessario abilitare manualmente la funzionalità SnapMirror a livello di cluster utilizzando il software Element. La funzionalità SnapMirror è disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento.

Dopo aver abilitato SnapMirror, è possibile creare relazioni SnapMirror dalla scheda Protezione dati nel software Element.

Il software NetApp Element 10.1 e versioni successive supportano la funzionalità SnapMirror per copiare e ripristinare snapshot con sistemi ONTAP .

I sistemi che eseguono Element 10.1 e versioni successive includono codice in grado di comunicare direttamente con SnapMirror sui sistemi ONTAP che eseguono 9.3 o versioni successive. L'API Element fornisce metodi per abilitare la funzionalità SnapMirror su cluster, volumi e snapshot. Inoltre, l'interfaccia utente di Element include funzionalità per gestire le relazioni SnapMirror tra il software Element e i sistemi ONTAP .

A partire dai sistemi Element 10.3 e ONTAP 9.4, è possibile replicare i volumi originati ONTAP nei volumi

Element in casi d'uso specifici con funzionalità limitate.

Per maggiori informazioni, vedere "Replica tra NetApp Element Software e ONTAP (ONTAP CLI)".

## Snapshot del volume per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un momento specifico, che può essere utilizzata in seguito per ripristinare un volume a quel momento specifico.

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

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

È possibile eseguire il backup degli snapshot da un cluster Element a un archivio oggetti esterno o a un altro cluster Element. Quando si esegue il backup di uno snapshot in un archivio oggetti esterno, è necessario disporre di una connessione all'archivio oggetti che consenta operazioni di lettura/scrittura.

È possibile acquisire uno snapshot di un singolo volume o di più volumi per la protezione dei dati.

## Cloni di volume

Un clone di un singolo volume o di più volumi è una copia dei dati effettuata in un dato momento. Quando si clona un volume, il sistema crea uno snapshot del volume e quindi crea una copia dei dati a cui fa riferimento lo snapshot.

Si tratta di un processo asincrono e la quantità di tempo richiesta dipende dalle dimensioni del volume che si sta clonando e dal carico attuale del cluster.

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

## Panoramica del processo di backup e ripristino per Element Storage

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.

È possibile eseguire il backup di un volume nel modo seguente:

- Un cluster di archiviazione SolidFire
- Un archivio di oggetti Amazon S3
- Un archivio di oggetti OpenStack Swift

Quando si ripristinano volumi da OpenStack Swift o Amazon S3, sono necessarie le informazioni manifest del processo di backup originale. Se si ripristina un volume di cui è stato eseguito il backup su un sistema di archiviazione SolidFire , non sono necessarie informazioni sul manifesto.

## Domini di protezione

Un dominio di protezione è un nodo o un insieme di nodi raggruppati insieme in modo tale che una parte o addirittura la totalità di esso possa guastarsi, mantenendo al contempo la disponibilità dei dati. I domini di protezione consentono a un cluster di storage di ripristinare automaticamente la funzionalità in caso di perdita di uno chassis (affinità dello chassis) o di un intero dominio (gruppo di chassis).

È possibile abilitare manualmente il monitoraggio del dominio di protezione utilizzando il punto di estensione NetApp Element Configuration nel plug-in NetApp Element per vCenter Server. È possibile selezionare una soglia del dominio di protezione in base ai domini dei nodi o degli chassis. È anche possibile abilitare il monitoraggio del dominio di protezione tramite l'API Element o l'interfaccia utente Web.

Un layout di dominio di protezione assegna ciascun nodo a uno specifico dominio di protezione.

Sono supportati due diversi layout di dominio di protezione, denominati livelli di dominio di protezione.

- A livello di nodo, ogni nodo si trova nel proprio dominio di protezione.
- A livello di chassis, solo i nodi che condividono uno chassis si trovano nello stesso dominio di protezione.
  - Il layout a livello di chassis viene determinato automaticamente dall'hardware quando il nodo viene aggiunto al cluster.
  - In un cluster in cui ogni nodo si trova in uno chassis separato, questi due livelli sono funzionalmente identici.

Quando si crea un nuovo cluster, se si utilizzano nodi di archiviazione che risiedono in uno chassis condiviso, potrebbe essere opportuno valutare la progettazione di una protezione contro gli errori a livello di chassis mediante la funzionalità Domini di protezione.

### Domini di protezione personalizzati

È possibile definire un layout di dominio di protezione personalizzato che corrisponda al layout specifico del telaio e del nodo e in cui ogni nodo sia associato a un solo dominio di protezione personalizzato. Per impostazione predefinita, a ciascun nodo viene assegnato lo stesso dominio di protezione personalizzato predefinito.

Se non vengono assegnati domini di protezione personalizzati:

- Il funzionamento del cluster non è interessato.
- Il livello personalizzato non è né tollerante né resiliente.

Quando si configurano domini di protezione personalizzati per un cluster, sono disponibili tre possibili livelli di protezione, che è possibile visualizzare nella dashboard dell'interfaccia utente Web di Element:

- Non protetto: il cluster di archiviazione non è protetto dal guasto di uno dei suoi domini di protezione personalizzati. Per risolvere questo problema, aggiungere ulteriore capacità di archiviazione al cluster o riconfigurare i domini di protezione personalizzati del cluster per proteggere il cluster da possibili perdite di dati.
- Tollerante agli errori: il cluster di archiviazione dispone di capacità libera sufficiente per impedire la perdita di dati dopo il guasto di uno dei suoi domini di protezione personalizzati.
- Resistente agli errori: il cluster di storage ha sufficiente capacità libera per autoripararsi dopo l'errore di uno dei suoi domini di protezione personalizzati. Una volta completato il processo di ripristino, il cluster sarà protetto dalla perdita di dati in caso di guasto di altri domini.

Se viene assegnato più di un dominio di protezione personalizzato, ciascun sottosistema assegnerà i duplicati a domini di protezione personalizzati separati. Se ciò non è possibile, si torna ad assegnare i duplicati a nodi separati. Ogni sottosistema (ad esempio, contenitori, sezioni, provider di endpoint di protocollo ed ensemble) esegue questa operazione in modo indipendente.

Puoi usare l'interfaccia utente dell'elemento per"configurare domini di protezione personalizzati" oppure puoi utilizzare i seguenti metodi API:

- "OttieniProtectionDomainLayout"- mostra in quale chassis e in quale dominio di protezione personalizzato si trova ciascun nodo.
- "ImpostaProtezioneDominioLayout"- consente di assegnare un dominio di protezione personalizzato a ciascun nodo.

### Doppia elica ad alta disponibilità

La protezione dei dati Double Helix è un metodo di replicazione che distribuisce almeno due copie ridondanti dei dati su tutte le unità di un sistema. L'approccio "senza RAID" consente a un sistema di assorbire più guasti simultanei su tutti i livelli del sistema di archiviazione e di ripararli rapidamente.

# Prestazioni e qualità del servizio

Un cluster di storage SolidFire è in grado di fornire parametri di qualità del servizio (QoS) in base al volume. È possibile garantire le prestazioni del cluster misurate in input e output al secondo (IOPS) utilizzando tre parametri configurabili che definiscono la QoS: IOPS minimi, IOPS massimi e IOPS a raffica.

SolidFire Active IQ dispone di una pagina di raccomandazioni QoS che fornisce consigli sulla configurazione ottimale e sull'impostazione delle impostazioni QoS.

### Parametri di qualità del servizio

I parametri IOPS sono definiti nei seguenti modi:

- **IOPS minimi**: il numero minimo di input e output sostenuti al secondo (IOPS) che il cluster di storage fornisce a un volume. Il valore Min IOPS configurato per un volume rappresenta il livello di prestazioni garantito per un volume. Le prestazioni non scendono al di sotto di questo livello.
- **IOPS massimi**: il numero massimo di IOPS sostenuti che il cluster di storage fornisce a un volume. Quando i livelli IOPS del cluster sono estremamente elevati, questo livello di prestazioni IOPS non viene superato.
- **Burst IOPS** - Numero massimo di IOPS consentiti in uno scenario di burst breve. Se un volume è stato eseguito al di sotto del numero massimo di IOPS, vengono accumulati crediti burst. Quando i livelli di prestazioni diventano molto elevati e vengono spinti al massimo, sul volume sono consentiti brevi raffiche di IOPS.

  Il software Element utilizza Burst IOPS quando un cluster è in esecuzione in uno stato di basso utilizzo degli IOPS del cluster.

  Un singolo volume può accumulare Burst IOPS e utilizzare i crediti per superare i propri Max IOPS fino al livello Burst IOPS per un "periodo di burst" impostato. Un volume può subire un burst fino a 60 secondi se il cluster ha la capacità di gestire il burst. Un volume accumula un secondo di credito burst (fino a un massimo di 60 secondi) per ogni secondo in cui il volume viene eseguito al di sotto del limite Max IOPS.

I burst IOPS sono limitati in due modi:

  - Un volume può superare il suo massimo IOPS per un numero di secondi pari al numero di crediti burst accumulati dal volume.
  - Quando un volume supera l'impostazione Max IOPS, è limitato dall'impostazione Burst IOPS. Pertanto, il burst IOPS non supera mai l'impostazione burst IOPS per il volume.

- **Larghezza di banda massima effettiva** - La larghezza di banda massima viene calcolata moltiplicando il numero di IOPS (in base alla curva QoS) per la dimensione IO.

  Esempio: le impostazioni dei parametri QoS pari a 100 IOPS minimi, 1000 IOPS massimi e 1500 IOPS burst hanno i seguenti effetti sulla qualità delle prestazioni:

  - I carichi di lavoro sono in grado di raggiungere e sostenere un massimo di 1000 IOPS finché non si manifesta sul cluster la condizione di contesa del carico di lavoro per gli IOPS. Gli IOPS vengono quindi ridotti in modo incrementale finché gli IOPS su tutti i volumi rientrano negli intervalli QoS designati e la contesa per le prestazioni viene alleviata.
  - Le prestazioni su tutti i volumi sono spinte verso il valore minimo di IOPS pari a 100. I livelli non scendono al di sotto dell'impostazione Min IOPS, ma potrebbero rimanere superiori a 100 IOPS quando la contesa del carico di lavoro viene alleviata.
  - Le prestazioni non sono mai superiori a 1000 IOPS, né inferiori a 100 IOPS per un periodo prolungato. Sono consentite prestazioni pari a 1500 IOPS (Burst IOPS), ma solo per i volumi che hanno accumulato crediti burst eseguendo al di sotto del Max IOPS e sono consentite solo per brevi periodi di tempo. I livelli di burst non sono mai sostenuti.

## Limiti del valore QoS

Ecco i possibili valori minimi e massimi per QoS.

| Parametri | Valore minimo | Predefinito | 4 4KB | 5 8KB | 6 16KB | 262 KB |
|---|---|---|---|---|---|---|
| IOPS minimi | 50 | 50 | 15.000 | 9.375* | 5556* | 385* |
| IOPS massimi | 100 | 15.000 | 200.000** | 125.000 | 74.074 | 5128 |
| IOPS a raffica | 100 | 15.000 | 200.000** | 125.000 | 74,074 | 5128 |

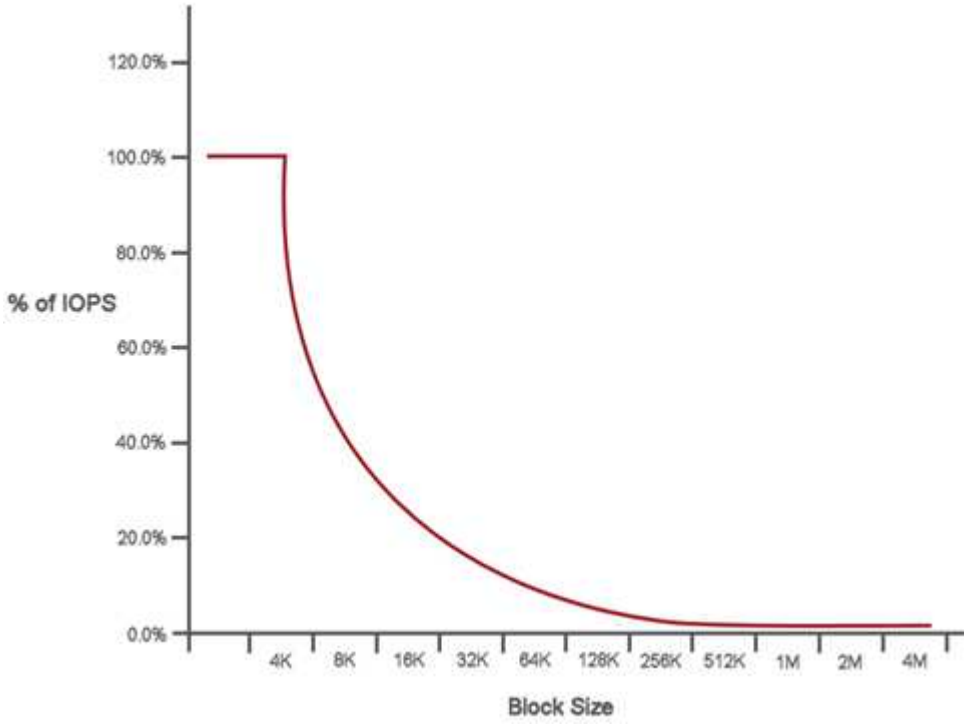
*Queste stime sono approssimative. **I valori Max IOPS e Burst IOPS possono essere impostati fino a 200.000; tuttavia, questa impostazione è consentita solo per superare efficacemente il limite delle prestazioni di un volume. Le prestazioni massime reali di un volume sono limitate dall'utilizzo del cluster e dalle prestazioni per nodo.

## Prestazioni QoS

La curva delle prestazioni QoS mostra la relazione tra la dimensione del blocco e la percentuale di IOPS.

Le dimensioni dei blocchi e la larghezza di banda hanno un impatto diretto sul numero di IOPS che un'applicazione può ottenere. Il software Element tiene conto delle dimensioni dei blocchi che riceve normalizzandole a 4k. In base al carico di lavoro, il sistema potrebbe aumentare le dimensioni dei blocchi. Con l'aumentare delle dimensioni dei blocchi, il sistema aumenta la larghezza di banda fino al livello necessario per elaborare blocchi di dimensioni maggiori. Con l'aumento della larghezza di banda, il numero di IOPS che il sistema è in grado di raggiungere diminuisce.

La curva delle prestazioni QoS mostra la relazione tra l'aumento delle dimensioni dei blocchi e la diminuzione della percentuale di IOPS:




Ad esempio, se le dimensioni dei blocchi sono 4k e la larghezza di banda è 4000 KBps, gli IOPS sono 1000. Se le dimensioni dei blocchi aumentano a 8k, la larghezza di banda aumenta a 5000 KBps e gli IOPS diminuiscono a 625. Tenendo conto delle dimensioni dei blocchi, il sistema garantisce che i carichi di lavoro a priorità inferiore che utilizzano dimensioni dei blocchi più elevate, come i backup e le attività dell'hypervisor, non assorbano troppe prestazioni necessarie al traffico a priorità superiore che utilizza dimensioni dei blocchi più piccole.

## Criteri QoS

Un criterio QoS consente di creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi.

Le policy QoS sono ideali per gli ambienti di servizio, ad esempio con server di database, applicazioni o infrastrutture che si riavviano raramente e necessitano di un accesso costante e paritario allo storage. La QoS per volume individuale è ideale per le VM con utilizzo leggero, come desktop virtuali o VM specializzate di tipo chiosco, che possono essere riavviate, accese o spente quotidianamente o più volte al giorno.

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

Per utilizzare i criteri QoS, il cluster selezionato deve essere Element 10.0 o versione successiva; in caso contrario, le funzioni dei criteri QoS non saranno disponibili.

## Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"

## Informazioni sul copyright



## Informazioni sul marchio commerciale