Concetti

Element Software

NetApp
August 21, 2024

Sommario

Concetti

Scopri i concetti di base relativi al software Element.

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

Trova ulteriori informazioni

- "Panoramica dello storage all-flash SolidFire"
- "Documentazione software SolidFire ed Element"

Panoramica del prodotto

Un sistema storage all-flash SolidFire è composto da componenti hardware discreti (dischi e nodi) che vengono combinati in un singolo pool di risorse di storage. Questo cluster unificato si presenta come un singolo sistema storage per l'utilizzo da parte di client esterni ed è gestito con il software NetApp Element.

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

Funzionalità di SolidFire

Un sistema SolidFire offre le seguenti funzionalità:

- Offre uno storage dalle performance elevate per la tua infrastruttura di cloud privato su larga scala
- Offre una scalabilità flessibile che consente di soddisfare le mutevoli esigenze di storage
- Utilizza un'interfaccia software per elementi di gestione dello storage basata su API
- Garantisce le performance utilizzando le policy di qualità del servizio
- Include il bilanciamento automatico del carico su tutti i nodi del cluster
- Ribilanciare automaticamente i cluster quando i nodi vengono aggiunti o sottratti

Implementazione di SolidFire

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

"Panoramica dell’architettura dello storage all-flash SolidFire"

Trova ulteriori informazioni

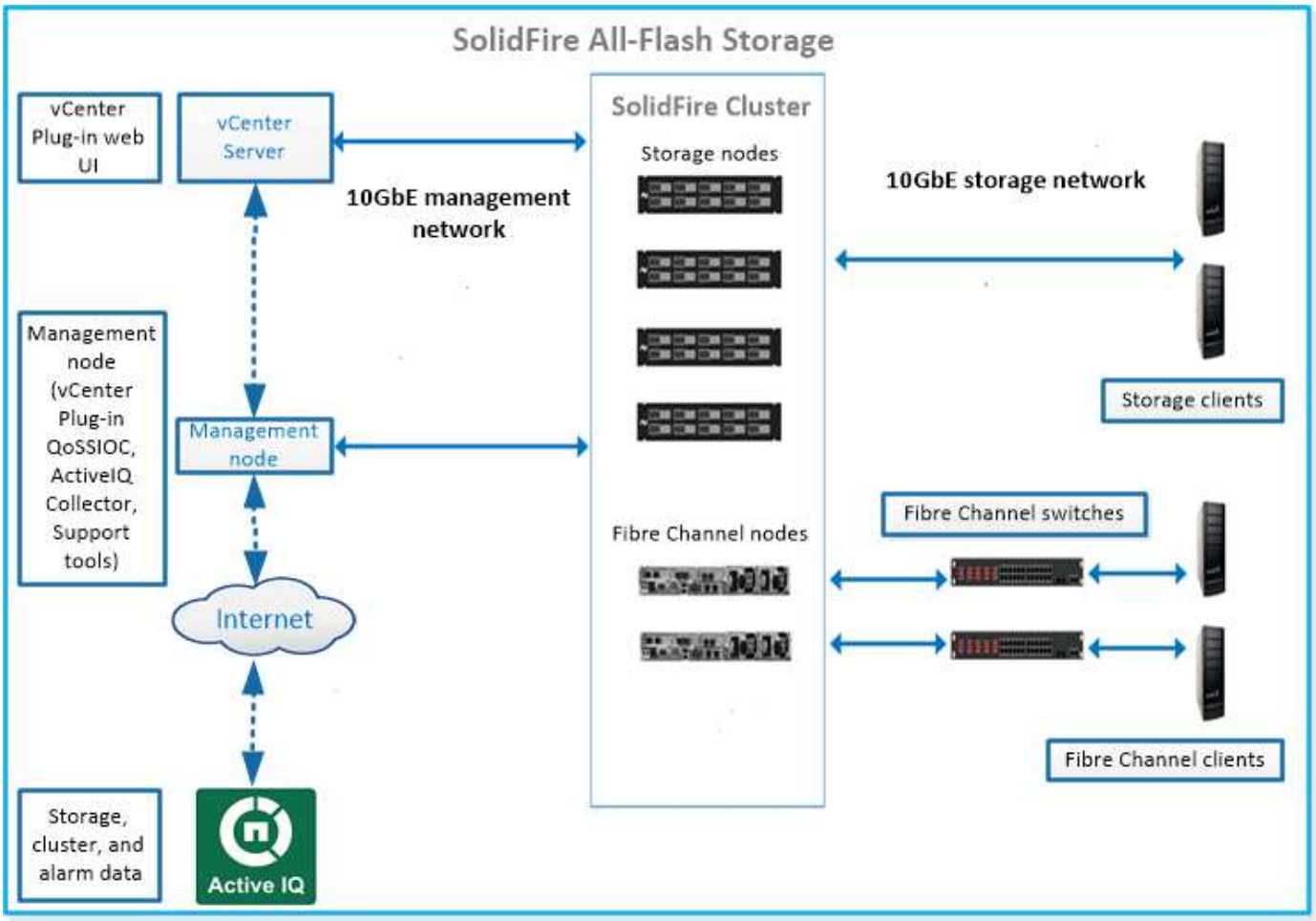
- "Panoramica dello storage all-flash SolidFire"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Panoramica dell’architettura di SolidFire

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

Un sistema storage SolidFire include i seguenti componenti hardware:

- **Cluster**: L’hub del sistema storage SolidFire che è un insieme di nodi.
- **Nodi**: I componenti hardware raggruppati in un cluster. Esistono due tipi di nodi:
  - Nodi di storage, ovvero server che contengono una raccolta di dischi
  - Nodi Fibre Channel (FC), utilizzati per la connessione ai client FC
- **Drives**: Utilizzato nei nodi di storage per memorizzare i dati per il cluster. Un nodo di storage contiene due tipi di dischi:
  - I dischi di metadati dei volumi memorizzano informazioni che definiscono i volumi e altri oggetti all’interno di un cluster.
  - I dischi a blocchi memorizzano i blocchi di dati per i volumi.



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

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

URL comuni

Di seguito sono riportati gli URL comuni utilizzati con un sistema di storage all-flash SolidFire:

URL	Descrizione
`https://[storage cluster MVIP address]`	Accedere all'interfaccia utente del software NetApp Element.
`https://activeiq.solidfire.com`	Monitorare i dati e ricevere avvisi in caso di colli di bottiglia delle performance o potenziali problemi del sistema.
`https://[management node IP address]`	Accedi a NetApp Hybrid Cloud Control per aggiornare l'installazione dello storage e i servizi di gestione degli aggiornamenti.

URL	Descrizione
`https://[IP address]:442`	Dall'interfaccia utente per nodo, accedere alle impostazioni di rete e cluster e utilizzare le utility e i test di sistema. "Scopri di più."
`https://[management node IP address]/mnode`	Utilizzare i servizi di gestione REST API e altre funzionalità dal nodo di gestione. "Scopri di più."
`https://[management node IP address]:9443`	Registrare il pacchetto vCenter Plug-in in vSphere Web Client. "Scopri di più."

Trova ulteriori informazioni

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

Interfacce software SolidFire

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

Opzioni

- Interfaccia utente del software NetApp Element
- API del software NetApp Element
- Plug-in NetApp Element per server vCenter
- NetApp Hybrid Cloud Control
- UI del nodo di gestione
- Utility e tool di integrazione aggiuntivi

Interfaccia utente del software NetApp Element

Consente di configurare lo storage Element, 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 presentate 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.

"Gestire lo storage con il software Element"

API del software NetApp Element

Consente di utilizzare un set di oggetti, metodi e routine per gestire lo storage degli elementi. L'API Element si basa sul protocollo JSON-RPC su HTTPS. È possibile monitorare le operazioni API nell'interfaccia utente Element attivando il log API; in questo modo è possibile visualizzare i metodi che vengono emessi al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi che vengono emessi.

"Gestire lo storage con l'API Element"

Plug-in NetApp Element per server vCenter

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

"Plug-in NetApp Element per server vCenter"

NetApp Hybrid Cloud Control

Consente di aggiornare i servizi di storage e gestione degli elementi e di gestire le risorse di storage utilizzando l'interfaccia NetApp Hybrid Cloud Control.

"Gestione e monitoraggio dello storage con la panoramica di NetApp Hybrid Cloud Control"

UI del nodo 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 test e utility del sistema operativo. Dall'interfaccia utente dell'API REST, è possibile accedere a un menu di API correlate al servizio che controllano la funzionalità del sistema basata sul servizio dal nodo di gestione.

Utility e tool di integrazione aggiuntivi

Anche se in genere si gestisce lo storage con NetApp Element, API NetApp Element e plug-in NetApp Element per vCenter Server, è possibile utilizzare utility e strumenti di integrazione aggiuntivi per accedere allo storage.

Elemento CLI

"Elemento CLI" Consente di controllare un sistema storage SolidFire utilizzando un'interfaccia a riga di comando senza dover utilizzare l'API Element.

Tool PowerShell Element

"Tool PowerShell Element" Consentire di utilizzare una raccolta di funzioni di Microsoft Windows PowerShell che utilizzano l'API Element per gestire un sistema storage SolidFire.

SDK elemento

"SDK elemento" Consente di gestire il cluster SolidFire utilizzando i seguenti 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 Postman di SolidFire

Consente ai programmatori di utilizzare una raccolta di "Postino" Funzioni che testano le chiamate API degli elementi.

Adattatore per la replica dello storage SolidFire

"Adattatore per la replica dello storage SolidFire" Si integra con VMware Site Recovery Manager (SRM) per consentire la comunicazione con cluster di storage SolidFire replicati ed eseguire flussi di lavoro supportati.

SolidFire Vro

"SolidFire Vro" Offre un metodo pratico per utilizzare l'API Element per amministrare il sistema di storage SolidFire con VMware vRealize Orchestrator.

Provider VSS di SolidFire

"Provider VSS di SolidFire" Integra le copie shadow VSS con snapshot e cloni degli elementi.

Trova ulteriori informazioni

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

SolidFire Active IQ

"SolidFire Active IQ" è uno strumento basato sul web che offre viste storiche costantemente aggiornate dei dati a livello di cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le performance e la capacità del sistema, oltre a essere sempre informato sullo stato dei cluster.

In SolidFire Active IQ sono disponibili le seguenti informazioni relative al sistema in uso:

- Numero di nodi e stato dei nodi: Integro, offline o guasto
- Rappresentazione grafica della CPU, dell'utilizzo della memoria e della limitazione dei nodi
- Dettagli sul nodo, come il numero di serie, la posizione dello slot nello chassis, il modello e la versione del software NetApp Element in esecuzione sul nodo di storage
- Informazioni relative a CPU e storage sulle macchine virtuali

Per ulteriori informazioni su SolidFire Active IQ, consultare "Documentazione SolidFire Active IQ".

Per ulteriori informazioni

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

Nodo di gestione per software Element

Il "Nodo di gestione (mNode)" È una macchina virtuale che viene eseguita in parallelo con uno o più cluster di storage basati su 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 utility di sistema e abilitare l'accesso al

supporto NetApp per la risoluzione dei problemi.

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

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

Servizi di gestione per lo storage all-flash SolidFire

A partire dalla release 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 release principali.

I servizi di gestione forniscono funzionalità di gestione estese e centrali per lo storage all-flash SolidFire. Questi servizi includono "NetApp Hybrid Cloud Control", Telemetria del sistema Active IQ, registrazione e aggiornamenti del servizio, nonché il servizio QoSSIOC per il plug-in Element per vCenter.

Scopri di più "release di servizi di gestione".

Nodi

I nodi sono risorse hardware o virtuali raggruppate in un cluster per fornire funzionalità di calcolo e storage a blocchi.

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

- Nodo di gestione
- Nodo storage
- Nodo Fibre Channel

stati dei nodi varia in base all'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 le risorse e le impostazioni del cluster, eseguire test e utility di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi. "Scopri di più"

Nodo storage

Un nodo di storage SolidFire è un server che contiene una raccolta di dischi che comunicano tra loro attraverso l'interfaccia di rete Bond10G. I dischi nel nodo contengono spazio di blocchi e metadati per lo storage e la gestione dei dati. Ogni nodo contiene un'immagine di fabbrica del software NetApp Element.

I nodi di storage hanno le seguenti caratteristiche:

- Ogni nodo ha un nome univoco. Se il nome di un nodo non viene specificato da un amministratore, per

impostazione predefinita è SF-XXXX, dove XXXX è costituito da quattro caratteri casuali generati dal sistema.

- Ogni nodo dispone di una propria cache di scrittura NVRAM (non-volatile Random Access Memory) dalle performance elevate per migliorare le prestazioni generali del sistema e ridurre la latenza di scrittura.
- Ogni nodo è collegato a due reti, storage e gestione, ciascuna con due collegamenti indipendenti per ridondanza e performance. Ciascun nodo richiede un indirizzo IP su ciascuna rete.
- È possibile creare un cluster con nuovi nodi di storage o aggiungere nodi di storage a un cluster esistente per aumentare la capacità e le performance dello storage.
- È possibile aggiungere o rimuovere nodi dal cluster in qualsiasi momento senza interrompere il servizio.

Nodo Fibre Channel

I nodi Fibre Channel SolidFire forniscono connettività a uno switch Fibre Channel, che è possibile collegare ai client Fibre Channel. I nodi Fibre Channel fungono da convertitore di protocollo tra i protocolli Fibre Channel e iSCSI, consentendo di aggiungere connettività Fibre Channel a qualsiasi cluster SolidFire nuovo o esistente.

I nodi Fibre Channel hanno le seguenti caratteristiche:

- Gli switch Fibre Channel gestiscono lo stato del fabric, fornendo 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 di altre porte.
- Più coppie di porte possono comunicare contemporaneamente in un fabric.

stato operativo del nodo

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

- **Disponibile**

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

- **In sospeso**

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

  Per accedere al nodo non è richiesta l'autenticazione.

- **Attivo in sospeso**

  Il sistema sta installando un 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.

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

Trova ulteriori informazioni

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

Cluster

Un cluster è l'hub di un sistema storage SolidFire ed è costituito da un insieme di nodi. È necessario disporre di almeno quattro nodi in un cluster per ottenere l'efficienza dello storage SolidFire. Un cluster viene visualizzato sulla rete come singolo gruppo logico ed è quindi possibile accedervi 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 del 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 scalare 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 dello storage (SVIP) consente l'accesso dell'host allo storage 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 non riesce, un altro nodo del 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 propria rete di gestione. Questo vale sia per i nodi di storage che per i nodi di gestione, ad eccezione del nodo di gestione 11.3 e successivo che non supporta IPv6. Quando si crea un cluster, è possibile utilizzare solo un indirizzo IPv4 o IPv6 singolo per MVIP e il tipo di indirizzo corrispondente deve essere configurato su tutti i nodi.

Ulteriori informazioni sui cluster

- Cluster di storage autorevoli
- Regola dei terzi
- Capacità inutilizzata
- Efficienza dello storage
- Quorum del cluster di storage

Cluster di storage 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 dispone di un solo cluster di storage, si tratta del cluster autorevole. Se il nodo di gestione dispone di due o più cluster di storage, uno di questi 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 in `token_url` Il campo è l'indirizzo IP virtuale di gestione (MVIP) del cluster di storage 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 avrà esito positivo.

Molte funzionalità di NetApp Hybrid Cloud Control sono progettate per funzionare con più cluster di storage, ma l'autenticazione e l'autorizzazione hanno dei limiti. Il limite dell'autenticazione e dell'autorizzazione è che l'utente del cluster autorevole può eseguire azioni su altri cluster legati 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 storage, è necessario assicurarsi che gli utenti definiti nei cluster autorevoli siano definiti in tutti gli altri cluster di storage con le stesse autorizzazioni. È possibile gestire gli utenti da "Interfaccia utente del software Element".

Vedere "creare e gestire le risorse del cluster di storage" per ulteriori informazioni sull'utilizzo delle risorse cluster di storage dei nodi di gestione.

Regola dei terzi

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

Capacità inutilizzata

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 aggiunta una maggiore capacità di 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.

Efficienza dello storage

I cluster di storage NetApp SolidFire utilizzano deduplica, compressione e thin provisioning per ridurre la quantità di storage fisico necessaria per l'archiviazione di un volume.

- **Compressione**

  La compressione riduce la quantità di storage fisico richiesta per un volume combinando i blocchi di dati in gruppi di compressione, ciascuno dei quali viene memorizzato come blocco singolo.

- **Deduplica**

  La deduplica riduce la quantità di storage fisico richiesta per un volume eliminando i blocchi di dati duplicati.

- **Thin provisioning**

  Un volume con thin provisioning o LUN è un volume per il quale lo storage non è riservato in anticipo. Invece, lo storage viene allocato in modo dinamico, in base alle esigenze. Lo spazio libero viene nuovamente rilasciato nel sistema di storage quando i dati nel volume o nel LUN vengono cancellati

Quorum del cluster di storage

Element Software crea un cluster di storage da nodi selezionati, che mantiene un database replicato della configurazione del cluster. Per poter mantenere il quorum per la resilienza del cluster, sono necessari almeno tre nodi per partecipare all'ensemble del cluster.

Sicurezza

Quando si utilizza il sistema di storage all-flash SolidFire, i dati vengono protetti da protocolli di sicurezza standard di settore.

Crittografia a riposo (hardware)

Tutti i dischi nei nodi di storage sono in grado di utilizzare la crittografia AES a 256 bit a livello di unità. Ogni disco dispone di una propria chiave di crittografia, che viene creata al momento della prima inizializzazione del disco. Quando si attiva la funzione di crittografia, viene creata una password a livello di cluster e i frammenti di password vengono quindi distribuiti a tutti i nodi del cluster. Nessun nodo singolo memorizza l'intera password. La password viene quindi utilizzata per proteggere con password tutti gli accessi ai dischi. La password è necessaria per sbloccare l'unità e non è necessaria a meno che l'alimentazione non venga rimossa dall'unità o l'unità non sia bloccata.

"Attivazione della funzione di crittografia hardware a riposo" non influisce sulle prestazioni o sull'efficienza del cluster. Se un disco o nodo abilitato alla crittografia viene rimosso dalla configurazione del cluster con l'API Element o l'interfaccia utente Element, la crittografia a riposo viene disattivata sui dischi. Una volta rimosso il disco, è possibile cancellarlo in modo sicuro utilizzando `SecureEraseDrives` Metodo API. Se un disco o nodo fisico viene rimosso forzatamente, i dati rimangono protetti dalla password a livello di cluster e dalle singole chiavi di crittografia dell'unità.

Crittografia a riposo (software)

Un altro tipo di crittografia a riposo e a riposo del software consente di crittografare tutti i dati scritti su SSD in un cluster di storage. "Se attivato", crittografa tutti i dati scritti e decrta tutti i dati letti automaticamente nel software. La crittografia software a riposo esegue il mirroring dell'implementazione dell'unità con crittografia automatica (SED) nell'hardware per garantire la sicurezza dei dati in assenza di SED.

> 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.

La crittografia a riposo basata su software e hardware può essere utilizzata in modo indipendente o in combinazione tra loro.

Gestione esterna delle chiavi

È possibile configurare Element Software in modo che utilizzi un servizio di gestione delle chiavi (KMS) conforme a KMIP di terze parti per gestire le chiavi di crittografia del cluster di storage. Quando si attiva questa funzione, la chiave di crittografia della password di accesso al disco a livello di cluster dello storage viene gestita da un KMS specificato dall'utente.

Element può utilizzare i seguenti servizi di gestione delle chiavi:

- Gemalto SafeNet KeySecure
- SafeNet IN KeySecure
- KeyControl HyTrust
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

Per ulteriori informazioni sulla configurazione della gestione esterna delle chiavi, vedere "introduzione alla

gestione esterna delle chiavi" documentazione.

Autenticazione a più fattori

L'autenticazione a più fattori (MFA) consente di richiedere agli utenti di presentare diversi tipi di prove per l'autenticazione con l'interfaccia utente Web o l'interfaccia utente del nodo di storage di NetApp Element 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 degli utenti e il provider di identità esistenti. È possibile configurare Element per l'integrazione con un provider di identità SAML 2.0 esistente, in grado di applicare più schemi di autenticazione, ad esempio password e SMS, password e messaggi di posta elettronica o altri metodi.

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

Per configurare MFA, vedere "attiva 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 per le comunicazioni HTTPS e la crittografia del disco.

Quando si attiva la modalità operativa FIPS 140-2 sul cluster, il cluster 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. Si utilizza `EnableFeature` API Element con `fips` Parametro per attivare la crittografia HTTPS FIPS 140-2. Nei cluster di storage con hardware compatibile con FIPS, è anche possibile attivare la crittografia del disco FIPS per i dati inattivi utilizzando `EnableFeature` API Element con `FipsDrives` parametro.

Per ulteriori informazioni sulla preparazione di un nuovo cluster di storage per la crittografia FIPS 140-2, vedere "Creare un cluster che supporti i dischi FIPS".

Per ulteriori informazioni sull'attivazione di FIPS 140-2 su un cluster già esistente, vedere "API dell'elemento EnableFeature".

Per ulteriori informazioni

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

Account e permessi

Per amministrare e fornire l'accesso alle risorse di storage del sistema, è necessario configurare account per le risorse di sistema.

Utilizzando lo storage Element, è possibile creare e gestire i seguenti tipi di account:

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

Account amministratore del cluster di storage

Esistono due tipi di account amministratore in un cluster di storage che esegue il software NetApp Element:

- **Primary cluster Administrator account**: 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 cluster**: È possibile assegnare a un account amministratore 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.

È possibile "gestire gli account degli amministratori del cluster" Creando, eliminando e modificando gli account amministratore del cluster, modificando la password dell'amministratore 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 su 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 è stato creato un volume virtuale, l'account è il container di storage.

Di seguito sono riportate alcune considerazioni aggiuntive:

- L'account contiene l'autenticazione CHAP richiesta 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 Gestione NetApp Element.

Account utente del cluster autorevoli

Gli account utente del cluster autorevoli possono eseguire l'autenticazione con 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 molto altro in tutti i cluster.

Gli account utente autorevoli vengono gestiti dal menu in alto a destra dell'opzione User Management (Gestione utente) in NetApp Hybrid Cloud Control.

Il "cluster di storage 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 al NetApp Hybrid Cloud Control. Gli utenti creati su altri cluster di storage *non possono* accedere a Hybrid Cloud Control.

- Se il nodo di gestione dispone di un solo cluster di storage, si tratta del cluster autorevole.

- Se il nodo di gestione dispone di due o più cluster di storage, uno di questi 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 hanno limitazioni necessarie. Il limite dell'autenticazione e dell'autorizzazione è che gli utenti del cluster autorevole possono eseguire azioni su altri cluster legati 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 storage, è necessario assicurarsi che gli utenti definiti nei cluster autorevoli siano definiti in tutti gli altri cluster di storage con le stesse autorizzazioni. Puoi gestire gli utenti da NetApp Hybrid Cloud Control.

Account di volume

Gli account specifici del volume sono specifici solo per il cluster di storage in cui sono stati creati. Questi account consentono di impostare autorizzazioni su volumi specifici della 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.

Storage

Volumi

Il sistema storage NetApp Element 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.

Lo storage degli elementi consente di creare, visualizzare, modificare, eliminare, clonare, backup o ripristino dei volumi per gli account utente. È inoltre possibile gestire ciascun volume di un cluster e aggiungere o rimuovere volumi in gruppi di accesso ai volumi.

Volumi persistenti

I volumi persistenti consentono ai dati di configurazione dei nodi di gestione di essere memorizzati in un cluster di storage specifico, piuttosto che localmente con una macchina virtuale, in modo che i dati possano essere conservati in caso di perdita o rimozione dei nodi di gestione. I volumi persistenti sono una configurazione del nodo di gestione opzionale ma consigliata.

Un'opzione per abilitare i volumi persistenti è inclusa negli script di installazione e aggiornamento quando "implementazione di un nuovo nodo di gestione". I volumi persistenti sono volumi su un cluster di storage basato su software Element che contengono informazioni di configurazione del nodo di gestione per la VM del nodo di gestione host che persistono oltre la vita della macchina virtuale. In caso di perdita del nodo di gestione, una macchina virtuale del nodo di gestione sostitutivo può riconnettersi e ripristinare i dati di configurazione per la macchina virtuale persa.

La funzionalità dei volumi persistenti, se attivata durante l'installazione o l'aggiornamento, crea automaticamente più volumi. Questi volumi, come qualsiasi volume basato su software Element, possono essere visualizzati utilizzando 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 in esecuzione 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 (vVol)

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 Virtual Volumes (vVol), è possibile allocare lo storage in base ai requisiti delle singole macchine virtuali.

Associazioni

Il cluster NetApp Element 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.

Endpoint del protocollo

Gli host VMware ESXi utilizzano proxy i/o logici noti come endpoint del protocollo per comunicare con i volumi virtuali. Gli host ESXi collegano i 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 con 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 del protocollo corrispondente. Ad esempio, un cluster a quattro nodi avrà quattro endpoint di protocollo.

ISCSI è l'unico protocollo supportato per il software NetApp Element. Il protocollo Fibre Channel non è supportato. 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.

Container di storage

I container di storage sono costrutti logici che vengono mappati agli account NetApp Element e utilizzati per la creazione di report e l'allocazione delle risorse. Raggruppano capacità di storage raw o capacità di storage aggregate che il sistema di storage può fornire ai volumi virtuali. Un datastore VVol creato in vSphere viene mappato a un singolo container di storage. Per impostazione predefinita, un singolo container di storage 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 container di storage.

I container di storage funzionano come gli account tradizionali e possono contenere volumi virtuali e volumi tradizionali. È supportato un massimo di quattro container di storage per cluster. Per utilizzare la funzionalità VVol, è necessario almeno un container di storage. È possibile rilevare i container di storage in vCenter durante la creazione di VVol.

Provider VASA

Per rendere vSphere consapevole 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 out-of-band tra vSphere e il cluster di elementi. È responsabile dell'esecuzione delle richieste sul cluster Element per conto di vSphere, come la creazione di macchine virtuali, la messa a disposizione di

vSphere delle macchine virtuali e la pubblicità delle funzionalità di storage su vSphere.

Il provider VASA viene eseguito come parte del cluster master nel software Element. Il cluster master è un servizio altamente disponibile che esegue il failover su qualsiasi nodo del cluster in base alle necessità. In caso di failover del cluster master, il provider VASA si sposta con esso, garantendo un'elevata disponibilità per il provider VASA. Tutte le attività di provisioning e gestione dello storage utilizzano il provider VASA, che gestisce le modifiche necessarie al cluster di elementi.

> Per Element 12,5 e versioni precedenti, non registrare più di un provider NetApp Element VASA su una singola istanza vCenter. Quando viene aggiunto un secondo provider VASA NetApp Element, questo rende inaccessibili tutti i datastore VVOL.

> Il supporto DI VASA per un massimo di 10 vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con vCenter. Per eseguire l'installazione, seguire le istruzioni nel manifest VASA39 e scaricare il file .tar.gz da "Download di software NetApp" sito. 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

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

Gruppi di accesso ai volumi

Creando e utilizzando i gruppi di accesso ai volumi, è possibile controllare l'accesso a un set di volumi. Quando si associano un set di volumi e un set di iniziatori a un gruppo di accesso al volume, il gruppo di accesso concede agli iniziatori l'accesso a tale set di volumi.

I gruppi di accesso ai volumi nello storage NetApp SolidFire consentono agli IQN iSCSI Initiator o alle 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 di rete Fibre Channel ai volumi del gruppo di accesso.

I gruppi di accesso ai volumi hanno i seguenti limiti:

- Un massimo di 128 iniziatori per gruppo di accesso al volume.
- Un massimo di 64 gruppi di accesso per volume.
- 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 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 di un cluster, fungendo da punto di ingresso per la comunicazione tra client e volumi. È possibile utilizzare gli iniziatori per l'accesso ai volumi di storage basato su CHAP piuttosto che su account. Un

singolo iniziatore, quando aggiunto a un gruppo di accesso al volume, consente ai membri del gruppo di accesso al volume di accedere a tutti i volumi di storage 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, cloning dei volumi, domini di protezione e alta disponibilità con la tecnologia Double Helix.

La protezione dei dati dello storage Element include i seguenti concetti:

- Tipi di replica remota
- Snapshot dei volumi per la protezione dei dati
- Cloni di volume
- Panoramica del processo di backup e ripristino per lo storage Element
- Domini di protezione
- Domini di protezione personalizzati
- Doppia Helix ad alta disponibilità

Tipi di replica 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 utilizzando SnapMirror

Per ulteriori 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 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.

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 appropriata per le seguenti situazioni:

- Replica di diversi sistemi su una breve distanza

- Un sito di disaster recovery geograficamente locale rispetto all'origine
- Applicazioni sensibili al tempo e protezione dei database
- Applicazioni di business continuity 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 i riconoscimenti dal cluster di destinazione. Durante la replica asincrona, le scritture vengono riconosciute al client (applicazione) dopo che sono state assegnate al cluster di origine.

La replica asincrona è appropriata per le seguenti situazioni:

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

Replica solo Snapshot

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.

È possibile impostare la frequenza delle repliche degli snapshot.

La replica di Snapshot non influisce sulla replica asincrona o sincrona.

Replica tra cluster Element e ONTAP utilizzando SnapMirror

Con la tecnologia NetApp SnapMirror, è possibile replicare le snapshot acquisite con 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 replica Snapshot di 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 mirroring, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di interruzione nel sito primario. I dati vengono mirrorati a livello di volume.

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita 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 trasmessi in peering. Una relazione peer consente a cluster e 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 di controllo di SnapMirror risiede nel software ONTAP; pertanto, tutte le relazioni di SnapMirror devono coinvolgere almeno un sistema ONTAP per eseguire il lavoro di coordinamento. Gli utenti gestiscono le relazioni tra i cluster Element e ONTAP principalmente attraverso l'interfaccia utente Element; tuttavia, alcune attività di gestione risiedono in Gestione di sistema NetApp ONTAP. Gli utenti possono inoltre gestire SnapMirror tramite l'interfaccia CLI e l'API, entrambe disponibili in ONTAP ed Element.

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

È necessario attivare manualmente la funzionalità SnapMirror a livello di cluster utilizzando il software Element. La funzionalità SnapMirror è disattivata per impostazione predefinita e non viene attivata

automaticamente durante una nuova installazione o un aggiornamento.

Dopo aver attivato SnapMirror, è possibile creare relazioni SnapMirror dalla scheda Data Protection (protezione dati) del software Element.

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

I sistemi che eseguono Element 10.1 e versioni successive includono codice in grado di comunicare direttamente con SnapMirror su sistemi ONTAP con versione 9.3 o superiore. 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 di 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 da ONTAP in volumi di elementi in casi di utilizzo specifici con funzionalità limitate.

Per ulteriori informazioni, consultare la documentazione di ONTAP.

Snapshot dei volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume che può essere utilizzata in seguito per ripristinare un volume all'ora specifica.

Sebbene le snapshot siano simili ai cloni dei volumi, le snapshot sono semplicemente repliche dei metadati dei volumi, 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 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; è inoltre possibile creare un clone di un volume da uno snapshot replicato.

È possibile eseguire il backup delle snapshot da un cluster di elementi a un archivio di oggetti esterno o a un altro cluster di elementi. 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.

È possibile creare un'istantanea di uno o più volumi per la protezione dei dati.

Cloni di volume

Un clone di uno o più volumi è 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.

Panoramica del processo di backup e ripristino per lo storage Element

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 nei seguenti modi:

- Un cluster di storage SolidFire
- Un archivio di oggetti Amazon S3
- Un archivio di oggetti 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.

Domini di protezione

Un dominio di protezione è un nodo o un insieme di nodi raggruppati in modo che qualsiasi parte o anche tutto l'IT possa guastarsi, mantenendo al contempo la disponibilità dei dati. I domini di protezione consentono a un cluster di storage di riparare automaticamente in caso di perdita di uno chassis (affinità dello chassis) o di un intero dominio (gruppo di chassis).

È possibile attivare manualmente il monitoraggio del dominio di protezione utilizzando il punto di estensione Configurazione NetApp Element nel plug-in NetApp Element per vCenter Server. È possibile selezionare una soglia del dominio di protezione in base ai domini del nodo o dello chassis. È inoltre possibile attivare il monitoraggio del dominio di protezione utilizzando l'API Element o l'interfaccia utente Web.

Un layout del dominio di protezione assegna ogni nodo a un dominio di protezione specifico.

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

- A livello di nodo, ciascun 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 ciascun nodo si trova in uno chassis separato, questi due livelli sono funzionalmente identici.

Quando si crea un nuovo cluster, se si utilizzano nodi di storage che risiedono in uno chassis condiviso, si consiglia di progettare la protezione dai guasti a livello di chassis utilizzando la funzione Protection Domains.

Domini di protezione personalizzati

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

Se non sono assegnati domini di protezione personalizzati:

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

Quando si configurano i domini di protezione personalizzati per un cluster, sono disponibili tre livelli di protezione, visibili dalla dashboard dell'interfaccia utente Web Element:

- Non protetto: Il cluster di storage non è protetto dal guasto di uno dei suoi domini di protezione

personalizzati. Per risolvere questo problema, aggiungere ulteriore capacità di storage al cluster o riconfigurare i domini di protezione personalizzati del cluster per proteggere il cluster da eventuali perdite di dati.

- Tolleranza agli errori: Il cluster di storage dispone di capacità libera sufficiente per evitare la perdita di dati dopo il guasto di uno dei suoi domini di protezione personalizzati.
- Fault Resilient (resiliente agli errori): Il cluster di storage dispone di capacità libera sufficiente per eseguire la riparazione automatica dopo il guasto di uno dei domini di protezione personalizzati. Una volta completato il processo di riparazione, 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 assegna i duplicati a domini di protezione personalizzati separati. Se ciò non è possibile, viene ripristinata l'assegnazione di duplicati a nodi separati. Ogni sottosistema (ad esempio, bin, slice, provider di endpoint del protocollo e gruppo) esegue questa operazione in modo indipendente.

È possibile utilizzare l'interfaccia utente di Element per "Configurare i domini di protezione personalizzati"Oppure è possibile utilizzare i seguenti metodi API:

- "GetProtectionDomainLayout" - Indica lo chassis e il dominio di protezione personalizzato in cui si trova ciascun nodo.
- "SetProtectionDomainLayout" Consente di assegnare un dominio di protezione personalizzato a ciascun nodo.

Doppia Helix ad alta disponibilità

La protezione dei dati Double Helix è un metodo di replica che distribuisce almeno due copie ridondanti dei dati su tutti i dischi all'interno di un sistema. L'approccio "RAID-less" consente a un sistema di assorbire più guasti simultanei in tutti i livelli del sistema storage e di ripararli rapidamente.

Performance e qualità del servizio

Un cluster di storage SolidFire è in grado di fornire parametri di qualità del servizio (QoS) per volume. È possibile garantire le prestazioni del cluster misurate in input e output al secondo (IOPS) utilizzando tre parametri configurabili che definiscono QoS: IOPS min, IOPS max e IOPS burst.

> SolidFire Active IQ dispone di una pagina di consigli sulla qualità del servizio che fornisce consigli sulla configurazione ottimale e sull'impostazione delle impostazioni di qualità del servizio.

Parametri della qualità del servizio

I parametri IOPS sono definiti nei seguenti modi:

- **IOPS minimo** - il numero minimo di IOPS (Inputs and Outputs per Second) sostenuti che il cluster di storage fornisce a un volume. Il livello minimo di IOPS configurato per un volume è il livello garantito di performance per un volume. Le performance non scendono al di sotto di questo livello.
- **Massimo IOPS** - il numero massimo di IOPS sostenuti che il cluster di storage fornisce a un volume. Quando i livelli di IOPS del cluster sono estremamente elevati, questo livello di performance IOPS non viene superato.

- **Burst IOPS** - numero massimo di IOPS consentiti in uno scenario a burst breve. Se un volume è stato eseguito al di sotto del massimo IOPS, i crediti burst vengono accumulati. Quando i livelli di performance diventano molto elevati e vengono trasferiti ai livelli massimi, sono consentiti brevi burst di IOPS sul volume.

  Il software Element utilizza gli IOPS Burst quando un cluster viene eseguito in uno stato di basso utilizzo degli IOPS del cluster.

  Un singolo volume può accumulare IOPS burst e utilizzare i crediti per ottenere un burst oltre i massimi IOPS fino al livello di IOPS burst per un "periodo di burst" impostato. Un volume può esplodere fino a 60 secondi se il cluster ha la capacità di ospitare il burst. Un volume aumenta di un secondo di credito burst (fino a un massimo di 60 secondi) per ogni secondo in cui il volume scende al di sotto del limite massimo di IOPS.

  Gli IOPS burst sono limitati in due modi:

  - Un volume può raggiungere un picco superiore al massimo IOPS per un numero di secondi pari al numero di crediti burst accumulati dal volume.
  - Quando un volume supera l'impostazione di massimo IOPS, è limitato dall'impostazione di burst IOPS. Pertanto, gli IOPS burst non superano mai l'impostazione di IOPS burst 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 di io.

  Esempio: Le impostazioni dei parametri QoS di 100 IOPS min, 1000 IOPS max e 1500 IOPS burst hanno i seguenti effetti sulla qualità delle performance:

  - I carichi di lavoro sono in grado di raggiungere e sostenere un massimo di 1000 IOPS fino a quando la condizione di conflitto del carico di lavoro per gli IOPS non diventa evidente nel cluster. Gli IOPS vengono quindi ridotti in modo incrementale fino a quando gli IOPS su tutti i volumi non rientrano negli intervalli di QoS designati e il conflitto per le performance viene ridotto.
  - Le performance su tutti i volumi vengono trasferite al minimo IOPS di 100. I livelli non scendono al di sotto dell'impostazione min IOPS, ma potrebbero rimanere superiori a 100 IOPS quando il conflitto del carico di lavoro viene sollevato.
  - Le performance non sono mai superiori a 1000 IOPS o inferiori a 100 IOPS per un periodo prolungato. Sono consentite performance di 1500 IOPS (burst IOPS), ma solo per quei volumi che hanno accumulato crediti burst con un'esecuzione inferiore al massimo di IOPS e sono consentiti 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 KB	5 8 KB	6 16KB	262 KB
IOPS minimi	50	50	15.000	9,375*	5556*	385*
IOPS max	100	15.000	200,000**	125.000	74.074	5128
IOPS burst	100	15.000	200,000**	125.000	74,074	5128

*Queste stime sono approssimative.
**È possibile impostare IOPS massimi e IOPS burst fino a 200,000; tuttavia, questa impostazione consente

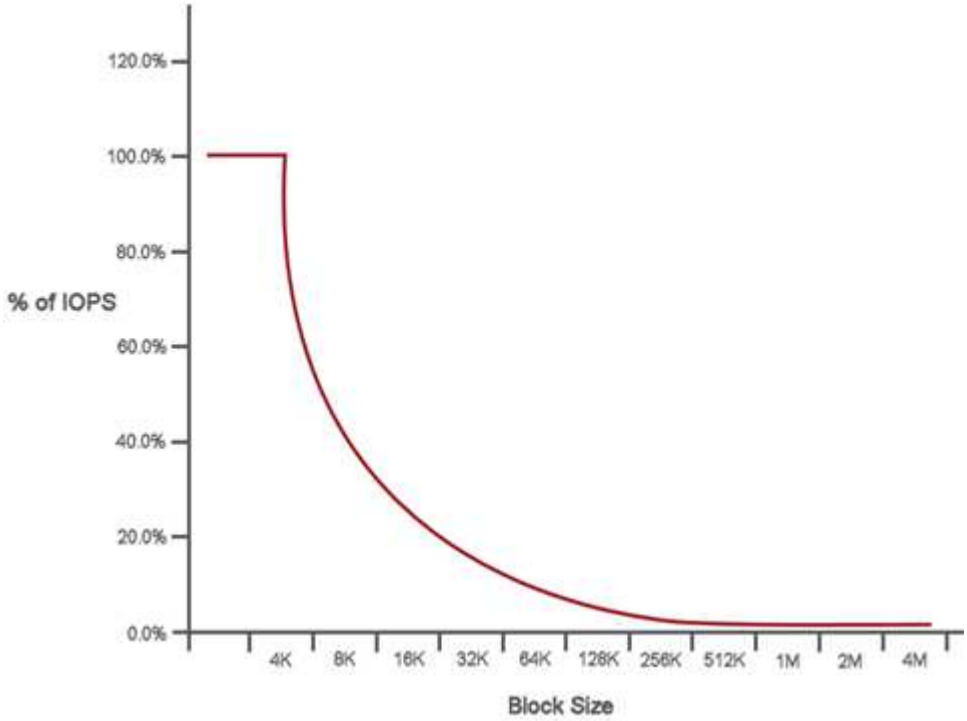
solo di rimuovere efficacemente le prestazioni di un volume. Le performance massime reali di un volume sono limitate dall'utilizzo del cluster e dalle performance per nodo.

Performance QoS

La curva delle performance 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 ricevuti normalizzando le dimensioni dei blocchi 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 a raggiungere un livello necessario per elaborare blocchi di dimensioni maggiori. Man mano che la larghezza di banda aumenta il numero di IOPS, il sistema è in grado di raggiungere una diminuzione.

La curva delle performance di 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 fino a 8k, la larghezza di banda aumenta fino a 5000 kbps e gli IOPS diminuiscono fino a 625. Tenendo conto delle dimensioni dei blocchi, il sistema garantisce che i carichi di lavoro con priorità più bassa che utilizzano blocchi di dimensioni più elevate, come backup e attività dell'hypervisor, non richiedano una quantità eccessiva delle performance richieste dal traffico con priorità più alta utilizzando blocchi di dimensioni più piccole.

Policy di QoS

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

Le policy di QoS sono le migliori per gli ambienti di servizio, ad esempio con database, applicazioni o server di infrastruttura che raramente si riavviano e necessitano di un accesso costante e uguale allo storage. La qualità del servizio dei singoli volumi è la soluzione migliore per le macchine virtuali di uso leggero, come desktop

virtuali o macchine virtuali specializzate di tipo Kiosk, che possono essere riavviate, accese o spente ogni giorno o più volte al giorno.

Le policy QoS e QoS non devono essere utilizzate insieme. 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.

> Il cluster selezionato deve essere l'elemento 10.0 o successivo per utilizzare i criteri QoS; in caso contrario, le funzioni dei criteri QoS non sono disponibili.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"