Concetti

NetApp HCI

NetApp
June 25, 2025

This PDF was generated from https://docs.netapp.com/it-it/hci19/docs/concept_hci_product_overview.html on June 25, 2025. Always check docs.netapp.com for the latest.

Sommario

Concetti . . . 1
- Panoramica del prodotto NetApp HCI . . . 1
  - Componenti di NetApp HCI . . . 1
  - URL NetApp HCI . . . 2
- Account utente . . . 2
  - Gestione dell'account utente . . . 2
  - Account amministratore del cluster di storage . . . 3
  - Account utente autorevoli . . . 3
  - Account di volume . . . 4
  - Trova ulteriori informazioni . . . 4
- Protezione dei dati . . . 4
  - Tipi di replica remota . . . 4
  - Snapshot dei volumi per la protezione dei dati . . . 6
  - Cloni di volume . . . 6
  - Panoramica del processo di backup e ripristino per lo storage SolidFire . . . 7
  - Domini di protezione . . . 7
  - Doppia Helix ad alta disponibilità . . . 7
  - Trova ulteriori informazioni . . . 8
- Cluster . . . 8
  - Cluster di storage autorevoli . . . 8
  - Capacità inutilizzata . . . 8
  - Cluster di storage a due nodi . . . 9
  - Cluster di storage con tre o più nodi . . . 10
  - Trova ulteriori informazioni . . . 10
- Nodi . . . 10
  - Nodo di gestione . . . 10
  - Nodi di storage . . . 11
  - Nodi di calcolo . . . 11
  - Nodi di controllo . . . 11
  - Trova ulteriori informazioni . . . 11
- Storage . . . 12
  - Modalità di manutenzione . . . 12
  - Volumi . . . 13
  - Gruppi di accesso ai volumi . . . 14
  - Iniziatori . . . 14
  - Domini di protezione personalizzati . . . 14
- Licenze NetApp HCI . . . 15
  - Licenze NetApp HCI e VMware vSphere . . . 15
  - Licenze NetApp HCI e ONTAP Select . . . 16
  - Trova ulteriori informazioni . . . 16
- Configurazioni massime di NetApp Hybrid Cloud Control . . . 16
- Sicurezza NetApp HCI . . . 16
  - Crittografia a riposo per i nodi di storage . . . 16

Crittografia software a riposo . . . 17
Gestione esterna delle chiavi . . . 17
Autenticazione a più fattori . . . 17
FIPS 140-2 per HTTPS e crittografia dei dati a riposo . . . 18
Performance e Quality of Service . . . 18
Parametri della qualità del servizio . . . 18
Limiti del valore QoS . . . 19
Performance QoS . . . 19
Policy di QoS . . . 20

Concetti

Panoramica del prodotto NetApp HCI

NetApp HCI è un'infrastruttura di cloud ibrido di livello Enterprise che combina storage, calcolo, networking e hypervisor e aggiunge funzionalità che abbracciano cloud pubblici e privati.

L'infrastruttura di cloud ibrido disaggregato di NetApp consente una scalabilità indipendente di calcolo e storage, adattandosi ai carichi di lavoro con performance garantite.

- Soddisfa la domanda di multicloud ibrido
- Scalabilità indipendente di calcolo e storage
- Semplifica l'orchestrazione dei servizi dati nei multicloud ibridi

Componenti di NetApp HCI

Ecco una panoramica dei vari componenti dell'ambiente NetApp HCI:

- NetApp HCI offre risorse di storage e di calcolo. Utilizza la procedura guidata **motore di implementazione NetApp** per implementare NetApp HCI. Una volta completata l'implementazione, i nodi di calcolo vengono visualizzati come host ESXi ed è possibile gestirli in VMware vSphere Web Client.
- **I servizi di gestione** o i microservizi includono Active IQ Collector, QoSSIOC per il plug-in vCenter e il servizio mNode; vengono aggiornati frequentemente come bundle di servizi. A partire dalla release Element 11.3, i **servizi di gestione** sono ospitati sul nodo di gestione, consentendo aggiornamenti più rapidi dei servizi software selezionati al di fuori delle release principali. 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.

  Scopri di più "release di servizi di gestione".

- **NetApp Hybrid Cloud Control** ti consente di gestire NetApp HCI. Con NetApp SolidFire Active IQ è possibile aggiornare i servizi di gestione, espandere il sistema, raccogliere i registri e monitorare l'installazione. Per accedere a NetApp Hybrid Cloud Control, accedere all'indirizzo IP del nodo di gestione.
- Il plug-in **NetApp Element per vCenter Server** è un tool basato sul web integrato con l'interfaccia utente vSphere. Il plug-in è un'estensione e un'interfaccia intuitiva e scalabile per VMware vSphere, in grado di gestire e monitorare cluster di storage che eseguono il software **NetApp Element**. Il plug-in fornisce un'alternativa all'interfaccia utente di Element. È possibile utilizzare l'interfaccia utente del plug-in per rilevare e configurare i cluster e gestire, monitorare e allocare lo storage dalla capacità del cluster per configurare datastore e datastore virtuali (per volumi virtuali). Un cluster viene visualizzato sulla rete come un singolo gruppo locale rappresentato agli host e agli amministratori da indirizzi IP virtuali. È inoltre possibile monitorare l'attività del cluster con report in tempo reale, inclusi messaggi di errore e di avviso per qualsiasi evento che potrebbe verificarsi durante l'esecuzione di varie operazioni.

  Scopri di più "Plug-in NetApp Element per server vCenter".

- Per impostazione predefinita, NetApp HCI invia le statistiche relative alle performance e agli avvisi al servizio **NetApp SolidFire Active IQ**. Come parte del tuo normale contratto di supporto, il supporto NetApp monitora questi dati e ti avvisa in caso di colli di bottiglia delle performance o potenziali problemi di sistema. Se non si dispone già di un account per il supporto NetApp (anche se si dispone di un account SolidFire Active IQ esistente), è necessario creare un account per poter usufruire di questo servizio.

Scopri di più "NetApp SolidFire Active IQ".

URL NetApp HCI

Di seguito sono riportati gli URL comuni utilizzati con NetApp HCI:

URL	Descrizione
`https://[IPv4 address of Bond1G interface on a storage node]`	Accedere alla procedura guidata del motore di implementazione NetApp per installare e configurare NetApp HCI. "Scopri di più."
<code><a href="https://<ManagementNodeIP&gt" class="bare">https://<ManagementNodeIP&gt; </code>	Accedi a NetApp Hybrid Cloud Control per aggiornare, espandere e monitorare l'installazione di NetApp HCI e aggiornare i servizi di gestione. "Scopri di più."
`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]:9443`	Registrare il pacchetto vCenter Plug-in in vSphere Web Client.
`https://activeiq.solidfire.com`	Monitorare i dati e ricevere avvisi in caso di colli di bottiglia delle performance o potenziali problemi del sistema.
`https://<ManagementNodeIP>/mnode`	Aggiornare manualmente i servizi di gestione utilizzando l'interfaccia utente REST API dal nodo di gestione.
`https://[storage cluster MVIP address]`	Accedere all'interfaccia utente del software NetApp Element.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Account utente

Per accedere alle risorse di storage del sistema, è necessario configurare gli account utente.

Gestione dell'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.

Utilizzando NetApp Hybrid Cloud Control, puoi creare e gestire i seguenti tipi di account:

- Account utente amministratore per il cluster di storage
- Account utente autorevoli
- Account di volumi specifici solo per il cluster di storage in cui sono stati creati.

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 degli amministratori 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 autorevoli

Gli account utente autorevoli possono autenticare qualsiasi risorsa storage associata all'istanza di nodi e cluster di NetApp Hybrid Cloud Control. 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.

Trova ulteriori informazioni

- "Gestire gli account utente"
- "Scopri di più sui cluster"
- "Plug-in NetApp Element per server vCenter"

Protezione dei dati

I termini di protezione dei dati di NetApp HCI includono diversi tipi di replica remota, snapshot dei volumi, cloning dei volumi, domini di protezione e alta disponibilità con la tecnologia Double Helix.

La protezione dei dati di NetApp HCI 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 SolidFire
- Domini di protezione
- 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

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 NetApp Snapshot™ 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.

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

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 SolidFire

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).

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

Sono supportati due diversi layout dei domini 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.

Puoi farlo manualmente "abilitare il monitoraggio del dominio di protezione" Utilizzo del 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.

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 dei domini di protezione.

È possibile definire un layout personalizzato del dominio di protezione, 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.

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.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"

Cluster

Un cluster è un gruppo di nodi, che funzionano come un insieme collettivo, che forniscono risorse di storage o di calcolo. A partire da NetApp HCI 1.8, è possibile disporre di un cluster di storage con due nodi. Un cluster di storage viene visualizzato sulla rete come un singolo gruppo logico ed è quindi possibile accedervi come storage a blocchi.

Il livello di storage in NetApp HCI è fornito dal software NetApp Element e il livello di gestione è fornito dal plug-in NetApp Element per vCenter Server. Un nodo di storage è un server che contiene una raccolta di dischi che comunicano tra loro attraverso l'interfaccia di rete Bond10G. Ciascun nodo di storage 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.

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.

Puoi gestire gli utenti con NetApp Hybrid Cloud Control.

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

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.

Cluster di storage a due nodi

A partire da NetApp HCI 1.8, è possibile configurare un cluster di storage con due nodi di storage.

- È possibile utilizzare alcuni tipi di nodi per formare il cluster di storage a due nodi. Vedere "Note sulla versione di NetApp HCI 1.8".

  In un cluster a due nodi, i nodi di storage sono limitati a nodi con dischi da 480 GB e 960 GB e i nodi devono essere dello stesso tipo di modello.

- I cluster di storage a due nodi sono ideali per implementazioni su piccola scala con carichi di lavoro che non dipendono da requisiti di capacità elevata e performance elevate.
- Oltre a due nodi di storage, un cluster di storage a due nodi include anche due **nodi di controllo NetApp HCI**.

  Scopri di più "Nodi di controllo."

- È possibile scalare un cluster di storage a due nodi in un cluster di storage a tre nodi. I cluster a tre nodi aumentano la resilienza offrendo la possibilità di eseguire il ripristino automatico in caso di guasti ai nodi di storage.
- I cluster di storage a due nodi offrono le stesse funzionalità e caratteristiche di sicurezza dei tradizionali cluster di storage a quattro nodi.
- I cluster di storage a due nodi utilizzano le stesse reti dei cluster di storage a quattro nodi. Le reti vengono configurate durante l'implementazione di NetApp HCI utilizzando la procedura guidata del motore di implementazione NetApp.

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. I nodi di controllo in un cluster a due nodi vengono utilizzati per garantire che vi sia un numero di nodi di storage sufficiente per formare un quorum di ensemble valido. Per la creazione dell'ensemble, i nodi di storage sono preferiti rispetto ai nodi di controllo. Per l'insieme minimo di tre nodi che coinvolge un cluster di storage a due nodi, vengono utilizzati due nodi di storage e un nodo di controllo.

In un insieme a tre nodi con due nodi di storage e un nodo di controllo, se un nodo di storage passa offline, il cluster passa in uno stato degradato. Dei due nodi di controllo, solo uno può essere attivo nell'insieme. Il secondo nodo di controllo non può essere aggiunto all'insieme, perché esegue il ruolo di backup. Il cluster rimane in stato degradato fino a quando il nodo di storage offline non ritorna in stato online o un nodo sostitutivo non si unisce al cluster.

Se un nodo di controllo non riesce, il nodo di controllo rimanente si unisce all'ensemble per formare un ensemble a tre nodi. È possibile implementare un nuovo nodo di controllo per sostituire il nodo di controllo non riuscito.

Riparazione automatica e gestione degli errori in cluster di storage a due nodi

Se un componente hardware si guasta in un nodo che fa parte di un cluster tradizionale, il cluster può ribilanciare i dati che si trovavano sul componente che non riusciva ad altri nodi disponibili nel cluster. Questa capacità di risanare automaticamente non è disponibile in un cluster di storage a due nodi, perché un minimo di tre nodi di storage fisici deve essere disponibile per il cluster per la riparazione automatica. Quando un nodo di un cluster a due nodi si guasta, il cluster a due nodi non richiede la rigenerazione di una seconda copia dei dati. Le nuove scritture vengono replicate per i dati del blocco nel nodo di storage attivo rimanente. Quando il nodo guasto viene sostituito e si unisce al cluster, i dati vengono ribilanciati tra i due nodi di storage fisici.

Cluster di storage con tre o più nodi

L'espansione da due nodi di storage a tre nodi di storage rende il cluster più resiliente consentendo la riparazione automatica in caso di guasti al nodo e al disco, ma non fornisce capacità aggiuntiva. È possibile espandere utilizzando "Interfaccia utente di NetApp Hybrid Cloud Control". Quando si esegue l'espansione da un cluster a due nodi a un cluster a tre nodi, la capacità può essere bloccata (vedere Capacità inutilizzata). La procedura guidata dell'interfaccia utente mostra avvisi relativi alla capacità inutilizzata prima dell'installazione. Un singolo nodo di controllo è ancora disponibile per mantenere il quorum dell'ensemble in caso di guasto di un nodo di storage, con un secondo nodo di controllo in standby. Quando si espande un cluster di storage a tre nodi in un cluster a quattro nodi, la capacità e le performance aumentano. In un cluster a quattro nodi, i nodi di controllo non sono più necessari per formare il quorum del cluster. Puoi espandere fino a 64 nodi di calcolo e 40 nodi di storage.

Trova ulteriori informazioni

- "Cluster di storage a due nodi NetApp HCI | TR-4823"
- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

Nodi

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

NetApp HCI e il software Element definiscono diversi ruoli di nodo per un cluster. I quattro tipi di ruoli dei nodi sono **nodo di gestione**, **nodo di storage**, **nodo di calcolo** e **nodi di controllo NetApp HCI**.

Nodo di gestione

Il nodo di gestione (talvolta abbreviato come mNode) interagisce con un cluster di storage per eseguire azioni di gestione, ma non fa parte 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.

Il nodo di gestione è una macchina virtuale (VM) che viene eseguita in parallelo con uno o più cluster di storage basati su software Element. Oltre agli aggiornamenti, viene utilizzato per fornire servizi di sistema come 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. 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, come Active IQ Collector, QoSSIOC per il plug-in vCenter e il servizio del nodo di gestione, vengono aggiornati frequentemente come bundle di servizi.

Nodi di storage

I nodi di storage NetApp HCI sono hardware che forniscono le risorse di storage per un sistema NetApp HCI. 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 NetApp HCI possono essere gestiti utilizzando il punto di estensione per la gestione NetApp Element.

Nodi di calcolo

I nodi di calcolo NetApp HCI sono hardware che fornisce risorse di calcolo, come CPU, memoria e rete, necessarie per la virtualizzazione nell'installazione di NetApp HCI. Poiché ogni server esegue VMware ESXi, la gestione dei nodi di calcolo NetApp HCI (aggiunta o rimozione di host) deve essere eseguita al di fuori del plug-in all'interno del menu host e cluster di vSphere. Indipendentemente dal fatto che si tratti di un cluster di storage a quattro nodi o di un cluster di storage a due nodi, il numero minimo di nodi di calcolo rimane due per un'implementazione NetApp HCI.

Nodi di controllo

I nodi di controllo NetApp HCI sono macchine virtuali eseguite su nodi di calcolo in parallelo con un cluster di storage basato su software Element. I nodi di controllo non ospitano servizi di sezioni o blocchi. Un nodo di controllo abilita la disponibilità del cluster di storage in caso di guasto di un nodo di storage. È possibile gestire e aggiornare i nodi di controllo allo stesso modo degli altri nodi di storage. Un cluster di storage può avere fino a quattro nodi di controllo. Il loro scopo principale è quello di garantire che esista un numero sufficiente di nodi del cluster per formare un quorum di ensemble valido.

Best practice: configurare le macchine virtuali del nodo di controllo per utilizzare il datastore locale del nodo di calcolo (impostazione predefinita NDE), non configurarle sullo storage condiviso, ad esempio i volumi di storage SolidFire. Per impedire la migrazione automatica delle macchine virtuali, impostare il livello di automazione DRS (Distributed Resource Scheduler) della macchina virtuale del nodo di controllo su **Disabled**. Ciò impedisce l'esecuzione di entrambi i nodi di controllo sullo stesso nodo di calcolo e la creazione di una configurazione di coppia non ad alta disponibilità (ha).

Scopri di più "Requisiti di risorse del nodo di controllo" e. "Requisiti dell'indirizzo IP del nodo di controllo".

In un cluster di storage a due nodi, vengono implementati almeno due nodi di controllo per la ridondanza in caso di guasto di un nodo di controllo. Quando il processo di installazione di NetApp HCI installa i nodi di controllo, in VMware vCenter viene memorizzato un modello di macchina virtuale che è possibile utilizzare per ridistribuire un nodo di controllo nel caso in cui venga accidentalmente rimosso, perso o danneggiato. È inoltre possibile utilizzare il modello per ridistribuire un nodo di controllo se è necessario sostituire un nodo di calcolo guasto che ospitava il nodo di controllo. Per istruzioni, vedere la sezione **ridistribuire i nodi di controllo per cluster di storage a due e tre nodi** "qui".

Trova ulteriori informazioni

- "Cluster di storage a due nodi NetApp HCI | TR-4823"
- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

Storage

Modalità di manutenzione

Se è necessario disattivare un nodo di storage per la manutenzione, ad esempio aggiornamenti software o riparazioni host, è possibile ridurre al minimo l'impatto i/o sul resto del cluster di storage attivando la modalità di manutenzione per tale nodo. È possibile utilizzare la modalità di manutenzione sia con i nodi appliance che con i nodi SDS aziendali SolidFire.

Quando un nodo di storage viene spento, viene visualizzato come **non disponibile** nella colonna Node Status (Stato nodo) della pagina Storage (archiviazione) in HCC, poiché questa colonna visualizza lo stato del nodo dal punto di vista del cluster. Lo stato di disattivazione del nodo è indicato dall'icona **Offline** accanto al nome host del nodo.

È possibile passare da un nodo di storage alla modalità di manutenzione solo se il nodo è integro (non presenta errori di blocco del cluster) e se il cluster di storage è tollerante a un guasto di un singolo nodo. Una volta attivata la modalità di manutenzione per un nodo integro e tollerante, il nodo non viene immediatamente sottoposto a transizione; viene monitorato fino a quando non si verificano le seguenti condizioni:

- Tutti i volumi ospitati sul nodo hanno eseguito il failover
- Il nodo non è più in hosting come principale per qualsiasi volume
- Viene assegnato un nodo di standby temporaneo per ogni volume sottoposto a failover

Una volta soddisfatti questi criteri, il nodo passa alla modalità di manutenzione. Se questi criteri non vengono soddisfatti entro 5 minuti, il nodo non entra in modalità di manutenzione.

Quando si disattiva la modalità di manutenzione per un nodo di storage, il nodo viene monitorato fino a quando non si verificano le seguenti condizioni:

- Tutti i dati vengono replicati completamente nel nodo
- Tutti i guasti del cluster di blocco sono stati risolti
- Tutte le assegnazioni temporanee dei nodi di standby per i volumi ospitati sul nodo sono state disattivate

Una volta soddisfatti questi criteri, il nodo esce dalla modalità di manutenzione. Se questi criteri non vengono soddisfatti entro un'ora, il nodo non riuscirà a uscire dalla modalità di manutenzione.

È possibile visualizzare gli stati delle operazioni della modalità di manutenzione quando si lavora con la modalità di manutenzione utilizzando l'API Element:

- **Disabled**: Non è stata richiesta alcuna manutenzione.
- **FailedToRecover**: Il nodo non è riuscito a ripristinare la manutenzione.
- **RecoveringFromMaintenance**: Il nodo è in fase di ripristino dalla manutenzione.
- **PreparingForMaintenance**: Vengono intraprese azioni per consentire a un nodo di eseguire la manutenzione.
- **ReadyForMaintenance**: Il nodo è pronto per la manutenzione.

Trova ulteriori informazioni

- "Abilitare la modalità di manutenzione con l'API Element"
- "Disattivare la modalità di manutenzione con l'API Element"
- "Documentazione API NetApp Element"
- "Plug-in NetApp Element per server vCenter"

Volumi

Il provisioning dello storage viene eseguito nel sistema NetApp Element come volumi. I volumi sono dispositivi a blocchi a cui si accede in rete utilizzando client iSCSI o Fibre Channel.

Il plug-in NetApp Element per vCenter Server 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.

Se si implementa un nodo di gestione per NetApp HCI utilizzando il motore di implementazione NetApp, i volumi persistenti vengono attivati e configurati automaticamente.

Un'opzione per abilitare i volumi persistenti è inclusa negli script di installazione e aggiornamento quando si implementa 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 con NetApp-HCI pre-messo in attesa del nome sul cluster assegnato. 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

Trova ulteriori informazioni

- "Gestire i volumi"
- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

Gruppi di accesso ai volumi

Un gruppo di accesso al volume è un insieme di volumi a cui gli utenti possono accedere utilizzando gli iniziatori iSCSI o Fibre Channel.

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 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.

Trova ulteriori informazioni

- "Gestire i gruppi di accesso ai volumi"
- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

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.

Trova ulteriori informazioni

- "Gestire gli iniziatori"
- "Gruppi di accesso ai volumi"
- "Gestire i gruppi di accesso ai volumi"
- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

Domini di protezione personalizzati

È possibile definire un layout personalizzato del dominio di protezione, 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.

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.

L'utilizzo di domini di protezione personalizzati presuppone che nessun nodo condivida uno chassis.

I seguenti metodi API Element espongono questi nuovi domini di protezione:

- GetProtectionDomainLayout - Mostra 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.

Contatta il supporto NetApp per ulteriori dettagli sull'utilizzo di domini di protezione personalizzati.

Trova ulteriori informazioni

"Gestire lo storage con l'API Element"

Licenze NetApp HCI

Quando si utilizza NetApp HCI, potrebbero essere necessarie licenze aggiuntive a seconda di ciò che si utilizza.

Licenze NetApp HCI e VMware vSphere

Le licenze VMware vSphere dipendono dalla configurazione:

Opzione di rete	Licensing
Opzione A: Due cavi per nodi di calcolo che utilizzano il tagging VLAN (tutti i nodi di calcolo)	Richiede l'utilizzo di vSphere Distributed Switch, che richiede la licenza VMware vSphere Enterprise Plus.
Opzione B: Sei cavi per nodi di calcolo che utilizzano VLAN con tag (nodo di calcolo a 4 nodi 2RU H410C)	Questa configurazione utilizza vSphere Standard Switch come impostazione predefinita. L'utilizzo opzionale di vSphere Distributed Switch richiede la licenza VMware Enterprise Plus.
Opzione C: Sei cavi per nodi di calcolo che utilizzano VLAN native e con tag (H410C, nodo di calcolo 2RU a 4 nodi)	Questa configurazione utilizza vSphere Standard Switch come impostazione predefinita. L'utilizzo opzionale di vSphere Distributed Switch richiede la licenza VMware Enterprise Plus.

Licenze NetApp HCI e ONTAP Select

Se è stata fornita una versione di ONTAP Select da utilizzare con un sistema NetApp HCI acquistato, si applicano le seguenti limitazioni aggiuntive:

- La licenza ONTAP Select, fornita in bundle con la vendita di un sistema NetApp HCI, può essere utilizzata solo in combinazione con i nodi di calcolo NetApp HCI.
- Lo storage per tali istanze di ONTAP Select deve risiedere solo sui nodi di storage NetApp HCI.
- È proibito l'utilizzo di nodi di calcolo di terze parti o di nodi di storage di terze parti.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Centro di documentazione software SolidFire ed Element"

Configurazioni massime di NetApp Hybrid Cloud Control

NetApp HCI include il controllo del cloud ibrido NetApp per semplificare il ciclo di vita del calcolo e la gestione dello storage. Supporta gli aggiornamenti del software Element sui nodi di storage per cluster di storage NetApp HCI e NetApp SolidFire, nonché gli aggiornamenti del firmware per i nodi di calcolo NetApp HCI in NetApp HCI. È disponibile per impostazione predefinita sui nodi di gestione in NetApp HCI.

Oltre a comunicare i componenti hardware e software forniti da NetApp in un'installazione di NetApp HCI, NetApp Hybrid Cloud Control interagisce con componenti di terze parti nell'ambiente del cliente, come VMware vCenter. NetApp qualifica la funzionalità di NetApp Hybrid Cloud Control e la sua interazione con questi componenti di terze parti nell'ambiente del cliente fino a una certa scala. Per un'esperienza ottimale con NetApp Hybrid Cloud Control, NetApp consiglia di non utilizzare limiti massimi di configurazione.

Se si superano questi valori massimi testati, potrebbero verificarsi problemi con NetApp Hybrid Cloud Control, ad esempio un'interfaccia utente più lenta e risposte API o funzionalità non disponibili. Se si impegna NetApp per il supporto dei prodotti con NetApp Hybrid Cloud Control in ambienti configurati oltre i massimi di configurazione, il supporto NetApp chiederà di modificare la configurazione in modo che rientri nei massimi di configurazione documentati.

Valori massimi di configurazione

NetApp Hybrid Cloud Control supporta ambienti VMware vSphere con un massimo di 500 nodi di calcolo NetApp. Supporta fino a 20 cluster di storage basati su software NetApp Element con 40 nodi di storage per cluster.

Sicurezza NetApp HCI

Quando si utilizza NetApp HCI, i dati sono protetti da protocolli di sicurezza standard di settore.

Crittografia a riposo per i nodi di storage

NetApp HCI consente di crittografare tutti i dati memorizzati nel cluster di storage.

Tutti i dischi nei nodi di storage in grado di crittografare utilizzano 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 di storage 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. Per sbloccare l'unità è necessaria la password e, poiché l'unità crittografa tutti i dati, i dati sono sempre protetti.

Quando si attiva la crittografia a riposo, le prestazioni e l'efficienza del cluster di storage rimangono inalterate. Inoltre, se si rimuove un disco o nodo abilitato alla crittografia dal cluster di storage con l'API Element o l'interfaccia utente Element, la crittografia a riposo viene disattivata sui dischi e i dischi vengono cancellati in modo sicuro, proteggendo i dati precedentemente memorizzati su tali dischi. Dopo aver rimosso l'unità, è possibile cancellarla in modo sicuro con `SecureEraseDrives` Metodo API. Se si rimuove forzatamente un'unità o un nodo dal cluster di storage, i dati rimangono protetti dalla password a livello di cluster e dalle singole chiavi di crittografia dell'unità.

Per informazioni sull'attivazione e la disattivazione della crittografia a riposo, vedere "Attivazione e disattivazione della crittografia per un cluster" Nel centro di documentazione SolidFire ed Element.

Crittografia software a riposo

La crittografia software a riposo consente di crittografare tutti i dati scritti negli SSD di un cluster di storage. Questo fornisce un livello primario di crittografia nei nodi SDS aziendali SolidFire che non includono unità con crittografia automatica (SED).

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 di External Key Management, vedere "Guida introduttiva alla gestione delle chiavi esterne" Nel centro di documentazione SolidFire ed Element.

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 "Attivazione dell'autenticazione a più fattori" Nel centro di documentazione SolidFire ed Element.

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

I cluster di storage NetApp SolidFire e i sistemi NetApp HCI 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 NetApp HCI o 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 "Creazione di 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".

Performance e Quality of Service

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.

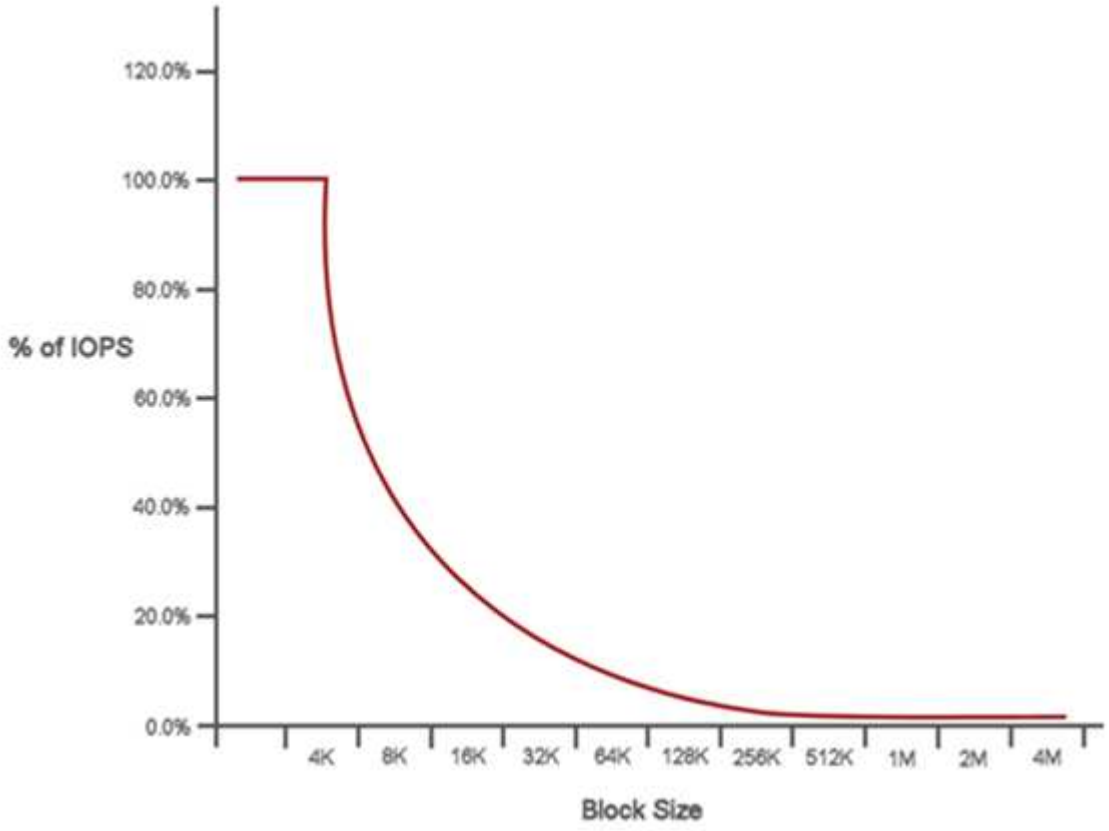
Performance QoS

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

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.